ADTRAN Switch Engine (ASE)

System Release 4.4-42

Command Reference Guide

6AMC0CRG-35C

November 2020

To the Holder of this Document

This document is intended for the use of ADTRAN customers only for the purposes of the agreement under which the document is submitted, and no part of it may be used, reproduced, modified or transmitted in any form or means without the prior written permission of ADTRAN.

The contents of this document are current as of the date of publication and are subject to change without notice.

Trademark Information

“ADTRAN” and the ADTRAN logo are registered trademarks of ADTRAN, Inc. Brand names and product names included in this document are trademarks, registered trademarks, or trade names of their respective holders.

Disclaimer of Liability

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products are given “as is”, and any liability arising in connection with such hardware or software products shall be governed by ADTRAN’s standard terms and conditions of sale unless otherwise set forth in a separately negotiated written agreement with ADTRAN that specifically applies to such hardware or software products.

To the fullest extent allowed by applicable law, in no event shall ADTRAN be liable for errors in this document for any damages, including but not limited to special, indirect, incidental or consequential, or any losses, such as but not limited to loss of profit, revenue, business interruption, business opportunity or data, that may arise from the use of this document or the information in it.

Table of Contents

List of Tables

Overview

This manual provides information about connecting your product, using the ADTRAN Switch Engine (ASE) command line interface (CLI), and executing the commands available with the ASE units.

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

If you are already familiar with ASE units and are looking for information on a specific command or group of commands, please proceed to “Command Descriptions Included in this Guide” on page 13 of this guide.

Products Supported

This document supports the products listed in Table Intro-1 below.

Table Intro-1 Supported Products

Product	P/N
NetVanta 1560-08-150W Switch	17108108PF2
NetVanta 1560-24-740W Switch	17108124PF2
NetVanta 1560-48-740W Switch	17108148PF2
NetVanta 1560-08-65W Switch	17101561PF2
NetVanta 1560-24-370W Switch	17101564PF2
NetVanta 1560-48-370W Switch	17101568PF2

Intended Audience

The intended audience for this information is the network administrator using the ASE product. The instructions assume familiarity with the intended use of the equipment, basic required installation and configuration skills, and knowledge of local and accepted networking practices.

Introduction to Command Line Interface

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

Introduction to Commands

The most important part is understanding that commands make the ASE unit function. The right commands lead to a fully functioning unit, whereas improperly entered or forgotten commands prevent the unit from functioning. To properly use commands, you must understand what function you want the ASE unit to complete and what syntax the unit understands

as instructions. Each command has its own role within the operating system, and it is the responsibility of the operator to become familiar with specific commands and command sets.

The following are key characteristics of the CLI:

- It is modal (certain operations are possible or impossible in specific modes)
- It is line-based (there are no screen editing features)
- It executes commands instantly upon end-of-line
- It is privilege-based (certain operations require the user to have a certain privilege level to succeed)
- It implements industrial de facto behavior for network equipment CLIs (structurally and behaviorally, it resembles CLIs found on other equipment while still possessing unique characteristics in some areas)

The CLI can be accessed directly using the serial console, or over the network through telnet or ssh. In each case, the user has to log in before CLI commands can be executed. This begins a session that lasts until logout.

Multiple sessions can co-exist at the same time, each providing separate environments: logged-in user ID, privilege level, command history, mode, and session settings. It is therefore perfectly possible for the same user to control several concurrent sessions, such as one serial console session and one ssh session.

The user database is either local or provided by a RADIUS or TACACS+ server. In case of a local user database, passwords and privilege levels are maintained on the device.

How Commands Function

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

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

Optionally, some commands use variables to specify information relevant only to your ASE unit. These variables are identified with angled brackets (< >). The description of the information required is contained within the symbols and displayed in italics. For example, the following command provides the command word **hostname** and includes the variable *<host name>*:

hostname *<host name>*

NOTE

Command words are not case sensitive, thus show, SHOW, and Show are identical. Conversely, parameters may either be case-sensitive or not, depending on the command and parameter in question.

ASE Command System

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

```
>enable
#configure terminal
(config)#line vty 1
(config-line)#
```

In the example above, the characters >, #, (config)#, and (config-line)# are the prompts after which commands are entered. In this example, the words in bold (**enable, configure terminal,** and **line vty 1**) are the entire commands and constitute what should be typed after the prompt. It is important to pay attention to the prompt you are given when communicating with your unit, because certain commands only work in certain modes, which are signified by the prompt.

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

```
(config)# clock [summer-time | timezone]
```

Again, remember the # is your prompt, the command word is clock, and your choices of arguments are **summer-time**, and **timezone**.

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

```
# hostname <host name>
```

In this case, # is your prompt, the command word is **hostname**, and the information needed from you is the name of the host (unit) *(<host name>*).

ASE Command System Help

Context sensitive help features embedded within the ASE CLI provide assistance in determining the correct command syntax, the full set of parameters required for a complete command, or additional relevant commands through the use of CLI shortcut keys. Table Intro-2 on page 10 lists the CLI shortcut keys and their operation.

Table Intro-2 CLI Shortcut Keys and their Operation

Shortcut Key	Description
?	Using the question mark, do any of the following: 1. Display a list of all subcommands in the current mode. For example: **#show ?** aaa Login methods access Access management access-list Access list aggregation Aggregation port configuration alarm Alarm auto-link Display Auto-link Status 2. Display a list of available commands beginning with certain letter(s). For example: **#show ag?** aggregation Aggregation port configuration <cr> 3. Obtain syntax help for a specific command by entering the command, a space, and then a question mark (?). The ASE CLI displays the range of values and a brief description of the next parameter expected for that particular command. For example: **#show aggregation ?** | Output modifiers mode Traffic distribution mode <cr>
Entering **?** a second time	After entering **?** to discover the next parameter for the command as shown above, you can enter the **?** a second time and receive the parameters available for the command as well as the number of parameters required to complete the command. For example, entering **aggregation mode ?** one time displays the aggregation modes available for configuration with their description as follows: (config)#**aggregation mode ?** dmac Destination MAC affects the distribution ip IP address affects the distribution port IP port affects the distribution smac Source MAC affects the distribution Entering **aggregation mode ?** a second time will return each parameter without a description and add a numerical value indicating how many of those parameters must be entered for the command to be valid. Entering the command a second time with the **?** appears as follows: (config)#**aggregation mode ?** {[smac] [dmac] [ip] [port]} *1 In this example, **smac**, **dmac**, **ip**, and **port** are the available next parameters for the aggregation mode command, and the ***1** indicates at least one of these parameters must be entered.
<Tab> key	Pressing the **<Tab>** key after entering a partial (but unique) command displays all available command parameters without a description. For example: **#show a<Tab>** aaa access access-list aggregation alarm auto-link Pressing the **<Tab>** key a second time completes the command, displays it on the command prompt line, and waits for further input.

Understanding Command Modes

As you begin communication, you should understand the command modes. Just as there are different levels of commands in the CLI, there are different modes for commands within ASE itself. Each command mode enables the user to access more commands, and make more changes in the unit's configuration.The modes are further influenced by the privilege level of the user; some modes or commands are only accessible to administrators while others require no privileges beyond login.

The ASE CLI has two main command modes: Enable and Global Configuration. These command modes are organized in a tiered hierarchy with Enable at the bottom and Global Configuration at the top. In addition, configuration command sets are available from Global Configuration mode. These command sets are broken down into categories of similar functions. For example, all commands pertaining to configuring the interfaces are grouped together.

Enable Mode

Enable mode is the base configuration mode for the ASE device. ADTRAN suggests that a password be required to access the Enable mode. Refer to the quick start guides shipped with your unit and located online at https://supportcommunity.adtran.com for more information on configuring a password.

From the Enable mode, you can access the configurations of your product, as well as handle how your unit boots and runs, among other things. Table Intro-3 describes the Enable mode.

Table Intro-3 Enable Mode

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

Global Configuration Mode

The Global Configuration mode is the highest level tier within ASE. The Global Configuration mode allows the user to make changes regarding the entire product system. All of your system's configurations are accessed through the Global Configuration mode. From this level, you can access not only line configurations, router configurations, and interface configurations, but also any other configurations or parameters on your system. Table Intro-4 on page 12 describes the Global Configuration mode.

Table Intro-4 Global Mode

Mode	Access By...	Mode Prompt	Accessible Commands

Global Config	Entering **config** while at the Enable mode as follows:
	`>enable`
	#
	`#config t`
		`(config)#`	■ Set the system's Enable-level password(s)
			■ Configure the system global IP parameters
			■ Configure the SNMP parameters
			■ Enter any of the configuration modes

Configuration Command Sets

Configuration Command Sets contain a group of commands that are specific to a particular interface, feature, protocol, etc. For example, there are specific command sets for VLANs, Ethernet interfaces, and IP. Table Intro-5 summarizes some of the command sets available in the ASE CLI. These command sets are available from Global Configuration Mode.

Table Intro-5 Configuration Command Sets Summary

Command Set	Accessed By...	Description
DHCP Server Pool Configuration	Specifying a Dynamic Host Configuration Protocol (DHCP) server address pool name as follows: `(config)#ip dhcp pool` *<name>*	Configure DHCP server address pools Prompt: (config-dhcp-pool)#
Gigabit Ethernet Interface	Specifying a Gigabit Ethernet interface number at the Global Configuration mode prompt as follows: `(config)#interface gigabitethernet` *<slot/port>*	Configure Gigabit Ethernet interfaces Prompt: (config-if)#
IPMC Profile	Specifying an IP Multicast Configuration (IPMC) profile name as follows: `(config)#ipmc profile` *<name>*	Configure IPMC profiles Prompt: (config-ipmc-profile)#
JSON Notification Host Configuration	Specifying a JavaScript Object Notation (JSON) notification host name as follows: `(config)#json notification host` *<name>*	Configure JSON notification hosts Prompt: (config-json-notif-host)#
Line	Specifying a terminal line number, console terminal line number, or virtual terminal line number as follows: `(config)#line [`*<number>* `| console 0 | vty` *<number>*`]`	Configure terminal lines Prompt: (config-line)#
SNMP Server Host	Specifying a SNMP server host name as follows: `(config)#snmp-server host` *<name>*	Configure SNMP server host entries Prompt: (config-snmps-host)#

Table Intro-5 Configuration Command Sets Summary (Continued)

Command Set	Accessed By...	Description
VLAN Interface	Specifying a VLAN interface number at the Global Configuration mode prompt as follows: `(config)#interface vlan <vlan ids>`	Configure VLAN interfaces Prompt: (config-if-vlan)#
LLAG Interface	Specifying a Local Link Aggregation Group (LLAG) as follows: `(config)#interface llag <id>`	Configure LLAG interfaces Prompt: (config-if-llag)#
QoS Egress Map	Specifying a Quality of Service (QoS) egress map ID as follows: `(config)#qos map egress <map id>`	Configure QoS Egress Map parameters Prompt: (config-qos-map-egress)#
QoS Ingress Map	Specifying a Quality of Service (QoS) ingress map ID as follows: `(config)#qos map ingress <map id>`	Configure QoS Ingress Map parameters Prompt: (config-qos-map-ingress)#

Command Mode Transitions

A user can transition between command modes and configuration command sets, subject to the user's privilege level and the current session privilege level.

Once in Enable mode, it is possible to enter into Global Configuration mode by entering the command **configure terminal**. Exit from Global Configuration mode is achieved by entering the command **end** or **exit** or pressing Ctrl-Z.

Access to a configuration command set (for example, Ethernet interfaces) goes through Global Configuration or another command set. Thus, it is possible to change directly from the VLAN command set to the Gigabit Ethernet interface command set.

Each mode and command set implements a scope for commands. Inside each mode, a particular subset of commands is available. To access other commands, one must generally change modes/command sets. This change is necessary because there are commands with identical prefixes in different modes. For example, there are commands that begin with 'ip' in Enable, Global Configuration, and VLAN Interface Configuration modes.

There is one exception to this: Enable mode commands (whether privileged or unprivileged) are accessible from within Global Configuration or one of the command sets by using the **do** command. See "Common Commands Set" on page 18.

Command Descriptions Included in this Guide

This portion of the guide provides a detailed listing of all available commands for the ASE CLI (organized by command set). Each command listing contains pertinent information, including the default value, a description of all subcommand parameters, functional notes for using the command, and a brief technology review. To search for information on a group of commands within a particular command set, use the linked references given in Table Intro-6 below.

Table Intro-6 ASE Command Sets Included in this Guide

Section	Topic	Scope
Volume1: System Command Sets		**This Volume describes the various commands associated with ASE device basic systems.**
1	“Common Commands Set”	Describes commands common to all sections of ASE device configuration.
2	“Enable Mode Command Set”	Describes commands issued from the ASE device Enable mode.
3	“Global Configuration Mode Command Set”	Describes commands issued from the ASE device Global Configuration mode.
Volume 2: Interface Command Sets		**This Volume describes commands used to configure ASE device interfaces.**
1	“GigabitEthernet Interface Command Set”	Describes the commands issued from the GigabitEthernet interfaces on the ASE device.
2	“Line Interface Command Set”	Describes the commands issued from the Line Interface on the ASE device.
3	“Local Link Aggregation Interface Command Set”	Describes the commands issued from the Local Link Aggregation Interface on the ASE device.
4	“VLAN Interface Command Set”	Describes the commands issued from the virtual local area network (VLAN) Interface on the ASE device.
Volume 3: Protocols and Services Command Sets		**This Volume describes commands associated with the various services and protocols supported by the ASE device.**
1	“DHCPv4 Server Pool Command Set”	Describes the commands used to configure the DHCP server pool.
2	“IPMC Profile Command Set”	Describes the commands used to configure the IPMC profile.
3	“JSON Host Command Set”	Describes the commands used to configure the JSON Host.
4	“SNMP Server Host Command Set”	Describes the commands used to configure the SNMP Server Host.

Table Intro-6 ASE Command Sets Included in this Guide (Continued)

Section	Topic	Scope
5	"QoS Egress Map Command Set"	Describes the commands used to configure the QoS Egress map.
6	"QoS Ingress Map Command Set"	Describes the commands used to configure the QoS Ingress map.
"Warranty" and "Contact Information"		Provides direction to Warranty Information plus contact information for Customer Care, Training and Sales.

Hazard and Conventional Symbols

WARNING!
Warning: Service affecting. Possible risk of system failure.

CAUTION!
Caution: Indicates that a failure to take or avoid a specific action could result in a loss of data.

NOTICE!
Notice: Provides information that is essential to the completion of a task.

NOTE
Note: Information that emphasizes or supplements important points of the main text.

Related Online Documents and Resources

Refer to Table Intro-7 for additional documentation available for ASE devices. Documents are available online at https://supportcommunity.adtran.com.

Table Intro-7 Related Online Documents and Resources

Title	Description
Configuring PoE in ASE	Outlines the PoE technology and its use and configuration in ASE devices.
Configuring the CLI in ASE	Outlines CLI structure and basics for ASE devices.
Configuring QoS in ASE	Outlines QoS configuration and use in ASE devices.
Configuring MRP and MVRP in ASE	Outlines MRP and MVRP technology, and their use and configuration in ASE devices.
Configuring DHCP in ASE	Outlines DHCP functionality and its use and configuration in ASE devices.
Configuring Layer 2 Services in ASE	Outlines Layer 2 services and protocols supported on the ASE device.

ASE Command Reference Guide

Volume 1: System Command Sets

1 Common Commands Set

1.1 Scope of this Section

This section outlines the common commands available on the ADTRAN Switch Engine (ASE) across different command modes. These commands allow you to execute commands from any command mode, or allow you to return to previous command modes.

1.2 Accessing Common Commands

Because these commands are common to many different command sets and configuration modes, they are not accessible by a single command, but can be entered from many different command sets.

1.3 Common Commands

Table 1-1 outlines the common commands available on the ASE device.

Table 1-1. Common Commands

Sub-Section	Command	See Page …
1.4	do	19
1.5	end	20
1.6	exit	21
1.7	help	22

1.4 do

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

1.4.1 Syntax Description

No subcommands.

1.4.2 Applicable Command Modes

Applies to all mode command sets.

1.4.3 Command History

ASE Release 4.4-41 Command was introduced.

1.4.4 Functional Notes

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

1.4.5 Usage Examples

The following example shows the **do** command used to view the 10 GigabitEthernet interface configuration while currently in the GigabitEthernet Interface Configuration mode:

```
(config)#interface gigabitethernet 1/1
(config-if)#do show interface 10gigabitethernet 1/2 status


Interface               Mode     Speed &      Flow    Max Frame  Excessive  Link
                                 Duplex      Control
--------------------  -------   ---------   ---------  ---------  ---------   ------
10GigabitEthernet 1/2  enabled   10Gfdx      disabled     10240     Discard    Down
(config-if)#
```

1.5 end

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

NOTE
When exiting the Global Configuration mode, enter the **copy running-config startup-config** command to save all configuration changes.

1.5.1 Syntax Description

No subcommands.

1.5.2 Applicable Command Modes

Applies to all mode command sets.

1.5.3 Command History

ASE Release 4.4-41	Command was introduced.

1.5.4 Usage Examples

The following example shows the **end** command being executed in an interface configuration mode:

```
(config-if)#end
#
```

1.6 exit

Use the **exit** command to exit the current configuration mode and enter the previous one.

1.6.1 Syntax Description

No subcommands.

1.6.2 Applicable Command Modes

Applies to all mode command sets.

1.6.3 Command History

ASE Release 4.4-41	Command was introduced.

1.6.4 Functional Notes

Using this command in an interface configuration mode will activate the Global Configuration mode. Using this command in the Basic mode, terminates the current session.

NOTE
When exiting the Global Configuration mode, enter the **copy running-config startup-config** command first to save all configuration changes.

1.6.5 Usage Examples

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

```
(config)#auto-link
(config)#exit
#
```

1.7 help

The **help** command displays the available methods for receiving help to guide you through the configuration process or help you to understand particular command syntax and parameters.

1.7.1 Syntax Description

No subcommands.

1.7.2 Applicable Command Modes

Applies to all mode command sets.

1.7.3 Command History

ASE Release 4.4-41	Command was introduced.

1.7.4 Usage Examples

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

```
(config)#help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
```

2 Enable Mode Command Set

2.1 Scope of this Section

This section outlines the commands available on the ADTRAN Switch Engine (ASE) in the Enable mode. The Enable mode is used to access basic configurations of your product, as well as handle how your unit boots and runs, among other things. In this command mode, you can manage the startup and running configurations of the ASE product, enable and disable **debug** commands, view **show** command output, and access additional configuration modes.

2.2 Accessing the Enable Mode

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

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

2.3 Common Commands

The commands listed in Table 2-1 are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the section listed below:

Table 2-1. Common Commands

Sub-Section	Command	See Page …
1.4	do	19
1.5	end	20
1.6	exit	21
1.7	help	22

2.4 Enable Mode Commands

Table 2-2 lists the available commands for the Enable mode.

Table 2-2. Enable Mode Commands

Sub-Section	Command	See Page …
2.5	alarm suppress	30
2.6	clear access management statistics	31
2.7	clear access-list ace statistics	32
2.8	clear dot1x statistics	33
2.9	clear eps <unit> wtr	34
2.10	clear erps	35
2.11	clear ip acd	36

Table 2-2. Enable Mode Commands (Continued)

Table 2-2. Enable Mode Commands (Continued)

Table 2-2. Enable Mode Commands (Continued)

Table 2-2. Enable Mode Commands (Continued)

Table 2-2. Enable Mode Commands (Continued)

Table 2-2. Enable Mode Commands (Continued)

Sub-Section	Command	See Page …
2.172	show web privilege group level	237
2.173	terminal	241
2.174	traceroute ip	242
2.175	veriphy	244

2.5 alarm suppress

Use the **alarm suppress** command to suppress a specified ASE alarm. Use the **no** form of this command to disable the alarm suppression. Variations of this command include:

```
alarm suppress <kword127>
alarm suppress <kword127> | begin <line>
alarm suppress <kword127> | exclude <line>
alarm suppress <kword127> | include <line>
```

2.5.1 Syntax Description

<kword127>	Specifies the alarm name to suppress. Enter the **show alarm** command, as described *on page 96* to determine the appropriate alarm name.
| begin *<line>*	Optional. Suppresses part of the alarm that begins with the specified text and every line thereafter.
| exclude *<line>*	Optional. Suppresses part of the alarm, excluding any lines containing the specified text.
| include *<line>*	Optional. Suppresses part of the alarm that contains the lines with the specified text.

2.5.2 Default Values

By default, the alarm suppression feature is disabled.

2.5.3 Command History

ASE Release 4.4-41	Command was introduced.

2.5.4 Usage Examples

The following example suppresses **alarm.herlev.switch2.port28**:

```
#alarm suppress alarm.herlev.switch2.port28
```

2.6 clear access management statistics

Use the **clear access management statistics** command to clear configuration and statistics associated with system access. Variations of this command include:

2.6.1 Syntax Description

`management`	Specifies access management configuration is cleared.
`statistics`	Specifies that statistics associated with access management configurations are cleared.

2.6.2 Command History

ASE Release 4.4-41	Command was introduced.

2.6.3 Default Values

No default values are necessary for this command.

2.6.4 Privilege Level

By default, this command has a privilege level of **15**.

2.6.5 Usage Examples

The following example specifies that access management configuration and associated statistical data are cleared:

```
#clear access management statistics
```

2.7 clear access-list ace statistics

Use the **clear access-list ace statistics** command to clear statistics associated with access lists.

2.7.1 Syntax Description

ace	Specifies that access list entries are cleared.
statistics	Specifies that traffic statistics associated with the access lists are cleared.

2.7.2 Command History

ASE Release 4.4-41	Command was introduced.

2.7.3 Default Values

No default values are necessary for this command.

2.7.4 Privilege Level

By default, this command has a privilege level of **15**.

2.7.5 Usage Examples

The following example clears all entries and statistics associated with access lists:

```
#clear access-list ace statistics
```

2.8 clear dot1x statistics

Use the **clear dot1x statistics** command to clear statistic counters associated with the IEEE standard for port-based network access control. Variations of this command include:

```
clear dot1x statistics
clear dot1x statistics interface <interface>
```

2.8.1 Syntax Description

interface *<interface>*	Optional. Specifies that information associated with a specific interface is cleared. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.8.2 Default Values

No default values are necessary for this command.

2.8.3 Privilege Level

By default, this command has a privilege level of **15**.

2.8.4 Command History

ASE Release 4.4-41	Command was introduced.

2.8.5 Usage Examples

The following example clears statistic counters associated with ports 1/1-8 on the Gigabit Ethernet interface:

```
#clear dot1x statistics interface GigabitEthernet 1/1-8
```

2.9 clear eps <*unit*> wtr

Use the **clear eps** <*unit*> **wtr** command to clear Ethernet Protection Switching (EPS) statistics.

2.9.1 Syntax Description

<unit>	Specifies the EPS instance number.
wtr	Clears active wait-to-restore (WTR) statistics.

2.9.2 Default Values

No default values are necessary for this command.

2.9.3 Command History

ASE Release 4.4-41	Command was introduced.

2.9.4 Usage Examples

The following example clears EPS statistics and active WTR for the EPS instance **2**:

```
#clear eps 2 wtr
```

2.10 clear erps

Use the **clear erps** command to clear statistics associated with Ethernet Ring Protection Switching (ERPS). Variations of this command include:

```
clear erps <group number>
clear erps statistics
```

2.10.1 Syntax Description

<group number>	Specifies the ERPS group numbers on which to clear statistics. Valid range is **1**-**64**.
statistics	Clears all ERPS statistics.

2.10.2 Default Values

No default values are necessary for this command.

2.10.3 Command History

ASE Release 4.4-41	Command was introduced.

2.10.4 Usage Examples

The following example clears all ERPS statistics:

```
#clear erps statistics
```

2.11 clear ip acd

Use the **clear ip acd** command to clear Internet Protocol version 4 (IPv4) Address Conflict Detection (ACD) statistics. Variations of this command include:

```
clear ip acd
clear ip acd | begin <line>
clear ip acd | exclude <line>
clear ip acd | include <line>
```

2.11.1 Syntax Description

| begin *<line>*	Optional. Clears IPv4 ACD statistics that begin with the specified text, and every line thereafter.
| exclude *<line>*	Optional. Clears IPv4 ACD statistics, excluding any lines containing the specified text.
| include *<line>*	Optional. Clears IPv4 ACD statistics with the specified text.

2.11.2 Default Values

No default values are necessary for this command.

2.11.3 Command History

ASE Release 4.4-41	Command was introduced.

2.11.4 Usage Examples

The following example clears all IPv4 ACD statistics:

```
#clear ip acd
```

2.12 clear ip arp

Use the **clear ip arp** command to clear the Internet Protocol version 4 (IPv4) Address Resolution Protocol (ARP) cache.

2.12.1 Syntax Description

No subcommands.

2.12.2 Default Values

No default values are necessary for this command.

2.12.3 Privilege Level

By default, this command has a privilege level of **0**.

2.12.4 Command History

ASE Release 4.4-41	Command was introduced.

2.12.5 Usage Examples

The following example clears the IPv4 ARP cache:

```
#clear ip arp
```

2.13 clear ip dhcp detailed statistics

Use the **clear ip dhcp detailed statistics** command to clear detailed traffic statistics associated with Internet Protocol version 4 (IPv4) Dynamic Host Control Protocol (DHCP). Variations of this command include:

```
clear ip dhcp detailed statistics all
clear ip dhcp detailed statistics all interface <interface>

clear ip dhcp detailed statistics client
clear ip dhcp detailed statistics client interface <interface>

clear ip dhcp detailed statistics helper
clear ip dhcp detailed statistics helper interface <interface>

clear ip dhcp detailed statistics relay
clear ip dhcp detailed statistics relay interface <interface>

clear ip dhcp detailed statistics server
clear ip dhcp detailed statistics server interface <interface>

clear ip dhcp detailed statistics snooping
clear ip dhcp detailed statistics snooping interface <interface>
```

2.13.1 Syntax Description

all	Specifies that all detailed DHCP related traffic statistics are cleared.
client	Specifies that all detailed traffic statistics related to the DHCP client are cleared.
helper	Optional. Specifies that detailed traffic statistics associated with normal Layer 2 or Layer 3 DHCP forwards are cleared.
server	Optional. Specifies that detailed traffic statistics related to the DHCP server are cleared.
snooping	Optional. Specifies that detailed traffic statistics associated with DHCP snooping are cleared.
relay	Optional. Specifies that detailed traffic statistics associated with the DHCP relay are cleared.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is cleared. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.13.2 Default Values

No default values are necessary for this command.

2.13.3 Privilege Level

By default, this command has a privilege level of **15**.

2.13.4 Command History

ASE Release 4.4-41	Command was introduced.

2.13.5 Usage Examples

The following example clears all detailed traffic statistics associated with IPv4 DHCP:

```
#clear ip dhcp detailed statistics all
```

2.14 clear ip dhcp relay statistics

Use the **clear ip dhcp relay statistics** command to clear all traffic statistics associated with the Internet Protocol version 4 (IPv4) Dynamic Control Host Protocol (DHCP) relay.

2.14.1 Syntax Description

No subcommands.

2.14.2 Default Values

No default values are necessary for this command.

2.14.3 Privilege Level

By default, this command has a privilege level of **15**.

2.14.4 Command History

ASE Release 4.4-41	Command was introduced.

2.14.5 Usage Examples

The following example clears all traffic statistics associated with the IPv4 DHCP relay:

```
#clear ip dhcp relay statistics
```

2.15 clear ip dhcp server

Use the **clear ip dhcp server** command to clear statistics associated with the Internet Protocol version 4 (IPv4) Dynamic Host Control Protocol (DHCP) server. Variations of this command include:

```
clear ip dhcp server binding <ipv4_ucast>
clear ip dhcp server binding type automatic
clear ip dhcp server binding type manual
clear ip dhcp server binding type expired
clear ip dhcp server statistics
```

2.15.1 Syntax Description

binding	Specifies that statistics associated with DHCP binding are cleared.
<ipv4_ucast>	Specifies the IPv4 address of the DHCP binding to be cleared.
type automatic	Specifies that automatic DHCP bindings are cleared. This bindings become expired once cleared.
type manual	Specifies that manual DHCP bindings are cleared. These binding become expired once cleared.
type expired	Specifies that expired DHCP bindings are cleared. These bindings are removed from the system.
statistics	Specifies that all DHCP server statistics are cleared.

2.15.2 Default Values

No default values are necessary for this command.

2.15.3 Privilege Level

By default, this command has a privilege level of **13**.

2.15.4 Command History

ASE Release 4.4-41	Command was introduced.

2.15.5 Usage Examples

The following example clears all server statistics associated with the IPv4 DHCP server:

```
#clear ip dhcp server statistics
```

2.16 clear ip dhcp snooping statistics

Use the **clear ip dhcp snooping statistics** command to clear all statistics associated with Internet Protocol version 4 (IPv4) Dynamic Host Control Protocol (DHCP) snooping. Variations of this command include:

```
clear ip dhcp snooping statistics
clear ip dhcp snooping statistics interface <interface>
```

2.16.1 Syntax Description

interface *<interface>*	Optional. Specifies that information associated with a specific interface is cleared. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.16.2 Default Values

No default values are necessary for this command.

2.16.3 Privilege Level

By default, this command has a privilege level of **13**. When the **interface** <*interface*> parameter is used, the command has a privilege level of **15**.

2.16.4 Command History

ASE Release 4.4-41	Command was introduced.

2.16.5 Usage Examples

The following example clears all statistics associated with IPv4 DHCP snooping:

```
#clear ip dhcp snooping statistics
```

2.17 clear ip igmp snooping statistics

Use the **clear ip igmp snooping statistics** command to clear statistics associated with Internet Protocol version 4 (IPv4) Internet Group Management Protocol (IGMP) snooping. Variations of this command include:

```
clear ip igmp snooping statistics
clear ip igmp snooping vlan <vlan ids> statistics
```

2.17.1 Syntax Description

vlan *<vlan ids>*	Optional. Clears the IGMP snooping statistics for the specified virtual local area network (VLAN) identification number. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

2.17.2 Default Values

No default values are necessary for this command.

2.17.3 Privilege Level

By default, this command has a privilege level of **15**.

2.17.4 Command History

ASE Release 4.4-41	Command was introduced.

2.17.5 Usage Examples

The following example clears the IPv4 IGMP snooping statistics for VLAN **3**:

```
#clear ip igmp snooping vlan 3 statistics
```

2.18 clear ip statistics

Use the **clear ip statistics** command to clear statistics associated with Internet Protocol version 4 (IPv4) traffic.

2.18.1 Syntax Description

No subcommands.

2.18.2 Default Values

No default values are necessary for this command.

2.18.3 Privilege Level

By default, this command has a privilege level of **0**.

2.18.4 Command History

ASE Release 4.4-41	Command was introduced.

2.18.5 Usage Examples

The following example clears all IPv4 statistics:

```
#clear ip statistics
```

2.19 clear ipv6 mld snooping statistics

Use the **clear ipv6 mld snooping statistics** command to clear statistics associated with Internet Protocol version 6 (IPv6) Multicast Listener Discovery (MLD) snooping. Variations of this command include:

```
clear ipv6 mld snooping statistics
clear ipv6 mld snooping vlan <vlan ids> statistics
```

2.19.1 Syntax Description

vlan *<vlan ids>*	Optional. Clears the IPv6 MLD snooping statistics for the specified virtual local area network (VLAN) identification number. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

2.19.2 Default Values

No default values are necessary for this command.

2.19.3 Privilege Level

By default, this command has a privilege level of **15**.

2.19.4 Command History

ASE Release 4.4-41	Command was introduced.

2.19.5 Usage Examples

The following example clears all IPv6 MLD snooping statistics on all VLANs:

```
#clear ipv6 mld snooping statistics
```

2.20 clear ipv6 neighbors

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

2.20.1 Syntax Description

No subcommands.

2.20.2 Default Values

No default values are necessary for this command.

2.20.3 Command History

ASE Release 4.4-41	Command was introduced.

2.20.4 Usage Examples

The following example clears the entries from the IPv6 neighbor cache:

```
#clear ipv6 neighbors
```

2.21 clear ipv6 statistics

Use the **clear ipv6 statistics** command to clear Internet Protocol version 6 (IPv6) traffic statistics.

2.21.1 Syntax Description

No subcommands.

2.21.2 Default Values

No default values are necessary for this command.

2.21.3 Command History

ASE Release 4.4-41	Command was introduced.

2.21.4 Usage Examples

The following example clears all IPv6 traffic statistics:

```
#clear ipv6 statistics
```

2.22 clear lacp statistics

Use the **clear lacp statistics** command to clear Link Aggregation Control Protocol (LACP) statistics.

2.22.1 Syntax Description

No subcommands.

2.22.2 Default Values

No default values are necessary for this command.

2.22.3 Privilege Level

By default, this command has a privilege level of **15**.

2.22.4 Command History

ASE Release 4.4-41	Command was introduced.

2.22.5 Usage Examples

The following example clears all LACP statistics:

```
#clear lacp statistics
```

2.23 clear link-oam statistics

Use the **clear link-oam statistics** command to clear the receive (Rx) and transmit (Tx) counters for link operations, administration, and management (OAM). Variations of this command include:

```
clear link-oam statistics
clear link-oam statistics interface <interface>
```

2.23.1 Syntax Description

interface *<interface>*	Optional. Specifies that information associated with a specific interface is cleared. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.23.2 Default Values

No default values are necessary for this command.

2.23.3 Command History

ASE Release 4.4-41	Command was introduced.

2.23.4 Usage Examples

The following example clears all link OAM transmit and receive counters:

```
#clear link-oam statistics
```

2.24 clear lldp statistics

Use the **clear lldp statistics** command to clear all statistics associated with Link Layer Discovery Protocol (LLDP). Variations of this command include:

```
clear lldp statistics
clear lldp statistics | begin <line>
clear lldp statistics | exclude <line>
clear lldp statistics | include <line>
clear lldp statistics global
clear lldp statistics global | begin <line>
clear lldp statistics global | exclude <line>
clear lldp statistics global | include <line>
clear lldp statistics interface <interface>
```

2.24.1 Syntax Description

| begin *<line>*	Optional. Clears the LLDP statistics that begin with the specified text and every line thereafter.
| exclude *<line>*	Optional. Clears the LLDP statistics, but excludes any lines containing the specified text.
| include *<line>*	Optional. Clears the LLDP statistics that contain the lines with the specified text.
global	Optional. Specifies that all global LLDP counters are cleared.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is cleared. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.24.2 Default Values

No default values are necessary for this command.

2.24.3 Privilege Level

By default, this command has a privilege level of **0**.

2.24.4 Command History

ASE Release 4.4-41	Command was introduced.

2.24.5 Usage Examples

The following example clears all LLDP global counters:

```
#clear lldp statistics global
```

2.25 clear logging

Use the **clear logging** command to clear system logging messages. Variations of this command include:

```
clear logging
clear logging error
clear logging informational
clear logging notice
clear logging warning
```

2.25.1 Syntax Description

error	Optional. Clears all error condition messages (severity 3).
informational	Optional. Clears all informational messages (severity 6).
notice	Optional. Clears all messages reflecting a normal but significant condition (severity 5).
warning	Optional. Clears all warning condition messages (severity 4).

2.25.2 Default Values

No default values are necessary for this command.

2.25.3 Privilege Level

By default, this command has a privilege level of **15**.

2.25.4 Command History

ASE Release 4.4-41	Command was introduced.

2.25.5 Functional Notes

The optional **error**, **informational**, **notice**, and **warning** parameters may be entered in multiple combinations and in any order within a single command.

2.25.6 Usage Examples

The following example clears all informational, error, and warning messages from the system log:

```
#clear logging informational error warning
```

2.26 clear mac address-table

Use the **clear mac address-table** command to clear the Media Access Control (MAC) address table entries.

2.26.1 Syntax Description

No subcommands.

2.26.2 Default Values

No default values are necessary for this command.

2.26.3 Privilege Level

By default, this command has a privilege level of **15**.

2.26.4 Command History

ASE Release 4.4-41	Command was introduced.

2.26.5 Usage Examples

The following example clears all MAC address table entries:

```
#clear mac address-table
```

2.27 clear mep <*unit*>

Use the **clear mep** <*unit*> command to clear measuring information on a specific maintenance entity point (MEP). Variations of this command include:

```
clear mep <unit> dm
clear mep <unit> lb
clear mep <unit> tst
clear mep <unit> lm
clear mep <unit> lm both
clear mep <unit> lm rx
clear mep <unit> lm tx
```

2.27.1 Syntax Description

<*unit*>	Specifies the MEP instance.
dm	Specifies that frame delay 2- way (ETH-DM) measuring information is cleared on the MEP.
lb	Specifies that LB measuring information is cleared on the MEP.
tst	Specifies that TST measuring information is cleared on the MEP.
lm	Specifies that single-ended frame loss (ETH-LM) measuring information is cleared on the MEP.
both	Optional. Specifies that only ETH-LM information in both directions is cleared.
rx	Optional. Specifies that only received ETH-LM information is cleared.
tx	Optional. Specifies that only transmitted ETH-LM information is cleared.

2.27.2 Default Values

No default values are necessary for this command.

2.27.3 Command History

ASE Release 4.4-41	Command was introduced.

2.27.4 Usage Examples

The following example clears all ETH-LM measuring information on MEP 3:

```
#clear mep 3 lm
```

2.28 clear mvr statistics

Use the **clear mvr statistics** command to clear running protocol counters associated with multicast virtual local area network (VLAN) registrations (MVRs). Variations of this command include:

```
clear mvr name <word16> statistics
clear mvr statistics
clear mvr vlan <vlan ids> statistics
```

2.28.1 Syntax Description

name *<word16>*	Optional. Specifies an MVR instance (by name) on which to clear the counters.
vlan *<vlan ids>*	Optional. Clears the MVR counters for the specified VLAN identification number. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

2.28.2 Default Values

No default values are necessary for this command.

2.28.3 Privilege Level

By default, this command has a privilege level of **15**.

2.28.4 Command History

ASE Release 4.4-41	Command was introduced.

2.28.5 Usage Examples

The following example clears the MVR counters for VLAN 25:

```
#clear mvr vlan 25 statistics
```

2.29 clear port-security dynamic

Use the **clear port-security dynamic** command to clear dynamic port security entries. Variations of this command include:

```
clear port-security dynamic
clear port-security dynamic address <mac_address>
clear port-security dynamic address <mac_address> vlan <vlan id>
clear port-security dynamic interface <interface>
clear port-security dynamic vlan <vlan_id>
```

2.29.1 Syntax Description

address *<mac_address>*	Optional. Specifies a Media Access Control (MAC) address entry to clear. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
interface *<interface>*	Optional. Specifies that information associated with a specific interface is cleared. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
vlan *<vlan_id>*	Optional. Clears port security entries for the specified virtual local area network (VLAN) identification number. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

2.29.2 Default Values

No default values are necessary for this command.

2.29.3 Command History

ASE Release 4.4-41	Command was introduced.

2.29.4 Usage Examples

The following example clears dynamic entries for port security on VLAN 1:

```
#clear port-security dynamic vlan 1
```

2.30 clear ptp <*number*> servo

Use the **clear ptp** <*number*> **servo** command to clear Precision Time Protocol (PTP) clock information from the specified servo.

2.30.1 Syntax Description

<*number*>	Specifies the servo to clear. Valid range is **0** to **3**.

2.30.2 Default Values

No default values are necessary for this command.

2.30.3 Command History

ASE Release 4.4-41	Command was introduced.

2.30.4 Usage Examples

The following example clears PTP information for servo 1:

```
#clear ptp 1 servo
```

2.31 clear sflow statistics

Use the **clear sflow statistics** command to clear sampled flow (sFlow) statistics for either receivers or samplers. Variations of this command include:

```
clear sflow statistics receiver
clear sflow statistics samplers
clear sflow statistics samplers interface <interface>
```

2.31.1 Syntax Description

receiver	Specifies that sFlow receiver statistics are cleared.
samplers	Specifies that sFlow sampler statistics are cleared.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is cleared. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.31.2 Default Values

No default values are necessary for this command.

2.31.3 Privilege Level

By default, this command has a privilege level of **15**.

2.31.4 Command History

ASE Release 4.4-41	Command was introduced.

2.31.5 Usage Examples

The following example clears the sFlow sampler statistics for port 1/1-48 on the Gigabit Ethernet interface:

```
#clear sflow statistics samplers interface GigabitEthernet 1/1-48
```

2.32 clear spanning-tree

Use the **clear spanning-tree** command to clear Spanning Tree Protocol (STP) bridge statistics and protocols. Variations of this command include:

```
clear spanning-tree detected-protocols
clear spanning-tree detected-protocols interface <interface>
clear spanning-tree statistics
clear spanning-tree statistics interface <interface>
```

2.32.1 Syntax Description

detected-protocols	Sets the STP migration check.
statistics	Clears the STP statistics.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.32.2 Default Values

No default values are necessary for this command.

2.32.3 Privilege Level

By default, this command has a privilege level of **15**.

2.32.4 Command History

ASE Release 4.4-41	Command was introduced.

2.32.5 Usage Examples

The following example clears STP migration check information on all switches and ports:

```
#clear spanning-tree detected-protocols interface *
```

2.33 clear statistics

Use the **clear statistics** command to clear statistics for one or more specified interfaces. Variations of this command include:

```
clear statistics
clear statistics interface <interface>
```

2.33.1 Syntax Description

interface *<interface>*	Optional. Specifies that information associated with a specific interface is cleared. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.33.2 Default Values

No default values are necessary for this command.

2.33.3 Privilege Level

By default, this command has a privilege level of **0**.

2.33.4 Command History

ASE Release 4.4-41	Command was introduced.

2.33.5 Usage Examples

The following example clears the statistics on ports 1/1-34 of the 1 Gigabit Ethernet interface:

```
#clear statistics GigabitEthernet 1/1-34
```

2.34 clear system led status

Use the **clear system led status** command to clear the LED error status from the system. Variations of this command include:

```
clear system led status all
clear system led status all | begin <line>
clear system led status all | exclude <line>
clear system led status all | include <line>
clear system led status fatal
clear system led status fatal | begin <line>
clear system led status fatal | exclude <line>
clear system led status fatal | include <line>
clear system led status software
clear system led status software | begin <line>
clear system led status software | exclude <line>
clear system led status software | include <line>
```

2.34.1 Syntax Description

all	Clears all LED error status and returns the LEDs to normal indication.
fatal	Clears LED fatal error status.
software	Clears LED generic software error status.
| begin *<line>*	Optional. Clears errors that begin with the specified text and every line thereafter.
| exclude *<line>*	Optional. Clears all errors, excluding any lines containing the specified text.
| include *<line>*	Optional. Clears errors that contain lines that include the specified text.

2.34.2 Default Values

No default values are necessary for this command.

2.34.3 Command History

ASE Release 4.4-41	Command was introduced.

2.34.4 Usage Examples

The following example clears all software error LED status:

```
#clear system led status software
```

2.35 copy running-config

Use the **copy running-config** command to copy the unit's running configuration file to either the startup configuration file or a specified URL file. Variations of this command include:

```
copy running-config startup-config
copy running-config <url_file>
copy running-config startup-config syntax-check
copy running-config <url_file> syntax-check
copy running-config startup-config | begin <line>
copy running-config startup-config | exclude <line>
copy running-config startup-config | include <line>
copy running-config <url_file> | begin <line>
copy running-config <url_file> | exclude <line>
copy running-config <url_file> | include <line>
copy running-config startup-config syntax-check | begin <line>
copy running-config startup-config syntax-check | exclude <line>
copy running-config startup-config syntax-check | include <line>
copy running-config <url_file> syntax-check | begin <line>
copy running-config <url_file> syntax-check | exclude <line>
copy running-config <url_file> syntax-check | include <line>
```

2.35.1 Syntax Description

running-config	Specifies that the running configuration is the file being copied.
startup-config	Copies the running configuration to the startup configuration file.
<url_file>	Copies the running configuration to the specified URL file located either in the unit's flash drive, or on a Trivial File Transfer Protocol (TFTP) server. Specify the URL file in the format: *<flash:filename>* or *<tftp://server/path-and-filename>*. Valid file name is a text string drawn from the alphabet (**A-Z**, **a-z**), digits (**0-9**), dot (**.**), hyphen (**-**), or underscore (**_**). Maximum file name length is 63 characters. A hyphen cannot be the first character. A file name of only dot (**.**) is not allowed.
syntax-check	Optional. Specifies that a syntax check is performed on the source configuration.
| begin *<line>*	Optional. Copies from lines that begin with the specified text and every line thereafter.
| exclude *<line>*	Optional. Copies the entire file, but excludes any lines containing the specified text.
| include *<line>*	Optional. The copied file includes only lines that contain the specified text.

2.35.2 Default Values

No default values are necessary for this command.

2.35.3 Privilege Level

By default, this command has a privilege level of **15**.

2.35.4 Command History

ASE Release 4.4-41	Command was introduced.

2.35.5 Usage Examples

The following example copies the unit's running configuration to the startup configuration:

```
#copy running-config startup-config
```

2.36 copy startup-config

Use the **copy startup-config** command to copy the unit's startup configuration file to either the running configuration file or a specified URL file. Variations of this command include:

```
copy startup-config running-config
copy startup-config <url_file>
copy startup-config running-config syntax-check
copy startup-config <url_file> syntax-check
copy startup-config running-config | begin <line>
copy startup-config running-config | exclude <line>
copy startup-config running-config | include <line>
copy startup-config <url_file> | begin <line>
copy startup-config <url_file> | exclude <line>
copy startup-config <url_file> | include <line>
copy startup-config running-config syntax-check | begin <line>
copy startup-config running-config syntax-check | exclude <line>
copy startup-config running-config syntax-check | include <line>
copy startup-config <url_file> syntax-check | begin <line>
copy startup-config <url_file> syntax-check | exclude <line>
copy startup-config <url_file> syntax-check | include <line>
```

2.36.1 Syntax Description

running-config	Copies the startup configuration to the running configuration file.
startup-config	Specifies that the startup configuration file is the file being copied.
<url_file>	Copies the startup configuration to the specified URL file located either in the unit's flash drive, or on a Trivial File Transfer Protocol (TFTP) server. Specify the URL file in the format: *<flash:filename>* or *<tftp://server/path-and-filename>*. Valid file name is a text string drawn from the alphabet (**A-Z**, **a-z**), digits (**0-9**), dot (**.**), hyphen (**-**), or underscore (**_**). Maximum file name length is 63 characters. A hyphen cannot be the first character. A file name of only dot (**.**) is not allowed.
syntax-check	Optional. Specifies that a syntax check is performed on the source configuration.
| begin *<line>*	Optional. Copies from lines that begin with the specified text and every line thereafter.
| exclude *<line>*	Optional. Copies the entire file, but excludes any lines containing the specified text.
| include *<line>*	Optional. The copied file includes only lines that contain the specified text.

2.36.2 Default Values

No default values are necessary for this command.

2.36.3 Privilege Level

By default, this command has a privilege level of **15**.

2.36.4 Command History

ASE Release 4.4-41	Command was introduced.

2.36.5 Usage Examples

The following example copies the unit's startup configuration to the running configuration:

```
#copy startup-config running-config
```

2.37 copy *<url_file>*

Use the **copy** *<url_file>* command to copy a specified file to the unit's running or startup configuration file. Variations of this command include:

```
copy <url_file> running-config
copy <url_file> startup-config
copy <url_file> running-config syntax-check
copy <url_file> startup-config syntax-check
copy <url_file> running-config | begin <line>
copy <url_file> running-config | exclude <line>
copy <url_file> running-config | include <line>
copy <url_file> startup-config | begin <line>
copy <url_file> startup-config | exclude <line>
copy <url_file> startup-config | include <line>
copy <url_file> running-config syntax-check | begin <line>
copy <url_file> running-config syntax-check | exclude <line>
copy <url_file> running-config syntax-check | include <line>
copy <url_file> startup-config syntax-check | begin <line>
copy <url_file> startup-config syntax-check | exclude <line>
copy <url_file> startup-config syntax-check | include <line>
```

2.37.1 Syntax Description

running-config	Specifies that the URL file is copied to the running configuration.
startup-config	Specifies that the URL file is copied to the startup configuration.
<url_file>	Specifies the URL file to be copied. URL files are located either in the unit's flash drive, or on a Trivial File Transfer Protocol (TFTP) server. Specify the URL file in the format: *<flash:filename>* or *<tftp://server/path-and-filename>*. Valid file name is a text string drawn from the alphabet (**A-Z**, **a-z**), digits (**0-9**), dot (**.**), hyphen (**-**), or underscore (**_**). Maximum file name length is 63 characters. A hyphen cannot be the first character. A file name of only dot (**.**) is not allowed.
syntax-check	Optional. Specifies that a syntax check is performed on the source configuration.
| begin *<line>*	Optional. Copies from lines that begin with the specified text and every line thereafter.
| exclude *<line>*	Optional. Copies the entire file, but excludes any lines containing the specified text.
| include *<line>*	Optional. The copied file includes only lines that contain the specified text.

2.37.2 Default Values

No default values are necessary for this command.

2.37.3 Privilege Level

By default, this command has a privilege level of **15**.

2.37.4 Command History

ASE Release 4.4-41	Command was introduced.

2.37.5 Usage Examples

The following example copies the URL file MYFILE from the unit's Flash drive to the unit's running configuration:

```
#copy flash:MYFILE running-config
```

2.38 delete <*url file*>

Use the **delete** <*url file*> command to delete a file from the unit's Flash drive.

2.38.1 Syntax Description

<url_file>	Specifies the file to be deleted from the unit's Flash drive. Specify the file in the format: *<flash:filename>*. Valid file name is a text string drawn from the alphabet (**A-Z**, **a-z**), digits (**0-9**), dot (**.**), hyphen (**-**), or underscore (**_**). Maximum file name length is 63 characters. A hyphen cannot be the first character. A file name of only dot (**.**) is not allowed.

2.38.2 Default Values

No default values are necessary for this command.

2.38.3 Privilege Level

By default, this command has a privilege level of **15**.

2.38.4 Command History

ASE Release 4.4-41	Command was introduced.

2.38.5 Usage Examples

The following example deletes the file TEXT1 from the Flash drive:

```
#delete flash:TEXT1
```

2.39 dir

Use the **dir** command to view the directory of all files in the unit's Flash drive. Variations of this command include:

```
dir
dir | begin <line>
dir | exclude <line>
dir | include <line>
```

2.39.1 Syntax Description

| begin *<line>*	Optional. Limits output to lines that begin with the specified text and every line thereafter.
| exclude *<line>*	Optional. Limits output by excluding any lines containing the specified text.
| include *<line>*	Optional. Limits output to that only containing the lines with the specified text.

2.39.2 Default Values

No default values are necessary for this command.

2.39.3 Privilege Level

By default, this command has a privilege level of **15**.

2.39.4 Command History

ASE Release 4.4-41	Command was introduced.

2.39.5 Usage Examples

The following example displays the Flash directory:

```
#dir
Directory of flash:
  r-2018-07-13 09:27:54    650 default-config
  rw 1970-01-01 00:30:38   10466 startup-config
2 files, 11116 bytes total.

Flash size: 3284992 bytes (3.1 MiB)
Flash free: 3239936 bytes (3.1 MiB)
```

2.40 disable <*level*>

Use the **disable** <*level*> command to disable the privilege commands for the specified level.

2.40.1 Syntax Description

`<level>`	Specifies the privilege level to disable. Commands with this privilege level will no longer be accessible in the session. Valid range is **0** to **15**, with a level of **15** being the administrator privilege level.

2.40.2 Default Values

By default, privilege levels are enabled on a per-command basis.

2.40.3 Command History

ASE Release 4.4-41	Command was introduced.

2.40.4 Functional Notes

Every command has a privilege level of **0** to **15**. Users can execute a command if the session's privilege level is greater than, or equal to, the commands privilege level. The privilege level **0** can typically only access basic system information. The privilege level **13** can typically configure all features on the ASE device, except for login accounts, authentication methods, multiple logins, administrator passwords, and enable passwords. The privilege level **15** can configure all features on the ASE device.

Privilege levels can be set on a per-session, per-user, and per-command basis. The following are the commands associated with configuring privilege levels:

- To configure privilege levels for a specific user, use the command "username" on page 472.
- To configure privilege levels for a specific line session, use the command "privilege level <level>" on page 616.
- To configure privilege levels associated with a specific password, use the command "enable" on page 293.
- To configure privilege levels on a per-command basis, use the command "privilege <mode> level <level> <command string>" on page 405.

The **disable** <*level*> command is used to disable the privilege level for commands at a certain level, thus overriding command privilege levels set by the session, user, or command. This feature can be beneficial if it is necessary to access higher level commands for a short amount of time, before enabling the command's privilege level again (using the command "enable <level>" on page 71).

2.40.5 Usage Examples

The following example disables privilege settings for commands at level **10**:

```
#disable 10
```

2.41 dot1x initialize

Use the **dot1x initialize** command to force immediate re-authentication for port-based Network Access Control. Variations of this command include:

```
dot1x initialize
dot1x initialize interface <interface>
```

2.41.1 Syntax Description

interface *<interface>*	Optional. Specifies that a specific interface is reauthenticated. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.41.2 Default Values

By default, this feature is disabled.

2.41.3 Command History

ASE Release 4.4-41	Command was introduced.

2.41.4 Usage Examples

The following example forces re-authentication on ports 1/1-26 on the Gigabit Ethernet interface:

```
#dot1x initialize interface GigabitEthernet 1/1-26
```

2.42 enable <*level*>

Use the **enable** <*level*> command to enable the privilege commands for the specified level.

2.42.1 Syntax Description

`<level>`	Specifies the privilege level to enable. Commands with this privilege level will be accessible in the session. Valid range is **0** to **15**, with a level of **15** being the administrator privilege level.

2.42.2 Default Values

By default, privilege levels are enabled on a per-command basis.

2.42.3 Command History

ASE Release 4.4-41	Command was introduced.

2.42.4 Functional Notes

Every command has a privilege level of **0** to **15**. Users can execute a command if the session's privilege level is greater than, or equal to, the commands privilege level. The privilege level **0** can typically only access basic system information. The privilege level **13** can typically configure all features on the ASE device, except for login accounts, authentication methods, multiple logins, administrator passwords, and enable passwords. The privilege level **15** can configure all features on the ASE device.

Privilege levels can be set on a per-session, per-user, and per-command basis. The following are the commands associated with configuring privilege levels:

- To configure privilege levels for a specific user, use the command "username" on page 472.
- To configure privilege levels for a specific line session, use the command "privilege level <level>" on page 616.
- To configure privilege levels associated with a specific password, use the command "enable" on page 293.
- To configure privilege levels on a per-command basis, use the command "privilege <mode> level <level> <command string>" on page 405.

The **enable** <*level*> command is used to enable the privilege level for commands at a certain level, thus overriding command privilege levels set by the session, user, or command. This feature can be beneficial if it is necessary to access higher level commands for a short amount of time, before disabling the command's privilege level again (using the command "disable <level>" on page 69).

2.42.5 Usage Examples

The following example enables privilege settings for commands at level **10**:

```
#enable 10
```

2.43 erps <*group number*> command

Use the **erps** <*group number*> **command** to execute commands for an Ethernet Ring Protection Switching (ERPS) group on a port interface. Variations of this command include:

```
erps <group number> command clear port0
erps <group number> command clear port1
erps <group number> command force port0
erps <group number> command force port1
erps <group number> command manual port0
erps <group number> command manual port1
```

2.43.1 Syntax Description

<group number>	Specifies the ERPS group number. Valid range is **1** to **64**.
clear	Specifies the clear command is executed.
force	Specifies the force command is executed.
manual	Specifies the manual command is executed.
port0	Specifies the ERPS port 0 interface.
port1	Specifies the ERPS port 1 interface.

2.43.2 Default Values

By default, ERPS is not configured on the interface.

2.43.3 Command History

ASE Release 4.4-41	Command was introduced.

2.43.4 Usage Examples

The following example executes the **clear** command on ERPS group **4** on the **port 1** interface:

```
#erps 4 command clear port1
```

2.44 firmware

Use the **firmware** command to swap or upgrade the unit's firmware. Variations of this command include:

firmware swap
firmware upgrade *<url_file>*

2.44.1 Syntax Description

swap	Specifies that the unit's firmware is swapped between the active and alternative firmware image.
upgrade *<url_file>*	Specifies that the unit's firmware is upgraded to the specified firmware image. Specify the URL of the firmware image in the format *<protocol>*`://`[*<username>*`[:`*<password>*`]@`*<host>*`[:`*<port>*`][/`*<path>*`]/`*<file name>*. The following special characters: **!"#$%&()+,;<=>?@[\]^`{|}~** should be percent encoded in the URL string. Valid file name is a text string drawn from the alphabet (**A-Z**, **a-z**), digits (**0-9**), dot (**.**), hyphen (**-**), or underscore (**_**). Maximum file name length is 63 characters. A hyphen cannot be the first character. A file name of only dot (**.**) is not allowed.

2.44.2 Default Values

No default values are necessary for this command.

2.44.3 Privilege Level

By default, this command has a privilege level of **15**.

2.44.4 Command History

ASE Release 4.4-41	Command was introduced.

2.44.5 Usage Examples

The following example upgrades the unit's firmware:

```
#firmware upgrade tftp://192.168.1.1/NV1560-24_v4.4-41-20200914.mfi
Programming image....
```

2.45 ip dhcp retry interface vlan <*vlan id*>

Use the **ip dhcp retry interface vlan** <*vlan id*> command to restart the Internet Protocol version 4 (IPv4) Dynamic Host Control Protocol (DHCP) query process.

2.45.1 Syntax Description

vlan *<vlan id>*	Specifies the virtual local area network ID of the VLAN interface on which to restart the DHCP query process. Valid range is **1** to **4095**.

2.45.2 Default Values

By default, DHCP is disabled.

2.45.3 Privilege Level

By default, this command has a privilege level of **15**.

2.45.4 Command History

ASE Release 4.4-41	Command was introduced.

2.45.5 Usage Examples

The following example restarts the IPv4 DHCP query process on VLAN 1:

```
#ip dhcp retry interface vlan 1
```

2.46 ipv6 dhcp-client restart

Use the ipv6 dhcp-client restart command to restart Internet Protocol version 6 (IPv6) Dynamic Host Control Protocol (DHCPv6) client service. Variations of this command include:

```
ipv6 dhcp-client restart
ipv6 dhcp-client restart interface vlan <vlan ids>
```

2.46.1 Syntax Description

interface vlan *<vlan ids>*	Optional. Specifies the virtual local area network (VLAN) IDs of IPv6 interfaces. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

2.46.2 Default Values

By default, DHCPv6 is disabled.

2.46.3 Command History

ASE Release 4.4-41	Command was introduced.

2.46.4 Usage Examples

The following example restarts DHCPv6 client service on IPv6 interface associated with VLAN 3:

```
#ipv6 dhcp-client restart interface vlan 3
```

2.47 link-oam remote-loopback

Use the **link -oam remote loopback** command to use link operations, administration, and management (OAM) to start or stop a loopback test on an interface. Variations of this command include:

link-oam remote-loopback start interface *<interface>*
link-oam remote-loopback stop interface *<interface>*

2.47.1 Syntax Description

start	Starts a remote loopback test on an interface.
stop	Stops a remote loopback test on an interface.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.47.2 Default Values

By default, link OAM is disabled.

2.47.3 Command History

ASE Release 4.4-41	Command was introduced.

2.47.4 Usage Examples

The following example starts a remote loopback test on ports 1/1-2 on the 10 Gigabit Ethernet interface:

```
#link-oam remote-loopback start interface 10GigabitEthernet 1/1-2
```

2.48 more <*url_file*>

Use the **more** <*url_file*> command to display a specified file. Variations of this command include:

```
more <url_file>
more <url_file> | begin <line>
more <url_file> | exclude <line>
more <url_file> | include <line>
```

2.48.1 Syntax Description

<url_file>	Specifies the file to display from either the unit's Flash drive, or a Trivial File Transfer Protocol (TFTP) server. Specify the URL file in the format: *<flash:filename>* or *<tftp://server/path-and-filename>*. Valid file name is a text string drawn from the alphabet (**A-Z**, **a-z**), digits (**0-9**), dot (**.**), hyphen (**-**), or underscore (**_**). Maximum file name length is 63 characters. A hyphen cannot be the first character. A file name of only dot (**.**) is not allowed.
| begin *<line>*	Optional. Limits the display to begin with the specified text and every line thereafter.
| exclude *<line>*	Optional. Limits the display to excluding any lines containing the specified text.
| include *<line>*	Optional. Limits the display to only lines that contain the specified text.

2.48.2 Default Values

No default values are necessary for this command.

2.48.3 Privilege Level

By default, this command has a privilege level of **15**.

2.48.4 Command History

ASE Release 4.4-41	Command was introduced.

2.48.5 Usage Examples

The following example displays the **ddd** file, beginning at line **a**, from a TFTP server:

```
#more tftp://192.168.1.1/ddd | begin a
% Loading /ddd from TFTP server 192.168.1.1
```

2.49 ping ip

Use the **ping ip** command to send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) echo messages. Variations of this command include:

```
ping ip <ipv4 address | domain name>
ping ip <ipv4 address | domain name> data <bytes>
ping ip <ipv4 address | domain name> quiet
ping ip <ipv4 address | domain name> repeat <packets>
ping ip <ipv4 address | domain name> saddr <ipv4 address>
ping ip <ipv4 address | domain name> size <bytes>
ping ip <ipv4 address | domain name> ttl <seconds>
ping ip <ipv4 address | domain name> verbose
ping ip <ipv4 address | domain name> sif <interface>
ping ip <ipv4 address | domain name> sif vlan <vlan id>
```

2.49.1 Syntax Description

<ipv4 address | domain name>	Specifies the destination IPv4 address or host name or fully qualified domain name (FQDN) to ping.
data *<bytes>*	Optional. Specifies the payload data byte value. Valid range is **0** to **255** bytes. Default value is **0** bytes.
quiet	Optional. Specifies the output is quiet.
repeat *<packets>*	Optional. Specifies the repeat packet count. Valid range is **1** to **60** packets. Default value is **5** packets.
saddr *<ipv4 address>*	Optional. Specifies an interface's source IPv4 address.
sif	Optional. Specifies a source interface.
<interface>	Optional. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
vlan *<vlan id>*	Specifies the VLAN interface as the source interface. Valid range is **1** to **4095**.
size *<bytes>*	Optional. Specifies the datagram size in bytes. Valid range is **2** to **1452** bytes. Default value is **56** bytes, and excludes Media Access Control (MAC), IP, and ICMP headers.
ttl *<seconds>*	Specifies the time to live (TTL) in seconds. Valid range is **1** to **255** seconds. Default value is **64** seconds.
verbose	Optional. Enables detailed messaging.

2.49.2 Default Values

No default values are necessary for this command.

2.49.3 Privilege Level

By default, this command has a privilege level of **0**.

2.49.4 Functional Notes

After specifying the target IPv4 address (or hostname) to ping, the following parameters can be entered multiple times and in any order: **data**, **quiet**, **repeat**, **saddr**, **size**, and **ttl**.

2.49.5 Command History

ASE Release 4.4-41	Command was introduced.

2.49.6 Usage Examples

The following example pings the IPv4 address **192.168.1.1** with a repeat count of **3** packets and a datagram size of **3** bytes:

```
#ping ip 192.168.1.1 repeat 3 size 3
PING 192.168.1.1 (192.168.1.1) : 3 data bytes

11 bytes from 192.168.1.1: seq=0 ttl=64
11 bytes from 192.168.1.1: seq=1 ttl=64
11 bytes from 192.168.1.1: seq=2 ttl=64

--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
```

2.50 ping ipv6

Use the **ping ipv6** command to send Internet Protocol version 6 (IPv6) Internet Control Message Protocol (ICMP) echo messages. Variations of this command include:

```
ping ipv6 <ipv6 address | domain name>
ping ipv6 <ipv6 address | domain name> data <bytes>
ping ipv6 <ipv6 address | domain name> quiet
ping ipv6 <ipv6 address | domain name> repeat <packets>
ping ipv6 <ipv6 address | domain name> saddr <ipv6 address>
ping ipv6 <ipv6 address | domain name> size <bytes>
ping ipv6 <ipv6 address | domain name> ttl <seconds>
ping ipv6 <ipv6 address | domain name> verbose
ping ipv6 <ipv6 address | domain name> sif <interface>
ping ipv6 <ipv6 address | domain name> sif vlan <vlan id>
```

2.50.1 Syntax Description

<ipv6 address | domain name>	Specifies the destination IPv6 address or host name or fully qualified domain name (FQDN) to ping.
data *<bytes>*	Optional. Specifies the payload data byte value. Valid range is **0** to **255** bytes. Default value is **0** bytes.
quiet	Optional. Specifies the output is quiet.
repeat *<packets>*	Optional. Specifies the repeat packet count. Valid range is **1** to **60** packets. Default value is **5** packets.
saddr *<ipv6 address>*	Optional. Specifies an interface's source IPv6 address.
sif	Optional. Specifies a source interface.
<interface>	Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
vlan *<vlan id>*	Specifies the VLAN interface as the source interface. Valid range is **1** to **4095**.
size *<bytes>*	Optional. Specifies the datagram size in bytes. Valid range is **2** to **1452** bytes. Default value is **56** bytes, and excludes Media Access Control (MAC), IP, and ICMP headers.
ttl *<seconds>*	Specifies the time to live (TTL) in seconds. Valid range is **1** to **255** seconds. Default value is **64** seconds.
verbose	Optional. Enables detailed messaging.

2.50.2 Default Values

No default values are necessary for this command.

2.50.3 Functional Notes

After specifying the target IPv4 address (or hostname) to ping, the following parameters can be entered multiple times and in any order: **data**, **quiet**, **repeat**, **saddr**, **size**, and **ttl**.

2.50.4 Command History

ASE Release 4.4-41	Command was introduced.

2.50.5 Usage Examples

The following example pings the IPv4 address **2001:DB8:1A0::3** with a repeat count of **3** packets and a datagram size of **3** bytes:

```
#ping ip 2001:DB8:1A0::3 repeat 3 size 3
PING 2001:DB8:1A0::3 (192.168.1.1) : 3 data bytes

11 bytes from 2001:DB8:1A0::3: seq=0 ttl=64
11 bytes from 2001:DB8:1A0::3: seq=1 ttl=64
11 bytes from 2001:DB8:1A0::3: seq=2 ttl=64

--- 2001:DB8:1A0::3 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
```

2.51 platform debug

Use the **platform debug** command to allow or deny debug command execution. Variations of this command include:

```
platform debug allow
platform debug deny
```

WARNING!
Turning on a large amount of debug information can adversely affect the performance of your unit.

2.51.1 Syntax Description

allow	Allows debug command execution on the ASE product.
deny	Denies debug command execution on the ASE product.

2.51.2 Default Values

By default, debug messaging is disabled.

2.51.3 Command History

ASE Release 4.4-41	Command was introduced.

2.51.4 Functional Notes

Issuing this command enables debug messaging for all features on the ASE device. Debug options are not available on the switch without enabling the debugging feature using the **platform debug allow** command. Once debug messaging has been enabled, enter **debug ?** from the Enable mode prompt to view the various available debug features.

Debug output is only available on the Console port.

2.51.5 Usage Examples

The following example denies debug command execution on the ASE product:

```
#platform debug deny
```

2.52 ptp <*number*> local-clock

Use the **ptp** <*number*> **local-clock** command to configure the Precision Time Protocol (PTP) local clock. Variations of this command include:

ptp *<number>* **local-clock ratio** *<ratio>*
ptp *<number>* **local-clock update**

2.52.1 Syntax Description

<number>	Specifies the PTP clock instance. Valid range is **0** to **3**.
ratio *<ratio>*	Configures the local master clock frequency ratio. Valid ratio range is **-10000000** to **10000000**, in units of **0**, **1** ppb. A ratio grater than 0 creates a faster clock, a ratio less than zero creates a slower clock.
update	Specifies that the local clock is synchronized to the operating system clock.

2.52.2 Default Values

By default, PTP is configured automatically.

2.52.3 Command History

ASE Release 4.4-41	Command was introduced.

2.52.4 Usage Examples

The following example specifies that local clock instance **1** is synchronized to the operating system clock:

```
#ptp 1 local-clock update
```

2.53 ptp <*number*> wireless delay

Use the **ptp** <*number*> **wireless delay** command to configure the Precision Time Protocol (PTP) clock wireless delay. Variations of this command include:

ptp *<number>* **wireless delay** *<base delay>* **interface** *<interface>*
ptp *<number>* **wireless delay** *<base delay>* *<incremental delay>* **interface** *<interface>*

2.53.1 Syntax Description

<number>	Specifies the PTP clock instance. Valid range is **0** to **3**.
<base delay>	Specifies the base wireless transmission delay in picoseconds. Valid range is **0** to **1000000000** picoseconds.
<incremental delay>	Optional. Specifies the incremental wireless transmission delay per byte. Valid range is **0** to **1000000** picoseconds.
interface *<interface>*	Limits PTP configuration to a single interface. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.53.2 Default Values

By default, PTP is configured automatically.

2.53.3 Command History

ASE Release 4.4-41	Command was introduced.

2.53.4 Functional Notes

PTP wireless mode configuration requires a two-step or operations, administration, and management (OAM)-based boundary clock.

2.53.5 Usage Examples

The following example specifies a base wireless transmission delay of **5** picoseconds for clock instance **2** on all switches and ports:

```
#ptp 2 wireless delay 5 interface *
Wireless mode not available for ptp instance 2, port 1
Wireless mode requires a two-step or Oam based BC
Wireless mode not available for ptp instance 2, port 2
Wireless mode requires a two-step or Oam based BC
```

2.54 ptp <*number*> wireless

Use the **ptp** <*number*> **wireless** command to enable Precision Time Protocol (PTP) wireless mode on one or more interface. Variations of this command include:

ptp *<number>* **wireless mode interface** *<interface>*
ptp *<number>* **wireless pre-notification interface** *<interface>*

2.54.1 Syntax Description

<number>	Specifies the PTP clock instance. Valid range is **0** to **3**.
mode	Enables wireless mode for the specified interface.
pre-notification	Issues a pre-notification message that the wireless modem configuration is changing.
interface *<interface>*	Specifies an interface on which to enable PTP wireless mode. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.54.2 Default Values

By default, PTP is configured automatically.

2.54.3 Command History

ASE Release 4.4-41	Command was introduced.

2.54.4 Functional Notes

PTP wireless mode configuration requires a two-step or operations, administration, and management (OAM)-based boundary clock.

2.54.5 Usage Examples

The following example enables PTP wireless mode for clock instance **2** on all switches and ports:

```
#ptp 2 wireless mode interface *
Wireless mode not available for ptp instance 2, port 1
Wireless mode requires a two-step or Oam based BC
Wireless mode not available for ptp instance 2, port 2
Wireless mode requires a two-step or Oam based BC
```

2.55 ptp cal

Use the **ptp cal** command to calibrate the Precision Time Protocol (PTP) clock. Variations of this command include:

```
ptp cal 1pps <value>
ptp cal p2p <interface>
ptp cal port <interface> mode 100m-cu reset
ptp cal port <interface> mode 10g reset
ptp cal port <interface> mode 10m-cu reset
ptp cal port <interface> mode 1g reset
ptp cal port <interface> mode 1g-cu reset
ptp cal port <interface> mode 2g5 reset
ptp cal port <interface> mode 5g reset
ptp cal port <interface> offset <value> cable-latency <value>
ptp cal port <interface> reset
ptp cal port <interface> start
ptp cal t-plane <interface> ext
ptp cal t-plane <interface> int
```

2.55.1 Syntax Description

1pps *<value>*	Calibrates the clock using 1 pulse-per-second (pps) measurements. Valid range is **-1000000** to **1000000**.
p2p	Calibrates the peer-to-peer round trip delay of the clock.
port	Calibrates the PTP clock on the specified port.
mode	Specifies the calibration mode per port. Valid options are 100m-cu, 10g, 10m-cu, 1g, 1g-cu, 2g5, and 5g.
offset *<value>*	Specifies the offset calibration. Valid range is **-1000000** to **1000000**.
cable-latency *<value>*	Specifies the latency of the cable used for calibration. defines the latency of the cable used for calibration. Valid range is **-1000000** to **1000000**.
reset	Resets the calibration.
start	Starts the calibration.
t-plane	Specifies the calibration for the T-plane.
ext	Specifies that external loopback is used.
int	Specifies that internal loopback is used.
<interface>	Specifies an interface for calibration. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.55.2 Default Values

By default, PTP is configured automatically.

2.55.3 Command Hisotry

ASE Release 4.4-41	Command was introduced.

2.55.4 Usage Examples

The following example calibrates the PTP clock on port 1/2 of the Gigabit Ethernet interface:

```
#ptp cal port GigabitEthernet 1/2 start
Starting calibration of port: 2 using external reference.
Deleting any existing PTP instances
Resetting VLAN configuration to default
Creating PTP slave used for calibration
--------------------------------------------------------------------------------
    -------
A PTP slave was setup for calibration.
Please wait for servo to lock. Then measure 1PPS difference between PTP master
    (reference)
and PTP slave (device under calibration) the continue calibration i.e. issue
    command:
    ptp cal port <port> offset <-100000-100000> cable-latency <-100000-100000>

--------------------------------------------------------------------------------
    -------
```

2.56 reload

Use the **reload** command to reload the ASE system. Variations of this command include:

```
reload cold
reload defaults
reload defaults keep-ip
```

2.56.1 Syntax Description

cold	Reloads the system cold.
defaults	Reloads the system defaults without rebooting the system.
keep-ip	Optional. Specifies that the VLAN 1 IP address remains configured.

2.56.2 Default Values

No default values are necessary for this command.

2.56.3 Privilege Level

By default, this command has a privilege level of **15**.

2.56.4 Command History

ASE Release 4.4-41	Command was introduced.

2.56.5 Usage Examples

The following example reloads the system defaults while keeping the VLAN 1 IP address:

```
#reload defaults keep-ip
```

2.57 send

Use the **send** command to send messages to other TeleType (TTY) lines. Variations of this command include:

```
send * <message>
send <line> <message>
send console 0 <message>
send vty <line> <message>
```

2.57.1 Syntax Description

*****	Sends the message to all TTY lines.
<line>	Sends the message to multiple lines. Valid range is **0** to **16**.
console 0	Sends the message to the primary terminal line.
vty *<line>*	Sends the message to virtual terminal lines. Valid range is **0** to **15**.
<message>	Specifies the message to be sent using a delimiting character at the beginning and end of the message (for example **'aaa'**). Messages cannot exceed **128** characters in length.

2.57.2 Default Values

No default values are necessary for this command.

2.57.3 Command History

ASE Release 4.4-41	Command was introduced.

2.57.4 Usage Examples

The following example sends an **aaa** message to all lines:

```
#send * 'aaa'
------------------------------
*** Message from line 0:
aaa
------------------------------
```

2.58 show aaa

Use the **show aaa** command to display configured Authentication, Authorization, and Accounting (AAA) methods. Variations of this command include:

```
show aaa
show aaa | begin <line>
show aaa | exclude <line>
show aaa | include <line>
```

2.58.1 Syntax Description

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

2.58.2 Default Values

No default values are necessary for this command.

2.58.3 Command History

ASE Release 4.4-41	Command was introduced.

2.58.4 Usage Examples

The following example displays configured AAA methods:

```
#show aaa
Authentication :
  console : local
  telnet  : local
  ssh     : local
  http    : local
Authorization:
  console : no, commands disabled
  telnet  : no, commands disabled
  ssh     : no, commands disabled
Accounting:
  console : no, commands disabled, exec disabled
  telnet  : no, commands disabled, exec disabled
  ssh     : no, commands disabled, exec disabled
```

2.59 show access management

Use the **show access management** command to display access management configuration information. Variations of this command include:

```
show access management
show access management | begin <line>
show access management | exclude <line>
show access management | include <line>
show access management <id>
show access management <id> | begin <line>
show access management <id> | exclude <line>
show access management <id> | include <line>
show access management statistics
show access management statistics | begin <line>
show access management statistics | exclude <line>
show access management statistics | include <line>
```

2.59.1 Syntax Description

<id>	Optional. Limits output to the specified ID of the access management entry list. Valid range is **1** to **16**.
statistics	Optional. Displays access management statistics.
| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.

2.59.2 Default Values

No default values are necessary for this command.

2.59.3 Privilege Level

By default, this command has a privilege level of **15**.

2.59.4 Command History

ASE Release 4.4-41	Command was introduced.

2.59.5 Functional Notes

For any output to be displayed by this command, access management must be enabled (using the **access management** *<id>* command as described on *on page 257*).

2.59.6 Usage Examples

The following example displays access management configuration information for entry list **3**:

```
#show access management 3
Access Management Statistics:
-----------------------------
HTTP     Receive:          0    Allow:          0    Discard:          0
HTTPS    Receive:          0    Allow:          0    Discard:          0
SNMP     Receive:          0    Allow:          0    Discard:          0
TELNET   Receive:          0    Allow:          0    Discard:          0
SSH      Receive:         59    Allow:         59    Discard:          0
```

2.60 show access-list

Use the **show access-list** command to display access list configuration information. Variations of this command include:

```
show access-list
show access-list | begin <Line>
show access-list | exclude <Line>
show access-list | include <Line>
show access-list ace statistics
show access-list ace statistics <entry id>
show access-list ace-status
show access-list ace-status arp-inspection
show access-list ace-status conflicts
show access-list ace-status dhcp
show access-list ace-status ip
show access-list ace-status ip-source-guard
show access-list ace-status ipmc
show access-list ace-status link-oam
show access-list ace-status loop-protect
show access-list ace-status mep
show access-list ace-status ptp
show access-list ace-status static
show access-list ace-status upnp
show access-list interface <interface>
show access-list rate-limiter
show access-list rate-limiter <id>
```

2.60.1 Syntax Description

| begin *<Line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<Line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<Line>*	Optional. Produces output that only displays lines with the specified text.
ace	Optional. Specifies that output is limited to access list entries.
statistics	Optional. Displays traffic statistics for all access list entries.
<entry id>	Optional. Limits display to a specific access list entry. Valid range is **1** to **512**.
ace-status	Optional. Displays local access list entry status.
arp-inspection	Optional. Displays access list entries that are configured by Address Resolution Protocol (ARP) inspection module.
conflicts	Optional. Displays access list entries that were not applied to the hardware due to hardware limitations.
dhcp	Optional. Displays access list entries that are configured by Dynamic Host Control Protocol (DHCP) modules.
ip	Optional. Displays access list entries that are configured by Internet Protocol (IP) module.
ip-source-guard	Optional. Displays access list entries that are configured by IP source guard module.

ipmc	Optional. Displays access list entries that are configured by IP multicast (IPmc) module.
link-oam	Optional. Displays access list entries that are configured by link operations, administration, and management (OAM) module.
loop-protect	Optional. Displays access list entries that are configured by loop protect module.
mep	Optional. Displays access list entries that are configured by maintenance endpoint (MEP) module.
ptp	Optional. Displays access list entries that are configured by Precision Time Protocol (PTP) module.
static	Optional. Displays access list entries that are configured manually.
upnp	Optional. Displays access list entries that are configured by UPnP module.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
rate-limiter	Optional. Specifies rate limiter information for the access list is displayed.
<id>	Optional. Limits the output to a specific rate limiter ID. Valid range is **1** to **16**.

2.60.2 Default Values

No default values are necessary for this command.

2.60.3 Privilege Level

By default, this command has a privilege level of **15**.

2.60.4 Command History

ASE Release 4.4-41	Command was introduced.

2.60.5 Usage Examples

The following example displays traffic statistics for access list entry **3**:

```
#show access-list statistics ace statistics 3

Switch access-list ace number: 0
```

2.61 show aggregation

Use the **show aggregation** command to display aggregation port configuration information. Variations of this command include:

```
show aggregation
show aggregation | begin <line>
show aggregation | exclude <line>
show aggregation | include <line>
show aggregation mode
```

2.61.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
mode	Optional. Specifies that traffic distribution information is included in the output.

2.61.2 Default Values

No default values are necessary for this command.

2.61.3 Privilege Level

By default, this command has a privilege level of **15**.

2.61.4 Command History

ASE Release 4.4-41	Command was introduced.

2.61.5 Usage Examples

The following example displays traffic distribution information for the aggregation port:

```
#show aggregation mode
Aggregation Mode:

SMAC  :  Enabled
DMAC  :  Disabled
IP    :  Enabled
Port  :  Enabled
```

2.62 show alarm

Use the **show alarm** command to display alarm information. Variations of this command include:

```
show alarm sources
show alarm sources | begin <line>
show alarm sources | exclude <line>
show alarm sources | include <line>
show alarm sources <filter>
show alarm status
show alarm status | begin <line>
show alarm status | exclude <line>
show alarm status | include <line>
show alarm status <filter>
```

2.62.1 Syntax Description

sources	Specifies that alarm sources are displayed.
status	Specifies that alarm status are displayed.
<filter>	Optional. Specifies a keyword on which to filter the alarm information. Keyword is limited to **127** characters.
| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.

2.62.2 Default Values

No default values are necessary for this command.

2.62.3 Command History

ASE Release 4.4-41	Command was introduced.

2.62.4 Usage Examples

The following example specifies that alarm sources for maintenance entity points (MEPs) are displayed. These sources are then used to configure alarms using the command “alarm <alarm name> <alarm expression>” as described *on page 275*.

```
#show alarm sources | include mep
mep.status.instance[int32_t]@Clevel    vtss_bool_t
mep.status.instance[int32_t]@Cmeg      vtss_bool_t
mep.status.instance[int32_t]@Cmep      vtss_bool_t
mep.status.instance[int32_t]@Cssf      vtss_bool_t
mep.status.instance[int32_t]@Cais      vtss_bool_t
mep.status.instance[int32_t]@Clck      vtss_bool_t
mep.status.instance[int32_t]@Atsf      vtss_bool_t
mep.status.instance[int32_t]@Atsd      vtss_bool_t
mep.status.instance[int32_t]@Ablk      vtss_bool_t
mep.status.instance[int32_t]@Cloop     vtss_bool_t
--MORE--
```

2.63 show auto-link

Use the **show auto-link** command to display configuration information for the Auto-link feature. Variations of this command include:

```
show auto-link
show auto-link | begin <line>
show auto-link | exclude <line>
show auto-link | include <line>
```

2.63.1 Syntax Description

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

2.63.2 Default Values

No default values are necessary for this command.

2.63.3 Command History

ASE Release 4.4-41	Command was introduced.

2.63.4 Usage Example

The following is sample output from the **show auto-link** command:

```
#show auto-link
Auto-Link Mode : Enabled
        Use Http: Enabled
        Server URL: 10.14.1.193:80/al/DiscoveryProcessor?action=devinfo
        SRV Prefix: http
        Primary Server: 10.14.1.193:80
        Recontact Interval: 3600 seconds
        Last Contact: Thu Jan  1 23:05:25 1970
        Next Contact: Fri Jan  2 00:05:25 1970
        Status: Discovered (CONNECTED)
        Last Contacted Server: 10.14.1.193:80
```

2.64 show board-data

Use the **show board-data** command to display the ASE model information.

2.64.1 Syntax Description

No subcommands.

2.64.2 Default Values

No default values are necessary for this command.

2.64.3 Command History

ASE Release 4.4-41 Command was introduced.

2.64.4 Usage Examples

The following example displays the board data information for the ASE product:

```
#show board-data

Model Name          :  NetVanta 1560-48-740W

Part Number         :  17108148PF2

Hardware Version    :  A
```

2.65 show clock

Use the **show clock** command to display the system time. Variations of this command include:

```
show clock
show clock detail
```

2.65.1 Syntax Description

detail	Optional. Displays detailed clock information.

2.65.2 Default Values

No default values are necessary for this command.

2.65.3 Privilege Level

By default, this command has a privilege level of **0**.

2.65.4 Command History

ASE Release 4.4-41	Command was introduced.

2.65.5 Usage Examples

The following example displays the system time:

```
#show clock

System Time : 1970-01-01T23:48:08+00:00
```

2.66 show ddmi

Use the **show ddmi** information to display the current discovery and dependency mapping information (DDMI) mode.

2.66.1 Syntax Description

No subcommands.

2.66.2 Default Values

No default values are necessary for this command.

2.66.3 Command History

ASE Release 4.4-41	Command was introduced.

2.66.4 Usage Examples

The following example displays the current DDMI mode:

```
#show ddmi

Current mode:  Enabled
```

2.67 show dot1x

Use the **show dot1x** command to display port-based network address control information. Variations of this command include:

```
show dot1x status
show dot1x status | begin <line>
show dot1x status | exclude <line>
show dot1x status | include <line>
show dot1x status brief
show dot1x status interface <interface>
show dot1x statistics eapol
show dot1x statistics eapol | begin <line>
show dot1x statistics eapol | exclude <line>
show dot1x statistics eapol | include <line>
show dot1x statistics eapol interface <interface>
show dot1x statistics radius
show dot1x statistics radius | begin <line>
show dot1x statistics radius | exclude <line>
show dot1x statistics radius | include <line>
show dot1x statistics radius interface <interface>
show dot1x statistics all
show dot1x statistics all | begin <line>
show dot1x statistics all | exclude <line>
show dot1x statistics all | include <line>
show dot1x statistics all interface <interface>
```

2.67.1 Syntax Description

status	Displays network address control status information, including administrative state, port state, and last source information.
brief	Optional. Displays a brief summary of port-based network address control information.
statistics	Displays network address control statistics.
eapol	Specifies that Extensible Authentication Protocol (EAP) over local area network (LAN) (EAPoL) information is displayed.
radius	Specifies that back-end server statistics are displayed.
all	Displays all network access control statistics.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.67.2 Default Values

No default values are necessary for this command.

2.67.3 Privilege Level

By default, this command has a privilege level of **0**.

2.67.4 Command History

ASE Release 4.4-41	Command was introduced.

2.67.5 Usage Examples

The following example displays back-end server statistics for port-based network access control configuration:

```
#show dot1x statistics radius
Interface  Rx Access    Rx Other    Rx Auth.    Rx Auth.    Tx          MAC
           Challenges   Requests    Successes   Failures    Responses   Address
---------- ----------- ----------- ----------- ----------- ----------- ---------
Gi 1/1               0           0           0           0           0        -
Gi 1/2               0           0           0           0           0        -
Gi 1/3               0           0           0           0           0        -
Gi 1/4               0           0           0           0           0        -
Gi 1/5               0           0           0           0           0        -
Gi 1/6               0           0           0           0           0        -
```

2.68 show eps

Use the **show eps** command to display Ethernet Protection Switching (EPS) information. Variations of this command include:

```
show eps
show eps | begin <line>
show eps | exclude <line>
show eps | include <line>
show eps <range>
show eps detail
```

2.68.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
<range>	Optional. Specifies the range of EPS instances.
detail	Optional. Displays detailed configuration information.

2.68.2 Default Values

No default values are necessary for this command.

2.68.3 Command History

ASE Release 4.4-41	Command was introduced.

2.68.4 Usage Examples

The following example displays sample output from the **show eps detail** command:

```
#show eps detail
EPS state is:
     Inst        State     Wstate     Pstate     TxAps r b     RxAps r b     FopPm
    FopCm     FopNr     FopNoAps


EPS Configuration is:
    Inst    Dom    Archi    Wflow    Pflow    Wmep    Pmep    APSmep    Direct
    Revert     Wtr     Hold     Aps

EPS Command is:
     Inst          Command
```

2.69 show erps

Use the **show erps** command to display Ethernet Ring Protection Switching (ERPS) statistics and configuration information. Variations of this command include:

```
show erps
show erps | begin <line>
show erps | exclude <line>
show erps | include <line>
show erps <group number>
show erps detail
show erps statistics
```

2.69.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<Line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
<group number>	Optional. Displays information for specific ERPS group numbers. Valid range is **1** to **64**.
detail	Optional. Displays detailed information.
statistics	Optional. Displays ERPS statistics.

2.69.2 Default Values

No default values are necessary for this command.

2.69.3 Command History

ASE Release 4.4-41	Command was introduced.

2.69.4 Usage Examples

The following example displays statistics for any configured ERPS groups:

```
#show erps statistics

% No ERPS groups configured
```

2.70 show green-ethernet

Use the **show green-ethernet** command to display Ethernet power reduction information. Variations of this command include:

```
show green-ethernet
show green-ethernet | begin <line>
show green-ethernet | exclude <line>
show green-ethernet | include <line>
show green-ethernet interface <interface>
show green-ethernet eee
show green-ethernet eee interface <interface>
show green-ethernet energy-detect
show green-ethernet energy-detect interface <interface>
show green-ethernet short-reach
show green-ethernet short-reach interface <interface>
```

2.70.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
eee	Optional. Displays energy-efficient Ethernet (EEE) status for a specific port or ports.
energy-detect	Optional. Displays green Ethernet energy-detect status for a specific port or ports.
short-reach	Optional. Displays green Ethernet short-reach status for a specific port or ports.

2.70.2 Default Values

No default values are necessary for this command.

2.70.3 Privilege Level

By default, this command has a privilege level of **15**.

2.70.4 Command History

ASE Release 4.4-41	Command was introduced.

2.70.5 Usage Examples

The following is sample output from the **show green-ethernet eee** command:

```
#show green-ethernet eee
Interface              Lnk  EEE Capable EEE Enabled  LP EEE Capable EEE In Power Save
-----------           ----- ----------- ----------- -------------   -----------------
GigabitEthernet 1/1    No     Yes      No            No             No
GigabitEthernet 1/2    No     Yes      No            No             No
GigabitEthernet 1/3    No     Yes      No            No             No
.....
10GigabitEthernet 1/1  No     No       N/A           N/A            N/A
10GigabitEthernet 1/2  No     No       N/A           N/A            N/A
```

2.71 show history

Use the **show history** command to display the CLI session command history. Variations of this command include:

```
show history
show history | begin <line>
show history | exclude <line>
show history | include <line>
```

2.71.1 Syntax Description

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

2.71.2 Default Values

No default values are necessary for this command.

2.71.3 Command History

ASE Release 4.4-41	Command was introduced.

2.71.4 Usage Examples

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

```
#show history
  show green-ethernet eee
  show history
```

2.72 show interface

Use the **show interface** command to display interface statistics. Variations of this command include:

```
show interface <interface> capabilities
show interface <interface> description
show interface <interface> status
show interface <interface> transceiver
show interface <interface> verify
show interface <interface> statistics
show interface <interface> statistics | begin <line>
show interface <interface> statistics | exclude <line>
show interface <interface> statistics | include <line>
show interface <interface> statistics bytes
show interface <interface> statistics bytes up
show interface <interface> statistics bytes down
show interface <interface> statistics discards
show interface <interface> statistics discards up
show interface <interface> statistics discards down
show interface <interface> statistics errors
show interface <interface> statistics errors up
show interface <interface> statistics errors down
show interface <interface> statistics packets
show interface <interface> statistics packets up
show interface <interface> statistics packets down
show interface <interface> statistics down bytes
show interface <interface> statistics down discards
show interface <interface> statistics down errors
show interface <interface> statistics down packets
show interface <interface> statistics up bytes
show interface <interface> statistics up discards
show interface <interface> statistics up errors
show interface <interface> statistics up packets
show interface <interface> switchport
show interface <interface> switchport | begin <line>
show interface <interface> switchport | exclude <line>
show interface <interface> switchport | include <line>
show interface <interface> switchport access
show interface <interface> switchport hybrid
show interface <interface> switchport trunk
show interface vlan
show interface vlan <vlan ids>
```

2.72.1 Syntax Description

interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.

| include *<line>*	Optional. Produces output that only displays lines with the specified text.
capabilities	Displays interface capabilites.
description	Displays a description of the interface.
statistics	Displays statistic counters for the interface.
bytes	Optional. Displays byte statistics for the interface.
discards	Optional. Displays discard statistics for the interface.
down	Optional. Displays which ports are down on the interface.
errors	Optional. Displays error statistics for the interface.
filtered	Optional. Displays filtered statistics for the interface.
packets	Optional. Displays packet statistics for the interface.
priority	Optional. Displays priority statistics for the interface.
up	Optional. Displays which ports are up on the interface.
status	Displays interface status.
switchport	Displays interface switchport information.
access	Optional. Displays access port status for the interface.
hybrid	Optional. Displays hybrid port status for the interface.
trunk	Optional. Displays trunk port status for the interface.
transceiver	Displays interface transceiver information.
verify	Displays the latest cable diagnostic results.
vlan	Displays virtual local area network (VLAN) interface statistics.
<vlan ids>	Optional. Limits the output to specific VLANs. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

2.72.2 Default Values

No default values are necessary for this command.

2.72.3 Privilege Level

By default, the **show interval vlan** command has a privilege level of **15**. The **show interface** <*interface*> commands have a privilege level of **0**.

2.72.4 Command History

ASE Release 4.4-41	Command was introduced.

2.72.5 Usage Examples

The following is sample output from the **show interface GigabitEthernet 1/1-2 capabilities** command:

```
#show interface GigabitEthernet 1/1-2 capabilities

GigabitEthernet 1/1 Capabilities:
 Speed cap:  10, 100, 1000, auto
```

```
 Duplex cap:  half, full, auto
 Trunk encap. type:  802.1Q
 Trunk mode:  access, hybrid, trunk
 Channel:  yes
 Broadcast suppression:  no
 Flowcontrol:  yes
 Fast Start:  no
 QoS scheduling:  tx-(8q)
 CoS rewrite:  yes
 ToS rewrite:  yes
 UDLD:  no
 Inline power:  yes
 RMirror:  yes
 PortSecure:  yes
 Dot1x:  yes

GigabitEthernet 1/2 Capabilities:

 Speed cap: 10, 100, 1000, auto
 Duplex cap:  half, full, auto
 Trunk encap. type:  802.1Q
 Trunk mode: access, hybrid, trunk
 Channel:  yes
 Broadcast suppression:  no
 Flowcontrol:  yes
 Fast Start:  no
 QoS scheduling:  tx-(8q)
 CoS rewrite:  yes
 ToS rewrite:  yes
 UDLD:  no
 Inline power:  yes
 RMirror:  yes
 PortSecure:  yes
 Dot1x:  yes
```

2.73 show ip acd

Use the **show ip acd** command to display Internet Protocol version 4 (IPv4) address conflict detection (ACD) information. Variations of this command include:

```
show ip acd
show ip acd | begin <line>
show ip acd | exclude <line>
show ip acd | include <line>
```

2.73.1 Syntax Description

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

2.73.2 Default Values

No default values are necessary for this command.

2.73.3 Command History

ASE Release 4.4-41	Command was introduced.

2.73.4 Usage Examples

Enter the command as follows to display IPv4 ACD information:

```
#show ip acd
```

2.74 show ip arp

Use the **show ip arp** command to display Internet Protocol version 4 (IPv4) Address Resolution Protocol (ARP) information. Variations of this command include:

```
show ip arp
show ip arp | begin <line>
show ip arp | exclude <line>
show ip arp | include <line>
show ip arp inspection
show ip arp inspection entry
show ip arp inspection entry dhcp-snooping interface <interface>
show ip arp inspection entry interface <interface>
show ip arp inspection entry static interface <interface>
show ip arp inspection interface <interface>
show ip arp inspection vlan <vlan ids>
```

2.74.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
inspection	Optional. Displays ARP inspection information.
entry	Optional. Displays ARP inspection entry information.
dhcp-snooping	Optional. Displays Dynamic Host Control Protocol (DHCP) snooping information.
static interface	Optional. Displays static entry information.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
vlan *<vlan ids>*	Optional. Limits the output to specific virtual local area networks (VLANs). You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

2.74.2 Default Values

No default values are necessary for this command.

2.74.3 Privilege Level

By default, the **show ip arp inspection interface** and the **show ip arp** commands have a privilege level of **0**. The **show ip arp inspection entry** command has a privilege level of **13**.

2.74.4 Command History

ASE Release 4.4-41	Command was introduced.

2.74.5 Usage Examples

Enter the command as follows to display IPv4 ARP information:

```
#show ip arp
```

2.75 show ip domain

Use the **show ip domain** command to display information about the Internet Protocol version 4 (IPv4) default domain name. Variations of this command include:

```
show ip domain
show ip domain | begin <line>
show ip domain | exclude <line>
show ip domain | include <line>
```

2.75.1 Syntax Description

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

2.75.2 Default Values

No default values are necessary for this command.

2.75.3 Command History

ASE Release 4.4-41	Command was introduced.

2.75.4 Usage Examples

Enter the command as follows to display domain name information:

```
#show ip domain
```

2.76 show ip dhcp detailed statistics

Use the **show ip dhcp detailed statistics** command to display detailed Internet Protocol version 4 (IPv4) Dynamic Host Control Protocol (DHCP) statistics. Variations of this command include:

```
show ip dhcp detailed statistics client
show ip dhcp detailed statistics client | begin <line>
show ip dhcp detailed statistics client | exclude <line>
show ip dhcp detailed statistics client | include <line>
show ip dhcp detailed statistics client interface <interface>
show ip dhcp detailed statistics combined
show ip dhcp detailed statistics combined | begin <line>
show ip dhcp detailed statistics combined | exclude <line>
show ip dhcp detailed statistics combined | include <line>
show ip dhcp detailed statistics combined interface <interface>
show ip dhcp detailed statistics normal-forward
show ip dhcp detailed statistics normal-forward | begin <line>
show ip dhcp detailed statistics normal-forward | exclude <line>
show ip dhcp detailed statistics normal-forward | include <line>
show ip dhcp detailed statistics normal-forward interface <interface>
show ip dhcp detailed statistics relay
show ip dhcp detailed statistics relay | begin <line>
show ip dhcp detailed statistics relay | exclude <line>
show ip dhcp detailed statistics relay | include <line>
show ip dhcp detailed statistics relay interface <interface>
show ip dhcp detailed statistics server
show ip dhcp detailed statistics server | begin <line>
show ip dhcp detailed statistics server | exclude <line>
show ip dhcp detailed statistics server | include <line>
show ip dhcp detailed statistics server interface <interface>
show ip dhcp detailed statistics snooping
show ip dhcp detailed statistics snooping | begin <line>
show ip dhcp detailed statistics snooping | exclude <line>
show ip dhcp detailed statistics snooping | include <line>
show ip dhcp detailed statistics snooping interface <interface>
```

2.76.1 Syntax Description

client	Displays statistics for the DHCP client.
combined	Displays all DHCP related statistics.
normal-forward	Displays DHCP normal Layer 2 or Layer 3 forwarding statistics.
relay	Displays DHCP relay statistics.
server	Displays DHCP server statistics.
snooping	Displays DHCP snooping statistics.
| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.

interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.76.2 Default Values

No default values are necessary for this command.

2.76.3 Privilege Level

By default, this command has a privilege level of **0**.

2.76.4 Command History

ASE Release 4.4-41	Command was introduced.

2.76.5 Usage Examples

Enter the command as follows to display all IPv4 DHCP related statistics:

```
#show ip dhcp detailed statistics combined
```

2.77 show ip dhcp excluded-address

Use the **show ip dhcp excluded-address** command to display Internet Protocol version 4 (IPv4) addresses contained in the Dynamic Host Control Protocol (DHCP) excluded IP address database. Variations of this command include:

```
show ip dhcp excluded-address
show ip dhcp excluded-address | begin <line>
show ip dhcp excluded-address | exclude <line>
show ip dhcp excluded-address | include <line>
```

2.77.1 Syntax Description

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

2.77.2 Default Values

No default values are necessary for this command.

2.77.3 Privilege Level

By default, this command has a privilege level of **0**.

2.77.4 Command History

ASE Release 4.4-41	Command was introduced.

2.77.5 Usage Examples

Enter the command as follows to display all IP addresses in the DHCP excluded IP address database:

```
#show ip dhcp excluded-address
```

2.78 show ip dhcp pool

Use the **show ip dhcp pool** command to display information related to any configured Internet Protocol version 4 (IPv4) Dynamic Host Control Protocol (DHCP) pool(s). Variations of this command include:

```
show ip dhcp pool
show ip dhcp pool | begin <line>
show ip dhcp pool | exclude <line>
show ip dhcp pool | include <line>
show ip dhcp pool <name>
```

2.78.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
<name>	Optional. Displays information associated with the specified DHCP pool. DHCP pool names are limited to **32** characters in length.

2.78.2 Default Values

No default values are necessary for this command.

2.78.3 Privilege Level

By default, this command has a privilege level of **0**.

2.78.4 Command History

ASE Release 4.4-41	Command was introduced.

2.78.5 Usage Examples

Enter the command as follows to display information for all configured DHCP pools:

```
#show ip dhcp pool
```

2.79 show ip dhcp relay

Use the **show ip dhcp relay** command to display Internet Protocol version 4 (IPv4) Dynamic Host Control Protocol (DHCP) relay configuration information. Variations of this command include:

```
show ip dhcp relay
show ip dhcp relay | begin <line>
show ip dhcp relay | exclude <line>
show ip dhcp relay | include <line>
show ip dhcp relay statistics
```

2.79.1 Syntax Description

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

2.79.2 Default Values

No default values are necessary for this command.

2.79.3 Privilege Level

By default, this command has a privilege level of **0**.

2.79.4 Command History

ASE Release 4.4-41	Command was introduced.

2.79.5 Usage Examples

Enter the command as follows to display DHCP relay information:

```
#show ip dhcp relay
```

2.80 show ip dhcp server

Use the **show ip dhcp server** command to display Internet Protocol version 4 (IPv4) Dynamic Host Control Protocol (DHCP) server information. Variations of this command include:

```
show ip dhcp server
show ip dhcp server | begin <line>
show ip dhcp server | exclude <line>
show ip dhcp server | include <line>
show ip dhcp server declined-ip
show ip dhcp server declined-ip <ipv4 address>
show ip dhcp server statistics
```

2.80.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<Line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<Line>*	Optional. Produces output that only displays lines with the specified text.
declined-ip	Optional. Displays any IPv4 addresses declined by DHCP.
<ipv4 address>	Optional. Specifies an IPv4 unicast address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
statistics	Optional. Displays IPv4 DHCP server traffic statistics.

2.80.2 Default Values

No default values are necessary for this command.

2.80.3 Privilege Level

By default, this command has a privilege level of **0**.

2.80.4 Command History

ASE Release 4.4-41	Command was introduced.

2.80.5 Usage Examples

Enter the command as follows to display DHCP server information:

```
#show ip dhcp server
```

2.81 show ip dhcp server binding

Use the **show ip dhcp server binding** command to display information for Internet Protocol version 4 (IPv4) Dynamic Host Control Protocol (DHCP) address bindings on the DHCP server. Variations of this command include:

```
show ip dhcp server binding
show ip dhcp server binding <ipv4 address>

show ip dhcp server binding state allocated
show ip dhcp server binding state allocated type automatic
show ip dhcp server binding state allocated type expired
show ip dhcp server binding state allocated type manual
show ip dhcp server binding state committed
show ip dhcp server binding state committed type automatic
show ip dhcp server binding state committed type expired
show ip dhcp server binding state committed type manual
show ip dhcp server binding state expired
show ip dhcp server binding state expired type automatic
show ip dhcp server binding state expired type expired
show ip dhcp server binding state expired type manual

show ip dhcp server binding type automatic
show ip dhcp server binding type automatic state automatic
show ip dhcp server binding type automatic state committed
show ip dhcp server binding type automatic state expired
show ip dhcp server binding type expired
show ip dhcp server binding type expired state automatic
show ip dhcp server binding type expired state committed
show ip dhcp server binding type expired state expired
show ip dhcp server binding type manual
show ip dhcp server binding type manual state automatic
show ip dhcp server binding type manual state committed
show ip dhcp server binding type manual state expired
```

2.81.1 Syntax Description

<ipv4 address>	Optional. Specifies an IPv4 unicast address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
state	Optional. Displays the state of the DHCP server address bindings.
allocated	Optional. Limits display to only DHCP server address bindings in the Allocated state.
committed	Optional. Limits display to only DHCP server address bindings in the Committed state.
expired	Optional. Limits display to only DHCP server address bindings in the Expired state.
type	Optional. Displays the type of DHCP server address bindings.
allocated	Optional. Limits display to only DHCP server address bindings that have been allocated.
expired	Optional. Limits display to only DHCP server address bindings that have expired.

manual	Optional. Limits display to only DHCP server address bindings that have been entered manually for a specific host.

2.81.2 Default Values

No default values are necessary for this command.

2.81.3 Privilege Level

By default, this command has a privilege level of **0**.

2.81.4 Command History

ASE Release 4.4-41	Command was introduced.

2.81.5 Usage Examples

Enter the command as follows to show all DHCP server address bindings:

```
#show ip dhcp server binding
```

2.82 show ip dhcp snooping

Use the **show ip dhcp snooping** command to display information for Internet Protocol version 4 (IPv4) Dynamic Host Control Protocol (DHCP) snooping. Variations of this command include:

```
show ip dhcp snooping
show ip dhcp snooping | begin <line>
show ip dhcp snooping | exclude <line>
show ip dhcp snooping | include <line>
show ip dhcp snooping interface <interface>
show ip dhcp snooping table
```

2.82.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
table	Optional. Displays the IPv4 DHCP snooping table entries.

2.82.2 Default Values

No default values are necessary for this command.

2.82.3 Privilege Level

By default, this command has a privilege level of **0**. The **show ip dhcp snooping table** variation has a privilege level of **15**.

2.82.4 Command History

ASE Release 4.4-41	Command was introduced.

2.82.5 Usage Examples

Enter the command as follows to display information about IPv4 DHCP snooping:

```
#show ip dhcp snooping
```

2.83 show ip http

Use the **show ip http** command to display configuration information for Internet Protocol version 4 (IPv4) Hypertext Transfer Protocol (HTTP). Variations of this command include:

```
show ip http
show ip http | begin <line>
show ip http | exclude <line>
show ip http | include <line>
```

2.83.1 Syntax Description

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

2.83.2 Default Values

No default values are necessary for this command.

2.83.3 Command History

ASE Release 4.4-41	Command was introduced.

2.83.4 Usage Examples

Enter the command as follows to display IPv4 HTTP information:

```
#show ip http
```

2.84 show ip igmp snooping

Use the **show ip igmp snooping** command to display Internet Protocol version 4 (IPv4) Internet Group Management Protocol (IGMP) snooping information. Variations of this command include:

```
show ip igmp snooping
show ip igmp snooping detail
show ip igmp snooping group-database
show ip igmp snooping group-database sfm-information
show ip igmp snooping mrouter
show ip igmp snooping vlan <vlan ids>
```

2.84.1 Syntax Description

detail	Optional. Displays detailed running configuration information and traffic statistics for IPv4 IGMP snooping.
group-database	Optional. Displays entries in the IPv4 IGMP snooping multicast group database.
sfm-information	Optional. Specifies that source filter multicast information for the IPv4 IGMP snooping multicast group database entries is displayed.
mrouter	Optional. Displays IPv4 IGMP multicast router port status.
vlan *<vlan ids>*	Optional. Displays IPv4 IGMP snooping information for a specified virtual local area network (VLAN). You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

2.84.2 Default Values

No default values are necessary for this command.

2.84.3 Privilege Level

By default, this command has a privilege level of **0**.

2.84.4 Command History

ASE Release 4.4-41	Command was introduced.

2.84.5 Usage Examples

Enter the command as follows to display detailed IPv4 IGMP information:

```
#show ip igmp snooping detail
```

2.85 show ip interface

Use the **show ip interface** command to display status and configuration information for Internet Protocol version 4 (IPv4) interfaces. Variations of this command include:

```
show ip interface
show ip interface | begin <line>
show ip interface | exclude <line>
show ip interface | include <line>
show ip interface brief
```

2.85.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
brief	Optional. Displays a brief summary of IPv4 interface information.

2.85.2 Default Values

No default values are necessary for this command.

2.85.3 Privilege Level

By default, this command has a privilege level of **0**.

2.85.4 Command History

ASE Release 4.4-41	Command was introduced.

2.85.5 Usage Examples

The following is sample output from the **show ip interface brief** command:

```
#show ip interface brief

Interface      Address             Method        Status
----------     -------------       --------      --------
VLAN1          192.168.1.1/24      Manual        UP
```

2.86 show ip name-server

Use the **show ip name-server** command to display Internet Protocol version 4 (IPv4) domain name system (DNS) information. Variations of this command include:

```
show ip name-server
show ip name-server | begin <line>
show ip name-server | exclude <line>
show ip name-server | include <line>
```

2.86.1 Syntax Description

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

2.86.2 Default Values

No default values are necessary for this command.

2.86.3 Privilege Level

By default, this command has a privilege level of **0**.

2.86.4 Command History

ASE Release 4.4-41	Command was introduced.

2.86.5 Usage Examples

Enter the command as follows to display IPv4 DNS information:

```
#show ip name-server
```

2.87 show ip route

Use the **show ip route** command to display the current Internet Protocol version 4 (IPv4) routing table. Variations of this command include:

```
show ip route
show ip route | begin <line>
show ip route | exclude <line>
show ip route | include <line>
```

2.87.1 Syntax Description

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

2.87.2 Default Values

No default values are necessary for this command.

2.87.3 Privilege Level

By default, this command has a privilege level of **0**.

2.87.4 Command History

ASE Release 4.4-41	Command was introduced.

2.87.5 Usage Examples

Enter the command as follows to display the IPv4 routing table:

```
#show ip route
```

2.88 show ip ssh

Use the **show ip ssh** command to display Internet Protocol version 4 (IPv4) Secure Shell (SSH) information. Variations of this command include:

```
show ip ssh
show ip ssh | begin <line>
show ip ssh | exclude <line>
show ip ssh | include <line>
```

2.88.1 Syntax Description

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

2.88.2 Default Values

No default values are necessary for this command.

2.88.3 Privilege Level

By default, this command has a privilege level of **15**.

2.88.4 Command History

ASE Release 4.4-41	Command was introduced.

2.88.5 Usage Examples

Enter the command as follows to display IPv4 SSH information:

```
#show ip ssh
```

2.89 show ip source binding

Use the **show ip source binding** command to display Internet Protocol version 4 (IPv4) Dynamic Host Control Protocol (DHCP) source address binding information. Variations of this command include:

```
show ip source binding
show ip source binding interface <interface>
show ip source binding dhcp-snooping
show ip source binding dhcp-snooping interface <interface>
show ip source binding static
show ip source binding static interface <interface>
```

2.89.1 Syntax Description

interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
dhcp-snooping	Optional. Displays IPv4 DHCP source address binding information learned from DHCP snooping.
static	Optional. Displays static IPv4 DHCP source address entries.

2.89.2 Default Values

No default values are necessary for this command.

2.89.3 Privilege Level

By default, this command has a privilege level of **13**.

2.89.4 Command History

ASE Release 4.4-41	Command was introduced.

2.89.5 Usage Examples

Enter the command as follows to display information about IPv4 DHCP source address bindings:

```
#show ip source binding
```

2.90 show ip statistics

Use the **show ip statistics** command to display Internet Protocol version 4 (IPv4) traffic statistics. Variations of this command include:

```
show ip statistics
show ip statistics | begin <line>
show ip statistics | exclude <line>
show ip statistics | include <line>
show ip statistics system
```

2.90.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
system	Optional. Limits output to ASE system traffic statistics.

2.90.2 Default Values

No default values are necessary for this command.

2.90.3 Privilege Level

By default, this command has a privilege level of **0**.

2.90.4 Command History

ASE Release 4.4-41	Command was introduced.

2.90.5 Usage Examples

Enter the command as follows to display IPv4 traffic statistics:

```
#show ip statistics
```

2.91 show ip verify source

Use the **show ip verify source** command to verify the Internet Protocol version 4 (IPv4) source address. Variations of this command include:

```
show ip verify source
show ip verify source interface <interface>
```

2.91.1 Syntax Description

interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.91.2 Default Values

No default values are necessary for this command.

2.91.3 Privilege Level

By default, this command has a privilege level of **0**.

2.91.4 Command History

ASE Release 4.4-41	Command was introduced.

2.91.5 Usage Examples

Enter the command as follows to display IPv4 source address information:

```
#show ip verify source
```

2.92 show ipmc

Use the **show ipmc** command to display Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) multicast configuration (IPMC) information. Variations of this command include:

```
show ipmc
show ipmc profile
show ipmc profile | begin <line>
show ipmc profile | exclude <line>
show ipmc profile | include <line>
show ipmc profile <name>
show ipmc profile detail
show ipmc range
show ipmc range | begin <line>
show ipmc range | exclude <line>
show ipmc range | include <line>
show ipmc range <range>
show ipmc range detail
```

2.92.1 Syntax Description

profile	Optional. Displays IPMC profile configuration.
<name>	Optional. Specifies an IPMC profile. Profile names are a maximum of 16 characters in length.
range	Optional. Displays a range of IPv4 and IPv6 multicast addresses.
<range>	Optional. Specifies a range entry name. Range entries are a maximum of 16 characters in length.
detail	Optional. Displays detailed information for an IPMC profile or range.
| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.

2.92.2 Default Values

No default values are necessary for this command.

2.92.3 Command History

ASE Release 4.4-41	Command was introduced.

2.92.4 Usage Examples

Enter the command as follows to display all IPMC information:

```
#show ipmc
```

2.93 show ipv6 dhcp-client

Use the **show ipv6 dhcp-client** command to display Internet Protocol version 6 (IPv6) Dynamic Host Control Protocol (DHCP) client configurations. Variations of this command include:

```
show ipv6 dhcp-client
show ipv6 dhcp-client | begin <line>
show ipv6 dhcp-client | exclude <line>
show ipv6 dhcp-client | include <line>
show ipv6 dhcp-client interface vlan <vlan ids>
```

2.93.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
vlan *<vlan ids>*	Optional. Limits the output to specific virtual local area networks (VLANs). You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

2.93.2 Default Values

No default values are necessary for this command.

2.93.3 Command History

ASE Release 4.4-41	Command was introduced.

2.93.4 Usage Examples

Enter the command as follows to display IPv6 DHCP client information:

```
#show ipv6 dhcp-client
```

2.94 show ipv6 interface

Use the **show ipv6 interface** command to display configuration information for Internet Protocol version 6 (IPv6) interfaces. Variations of this command include:

```
show ipv6 interface
show ipv6 interface | begin <line>
show ipv6 interface | exclude <line>
show ipv6 interface | include <line>
show ipv6 interface brief
```

2.94.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
brief	Optional. Provides a brief statistical and configuration summary of IPv6 interfaces.

2.94.2 Default Values

No default values are necessary for this command.

2.94.3 Command History

ASE Release 4.4-41	Command was introduced.

2.94.4 Usage Examples

Enter the command as follows to display IPv6 interface configuration information:

```
#show ipv6 interface
```

2.95 show ipv6 mld snooping

Use the **show ipv6 mld snooping** command to display Internet Protocol version 6 (IPv6) Multicast Listener Discovery (MLD) snooping information. Variations of this command include:

```
show ipv6 mld snooping
show ipv6 mld snooping detail
show ipv6 mld snooping group-database
show ipv6 mld snooping group-database sfm-information
show ipv6 mld snooping mrouter
show ipv6 mld snooping vlan <vlan ids>
```

2.95.1 Syntax Description

detail	Optional. Displays detailed MLD snooping statistics and information.
group-database	Optional. Displays MLD group database entries.
sfm-information	Optional. Includes MLD source filter multicast information in command output.
mrouter	Optional. Displays MLD router port status.
vlan *<vlan ids>*	Optional. Displays the MLD information for the specified virtual local area network (VLAN) instance. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

2.95.2 Default Values

No default values are necessary for this command.

2.95.3 Privilege Level

By default, this command has a privilege level of **0**.

2.95.4 Command History

ASE Release 4.4-41	Command was introduced.

2.95.5 Usage Examples

The following is sample output from the **show ipv6 mld snooping detail** command:

```
#show ipv6 mld snooping

MLD Snooping is enabled to start snooping MLD control plane.
Multicast streams destined to unregistered MLD groups will be flooding.
```

2.96 show ipv6 neighbor

Use the **show ipv6 neighbor** command to display Internet Protocol version 6 (IPv6) Neighbor Discovery (ND) cache. This cache contains information about IPv6 nodes that have been added to the cache, including the link-layer IPv6 address and the reachability state of that neighbor. Variations of this command include:

```
show ipv6 neighbor
show ipv6 neighbor | begin <line>
show ipv6 neighbor | exclude <line>
show ipv6 neighbor | include <line>
```

2.96.1 Syntax Description

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

2.96.2 Default Values

No default values are necessary for this command.

2.96.3 Command History

ASE Release 4.4-41	Command was introduced.

2.96.4 Usage Examples

Enter the command as follows to display IPv6 ND information:

```
#show ipv6 neighbor
```

2.97 show ipv6 route

Use the **show ipv6 route** command to display the contents of the Internet Protocol version 6 (IPv6) route table. Variations of this command include:

```
show ipv6 route
show ipv6 route | begin <line>
show ipv6 route | exclude <line>
show ipv6 route | include <line>
```

2.97.1 Syntax Description

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

2.97.2 Default Values

No default values are necessary for this command.

2.97.3 Command History

ASE Release 4.4-41	Command was introduced.

2.97.4 Usage Examples

Enter the command as follows to display IPv6 routing information:

```
#show ipv6 route
```

2.98 show ipv6 statistics

Use the **show ipv6 statistics** command to display Internet Protocol version 6 (IPv6) traffic statistics. Variations of this command include:

```
show ipv6 statistics
show ipv6 statistics | begin <line>
show ipv6 statistics | exclude <line>
show ipv6 statistics | include <line>
show ipv6 statistics interface vlan <vlan ids>
```

2.98.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
vlan *<vlan ids>*	Optional. Displays IPv6 traffic statistics for the specified virtual local area network (VLAN) instance. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

2.98.2 Default Values

No default values are necessary for this command.

2.98.3 Command History

ASE Release 4.4-41	Command was introduced.

2.98.4 Usage Examples

Enter the command as follows to display all IPv6 traffic statistics:

```
#show ipv6 statistics
```

2.99 show lacp

Use the **show lacp** command to display Link Aggregation Control Protocol (LACP) configuration information. Variations of this command include:

```
show lacp

show lacp internal
show lacp internal | begin <line>
show lacp internal | exclude <line>
show lacp internal | include <line>
show lacp internal detail

show lacp neighbor
show lacp neighbor | begin <line>
show lacp neighbor | exclude <line>
show lacp neighbor | include <line>
show lacp neighbor detail

show lacp statistics
show lacp statistics | begin <line>
show lacp statistics | exclude <line>
show lacp statistics | include <line>
show lacp statistics detail

show lacp system-id
show lacp system-id | begin <line>
show lacp system-id | exclude <line>
show lacp system-id | include <line>
show lacp system-id detail
```

2.99.1 Syntax Description

internal	Optional. Displays internal LACP configuration.
neighbor	Optional. Displays neighbor LACP configuration.
statistics	Optional. Displays internal LACP statistics.
system-id	Optional. Displays the LACP system ID.
detail	Optional. Additionally displays the LACP status.
| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.

2.99.2 Default Values

No default values are necessary for this command.

2.99.3 Privilege Level

By default, this command has a privilege level of **15**.

2.99.4 Command History

ASE Release 4.4-41	Command was introduced.

2.99.5 Usage Examples

The following example displays internal LACP configurations:

```
#show lacp internal

Port    Mode    Key    Role    Timeout    Priority
----    -----   -----  -----   -------    ---------
1      Disabled  Auto  Active  Fast       32768
2      Disabled  Auto  Active  Fast       32768
3      Disabled  Auto  Active  Fast       32768
4      Disabled  Auto  Active  Fast       32768
5      Disabled  Auto  Active  Fast       32768
6      Disabled  Auto  Active  Fast       32768
7      Disabled  Auto  Active  Fast       32768
```

2.100 show licenses

Use the **show licenses** command to display feature licensing information. Variations of this command include:

```
show licenses
show licenses | begin <line>
show licenses | exclude <line>
show licenses | include <line>
show licenses component <unit>
show licenses component <unit> description
show licenses component <unit> description mtd <word>
show licenses component <unit> description mtd <word> section <unit>
show licenses component <unit> description section <unit>
show licenses component <unit> mtd <word>
show licenses component <unit> mtd <word> section <unit>
show licenses component <unit> section <unit>
show licenses description
show licenses description mtd <word>
show licenses description mtd <word> section <unit>
show licenses description section <unit>
show licenses mtd <word>
show licenses mtd <word> section <unit>
show licenses section <unit>
```

2.100.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
component *<unit>*	Optional. Displays license information for a specific component based on the component ID.
description	Optional. Displays detailed license information.
mtd *<word>*	Optional. Displays license information for a specific memory technology device (MTD) file based on the file name.
section *<unit>*	Optional. Displays license information for a specific section based on a component ID.

2.100.2 Default Values

No default values are necessary for this command.

2.100.3 Command History

ASE Release 4.4-41	Command was introduced.

2.100.4 Usage Examples

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

```
#show licenses

Image Name    Section ID   Component ID    Component Name    Version    Type   Url
----------    ----------   ------------    --------------    --------   ----   ----
RedBoot       No licenses found
linux         0            0               libstdc++         6.3.0      GPLv3 (with
   exception)    http://ftpmirror.gnu.org/gcc/gcc-6.3.0/gcc-6.3.0.tar.bz2
linux         0            1               uclibc            1.0.22     LGPLv2.1+
   http://downloads.uclibc-ng.org/releases/1.0.22/uClibc-ng-1.0.22.tar.xz
```

2.101 show line

Use the **show line** command to display TeleType (TTY) line information. Variations of this command include:

```
show line
show line | begin <line>
show line | exclude <line>
show line | include <line>
show line alive
```

2.101.1 Syntax Description

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

2.101.2 Default Values

No default values are necessary for this command.

2.101.3 Command History

ASE Release 4.4-41	Command was introduced.

2.101.4 Usage Examples

The following is sample output from the **show line** command that displays live line information:

```
#show line alive

Line is con 0.
--------------
  * You are at this line now.
  Alive from Console.
  Default privileged level is 2.
  Command line editing is enabled.
  Display EXEC banner is enabled.
  Display Day banner is enabled.
  Terminal width is 80.
           length is 24.
           history size is 32.
           exec-timeout is 10 min 0 second.

  Current session privilege is 15.
  Elapsed time is 0 day 2 hour 19 min 54 sec.
  Idle time is 0 day 0 hour 0 min 0 sec.
```

2.102 show link-oam

Use the **show link-oam** command to display link operations, administration, and management (OAM) configuration and information. Variations of this command include:

```
show link-oam
show link-oam | begin <line>
show link-oam | exclude <line>
show link-oam | include <line>
show link-oam interface <interface>
show link-oam link-monitor
show link-oam statistics
show link-oam status
```

2.102.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
link-monitor	Optional. Displays link monitor status information.
statistics	Optional. Displays link statistics.
status	Optional. Displays local and remote node status information.

2.102.2 Default Values

No default values are necessary for this command.

2.102.3 Command History

ASE Release 4.4-41	Command was introduced.

2.102.4 Usage Examples

The following example displays link OAM statistics for the **GigabitEthernet 1/1** interface:

```
#show link-oam

Interface              Control      Mode       Status
------------           ---------    ------    --------
GigabitEthernet 1/1    disabled     passive    non operational
```

2.103 show lldp

Use the **show lldp** command to display the Link Layer Discovery Protocol (LLDP) transmit interval and transmitted time to live (TTL). Variations of this command include:

```
show lldp
show lldp | begin <line>
show lldp | exclude <line>
show lldp | include <line>
show lldp interface <interface>
```

2.103.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.103.2 Default Values

No default values are necessary for this command.

2.103.3 Command History

ASE Release 4.4-41	Command was introduced.

2.103.4 Usage Examples

Enter the command as follows to display all LLDP information:

```
#show lldp
```

2.104 show lldp eee

Use the **show lldp eee** command to display Link Layer Discovery Protocol (LLDP) local and neighbor energy-efficient Ethernet (EEE) information. Variations of this command include:

```
show lldp eee
show lldp eee | begin <line>
show lldp eee | exclude <line>
show lldp eee | include <line>
show lldp eee interface <interface>
```

2.104.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.104.2 Default Values

No default values are necessary for this command.

2.104.3 Command History

ASE Release 4.4-41	Command was introduced.

2.104.4 Usage Examples

The following example displays LLDP EEE information for the interface **GigabitEthernet 1/1**:

```
#show lldp eee interface GigabitEthernet 1/1
No LLDP entries found
```

2.105 show lldp med media-vlan-policy

Use the **show lldp med media-vlan-policy** command to display Link Layer Detection Protocol- Media Endpoint Discovery (LLDP-MED) media policies on the virtual local area network (VLAN). Variations of this command include:

```
show lldp med media-vlan-policy
show lldp med media-vlan-policy | begin <line>
show lldp med media-vlan-policy | exclude <line>
show lldp med media-vlan-policy | include <line>
show lldp med media-vlan-policy <number>
```

2.105.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
<number>	Optional. Specifies a specific policy number. Valid range is **0** to **31**.

2.105.2 Default Values

No default values are necessary for this command.

2.105.3 Privilege Level

By default, this command has a privilege level of **0**.

2.105.4 Command History

ASE Release 4.4-41	Command was introduced.

2.105.5 Usage Examples

Enter the command as follows to display information for media policies on all VLANs that support LLDP-MED:

```
#show lldp med media-vlan-policy
```

2.106 show lldp med remote-device

Use the **show lldp med remote-device** command to display Link Layer Detection Protocol-Media Endpoint Discovery (LLDP-MED) information for remote device neighbors. Variations of this command include:

```
show lldp med remote-device
show lldp med remote-device | begin <line>
show lldp med remote-device | exclude <line>
show lldp med remote-device | include <line>
show lldp med remote-device interface <interface>
```

2.106.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.106.2 Default Values

No default values are necessary for this command.

2.106.3 Command History

ASE Release 4.4-41	Command was introduced.

2.106.4 Usage Examples

Enter the command as follows to display LLDP-MED information for neighbors of remote devices:

```
#show lldp med remote-device
```

2.107 show lldp neighbors

Use the **show lldp neighbors** command to display information about neighbors of this device learned about via Link Layer Discovery Protocol (LLDP). Variations of this command include:

```
show lldp neighbors
show lldp neighbors | begin <line>
show lldp neighbors | exclude <line>
show lldp neighbors | include <line>
show lldp neighbors interface <interface>
```

2.107.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.107.2 Default Values

No default values are necessary for this command.

2.107.3 Privilege Level

By default, this command has a privilege level of **0**.

2.107.4 Command History

ASE Release 4.4-41	Command was introduced.

2.107.5 Usage Examples

Enter the command as follows to display LLDP neighbor information:

```
#show lldp neighbors
```

2.108 show lldp preempt

Use the **show lldp preempt** command to display Link Layer Discovery Protocol (LLDP) preemptive behavior configurations for local and neighboring devices. Variations of this command include:

```
show lldp preempt
show lldp preempt | begin <line>
show lldp preempt | exclude <line>
show lldp preempt | include <line>
show lldp preempt interface <interface>
```

2.108.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.108.2 Default Values

No default values are necessary for this command.

2.108.3 Command History

ASE Release 4.4-41	Command was introduced.

2.108.4 Usage Examples

Enter the command as follows to display all preemptive behaviors for LLDP local and neighboring devices:

```
#show lldp preempt
```

2.109 show lldp statistics

Use the **show lldp statistics** command to display statistics about Link Layer Discovery Protocol (LLDP). Variations of this command include:

```
show lldp statistics
show lldp statistics | begin <line>
show lldp statistics | exclude <line>
show lldp statistics | include <line>
show lldp statistics interface <interface>
```

2.109.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.109.2 Default Values

No default values are necessary for this command.

2.109.3 Privilege Level

By default, this command has a privilege level of **0**.

2.109.4 Command History

ASE Release 4.4-41	Command was introduced.

2.109.5 Usage Examples

Enter the command as follows to display all LLDP statistics:

```
#show lldp statistics
```

2.110 show logging

Use the **show logging** command to display system log messages. Variations of this command include:

```
show logging
show logging | begin <line>
show logging | exclude <line>
show logging | include <line>
show logging <number>
show logging <number> | exclude <line>
show logging <number> | include <line>
show logging <number> switch <switch id>
show logging error
show logging informational
show logging notice
show logging warning
```

2.110.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
<number>	Optional. Specifies a logging ID. Valid range is **1** to **4294967295**.
switch *<switch id>*	Optional. Specifies a switch for which to display logging information.
error	Optional. Displays error conditions (Severity 3).
informational	Optional. Displays informational messages (Severity 6).
notice	Optional. Displays normal but significant conditions (Severity 5).
warning	Optional. Displays warning conditions (Severity 4).

2.110.2 Default Values

No default values are necessary for this command.

2.110.3 Privilege Level

By default, this command has a privilege level of **15**.

2.110.4 Command History

ASE Release 4.4-41	Command was introduced.

2.110.5 Usage Examples

Enter the command as follows to display informational messages:

```
#show logging informational
Switch logging host mode is disabled
Switch logging host address is null
Switch logging level is informational

Number of entries on Switch 1:
Error    :0
Warning  :0
Notice   :55
Informational: 1
All      :56

ID        Level           Time & Message
----      -----           --------------
   1     Informational   1970-01-01T00:00:45+00:00
                         SYS-BOOTING: Switch just made a cold boot.
```

2.111 show loop-protect

Use the **show loop-protect** command to display loop protection configuration information. Variations of this command include:

```
show loop-protect
show loop-protect interface <interface>
```

2.111.1 Syntax Description

interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.111.2 Default Values

No default values are necessary for this command.

2.111.3 Privilege Level

By default, this command has a privilege level of **13**.

2.111.4 Command History

ASE Release 4.4-41	Command was introduced.

2.111.5 Usage Examples

The following example displays loop protection information for interface **GigabitEthernet 1/3**:

```
#show loop-protect interface GigabitEthernet 1/3

Loop Protection Configuration
=============================
Loop Protection   :Disable
Transmission Time : 5 sec
Shutdown Time     : 180 sec

GigabitEthernet 1/3
===================
  Loop protect mode is enabled.
  Action is shutdown.
  Transmit mode is enabled.
  No loop.
  The number of loops is 0.
  Status is down.
```

2.112 show mac address-table

Use the **show mac address-table** command to display media access control (MAC) address table information. Variations of this command include:

```
show mac address-table
show mac address-table | begin <line>
show mac address-table | exclude <line>
show mac address-table | include <line>
show mac address-table interface <interface>
show mac address-table vlan <vlan ids>
```

2.112.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
vlan *<vlan ids>*	Optional. Displays MAC address table information for a specific virtual local area network (VLAN) instance. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

2.112.2 Default Values

No default values are necessary for this command.

2.112.3 Privilege Level

By default, this command has a privilege level of **0**.

2.112.4 Command History

ASE Release 4.4-41	Command was introduced.

2.112.5 Usage Examples

Enter the command as follows to display all MAC address table entries:

```
#show mac address-table
```

2.113 show mac address-table address <*mac address*>

Use the **show mac address-table address** <*mac address*> command to display media access control (MAC) address table entries for specific addresses. Variations of this command include:

show mac address-table address *<mac address>*
show mac address-table *<mac address>* **vlan** *<vlan id>s*

2.113.1 Syntax Description

<mac address>	Specifies a 48-bit MAC address for which to display MAC address table entries. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
vlan *<vlan ids>*	Optional. Displays MAC address table entries for the specified MAC address for a specific virtual local area network (VLAN) instance. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

2.113.2 Default Values

No default values are necessary for this command.

2.113.3 Command History

ASE Release 4.4-41	Command was introduced.

2.113.4 Usage Examples

Enter the command as follows to display MAC address table entires for the MAC address **00:A0:C8:00:00:01**:

```
#show mac address-table address 00:A0:C8:00:00:01
```

2.114 show mac address-table aging-time

Use the **show mac address-table aging-time** command to display information regarding the amount of time dynamic entries remain in the media access control (MAC) address table.

2.114.1 Syntax Description

No subcommands.

2.114.2 Default Values

No default values are necessary for this command.

2.114.3 Command History

ASE Release 4.4-41	Command was introduced.

2.114.4 Usage Examples

Enter the command as follows to display the aging time for MAC address table entries:

```
#show mac address-table aging-time
```

2.115 show mac address-table conf

Use the **show mac address-table conf** command to display user-added static media access control (MAC) address entries in the MAC address table.

2.115.1 Syntax Description

No subcommands.

2.115.2 Default Values

No default values are necessary for this command.

2.115.3 Command History

ASE Release 4.4-41	Command was introduced.

2.115.4 Usage Examples

Enter the command as follows to display all manually entered static MAC address table entries:

```
#show mac address-table conf
```

2.116 show mac address-table count

Use the **show mac address-table count** command to display information regarding the number of media access control (MAC) addresses in use (both static and dynamic). Variations of this command include:

```
show mac address-table count
show mac address-table count interface <interface>
show mac address-table count vlan <vlan ids>
```

2.116.1 Syntax Description

interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
vlan *<vlan ids>*	Optional. Displays MAC address table information for a specific virtual local area network (VLAN) instance. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

2.116.2 Default Values

No default values are necessary for this command.

2.116.3 Command History

ASE Release 4.4-41	Command was introduced.

2.116.4 Usage Examples

The following example displays the number of MAC addresses in use on the **GigabitEthernet 1/4** interface:

```
#show mac address-table count interface GigabitEthernet 1/4

Port Dynamic Addresses
GigabitEthernet 1/4             0

Total learned dynamic addresses for the switch: 0
Total static addresses in table: 1
```

2.117 show mac address-table learning

Use the **show mac address-table learning** command to display the state of media access control (MAC) address table entries. Address states included in command output are the learn, disable, and secure states. Variations of this command include:

```
show mac address-table learning
show mac address-table learning interface <interface>
show mac address-table learning vlan <vlan ids>
```

2.117.1 Syntax Description

interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
vlan *<vlan ids>*	Optional. Displays MAC address state information for a specific virtual local area network (VLAN) instance. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

2.117.2 Default Values

No default values are necessary for this command.

2.117.3 Command History

ASE Release 4.4-41	Command was introduced.

2.117.4 Usage Examples

Enter the command as follows to display the state of all MAC address table entries:

```
#show mac address-table learning
```

2.118 show mac address-table static

Use the **show mac address-table static** command to display information regarding static media access control (MAC) address table entries.

2.118.1 Syntax Description

No subcommands.

2.118.2 Default Values

No default values are necessary for this command.

2.118.3 Command History

ASE Release 4.4-41	Command was introduced.

2.118.4 Usage Examples

Enter the command as follows to display information about static MAC address table entries:

```
#show mac address-table static
```

2.119 show mep

Use the show mep command to display information regarding maintenance entity points (MEPs). Variations of this command include:

```
show mep
show mep | begin <line>
show mep | exclude <line>
show mep | include <line>
show mep detail
show mep lm-hli detail
show mep <range>
show mep <range> detail
show mep <range> lm-hli detail

show mep ais
show mep ais detail
show mep ais lm-hli
shoe mep ais lm-hli detail
show mep <range> ais
show mep <range> ais detail
show mep <range> ais lm-hli
show mep <range> ais lm-hli detail

show mep aps
show mep aps detail
show mep aps lm-hli
show mep aps lm-hli detail
show mep <range> aps
show mep <range> aps detail
show mep <range> aps lm-hli
show mep <range> aps lm-hli detail


show mep bfd
show mep bfd detail
show mep bfd lm-hli
show mep bfd lm-hli detail
show mep <range> bfd
show mep <range> bfd detail
show mep <range> bfd lm-hli
show mep <range> bfd lm-hli detail

show mep cc
show mep cc detail
show mep cc lm-hli
show mep cc lm-hli detail
show mep <range> cc
show mep <range> cc detail
show mep <range> cc lm-hli
show mep <range> cc lm-hli detail

show mep client
show mep client detail
show mep client lm-hli
show mep client lm-hli detail
show mep <range> client
show mep <range> client detail
show mep <range> client lm-hli
```

```
show mep <range> client lm-hli detail

show mep dm
show mep dm detail
show mep dm lm-hli
show mep dm lm-hli detail
show mep <range> dm
show mep <range> dm detail
show mep <range> dm lm-hli
show mep <range> dm lm-hli detail

show mep lb
show mep lb detail
show mep lb lm-hli
show mep lb lm-hli detail
show mep <range> lb
show mep <range> lb detail
show mep <range> lb lm-hli
show mep <range> lb lm-hli detail

show mep lck
show mep lck detail
show mep lck lm-hli
show mep lck lm-hli detail
show mep <range> lck
show mep <range> lck detail
show mep <range> lck lm-hli
show mep <range> lck lm-hli detail

show mep lm
show mep lm detail
show mep lm lm-hli
show mep lm lm-hli detail
show mep <range> lm
show mep <range> lm detail
show mep <range> lm lm-hli
show mep <range> lm lm-hli detail

show mep lm-avail
show mep lm-avail detail
show mep lm-avail lm-hli
show mep lm-avail lm-hli detail
show mep <range> lm-avail
show mep <range> lm-avail detail
show mep <range> lm-avail lm-hli
show mep <range> lm-avail lm-hli detail

show mep lm-hli
show mep lm-hli detail
show mep <range> lm-hli
show mep <range> lm-hli detail

show mep lst
show mep lst detail
show mep lst lm-hli
show mep lst lm-hli detail
show mep <range> lst
show mep <range> lst detail
show mep <range> lst lm-hli
```

```
show mep <range> lst lm-hli detail

show mep lt
show mep lt detail
show mep lt lm-hli
show mep lt lm-hli detail
show mep <range> lt
show mep <range> lt detail
show mep <range> lt lm-hli
show mep <range> lt lm-hli detail

show mep peer
show mep peer detail
show mep peer lm-hli
show mep peer lm-hli detail
show mep <range> peer
show mep <range> peer detail
show mep <range> peer lm-hli
show mep <range> peer lm-hli detail

show mep pm
show mep pm detail
show mep pm lm-hli
show mep pm lm-hli detail
show mep <range> pm
show mep <range> pm detail
show mep <range> pm lm-hli
show mep <range> pm lm-hli detail

show mep rt
show mep rt detail
show mep rt lm-hli
show mep rt lm-hli detail
show mep <range> rt
show mep <range> rt detail
show mep <range> rt lm-hli
show mep <range> rt lm-hli detail

show mep syslog
show mep syslog detail
show mep syslog lm-hli
show mep syslog lm-hli detail
show mep <range> syslog
show mep <range> syslog detail
show mep <range> syslog lm-hli
show mep <range> syslog lm-hli detail

show mep tlv
show mep tlv detail
show mep tlv lm-hli
show mep tlv lm-hli detail
show mep <range> tlv
show mep <range> tlv detail
show mep <range> tlv lm-hli
show mep <range> tlv lm-hli detail

show mep tst
show mep tst detail
show mep tst lm-hli
```

```
show mep tst lm-hli detail
show mep <range> tst
show mep <range> tst detail
show mep <range> tst lm-hli
show mep <range> tst lm-hli detail
```

2.119.1 Syntax Description

| begin *<Line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<Line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<Line>*	Optional. Produces output that only displays lines with the specified text.
<range>	Optional. Specifies a range of MEP instances for which to display information.
detail	Optional. Displays detailed MEP state and configuration information.
lm-hli	Optional. Displays MEP loss measurement (LM) high loss interval (HLI) information.
ais	Optional. Displays MEP alarm indication signal (AIS) information.
aps	Optional. Displays MEP automatic protection switching (APS) information.
cc	Optional. Displays MEP continuity check (CC) information.
client	Optional. Displays MEP client information.
dm	Optional. Displays MEP delay measurement (DM) information.
lb	Optional. Displays MEP load balancing (LB) information.
lck	Optional. Displays MEP locked signal function (LCK) information.
lm	Optional. Displays MEP LM information.
lm-avail	Optional. Displays MEP LM availability status.
lst	Optional. Displays MEP link state tracking (LST) information.
lt	Optional. Displays MEP LT information.
peer	Optional. Displays peer MEP information.
pm	Optional. Displays MEP performance monitoring (PM) information.
syslog	Optional. Displays MEP syslog information.
tlv	Optional. Displays MEP TLY information.
tst	Optional. Displays MEP test (TST) information.

2.119.2 Default Values

No default values are necessary for this command.

2.119.3 Command History

ASE Release 4.4-41	Command was introduced.

2.119.4 Usage Examples

The following example of this command displays detailed **LM-HLI** information for MEP **3**:

```
#show mep 3 ais detail lm-hli
MEP LM High Loss Interval state is:
  Inst   Peer   Near Count    Far Count    Near/Far Consec. Count

MEP LM High Loss Interface Configuration is:
  Inst   Interval    FLR Threshold

MEP AIS Configuration is:
  Inst    Rate    Protection
```

2.120 show monitor

Use the **show monitor** command to display the state of different system events. Variations of this command include:

```
show monitor
show monitor session <number>
show monitor session all
show monitor session remote
```

2.120.1 Syntax Description

session *<number>*	Optional. Displays information for a specific MIRROR session. Valid session range is **1** to **5**.
all	Optional. Displays information for all MIRROR sessions.
remote	Optional. Displays information for remote MIRROR sessions only.

2.120.2 Default Values

No default values are necessary for this command.

2.120.3 Command History

ASE Release 4.4-41	Command was introduced.

2.120.4 Usage Examples

The following example displays information for remote MIRROR sessions:

```
#show monitor remote
Session 1
---------
Mode                : Disabled
Type                : Mirror
Source VLAN(s)      :
CPU Port            :

Session 2
---------
Mode                : Disabled
Type                : Mirror
Source VLAN(s)      :
CPU Port            :
```

2.121 show mrp status

Use the **show mrp status** command to display Media Redundancy Protocol (MRP) information. Variations of this command include:

```
show mrp status
show mrp status interface <interface>
show mrp status all
show mrp status all interface <interface>
show mrp status mvrp
show mrp status mvrp interface <interface>
```

2.121.1 Syntax Description

interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
all	Optional. Displays MRP statistics for all MRP applications.
mvrp	Optional. Displays MRP statistics for the Multiple virtual local area network (VLAN) Registration Protocol (MVRP) application.

2.121.2 Default Values

No default values are necessary for this command.

2.121.3 Command History

ASE Release 4.4-41	Command was introduced.

2.121.4 Usage Examples

The following example displays MRP status information for the interface **GigabitEthernet 1/1-2**:

```
#show mrp status interface GigabitEthernet 1/1-2

GigabitEthernet 1/1:
--------------------
MRP Appl     FailedRegistrations       LastPduOrigin
-------      -------------------       -------------
MVRP         0                         00-00-00-00-00-00

GigabitEthernet 1/2:
--------------------
MRP Appl     FailedRegistrations       LastPduOrigin
-------      -------------------       -------------
MVRP         0                         00-00-00-00-00-00
```

2.122 show mvr

Use the **show mvr** command to display multicast virtual local area network (VLAN) registration (MVR) configuration information. Variations of this command include:

```
show mvr
show mvr | begin <line>
show mvr | exclude <line>
show mvr | include <line>
show mvr detail
show mvr group-database
show mvr group-database interface <interface>
show mvr name <name>
show mvr sfm-information
show mvr vlan <vlan ids>
```

2.122.1 Syntax Description

| begin *<Line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<Line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<Line>*	Optional. Produces output that only displays lines with the specified text.
detail	Optional. Displays detailed information and statistics of the MVR group database.
group-database	Optional. Displays information about the MVR multicast group database.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
name *<name>*	Optional. Displays information for a specific MVR VLAN instance. MVR VLAN names are a maximum of **16** characters in length.
sfm-information	Optional. Includes MVR source filter multicast information in the output.
vlan *<vlan ids>*	Optional. Displays MVR information for the specified VLAN instance. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

2.122.2 Default Values

No default values are necessary for this command.

2.122.3 Privilege Level

By default, this command has a privilege level of **0**.

2.122.4 Command History

ASE Release 4.4-41	Command was introduced.

2.122.5 Usage Examples

The following example displays MVR information for VLAN **11**:

```
#show mvr vlan 11
MVR is currently disabled, please enable MVR to start group registration.
%Invalid MVR IGMP VLAN 11.
```

2.123 show ntp status

Use the **show ntp status** command to display Network Time Protocol (NTP) status information.

2.123.1 Syntax Description

No subcommands.

2.123.2 Default Values

No default values are necessary for this command.

2.123.3 Privilege Level

By default, this command has a privilege level of **13**.

2.123.4 Command History

ASE Release 4.4-41	Command was introduced.

2.123.5 Usage Examples

The following is sample output from the **show ntp status** command:

```
#show ntp status
NTP Mode : disabled
Idx    Server IP host address (a.b.c.d) or a host name string
---    ------------------------------------------------------
1
2
3
4
5
```

2.124 show platform

Use the **show platform** command to display platform configuration information. Variations of this command include:

```
show platform debug
show platform phy
show platform phy | begin <line>
show platform phy | exclude <line>
show platform phy | include <line>
show platform phy interface <interface>
show platform phy failover
show platform phy id
show platform phy id interface <interface>
show platform phy instance
```

2.124.1 Syntax Description

debug	Displays whether platform debug messaging is enabled or disabled.
phy	Displays PHY platform information.
| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
failover	Optional. Displays PHY failover information.
id	Optional. Displays PHY information on an ID-basis.
instance	Optional. Displays PHY instance information.

2.124.2 Default Values

No default values are necessary for this command.

2.124.3 Privilege Level

By default, this command has a privilege level of **15**.

2.124.4 Command History

ASE Release 4.4-41	Command was introduced.

2.124.5 Usage Examples

The following example displays PHY information for interface **GigabitEthernet 1/1**:

```
#show platform phy interface GigabitEthernet 1/1
Port    API Inst     WAN/LAN/1G     Mode     Duplex    Speed     Link
----    --------     ----------     ----     ------    -----     ----
1       Default      1G             ANEG     FDX       1G        No
```

2.125 show poe

Use the **show poe** command to display Power over Ethernet (PoE) information. Variations of this command include:

```
show poe
show poe | begin <line>
show poe | exclude <line>
show poe | include <line>
show poe interface <interface>
show poe auto-check
show poe auto-check interface <interface>
show poe config
show poe config interface <interface>
show poe power-delay
show poe power-delay interface <interface>
show poe profile
show poe profile id <number>
```

2.125.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
auto-check	Optional. Displays PoE auto-check information.
config	Optional. Displays PoE configuration information.
power-delay	Optional. Displays PoE power delay configuration information.
profile	Optional. Displays the PoE scheduling profile.
id *<number>*	Optional. Specifies a PoE scheduling profile ID. ID range is **1** to **16**.

2.125.2 Default Values

No default values are necessary for this command.

2.125.3 Privilege Level

By default, this command has a privilege level of **0**.

2.125.4 Command History

ASE Release 4.4-41	Command was introduced.

2.125.5 Usage Examples

The following example displays PoE auto-check information for interface GigabitEthernet 1/1-2:

```
#show poe auto-check interface GigabitEthernet 1/1-2

Ping Check   : Disabled

Port  Ping IP Address  Start up  Interval  Retry    Failure         Failure  Reboot
                        Time      Time      Time       Log           Action   Time
-------------------------------------------------------------------------------------
1     0.0.0.0          60        30         1     error=0, total=0  Nothing    15
2     0.0.0.0          60        30         1     error=0, total=0  Nothing    15
```

2.126 show port-security

Use the **show port-security** command to display port security configuration and status information. Variations of this command include:

```
show port-security
show port-security | begin <line>
show port-security | exclude <line>
show port-security | include <line>
show port-security interface <interface>
show port-security address
show port-security address interface <interface>
show port-security switch
show port-security switch interface <interface>
```

2.126.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
address	Optional. Displays media access control (MAC) addresses learned by the port security feature.
switch	Optional. Displays port security information for the switch.

2.126.2 Default Values

No default values are necessary for this command.

2.126.3 Privilege Level

By default, this command has a privilege level of **0**.

2.126.4 Command History

ASE Release 4.4-41	Command was introduced.

2.126.5 Usage Examples

The following example displays port security information for the **GigabitEthernet 1/1** interface:

```
#show port-security interface GigabitEthernet 1/1

Users:
 P = Port Security (Admin)
 S = 802.1X
 V = Voice VLAN

Interface    Users    Limit   Current   Violating   Violation Mode    State
---------    -----    -----   ------    --------   ---------------    -----
Gi 1/4       ---      N/A     0         N/A        Disabled           No users

Aging disabled
Hold time: 300 seconds
```

2.127 show privilege

Use the **show privilege** command to display command privilege information. Variations of this command include:

```
show privilege
show privilege | begin <line>
show privilege | exclude <line>
show privilege | include <line>
```

2.127.1 Syntax Description

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

2.127.2 Default Values

No default values are necessary for this command.

2.127.3 Command History

ASE Release 4.4-41	Command was introduced.

2.127.4 Usage Examples

Enter the command as follows to display command privilege information:

```
#show privilege
```

2.128 show process

Use the **show process** command to display information about ongoing processes in the ASE device. Variations of this command include:

```
show process list
show process list | begin <line>
show process list | exclude <line>
show process list | include <line>
show process list detail
show process load
```

2.128.1 Syntax Description

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

2.128.2 Default Values

No default values are necessary for this command.

2.128.3 Command History

ASE Release 4.4-41	Command was introduced.

2.128.4 Usage Examples

The following example displays the process load on the ASE device:

```
#show process load
1.65 1.62 1.63 1/169 183
```

2.129 show ptp

Use the **show ptp** command to display Precision Time Protocol (PTP) information. Variations of this command include:

```
show ptp
show ptp | begin <line>
show ptp | exclude <line>
show ptp | include <line>
show ptp cal
show ptp ext
show ptp servo
show ptp servo mode-ref
show ptp servo source
show ptp system-time
```

2.129.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
cal	Optional. Displays the PTP calibration.
ext	Optional. Displays the one pulse-per-second (1PPS) and external clock configuration and the voltage controlled crystal oscillator (VCXO) frequency rate adjustment.
servo	Optional. Displays PTP servo information.
mode-ref	Optional. Displays the PTP servo reference mode.
source	Optional. Displays the PTP servo source information.
system-time	Optional. Displays the PTP system time synchronization mode.

2.129.2 Default Values

No default values are necessary for this command.

2.129.3 Command History

ASE Release 4.4-41	Command was introduced.

2.129.4 Usage Examples

The following example displays the external clock speed and configuration, as well as VCXO frequency rate adjustment for the switch:

```
#show ptp etx
PTP External One PPS mode: Diable, Clock output enabled: False, frequency : 1,
    Preferred adj method: Auto
```

2.130 show ptp <*number*>

Use the **show ptp** <*number*> command to display Precision Time Protocol (PTP) information for a specific clock configuration. Variations of this command include:

```
show ptp <number> clk
show ptp <number> current
show ptp <number> default
show ptp <number> filter
show ptp <number> filter-type
show ptp <number> foreign-master-record
show ptp <number> foreign-master-record interface <interface>
show ptp <number> ho
show ptp <number> local-clock
show ptp <number> log-mode
show ptp <number> master-table-unicast
show ptp <number> parent
show ptp <number> port-ds
show ptp <number> port-ds interface <interface>
show ptp <number> port-state
show ptp <number> port-state interface <interface>
show ptp <number> port-statistics
show ptp <number> port-statistics interface <interface>
show ptp <number> servo
show ptp <number> slave
show ptp <number> slave-cfg
show ptp <number> slave-table-unicast
show ptp <number> time-property
show ptp <number> uni
show ptp <number> virtual-port
show ptp <number> wireless
show ptp <number> wireless interface <interface>
```

2.130.1 Syntax Description

<number>	Specifies the PTP master clock instance for which to display information. Valid range is **0** to **3**.
clk	Displays PTP slave clock information.
current	Displays current PTP configuration information.
default	Displays the default PTP configuration.
filter	Displays PTP filter settings information.
filter-type	Displays PTP filter type information.
foreign-master-record	Displays PTP port foreign master information.
ho	Displays the PTP slave clock holdover configuration.
local-clock	Displays the local clock current time.
log-mode	Displays PTP log information.
master-table-unicast	Displays a list of slave clocks currently connected to PTP master clocks through unicast negotiation.
parent	Displays PTP parent data information.
port-ds	Displays PTP port data information.
port-state	Displays PTP port state information.

port-statistics	Displays PTP port statistics.
servo	Displays PTP servo configuration information.
slave	Displays the lock threshold for PTP slave clocks.
slave-cfg	Displays the lock configuration of PTP slave clocks.
slave-table-unicast	Displays the unicast table of slave clocks connected to the specific master clock instance through unicast negotiations.
time-property	Displays the configured PTP time properties.
uni	Displays configuration information for slave clocks connected to the master through unicast negotiations.
virtual-ports	Displays the configuration of a PTP clock virtual port.
wireless	Displays the PTP wireless configuration.
interface *<interface>*	Optional. Specifies that information associated a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.130.2 Default Values

No default values are necessary for this command.

2.130.3 Command History

ASE Release 4.4-41	Command was introduced.

2.130.4 Usage Examples

Enter the command as follows to display current PTP configuration information for the PTP clock **2**:

```
#show ptp 2 current
```

2.131 show ptp ms-pvd

Use the **show ptp ms-pvd** command to display Precision Time Protocol (PTP) packet delay variation configuration for master-to-slave (MS-PVD) clock transmissions. Variations of this command include:

```
show ptp ms-pvd all-apr-statistics
show ptp ms-pvd all-apr-statistics cgu <number>
show ptp ms-pvd apr
show ptp ms-pvd apr cgu <number>
show ptp ms-pvd cgu <number>
show ptp ms-pvd cgu <number> server <number> status <number>
show ptp ms-pvd cur-path-delays
show ptp ms-pvd cur-path-delays cgu <number>
show ptp ms-pvd path-statistics
show ptp ms-pvd path-statistics cgu <number>
show ptp ms-pvd psl-fcl-config
show ptp ms-pvd psl-fcl-config cgu <number>
```

2.131.1 Syntax Description

all-apr-statistics	Displays all PTP MS-PVD APR statistics.
apr	Displays PTP MS-PVD APR information.
cgu *<number>*	Displays PTP MS-PVD information an a per-CGU basis. Valid range is **0** to **3**.
cur-path-delays	Displays PTP MS-PVD current path delays.
path-statistics	Displays PTP MS-PVD path statistics.
psl-fcl-config	Displays the PTP MS-PVD PSL-FCL configuration information.

2.131.2 Default Values

No default values are necessary for this command.

2.131.3 Command History

ASE Release 4.4-41	Command was introduced.

2.131.4 Usage Examples

Enter the command as follows to display PTP MS-PVD APR information:

```
#show ptp ms-pvd
```

2.132 show pvlan

Use the **show pvlan** command to display private virtual local area network (PVLAN) configuration information. Variations of this command include:

```
show pvlan
show pvlan <vlan ids>
show pvlan isolation
show pvlan isolation interface <interface>
```

2.132.1 Syntax Description

<vlan ids>	Optional. Limits output to the specified VLAN IDs. VLANs can be specified by single ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid *<vlan ids>* range is **1** to **4095**.
isolation	Optional. Displays the PVLAN isolation configuration.
interface *<interface>*	Optional. Specifies that information associated a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.132.2 Default Values

No default values are necessary for this command.

2.132.3 Privilege Level

By default, this command has a privilege level of **13**.

2.132.4 Command History

ASE Release 4.4-41	Command was introduced.

2.132.5 Usage Examples

The following is sample output from the **show pvlan isolation** command:

```
#show pvlan isolation
Port                  Isolation
----------------      ------------------
GigabitEthernet 1/1   Disabled
GigabitEthernet 1/2   Disabled
GigabitEthernet 1/3   Disabled
GigabitEthernet 1/4   Disabled
```

2.133 show qos

Use the **show qos** command to display Quality of Service (QoS) configuration information. Variations of this command include:

```
show qos
show qos | begin <line>
show qos | exclude <line>
show qos | include <line>
show qos interface <interface>
```

2.133.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
interface *<interface>*	Optional. Specifies that information associated a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.133.2 Default Values

No default values are necessary for this command.

2.133.3 Privilege Level

By default, this command has a privilege level of **15**.

2.133.4 Command History

ASE Release 4.4-41	Command was introduced.

2.133.5 Usage Examples

The following is sample output from the **show qos interface** command:

```
#show qos interface GigabitEthernet 1/1
interface GigabitEthernet 1/1
 qos cos 0
 qos pcp 0
 qos dpl 0
 qos dei 0
 qos class 0
 qos trust tag disabled
 qos map tag-cos pcp 0 dei 0 cos 1 dpl 0
 qos map tag-cos pcp 0 dei 1 cos 1 dpl 1
 qos map tag-cos pcp 1 dei 0 cos 0 dpl 0
 qos map tag-cos pcp 1 dei 1 cos 0 dpl 1
 qos map tag-cos pcp 2 dei 0 cos 2 dpl 0
```

```
qos map tag-cos pcp 2 dei 1 cos 2 dpl 1
qos map tag-cos pcp 3 dei 0 cos 3 dpl 0
qos map tag-cos pcp 3 dei 1 cos 3 dpl 1
qos map tag-cos pcp 4 dei 0 cos 4 dpl 0
qos map tag-cos pcp 4 dei 1 cos 4 dpl 1
qos map tag-cos pcp 5 dei 0 cos 5 dpl 0
qos map tag-cos pcp 5 dei 1 cos 5 dpl 1
qos map tag-cos pcp 6 dei 0 cos 6 dpl 0
qos map tag-cos pcp 6 dei 1 cos 6 dpl 1
qos map tag-cos pcp 7 dei 0 cos 7 dpl 0
qos map tag-cos pcp 7 dei 1 cos 7 dpl 1
qos trust dscp disabled
qos policer mode: disabled, rate: 500 kbps
qos queue-policer queue 0 mode: disabled, rate: 500 kbps
qos queue-policer queue 1 mode: disabled, rate: 500 kbps
qos queue-policer queue 2 mode: disabled, rate: 500 kbps
qos queue-policer queue 3 mode: disabled, rate: 500 kbps
qos queue-policer queue 4 mode: disabled, rate: 500 kbps
qos queue-policer queue 5 mode: disabled, rate: 500 kbps
qos queue-policer queue 6 mode: disabled, rate: 500 kbps
qos queue-policer queue 7 mode: disabled, rate: 500 kbps
qos port shaper: enabled, rate: 500 kbps, mode: line-rate
qos queue-shaper queue 0: disabled, rate: 500 kbps, mode: line-rate
qos queue-shaper queue 1: disabled, rate: 500 kbps, mode: line-rate
qos queue-shaper queue 2: disabled, rate: 500 kbps, mode: line-rate
qos queue-shaper queue 3: disabled, rate: 500 kbps, mode: line-rate
qos queue-shaper queue 4: disabled, rate: 500 kbps, mode: line-rate
qos queue-shaper queue 5: disabled, rate: 500 kbps, mode: line-rate
qos queue-shaper queue 6: disabled, rate: 500 kbps, mode: line-rate
qos queue-shaper queue 7: disabled, rate: 500 kbps, mode: line-rate
qos wrr mode: disabled
qos tag-remark classified
qos map cos-tag cos 0 dpl 0 pcp 1 dei 0
qos map cos-tag cos 0 dpl 1 pcp 1 dei 1
qos map cos-tag cos 1 dpl 0 pcp 0 dei 0
qos map cos-tag cos 1 dpl 1 pcp 0 dei 1
qos map cos-tag cos 2 dpl 0 pcp 2 dei 0
qos map cos-tag cos 2 dpl 1 pcp 2 dei 1
qos map cos-tag cos 3 dpl 0 pcp 3 dei 0
qos map cos-tag cos 3 dpl 1 pcp 3 dei 1
qos map cos-tag cos 4 dpl 0 pcp 4 dei 0
qos map cos-tag cos 4 dpl 1 pcp 4 dei 1
qos map cos-tag cos 5 dpl 0 pcp 5 dei 0
qos map cos-tag cos 5 dpl 1 pcp 5 dei 1
qos map cos-tag cos 6 dpl 0 pcp 6 dei 0
qos map cos-tag cos 6 dpl 1 pcp 6 dei 1
qos map cos-tag cos 7 dpl 0 pcp 7 dei 0
qos map cos-tag cos 7 dpl 1 pcp 7 dei 1
qos dscp-translate disabled
qos dscp-classify disabled
qos dscp-remark disabled
qos wred-group 1
qos ingress-map disabled
qos egress-map disabled
```

2.134 show qos maps

Use the **show qos maps** command to display Quality of Service (QoS) map configurations. Variations of this command include:

```
show qos maps cos-dscp
show qos maps dscp-classify
show qos maps dscp-cos
show qos maps dscp-egress-translation
show qos maps dscp-ingress-translation
show qos maps egress
show qos maps ingress
```

2.134.1 Syntax Description

cos-dscp	Displays configured Class of Service (CoS)-to-Differentiated Service Code Points (DSCP) maps.
dscp-classify	Displays configured DSCP classification maps for ingress traffic.
dscp-cos	Displays configured DSCP-to-CoS maps.
dscp-egress-translation	Displays configured DSCP translation maps for egress traffic.
dscp-ingress-translation	Displays configured DSCP translation maps for egress traffic.
egress	Displays configured QoS egress maps.
ingress	Displays configured QoS ingress maps.

2.134.2 Default Values

No default values are necessary for this command.

2.134.3 Privilege Level

By default, this command has a privilege level of **15**.

2.134.4 Command History

ASE Release 4.4-41	Command was introduced.

2.134.5 Usage Examples

The following is sample output from the **show qos maps ingress** command:

```
#show qos maps ingress
ingress map: 12, key: pcp, action:
ingress map: 20, key: pcp, action:
ingress map: 99, key: pcp, action:
ingress map: 100, key: pcp, action: cos class
```

2.135 show qos qce

Use the **show qos qce** command to display all configured Quality of Service (QoS) control list entries (QCEs). Variations of this command include:

```
show qos qce
show qos qce <qce id>
```

2.135.1 Syntax Description

<qce id>	Limits output to a single QCE. Valid range is **1** to **256**.

2.135.2 Default Values

No default values are necessary for this command.

2.135.3 Privilege Level

By default, this command has a privilege level of **15**.

2.135.4 Command History

ASE Release 4.4-41	Command was introduced.

2.135.5 Usage Examples

The following is sample output from the **show qos qce** command:

```
#show qos qce
% QOS: no qce entries found!
```

2.136 show qos storm

Use the **show qos storm** command to display configured Quality of Service (QoS) storm policers.

2.136.1 Syntax Description

No subcommands.

2.136.2 Default Values

No default values are necessary for this command.

2.136.3 Privilege Level

By default, this command has a privilege level of **15**.

2.136.4 Command History

ASE Release 4.4-41	Command was introduced.

2.136.5 Usage Examples

The following is sample output from the **show qos storm** command:

```
#show qos storm
qos storm:
==========
Unicast  : disabled       10 fps
Multicast: disabled       10 fps
Broadcast: disabled       10 fps
Storm detected: FALSE
```

2.137 show qos wred

Use the **show qos wred** command to display all Quality of Service (QoS) Weighted Random Early Detection (WRED) configurations and statistics.

2.137.1 Syntax Description

No subcommands.

2.137.2 Default Values

No default values are necessary for this command.

2.137.3 Privilege Level

By default, this command has a privilege level of **15**.

2.137.4 Command History

ASE Release 4.4-41	Command was introduced.

2.137.5 Usage Examples

The following is sample output from the **show qos wred** command:

```
#show qos wred
qos wred:
=========
Group  Queue  Dpl  Mode      Min Fl  Max Dp or Fl
-----  -----  ---  --------  ------  ----------------------
    1      0    1  disabled    0 %    50 % Drop Probability
    1      0    2  disabled    0 %    50 % Drop Probability
    1      0    3  disabled    0 %    50 % Drop Probability
    1      1    1  disabled    0 %    50 % Drop Probability
    1      1    2  disabled    0 %    50 % Drop Probability
    1      1    3  disabled    0 %    50 % Drop Probability
    1      2    1  disabled    0 %    50 % Drop Probability
    1      2    2  disabled    0 %    50 % Drop Probability
    1      2    3  disabled    0 %    50 % Drop Probability
    1      3    1  disabled    0 %    50 % Drop Probability
    1      3    2  disabled    0 %    50 % Drop Probability
    1      3    3  disabled    0 %    50 % Drop Probability
    1      4    1  disabled    0 %    50 % Drop Probability
    1      4    2  disabled    0 %    50 % Drop Probability
    1      4    3  disabled    0 %    50 % Drop Probability
    1      5    1  disabled    0 %    50 % Drop Probability
    1      5    2  disabled    0 %    50 % Drop Probability
    1      5    3  disabled    0 %    50 % Drop Probability
    1      6    1  disabled    0 %    50 % Drop Probability
    1      6    2  disabled    0 %    50 % Drop Probability
    1      6    3  disabled    0 %    50 % Drop Probability
    1      7    1  disabled    0 %    50 % Drop Probability
    1      7    2  disabled    0 %    50 % Drop Probability
    1      7    3  disabled    0 %    50 % Drop Probability
    2      0    1  disabled    0 %    50 % Drop Probability
    2      0    2  disabled    0 %    50 % Drop Probability
    ---MORE---
```

2.138 show radius-server

Use the **show radius-server** command to display Remote Authentication Dial-In User Service (RADIUS) server configuration and statistics. Variations of this command include:

```
show radius-server
show radius-server | begin <line>
show radius-server | exclude <line>
show radius-server | include <line>
show radius-server statistics
```

2.138.1 Syntax Description

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

2.138.2 Default Values

No default values are necessary for this command.

2.138.3 Privilege Level

By default, this command has a privilege level of **15**.

2.138.4 Command History

ASE Release 4.4-41	Command was introduced.

2.138.5 Usage Examples

The following is sample output from the **show radius-server statistics** command:

```
#show radius-server statistics
Global RADIUS Server Timeout       : 5 seconds
Global RADIUS Server Retransmit    : 3 times
Global RADIUS Server Deadtime      : 0 minutes
Global RADIUS server Key           :
Global RADIUS Server Attribute 4   :
Global RADIUS Server Attribute 95  :
Global RADIUS Server Attribute 32  :
No servers configured!
```

2.139 show rmon

Use the **show rmon** command to display remote monitoring (RMON) statistics and event information. Variations of this command include:

```
show rmon alarm
show rmon alarm <list id>
show rmon event
show rmon event <list id>
show rmon history
show rmon history <list id>
show rmon statistics
show rmon statistics <list id>
```

2.139.1 Syntax Description

alarm	Specifies that the RMON alarm table is displayed.
event	Specifies that the RMON event table is displayed.
history	Specifies that the RMON history table is displayed.
statistics	Specifies that the RMON statistics table is displayed.
<list id>	Optional. Limits output to single alarm, even, history, or statistics list. Valid range is **1** to **65535**.

2.139.2 Default Values

No default values are necessary for this command.

2.139.3 Privilege Level

By default, this command has a privilege level of **15**.

2.139.4 Command History

ASE Release 4.4-41	Command was introduced.

2.139.5 Usage Examples

Enter the command as follows to display all RMON alarms:

```
#show rmon alarm
```

2.140 show running-config

Use the **show running-config** command to display all the nondefault parameters contained in the current running configuration file. Specific portions of the running configuration may be displayed, based on the command entered. Variations of this command include:

```
show running-config
show running-config | begin <line>
show running-config | exclude <line>
show running-config | include <line>
show running-config all-defaults
show running-config feature access
show running-config feature access all-defaults
show running-config feature access-list
show running-config feature access-list all-defaults
show running-config feature aggregation
show running-config feature aggregation all-defaults
show running-config feature alarm
show running-config feature alarm all-defaults
show running-config feature arp-inspection
show running-config feature arp-inspection all-defaults
show running-config feature auth
show running-config feature auth all-defaults
show running-config feature auto-link
show running-config feature auto-link all-defaults
show running-config feature clock
show running-config feature clock all-defaults
show running-config feature ddmi
show running-config feature ddmi all-defaults
show running-config feature dhcp
show running-config feature dhcp all-defaults
show running-config feature dhcp-snooping
show running-config feature dhcp-snooping all-defaults
show running-config feature dhcp_server
show running-config feature dhcp_server all-defaults
show running-config feature dhcp6_client_interface
show running-config feature dhcp6_client_interface all-defaults
show running-config feature dns
show running-config feature dns all-defaults
show running-config feature dot1x
show running-config feature dot1x all-defaults
show running-config feature eps
show running-config feature eps all-defaults
show running-config feature erps
show running-config feature erps all-defaults
show running-config feature green-ethernet
show running-config feature green-ethernet all-defaults
show running-config feature GVRP
show running-config feature GVRP all-defaults
show running-config feature http
show running-config feature http all-defaults
show running-config feature icli
show running-config feature icli all-defaults
show running-config feature ip-igmp-snooping
show running-config feature ip-igmp-snooping all-defaults
show running-config feature ip-igmp-snooping-port
show running-config feature ip-igmp-snooping-port all-defaults
show running-config feature ip-igmp-snooping-vlan
show running-config feature ip-igmp-snooping-vlan all-defaults
```

```
show running-config feature ipmc-profile
show running-config feature ipmc-profile all-defaults
show running-config feature ipmc-profile-range
show running-config feature ipmc-profile-range all-defaults
show running-config feature ipv4
show running-config feature ipv4 all-defaults
show running-config feature ipv6
show running-config feature ipv6 all-defaults
show running-config feature ipv6-mld-snooping
show running-config feature ipv6-mld-snooping all-defaults
show running-config feature ipv6-mld-snooping-port
show running-config feature ipv6-mld-snooping-port all-defaults
show running-config feature ipv6-mld-snooping-vlan
show running-config feature ipv6-mld-snooping-vlan all-defaults
show running-config feature json_rpc_notification
show running-config feature json_rpc_notification all-defaults
show running-config feature lacp
show running-config feature lacp all-defaults
show running-config feature link-oam
show running-config feature link-oam all-defaults
show running-config feature lldp
show running-config feature lldp all-defaults
show running-config feature logging
show running-config feature logging all-defaults
show running-config feature loop-protect
show running-config feature loop-protect all-defaults
show running-config feature mac
show running-config feature mac all-defaults
show running-config feature mep
show running-config feature mep all-defaults
show running-config feature MRP
show running-config feature MRP all-defaults
show running-config feature mstp
show running-config feature mstp all-defaults
show running-config feature mvr
show running-config feature mvr all-defaults
show running-config feature MVRP
show running-config feature MVRP all-defaults
show running-config feature mvr-port
show running-config feature mvr-port all-defaults
show running-config feature ntp
show running-config feature ntp all-defaults
show running-config feature poe
show running-config feature poe all-defaults
show running-config feature port
show running-config feature port all-defaults
show running-config feature port-security
show running-config feature port-security all-defaults
show running-config feature ptp
show running-config feature ptp all-defaults
show running-config feature pvlan
show running-config feature pvlan all-defaults
show running-config feature qos
show running-config feature qos all-defaults
show running-config feature rmon
show running-config feature rmon all-defaults
show running-config feature snmp
show running-config feature snmp all-defaults
show running-config feature source-guard
```

```
show running-config feature source-guard all-defaults
show running-config feature ssh
show running-config feature ssh all-defaults
show running-config feature thermal-protect
show running-config feature thermal-protect all-defaults
show running-config feature udld
show running-config feature udld all-defaults
show running-config feature upnp
show running-config feature upnp all-defaults
show running-config feature user
show running-config feature user all-defaults
show running-config feature vlan
show running-config feature vlan all-defaults
show running-config feature voice-vlan
show running-config feature voice-vlan all-defaults
show running-config feature vtss-rmirror
show running-config feature vtss-rmirror all-defaults
show running-config feature web-privilege-group-level
show running-config feature web-privilege-group-level all-defaults
show running-config interface <interface>
show running-config line console <console id>
show running-config line console <console id> all-defaults
show running-config line vty <vty id>
show running-config line vty <vty id> all-defaults
show running-config vlan
show running-config vlan <vlan ids>
show running-config vlan <vlan ids> all-defaults
```

2.140.1 Syntax Description

| begin *<Line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<Line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<Line>*	Optional. Produces output that only displays lines with the specified text.
all-defaults	Optional. Specifies default values are included in the output.
feature	Optional. Limits current running configuration output to a specific feature.
access	Optional. Displays the current running configuration of device access parameters.
access-list	Optional. Displays the current running configuration of any access control lists (ACLs).
aggregation	Optional. Displays the current running configuration of aggregated groups.
alarm	Optional. Displays the current running configuration of alarms.
arp-inspection	Optional. Displays the current running configuration of ARP inspection.
auth	Optional. Displays the current running configuration of authorization settings.

clock	Optional. Displays the current running configuration of the clock.
ddmi	Optional. Displays the current running configuration for all DDMI settings.
dhcp	Optional. Displays the current running configuration for all Dynamic Host Control Protocol (DHCP) settings.
dhcp-snooping	Optional. Displays the current running configuration for all DHCP snooping settings.
dhcp_server	Optional. Displays the current running configuration for all DHCP server settings.
dhcp6_client_interface	Optional. Displays the current running configuration of the DHCPv6 client interface.
dns	Optional. Displays the current running configuration for Domain Naming System (DNS) settings.
dot1x	Optional. Displays the current running configuration for all IEEE 802.1x settings.
eps	Optional. Displays the current running configuration for the external power supply (EPS).
erps	Optional. Displays the current running configuration for all Ethernet Ring Protection Switching (ERPS) settings.
green-ethernet	Optional. Displays the current running configuration for all green Ethernet settings.
GVRP	Optional. Displays the current running configuration for all GARP VLAN Registration Protocol (GVRP) settings.
http	Optional. Displays the current running configuration for all Hypertext Transfer Protocol (HTTP) settings.
icli	Optional. Displays the current running configuration of the command line interface (CLI).
ip-igmp-snooping	Optional. Displays the current running configuration for all IP Internet Group Management Protocol (IGMP) snooping settings.
ip-igmp-snooping-port	Optional. Displays the current running configuration for all IP IGMP snooping parameters on per-port basis.
ip-igmp-snooping-vlan	Optional. Displays the current running configuration for all IP IGMP snooping parameters on a per-virtual local area network (VLAN) basis.
ipmc-profile	Optional. Displays the current running configuration for all IP Multimedia Communications (IPMC) settings.
ipmc-profile-range	Optional. Displays the current running configuration for all IPMC profiles.
ipv4	Optional. Displays the current running configuration for all Internet Protocol version 4 (IPv4) settings.
ipv6	Optional. Displays the current running configuration for all Internet Protocol version 6 (IPv6) settings.

ipv6-mld-snooping	Optional. Displays the current running configuration for all IPv6 Mulitcast Listener Discovery (MLD) snooping configurations.
ipv6-mld-snooping-port	Optional. Displays the current running configuration for all IPv6 MLD snooping configurations on a per-port basis.
ipv6-mld-snooping-vlan	Optional. Displays the current running configuration for all IPv6 MLD snooping configurations on a per-VLAN basis.
json_rpc_notification	Optional. Displays the current running configuration for all JavaScript Object Notation (JSON) remote procedure call (RPC) notifications.
lacp	Optional. Displays the current running configuration for all Link Aggregation Control Protocol (LACP) settings.
link-oam	Optional. Displays the current running configuration for all link Operation, Administration, and Maintenance (OAM) settings.
lldp	Optional. Displays the current running configuration for all Link Layer Discovery Protocol (LLDP) settings.
logging	Optional. Displays the current running configuration of the logging feature.
loop-protect	Optional. Displays the current running configuration of the loop protection feature.
mac	Optional. Displays the current running configuration for all Media Access Control (MAC) settings.
mep	Optional. Displays the current running configuration for maintenance endpoints (MEPs).
MRP	Optional. Displays the current running configuration for all Media Redundancy Protocol (MRP) settings.
mstp	Optional. Displays the current running configuration for Multiple Spanning Tree Protocol (MSTP) settings.
mvr	Optional. Displays the current running configuration for all Multicast VLAN Registration (MVR) settings.
mvr-port	Optional. Displays the current running configuration for all MVR settings on a per-port basis.
MVRP	Optional. Displays the current running configuration for all MVR Protocol (MVRP) settings.
ntp	Optional. Displays the current running configuration for all Network Time Protocol (NTP) settings.
poe	Optional. Displays the current running configuration for Power over Ethernet (PoE) settings.
port	Optional. Displays the current running configuration for all ports.
port-security	Optional. Displays the current running configuration for all port security settings.
ptp	Optional. Displays the current running configuration for all Precision Time Protocol (PTP) settings.

pvlan	Optional. Displays the current running configuration for all private VLANs (PVLANs).
qos	Optional. Displays the current running configuration for all Quality of Service (QoS) settings.
rmon	Optional. Displays the current running configuration for all remote monitoring sessions.
snmp	Optional. Displays the current running configuration for all Simple Network Management Protocol (SNMP) settings.
source-guard	Optional. Displays the current running configuration for all source guard settings.
ssh	Optional. Displays the current running configuration for all secure shell (SSH) settings.
thermal-protect	Optional. Displays the current running configuration for all thermal protection settings.
udld	Optional. Displays the current running configuration for all Unidirectional Link Detection (UDLD) settings.
upnp	Optional. Displays the current running configuration for all Universal Plug-n-Play (UPNP) settings.
user	Optional. Displays the current running configuration for all device users.
vlan	Optional. Displays the current running configuration for all VLANs.
voice-vlan	Optional. Displays the current running configuration for all voice VLANs.
vtss-rmirror	Optional. Displays the current running configuration for all virtual tape servers (VTSs) used in conjunction with remote mirroring.
web-privilege-group-level	Optional. Displays the current running configuration for the Web privilege level of all user groups.
line	Optional. Displays the current running configuration for all line settings.
console *<console id>*	Displays the current running configuration for console line settings of a particular console ID.
vty *<vty id>*	Displays the current running configuration for VTY line settings of a particular VTY ID.
vlan	Optional. Displays the current running configuration for all VLANs.
<vlan ids>	Optional. Displays the current running configuration for a single VLAN, or a range of VLANs. Valid range is **1** to **4095**.

2.140.2 Default Values

No default values are necessary for this command.

2.140.3 Privilege Level

By default, this command has a privilege level of **15**.

2.140.4 Command History

ASE Release 4.4-41	Command was introduced.

2.140.5 Usage Examples

Enter the command as follows to display the current running configuration for all PoE settings:

```
#show running-config feature poe
```

2.141 show sflow

Use the **show sflow** command to display sFlow traffic capturing information. Variations of this command include:

```
show sflow
show sflow | begin <line>
show sflow | exclude <line>
show sflow | include <line>
show sflow statistics receiver
show sflow statistics samplers
show sflow statistics samplers interface <interface>
```

2.141.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<Line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<Line>*	Optional. Produces output that only displays lines with the specified text.
statistics receivers	Optional. Limits output to sFlow receiver statistics.
statistics samplers	Optional. Limits output to sFlow sampler statistics.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.141.2 Default Values

No default values are necessary for this command.

2.141.3 Privilege Level

By default, this command has a privilege level of **0**.

2.141.4 Command History

ASE Release 4.4-41	Command was introduced.

2.141.5 Usage Examples

The following is sample output from the **show sflow statistics samplers interface GigabitEthernet 1/1** command:

```
#show sflow statistics samplers interface GigabitEthernet 1/1
Per-Port Statistics:
====================

Interface              Flow Samples            Counter Samples
---------------      ----------------        ------------------
GigabitEthernet 1/1                0                          0
```

2.142 show snmp

Use the **show snmp** command to view the current system Simple Network Management Protocol (SNMP) configuration. Variations of this command include:

```
show snmp
show snmp | begin <line>
show snmp | exclude <line>
show snmp | include <line>
```

2.142.1 Syntax Description

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

2.142.2 Default Values

No default values are necessary for this command.

2.142.3 Privilege Level

By default, this command has a privilege level of **15**.

2.142.4 Command History

ASE Release 4.4-41	Command was introduced.

2.142.5 Usage Examples

To view the current system SNMP configuration, enter the command as follows:

```
#show snmp
```

2.143 show snmp access

Use the **show snmp access** command to view the current Simple Network Management Protocol (SNMP) access group configuration. Variations of this command include:

```
show snmp access
show snmp access <group name> v1
show snmp access <group name> v1 auth
show snmp access <group name> v1 noauth
show snmp access <group name> v1 priv
show snmp access <group name> v2
show snmp access <group name> v2 auth
show snmp access <group name> v2 noauth
show snmp access <group name> v2 priv
show snmp access <group name> v3
show snmp access <group name> v3 auth
show snmp access <group name> v3 noauth
show snmp access <group name> v3 priv
show snmp access <group name> any
show snmp access <group name> any auth
show snmp access <group name> any noauth
show snmp access <group name> any priv
```

2.143.1 Syntax Description

<group name>	Optional. Specifies the SNMP access group to view. Group names are entered as a text string, with a maximum of 32 characters in length.
v1	Optional. Displays SNMP information for access groups that use SNMP version **1**.
v2	Optional. Displays SNMP information for access groups that use SNMP version **2**.
v3	Optional. Displays SNMP information for access groups that use SNMP version **3**.
any	Optional. Displays SNMP information for access groups that use any SNMP version.
auth	Optional. Displays SNMP information for access groups with the **authNoPriv** security level.
noauth	Optional. Displays SNMP information for access groups with the **noAuthNoPriv** security level.
priv	Optional. Displays SNMP information for access groups with the **authPriv** security level.

2.143.2 Default Values

No default values are necessary for this command.

2.143.3 Privilege Level

By default, this command has a privilege level of **15**.

2.143.4 Command History

ASE Release 4.4-41	Command was introduced.

2.143.5 Usage Examples

Enter the command as follows to display all SNMP access group information:

```
#show snmp access
```

2.144 show snmp community

Use the **show snmp community** command to view the current Simple Network Management Protocol (SNMP) community configurations. Variations of this command include:

```
show snmp community
show snmp community <community name>
```

2.144.1 Syntax Description

<community name>	Optional. Specifies the SNMP community to view. Community names are entered as a text string, with a maximum of 32 characters in length.

2.144.2 Default Values

No default values are necessary for this command.

2.144.3 Privilege Level

By default, this command has a privilege level of **15**.

2.144.4 Command History

ASE Release 4.4-41	Command was introduced.

2.144.5 Usage Examples

Enter the command as follows to display all SNMP community information:

```
#show snmp community
```

2.145 show snmp host

Use the **show snmp host** command to view current Simple Network Management Protocol (SNMP) host configurations. Variations of this command include:

```
show snmp host
show snmp host <host name>
```

2.145.1 Syntax Description

<host name>	Optional. Specifies the SNMP host to view. Host names are entered as a text string, with a maximum of 32 characters in length.

2.145.2 Default Values

No default values are necessary for this command.

2.145.3 Privilege Level

By default, this command has a privilege level of **15**.

2.145.4 Command History

ASE Release 4.4-41	Command was introduced.

2.145.5 Usage Examples

Enter the command as follows to display all SNMP host information:

```
#show snmp host
```

2.146 show snmp mib

Use the **show snmp mib** command to view Simple Network Management Protocol (SNMP) management information base (MIB) information. Variations of this command include:

```
show snmp mib context
show snmp mib ifmib ifIndex
show snmp mib ifmib ifIndex aggregation
show snmp mib ifmib ifIndex port
show snmp mib ifmib ifIndex vlan
```

2.146.1 Syntax Description

`context`	Specifies the MIB context is displayed.
`ifmib ifIndex`	Specifies the IF-MIB, and its defined **ifIndex**, are displayed.
`aggregation`	Optional. Limits output to IF-MIB information for aggregated groups.
`port`	Optional. Limits output to IF-MIB information for ports.
`vlan`	Optional. Limits output to IF-MIB information for virtual local area networks (VLANs).

2.146.2 Default Values

No default values are necessary for this command.

2.146.3 Privilege Level

By default, this command has a privilege level of **15**.

2.146.4 Command History

ASE Release 4.4-41	Command was introduced.

2.146.5 Usage Examples

Enter the command as follows to display the context of all SNMP MIBs:

```
#show snmp mib context
```

2.147 show snmp security-to-group

Use the **show snmp security-to-group** command to view the configured security to the Simple Network Management Protocol (SNMP) group. Variations of this command include:

```
show snmp security-to-group
show snmp security-to-group v1 <group name>
show snmp security-to-group v2 <group name>
show snmp security-to-group v3 <group name>
```

2.147.1 Syntax Description

v1	Optional. Displays SNMP information for groups that use SNMP version **1**.
v2	Optional. Displays SNMP information for groups that use SNMP version **2**.
v3	Optional. Displays SNMP information for groups that use SNMP version **3**.
<group name>	Optional. Specifies the SNMP group to view. Group names are entered as a text string, with a maximum of 32 characters in length.

2.147.2 Default Values

No default values are necessary for this command.

2.147.3 Privilege Level

By default, this command has a privilege level of **15**.

2.147.4 Command History

ASE Release 4.4-41	Command was introduced.

2.147.5 Usage Examples

Enter the command as follows to display the security configurations for SNMP groups:

```
#show snmp security-to-group
```

2.148 show snmp trap

Use the show snmp trap command to display traps associated with Simple Network Management Protocol (SNMP) configurations. Variations of this command include:

```
show snmp trap
show snmp trap alarmTrapStatus
show snmp trap authenticationFailure
show snmp trap coldStart
show snmp trap entConfigChange
show snmp trap fallingAlarm
show snmp trap ipTrapInterfacesLink
show snmp trap linkDown
show snmp trap linkUp
show snmp trap lldpRemTablesChange
show snmp trap newRoot
show snmp trap psecTrapGlobalsMain
show snmp trap psecTrapInterfaces
show snmp trap risingAlarm
show snmp trap topologyChange
show snmp trap warmStart
```

2.148.1 Syntax Description

`alarmTrapStatus`	Optional. Displays information for the **alarmTrapStatus** trap.
`authenticationFailure`	Optional. Displays information for the **authenticationFailure** trap.
`coldStart`	Optional. Displays information for the **coldStart** trap.
`entConfigChange`	Optional. Displays information for the **entConfigChange** trap.
`fallingAlarm`	Optional. Displays information for the **failingAlarm** trap.
`ipTrapInterfacesLink`	Optional. Displays information for the **ipTrapInterfacesLink** trap.
`linkDown`	Optional. Displays information for the **linkDown** trap.
`linkUp`	Optional. Displays information for the **linkUp** trap.
`lldpRemTablesChange`	Optional. Displays information for the **lldpRemTablesChange** trap.
`newRoot`	Optional. Displays information for the **newRoot**.
`psecTrapGlobalsMain`	Optional. Displays information for the **psecTrapGlobalsMain** trap.
`psecTrapInterfaces`	Optional. Displays information for the **psecTrapInterfaces** trap.
`risingAlarm`	Optional. Displays information for the **risingAlarm** trap.
`topologyChange`	Optional. Displays information for the **topologyChange** trap.
`warmStart`	Optional. Displays information for the **warmStart** trap.

2.148.2 Default Values

No default values are necessary for this command.

2.148.3 Command History

ASE Release 4.4-41	Command was introduced.

2.148.4 Usage Examples

Enter the command as follows to display information for all SNMP traps:

```
#show snmp trap
```

2.149 show snmp user

Use the **show snmp user** command to view the current Simple Network Management Protocol (SNMP) user configurations. Variations of this command include:

```
show snmp user
show snmp user <name> <engine id>
```

2.149.1 Syntax Description

<name>	Optional. Specifies the SNMP user to view. User names are entered as a text string, with a maximum of 32 characters in length.
<engine id>	Optional. Specifies the SNMP engine ID.for the system. Engine IDs are the 12-octet hexadecimal representation (24 characters using 0 through 9 and/or a through f) defining a system on the management domain.

2.149.2 Default Values

No default values are necessary for this command.

2.149.3 Privilege Level

By default, this command has a privilege level of **15**.

2.149.4 Command History

ASE Release 4.4-41	Command was introduced.

2.149.5 Usage Examples

Enter the command as follows to display information for all SNMP users:

```
#show snmp user
```

2.150 show snmp view

Use the **show snmp view** command to display current management information base (MIB) configuration for Simple Network Management Protocol (SNMP) configurations. Variations of this command include:

```
show snmp view
show snmp view <mib name> <mib oid>
```

2.150.1 Syntax Description

<mib name>	Optional. Specifies a MIB configuration to display. MIB names cannot be longer than 32 characters in length.
<mib oid>	Optional. Specifies the object identifier (OID) for the MIB. MIB OIDs cannot be more than 255 characters in length.

2.150.2 Default Values

No default values are necessary for this command.

2.150.3 Privilege Level

By default, this command has a privilege level of **15**.

2.150.4 Command History

ASE Release 4.4-41	Command was introduced.

2.150.5 Usage Examples

The following is sample output from the **show snmp view** command:

```
#show snmp view
View Name    : default_view
OID Subtree  : .1
View Type    : included
```

2.151 show spanning-tree

Use the **show spanning-tree** command to display the status of the spanning tree protocol (STP) or Multiple Spanning Tree Protocol (MSTP). Variations of this command include:

```
show spanning-tree
show spanning-tree | begin <line>
show spanning-tree | exclude <line>
show spanning-tree | include <line>
show spanning-tree active
show spanning-tree detailed
show spanning-tree detailed interface <interface>
show spanning-tree interface <interface>
show spanning-tree mst <instance>
show spanning-tree mst configuration
show spanning-tree mst interface <interface>
show spanning-tree summary
```

2.151.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
active	Optional. Displays active STP interfaces.
detailed	Optional. Displays detailed STP statistics.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
mst	Optional. Limits output to Multiple Spanning Tree (MST) instances (MSTIs).
<instance>	Optional. Specifies a particular MSTI to view. Valid range is 0 to 7, where 0 is the Common and Internal Spanning Tree instance (CIST), and 1 to 7 are MSTI1 through MSTI7, respectively.
configuration	Optional. Displays the mapping configuration between virtual local area networks (VLANs) and MSTIs.
summary	Optional. Summarizes STP configuration.

2.151.2 Default Values

No default values are necessary for this command.

2.151.3 Privilege Level

By default, this command has a privilege level of **15**.

2.151.4 Command History

ASE Release 4.4-41	Command was introduced.

2.151.5 Usage Examples

The following is sample output from the **show spanning-tree summary** command:

```
#show spanning-tree summary
Protocol Version    : MSTP
Hello Time          : 2
Max Age             : 20
Forward Delay       : 15
Tx Hold Count       : 6
Max Hop Count       : 20
BPDU Filtering      : Disabled
BPDU Guard          : Disabled
Error Recovery      : Disabled

CIST Bridge is active
```

2.152 show svl

Use the **show svl** command to display configurations and statistics for the shared virtual local area network (VLAN) learning (SVL) feature. Variations of this command include:

```
show svl
show svl | begin <line>
show svl | exclude <line>
show svl | include <line>
show svl fid
show svl fid <fid>
show svl vlan
show svl vlan <vlan ids>
```

2.152.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
fid	Optional. Displays the filter IDs associated with all VLANs.
<fid>	Optional. Limits the output to a single filter ID and its associated VLANs. Valid range is **1** to **4095**.
vlan	Optional. Displays the VLANs configured for SVL.
<vlan ids>	Optional. Limits the output to specific VLANs. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

2.152.2 Default Values

No default values are necessary for this command.

2.152.3 Command History

ASE Release 4.4-41	Command was introduced.

2.152.4 Usage Examples

The following is sample output from the **show svl fid** command:

```
#show svl fid 1
FID         VLANs
-----       ---------------
   1        1 (default)
```

2.153 show switchport forbidden

Use the **show switchport forbidden** command to view the forbidden virtual local area networks (VLANs) associated with individual ports. These VLANs are ones in which the port cannot participate. Variations of this command include:

```
show switchport forbidden
show switchport forbidden | begin <line>
show switchport forbidden | exclude <line>
show switchport forbidden | include <line>
show switchport forbidden name <vlan name>
show switchport forbidden vlan <vlan ids>
```

2.153.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
name *<vlan name>*	Optional. Displays port information for a specific forbidden VLAN.
vlan *<vlan ids>*	Optional. Limits the output to specific VLANs. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

2.153.2 Default Values

No default values are necessary for this command.

2.153.3 Privilege Level

By default, this command has a privilege level of **0**.

2.153.4 Command History

ASE Release 4.4-41	Command was introduced.

2.153.5 Usage Examples

Enter the command as follows to display all forbidden VLANs and their associated interfaces:

```
#show switchport forbidden
```

2.154 show system

Use the **show system** command to display ASE system information. Variations of this command include:

```
show system cpu status
show system led status
```

2.154.1 Syntax Description

cpu status	Displays the average load of the central processing unit (CPU).
led status	Displays the status of the system light-emitting diodes (LEDs).

2.154.2 Default Values

No default values are necessary for this command.

2.154.3 Privilege Level

By default, this command has a privilege level of **0**.

2.154.4 Command History

ASE Release 4.4-41	Command was introduced.

2.154.5 Usage Examples

Enter the command as follows to display LED information for the system:

```
#show system led status
System LED: green, solid, normal indication.
```

2.155 show tacacs-server

Use the **show tacacs-server** command to display the current configuration of the terminal access controller access control system (TACACS+) server.

2.155.1 Syntax Description

No subcommands.

2.155.2 Default Values

No default values are necessary for this command.

2.155.3 Privilege Level

By default, this command has a privilege level of **15**.

2.155.4 Command History

ASE Release 4.4-41	Command was introduced.

2.155.5 Usage Examples

Enter the command as follows to display the current configuration of the TACACS+ server:

```
#show tacacs-server
Global TACACS+ Server Timeout     : 5 seconds
Global TACACS+ Server Deadtime    : 0 minutes
Global TACACS+ Server Key         :
No servers configured!
```

2.156 show terminal

Use the **show terminal** command to view the terminal configuration. Variations of this command include:

```
show terminal
show terminal | begin <line>
show terminal | exclude <line>
show terminal | include <line>
```

2.156.1 Syntax Description

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

2.156.2 Default Values

No default values are necessary for this command.

2.156.3 Command History

ASE Release 4.4-41	Command was introduced.

2.156.4 Usage Examples

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

```
#show terminal
Line is con 0.
--------------
  *You are at this line now.
  Alive from Console.
  Default privileged level is 2.
  Command line editing is enabled.
  Display EXEC banner is enabled.
  Display Day banner is enabled.
  Terminal width is 80.
           length is 24.
           history size is 32.
           exec-timeout is 10 min 0 second.
  Current session privilege is 15.
  Elapsed time is 0 day 1 hour 33 min 36 sec.
  Idle time is 0 day 0 hour 0 min 0 sec.
```

2.157 show thermal-protect

Use the **show thermal-protect** command to display the thermal protection status.

2.157.1 Syntax Description

No subcommands.

2.157.2 Default Values

No default values are necessary for this command.

2.157.3 Privilege Level

By default, this command has a privilege level of **15**.

2.157.4 Command History

ASE Release 4.4-41 Command was introduced.

2.157.5 Usage Examples

The following is sample output from the **show thermal-protect** command:

```
#show thermal-protect
Interface     Chip Temp.  Port Status
Gi 1/1        62 C        Port link operating normally
Gi 1/2        62 C        Port link operating normally
Gi 1/3        62 C        Port link operating normally
Gi 1/4        62 C        Port link operating normally
Gi 1/5        59 C        Port link operating normally
Gi 1/6        60 C        Port link operating normally
Gi 1/7        60 C        Port link operating normally
Gi 1/8        59 C        Port link operating normally
```

2.158 show udld

Use the **show udld** command to view statistics and configuration information for the Unidirectional Link Detection (UDLD) protocol. Variations of this command include:

```
show udld
show udld | begin <line>
show udld | exclude <line>
show udld | include <line>
show udld interface <interface>
```

2.158.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.158.2 Default Values

No default values are necessary for this command.

2.158.3 Command History

ASE Release 4.4-41	Command was introduced.

2.158.4 Usage Examples

The following example displays UDLD information for the GigabitEthernet 1/3 interface:

```
#show udld interface GigabitEthernet 1/3

GigabitEthernet 1/3
------------------------------------------------------
UDLD Mode                   : Disable
Admin State                 : Disable
Message Time Interval (Sec) : 7
Device ID (local)           : 02-00-C1-A8-D2-E2
Device Name (local)         :
Bidirectional state         : Indeterminate

No neighbor cache information stored
------------------------------------------------------
```

2.159 show upnp

Use the **show upnp** command to display Universal Plug-n-Play (UPNP) statistics and configuration information. Variations of this command include:

```
show upnp
show upnp | begin <line>
show upnp | exclude <line>
show upnp | include <line>
```

2.159.1 Syntax Description

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

2.159.2 Default Values

No default values are necessary for this command.

2.159.3 Privilege Level

By default, this command has a privilege level of **15**.

2.159.4 Command History

ASE Release 4.4-41	Command was introduced.

2.159.5 Usage Examples

The following example displays the UPNP configuration for the switch:

```
#show upnp
UPnP Mode                    : Disable
UPnP TTL                     : 4
UPnP Advertising Duration    : 100
UpnP IP Addressing Mode      : dynamic
UpnP Static IP Interface ID  : 1
```

2.160 show user-privilege

Use the **show user-privilege** command to display the privilege level configurations for all users.

2.160.1 Syntax Description

No subcommands.

2.160.2 Default Values

No default values are necessary for this command.

2.160.3 Command History

ASE Release 4.4-41 Command was introduced.

2.160.4 Usage Examples

The following is sample output from the **show user-privilege** command:

```
#show user-privilege
username admin privilege 15 password encrypted a1d7204a093a93449c0f46c20fff18d13
69273e6734f944cee7ec8d52848ad37d89ffddd91cbb0af25e00eecf93d69e4e0182d944a2b8e5f2
04efac6c1dbd1aa
```

2.161 show users

Use the **show users** command to display configuration user information for each terminal line. Variations of this command include:

```
show users
show users | begin <line>
show users | exclude <line>
show users | include <line>
show users myself
```

2.161.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
myself	Optional. Display the configuration of the current user.

2.161.2 Default Values

No default values are necessary for this command.

2.161.3 Command History

ASE Release 4.4-41	Command was introduced.

2.161.4 Usage Examples

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

```
# show users
Line is con 0.
    Connection is from Console.
    User name is admin.
    Privilege is 15.
    Elapsed time is 0 day 6 hour 30 min 55 sec.
    Idle time is 0 day 0 hour 2 min 22 sec.

Line is vty 1.
    Connection is from 172.22.110.49:51801 by Telnet.
    User name is admin.
    Privilege is 15.
    Elapsed time is 0 day 0 hour 6 min 40 sec.
    Idle time is 0 day 0 hour 6 min 40 sec.

Line is vty 2.
    * You are at this line now.
    Connection is from 172.22.108.126:49486 by Telnet.
    User name is admin.
    Privilege is 15.
    Elapsed time is 0 day 0 hour 0 min 2 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.
```

2.162 show version

Use the **show version** command to display the hardware and software status of the system. Variations of this command include:

```
show version
show version | begin <line>
show version | exclude <line>
show version | include <line>
show version brief
```

2.162.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<line>*	Optional. Produces output that only displays lines with the specified text.
brief	Optional. Displays a brief summary of system hardware and software information.

2.162.2 Default Values

No default values are necessary for this command.

2.162.3 Privilege Level

By default, this command has a privilege level of **0**.

2.162.4 Command History

ASE Release 4.4-41	Command was introduced.

2.162.5 Usage Examples

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

```
#show version brief
Version      : v4.4-34
Build Date   : 2019-02-06T05:52:47+00:00
Code Revision: 71b948b
```

2.163 show vlan all

Use the **show vlan all** command to display the status of all configured virtual local area networks (VLANs) on the ASE switch. Variations of this command include:

```
show vlan all
show vlan all brief
show vlan all id <vlan ids>
show vlan all name <name>
```

2.163.1 Syntax Description

brief	Optional. Limits the output to summary information.
id *<vlan ids>*	Optional. Displays the VLAN status information by VLAN ID. Specify a single VLAN ID, or a range of VLAN IDs separated by a hyphen or comma. Valid range is **1** to **4095**.
name *<name>*	Optional. Displays the VLAN status information by VLAN name.

2.163.2 Default Values

No default values are necessary for this command.

2.163.3 Command History

ASE Release 4.4-41	Command was introduced.

2.163.4 Usage Examples

The following is sample output from this command:

```
#show vlan all
VLAN  Name                             Interfaces
----  -------------------------------  ----------
1     default                          Gi 1/1,3-10
10    VLAN0010                         Gi 1/2
```

2.164 show vlan brief

Use the **show vlan brief** command to display a brief summary of configured virtual local area network (VLAN) status. Variations of this command include:

```
show vlan brief
show vlan brief all
```

2.164.1 Syntax Description

all	Optional. Specifies that information for all configured VLANs is shown. If this parameter is not included, only access VLAN information is displayed.

2.164.2 Default Values

No default values are necessary for this command.

2.164.3 Privilege Level

By default, this command has a privilege level of **13**.

2.164.4 Command History

ASE Release 4.4-41	Command was introduced.

2.164.5 Usage Examples

The following is sample output from this command:

```
#show vlan brief all
VLAN  Name                             Interfaces
----  -------------------------------  ----------
1     default                          Gi 1/1,3-10
10    VLAN0010                         Gi 1/2
```

2.165 show vlan id <*vlan ids*>

Use the **show vlan id** <*vlan ids*> command display virtual local area network (VLAN) information by VLAN ID. Variations of this command include:

```
show vlan id <vlan ids>
show vlan id <vlan ids> all
```

2.165.1 Syntax Description

<vlan ids>	Optional. Limits the output to specific VLANs. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.
all	Optional. Specifies that information for all configured VLANs is shown. If this parameter is not included, only access VLAN information is displayed.

2.165.2 Default Values

No default values are necessary for this command.

2.165.3 Privilege Level

By default, this command has a privilege level of **13**.

2.165.4 Command History

ASE Release 4.4-41	Command was introduced.

2.165.5 Usage Examples

Enter the command as follows:

```
#show vlan id 5 all
```

2.166 show vlan ip-subnet

Use the **show vlan ip-subnet** command to display virtual local area network (VLAN) information for all Internet Protocol version 4 (IPv4) addresses. Variations of this command include:

```
show vlan ip-subnet
show vlan ip-subnet <ipv4 address>
```

2.166.1 Syntax Description

<ipv4 address>	Optional. Specifies that VLAN information for a specific IPv4 address is displayed. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

2.166.2 Default Values

No default values are necessary for this command.

2.166.3 Privilege Level

By default, this command has a privilege level of **13**.

2.166.4 Command History

ASE Release 4.4-41	Command was introduced.

2.166.5 Usage Examples

Enter the command as follows:

```
#show vlan ip-subnet
```

2.167 show vlan mac address

Use the **show vlan mac address** command to display virtual local area network (VLAN) information by Media Access Control (MAC) address. Variations of this command include:

```
show vlan mac address
show vlan mac address <mac address>
```

2.167.1 Syntax Description

<mac address>	Optional. Specifies that information for a single unicast MAC address is displayed. MAC addresses are entered in the format **HH:HH:HH:HH:HH:HH**.

2.167.2 Default Values

No default values are necessary for this command.

2.167.3 Privilege Level

By default, this command has a privilege level of **13**.

2.167.4 Command History

ASE Release 4.4-41	Command was introduced.

2.167.5 Usage Examples

Enter the command as follows:

```
#show vlan mac address
```

2.168 show vlan name <*name*>

Use the **show vlan name** <*name*> command to display information a single, named virtual local area network (VLAN) instance.

2.168.1 Syntax Description

<*name*>	Specifies the name of the VLAN instance.

2.168.2 Default Values

No default values are necessary for this command.

2.168.3 Privilege Level

By default, this command has a privilege level of **13**.

2.168.4 Command History

ASE Release 4.4-41	Command was introduced.

2.168.5 Usage Examples

Enter the command as follows:

```
#show vlan name MYVLAN1
```

2.169 show vlan protocol

Use the **show vlan protocol** command to display virtual local area network (VLAN) information by protocol. Variations of this command include:

```
show vlan protocol eth2
show vlan protocol llc
show vlan protocol snap
```

2.169.1 Syntax Descritption

eth2	Specifies that VLAN information for the ETH2 protocol is displayed.
llc	Specifies that VLAN information for the Link Layer Control (LLC) protocol is displayed.
snap	Specifies that VLAN information for the Subnetwork Access Protocol (SNAP) is displayed.

2.169.2 Default Values

No default values are necessary for this command.

2.169.3 Privilege Level

By default, this command has a privilege level of **13**.

2.169.4 Command History

ASE Release 4.4-41	Command was introduced.

2.169.5 Usage Examples

Enter the command as follows:

```
#show vlan protocol llc
```

2.170 show vlan status

Use the **show vlan status** command to display information for virtual local area networks (VLANs) used by specific features on the ASE device. Variations of this command include:

```
show vlan status
show vlan status admin
show vlan status interface <interface>
show vlan status all
show vlan status all interface <interface>
show vlan status combined
show vlan status combined interface <interface>
show vlan status conflicts
show vlan status conflicts interface <interface>
show vlan status erps
show vlan status erps interface <interface>
show vlan status gvrp
show vlan status gvrp interface <interface>
show vlan status interface <interface>
show vlan status mep
show vlan status mep interface <interface>
show vlan status mstp
show vlan status mstp interface <interface>
show vlan status mvr
show vlan status mvr interface <interface>
show vlan status nas
show vlan status nas interface <interface>
show vlan status rmirror
show vlan status rmirror interface <interface>
show vlan status vcl
show vlan status vcl interface <interface>
show vlan status voice-vlan
show vlan status voice-vlan interface <interface>
```

2.170.1 Syntax Description

admin	Optional. Specifies that information for VLANs created by the administrator is displayed.
all	Optional. Specifies that information for all user VLANs are displayed.
combined	Optional. Specifies that status information for all VLANs is displayed.
conflicts	Optional. Specifies that VLANs with conflicts are displayed.
erps	Optional. Specifies that VLANs used by Ethernet Ring Protection Switching (ERPS) are displayed.
gvrp	Optional. Specifies that VLANs used by GVRP are displayed.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

mep	Optional. Specifies that VLANs used by the maintenance endpoint (MEP) are displayed.
mstp	Optional. Specifies that VLANs used by Multiple Spanning Tree Protocol (MSTP) are displayed.
mvr	Optional. Specifies that VLANs used by Multiple VLAN Registration (MVR) are displayed.
nas	Optional. Specifies that VLANs used by network attached storage (NAS) are displayed.
rmirror	Optional. Specifies that VLANs used by remote mirroring are displayed.
vcl	Optional. Specifies that VLANs used by VCL are displayed.
voice-vlan	Optional. Specifies that VLANs used by voice VLANs are displayed.

2.170.2 Default Values

No default values are necessary for this command.

2.170.3 Privilege Level

By default, this command has a privilege level of **13**.

2.170.4 Command History

ASE Release 4.4-41	Command was introduced.

2.170.5 Usage Examples

The following is sample output from this command:

```
#show vlan status interface gigabitethernet 1/1
GigabitEthernet 1/1 :
---------------------
VLAN User PortType  PVID  Frame Type Ing Filter  Tx Tag  U  VID  Conflicts
--------- --------  -----  ---------  ---------  ------- --  ---- --------Combined
    C-Port    1     All        Enabled     None    1        No
Admin     C-Port    1     All        Enabled     None    1

NAS                                                              No
GVRP                                                             No
MVR                                                              No
Voice VLAN                                                       No
MSTP                                                             No
ERPS                                                             No
MEP                                                              No
VCL                                                              No
RMirror                                                          No
```

2.171 show voice vlan

Use the **show voice vlan** command to display information for virtual local area networks (VLANs) used for voice traffic (voice VLANs). Variations of this command include:

```
show voice vlan
show voice vlan | begin <line>
show voice vlan | exclude <line>
show voice vlan | include <line>
show voice vlan interface <interface>
show voice vlan oui
show voice vlan oui <oui>
```

2.171.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.
| exclude *<Line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<Line>*	Optional. Produces output that only displays lines with the specified text.
interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
oui	Optional. Displays the OUI information for Voice over IP (VoIP) devices connected to the voice VLAN.
<oui>	Optional. Limits displayed OUI information to a single OUI address.Enter OUI addresses as a 24-bit number in the format **00:00:00**.

2.171.2 Default Values

No default values are necessary for this command.

2.171.3 Privilege Level

By default, this command has a privilege level of **15**.

2.171.4 Command History

ASE Release 4.4-41	Command was introduced.

2.171.5 Usage Examples

The following is sample output from this command:

```
#show voice vlan interface GigabitEthernet 1/1

GigabitEthernet 1/1:
--------------------
GigabitEthernet 1/1 switchport voice vlan mode is disabled
GigabitEthernet 1/1 switchport voice security is disabled
GigabitEthernet 1/1 switchport voice discovery protocol is oui
```

2.172 show web privilege group level

Use the **show web privilege group level** command to display the privilege levels of all protocols that access the Internet. Variations of this command include:

```
show web privilege group level
show web privilege group | begin <line>
show web privilege group | exclude <line>
show web privilege group | include <line>
show web privilege group Aggregation level
show web privilege group Alarm level
show web privilege group AUTOLINK level
show web privilege group DDMI level
show web privilege group DHCP level
show web privilege group DHCPv6_Client level
show web privilege group Debug level
show web privilege group Diagnostics level
show web privilege group EPS level
show web privilege group ERPS level
show web privilege group ETH_LINK_OAM level
show web privilege group FRR level
show web privilege group Firmware level
show web privilege group Green_Ethernet level
show web privilege group IP level
show web privilege group IPMC_Snooping
show web privilege group LACP level
show web privilege group LLDP level
show web privilege group Loop_Protect level
show web privilege group MAC_Table level
show web privilege group MEP level
show web privilege group Miscellaneous level
show web privilege group MRP level
show web privilege group MVR level
show web privilege group NTP level
show web privilege group POE level
show web privilege group Ports level
show web privilege group Private_VLANs level
show web privilege group PTP level
show web privilege group QoS level
show web privilege group RMirror level
show web privilege group Security(access) level
show web privilege group Security(network) level
show web privilege group sFlow level
show web privilege group Spanning_Tree level
show web privilege group System level
show web privilege group UDLD level
show web privilege group uFDMA_AIL level
show web privilege group uFDMA_CIL level
show web privilege group UPnP level
show web privilege group VCL level
show web privilege group VLAN_Translation level
show web privilege group VLANs level
show web privilege group Voice_VLAN level
show web privilege group XXRP level
```

2.172.1 Syntax Description

| begin *<line>*	Optional. Produces output that begins with specific lines, including the specified text and every line thereafter.

| exclude *<Line>*	Optional. Produces output that excludes any lines containing the specified text.
| include *<Line>*	Optional. Produces output that only displays lines with the specified text.
Aggregation	Optional. Displays the privilege level of aggregated groups.
Alarm	Optional. Displays the privilege level of alarms.
AUTOLINK	Optional. Displays the privilege level of the Autolink feature.
DDMI	Optional. Displays the privilege level of the DDMI feature.
DHCP	Optional. Displays the privilege level of the Dynamic Host Control Protocol (DHCP) feature.
DHCPv6_Client	Optional. Displays the privilege level of the DHCPv6 client.
Debug	Optional. Displays the privilege level of debug messaging.
Diagnostics	Optional. Displays the privilege level of diagnostic configurations.
EPS	Optional. Displays the privilege level of the external power supply (EPS).
ERPS	Optional. Displays the privilege level of Ethernet Ring Protection Switching (ERPS) configurations.
ETH_LINK_OAM	Optional. Displays the privilege level of Ethernet link Operations, Administration, and Management (OAM) configurations.
FRR	Optional. Displays the privilege level of FRR.
Firmware	Optional. Displays the privilege level of firmware configurations.
Green-Ethernet	Optional. Displays the privilege level of green Ethernet settings.
IP	Optional. Displays the privilege level of IP configurations.
IPMC_Snooping	Optional. Displays the privilege level of IPMC snooping.
LACP	Optional. Displays the privilege level of Link Aggregation Control Protocol (LACP) settings.
LLDP	Optional. Displays the privilege level of Link Layer Discovery Protocol (LLDP) settings.
Loop-Protect	Optional. Displays the privilege level of the loop protection feature.
MAC_Table	Optional. Displays the privilege level of the Media Access Control (MAC) table.
MEP	Optional. Displays the privilege level of maintenance endpoints (MEPs).
Miscellaneous	Optional. Displays privilege level of miscellaneous features.
MRP	Optional. Displays the privilege level of Media Redundancy Protocol (MRP).
MVR	Optional. Displays the privilege level of Multicast VLAN Registration (MVR).

NTP	Optional. Displays the privilege level of Network Time Protocol (NTP).
POE	Optional. Displays the privilege level of Power over Ethernet (PoE).
Ports	Optional. Displays the privilege level of configured ports.
Private_VLANs	Optional. Displays the privilege level of private virtual local area networks (VLANs).
PTP	Optional. Displays the privilege level of Precision Time Protocol (PTP).
QoS	Optional. Displays the privilege level of Quality of Service (QoS).
RMirror	Optional. Displays the privilege level of remote monitoring sessions.
Security(access)	Optional. Displays the privilege level of access security.
Security(network)	Optional. Displays the privilege level of network security.
sFlow	Optional. Display the privilege level of sFlow.
Spanning_Tree	Optional. Displays the privilege level of the spanning tree protocol.
System	Optional. Displays the system privilege level.
UDLD	Optional. Displays the privilege level of Unidirectional Link Detection (UDLD).
uFDMA_AIL	Optional. Displays the privilege level of uFDMA AIL.
uFDMA_CIL	Optional. Displays the privilege level of uFDMA CIL.
UPnP	Optional. Displays the privilege level of Universal Plug-n-Play (UPNP).
VCL	Optional. Displays the privilege level of VCL.
VLAN_Translation	Optional. Displays the privilege level for VLAN translations.
VLANs	Optional. Displays the privilege level of all VLANs.
Voice-VLAN	Optional. Displays the privilege level of voice VLANs.
XXRP	Optional. Displays the privilege level of XXRP.

2.172.2 Default Values

No default values are necessary for this command.

2.172.3 Privilege Level

By default, this command has a privilege level of **0**.

2.172.4 Command History

ASE Release 4.4-41	Command was introduced.

2.172.5 Usage Examples

The following is sample output from this command:

```
#show web privilege group level
Group Name                       Privilege Level
                                 CRO CRW SRO SRW
-------------------------------- --- --- --- ---
Aggregation                        5  10   5  10
Alarm                              5  10   5  10
AUTOLINK                           5  10   5  10
DDMI                               5  10   5  10
Debug                             15  15  15  15
DHCP                               5  10   5  10
DHCPv6_Client                      5  10   5  10
Diagnostics                        5  10   5  10
EPS                                5  10   5  10
ERPS                               5  10   5  10
ETH_LINK_OAM                       5  10   5  10
Firmware                           5  10   5  10
FRR                                5  10   5  10
Green_Ethernet                     5  10   5  10
IP                                 5  10   5  10
IPMC_Snooping                      5  10   5  10
LACP                               5  10   5  10
LLDP                               5  10   5  10
Loop_Protect                       5  10   5  10
MAC_Table                          5  10   5  10
MEP                                5  10   5  10
Miscellaneous                     15  15  15  15
MRP                                5  10   5  10
MVR                                5  10   5  10
NTP                                5  10   5  10
POE                                5  10   5  10
Ports                              5  10   1  10
Private_VLANs                      5  10   5  10
PTP                                5  10   5  10
QoS                                5  10   5  10
RMirror                            5  10   5  10
Security(access)                  10  10   5  10
Security(network)                  5  10   5  10
sFlow                              5  10   5  10
Spanning_Tree                      5  10   5  10
System                             5  10   1  10
UDLD                               5  10   5  10
uFDMA_AIL                          5  10   5  10
uFDMA_CIL                          5  10   5  10
UPnP                               5  10   5  10
VCL                                5  10   5  10
VLAN_Translation                   5  10   5  10
VLANs                              5  10   5  10
Voice_VLAN                         5  10   5  10
XXRP                               5  10   5  10
```

2.173 terminal

Use the **terminal** command to configure system command line interface (CLI) settings, such as display settings, timeout values, and history storage functions. Variations of this command include:

```
terminal editing
terminal exec-timeout <minutes>
terminal exec-timeout <minutes> <seconds>
terminal history size <number>
terminal length <number>
terminal width <number>
```

2.173.1 Syntax Description

editing	Enables command line editing.
exec-timeout *<minutes>*	Specifies the time (in minutes) before the CLI disconnects. Valid range is **0** to **1440** minutes.
<seconds>	Optional. Specifies the time (in seconds) before the CLI disconnects. Used in conjunction with the timeout interval specified in minutes. Valid range is **0** to **3600** seconds.
history size *<number>*	Specifies the history buffer size by defining the number of commands stored in the buffer. Valid range is **0** to **32** commands. Setting this value to 0 disables the history buffer.
length *<number>*	Specifies the number of lines allowed on the screen. Valid range is **3** to **512**. You can set this value to 0 to specify pausing does not occur.
width *<number>*	Specifies the number of characters allowed in the display width. Valid range is **40** to **512** characters. Setting this value to **0** specifies an unlimited width for the display screen.

2.173.2 Default Values

No default values are necessary for this command.

2.173.3 Command History

ASE Release 4.4-41	Command was introduced.

2.173.4 Usage Examples

The following example configures the display timeout for **3** minutes:

```
#terminal exec-timeout 3
```

2.174 traceroute ip

Use the **traceroute ip** command to display the Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) routes a packet takes to reach the specified destination. Variations of this command include:

```
traceroute ip
traceroute ip <ipv4 address | hostname>
traceroute ip <ipv4 address | hostname> dscp <value>
traceroute ip <ipv4 address | hostname> firstttl <number>
traceroute ip <ipv4 address | hostname> icmp
traceroute ip <ipv4 address | hostname> maxttl <number>
traceroute ip <ipv4 address | hostname> numeric
traceroute ip <ipv4 address | hostname> probes <number>
traceroute ip <ipv4 address | hostname> saddr <ipv4 address>
traceroute ip <ipv4 address | hostname> sif <interface>
traceroute ip <ipv4 address | hostname> sif vlan <vlan id>
traceroute ip <ipv4 address | hostname> timeout <value>

traceroute ip <ipv6 address | hostname>
traceroute ip <ipv6 address | hostname> dscp <value>
traceroute ip <ipv6 address | hostname> firstttl <number>
traceroute ip <ipv6 address | hostname> icmp
traceroute ip <ipv6 address | hostname> maxttl <number>
traceroute ip <ipv6 address | hostname> numeric
traceroute ip <ipv6 address | hostname> probes <number>
traceroute ip <ipv6 address | hostname> saddr <ipv6 address>
traceroute ip <ipv6 address | hostname> sif <interface>
traceroute ip <ipv6 address | hostname> sif vlan <vlan id>
traceroute ip <ipv6 address | hostname> timeout <value>
```

2.174.1 Syntax Description

<ipv4 address | hostname>	Optional. Specifies the IPv4 address or host name of the remote system's route to trace. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<ipv6 address | hostname>	Optional. Specifies the IPv6 address of host name of the remote system's route to trace. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
dscp *<value>*	Optional. Specifies a DSCP value to trace. Valid range 0 to 63; default value of 0.
fistttl *<number>*	Optional. Specifies the starting Time To Live (TTL) value for the trace. Default value is 1.
icmp	Optional. Specifies Internet Control Message Protocol (ICMP) is used instead of User Datagram Protocol (UDP) for the trace.
maxttl *<number>*	Optional. Specifies the maximum TTL for the trace. Default value is 30.
numeric	Optional. Prints numeric addresses from the trace.

probes *<number>*	Optional. Specifies the number of probes per-hop. Valid range is **1** to **60**; default value is **3**.
saddr	Optional. Specifies the source IP address for the trace.
<ipv4 address>	Specifies the source address is an IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<ipv6 address>	Specifies the source address is an IPv6 address. Pv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
sif *<interface>*	Optional. Specifies the egress interface to use for the trace. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.
sif vlan *<vlan id>*	Optional. Specifies the egress virtual local area network (VLAN) to use for the trace. Valid ID range is **1** to **4095**.
timeout *<value>*	Optional. Specifies the time to wait for a response from the trace. Valid range is **1** to **86400** seconds; default value is **3**.

2.174.2 Default Values

No default values are necessary for this command.

2.174.3 Command History

ASE Release 4.4-41	Command was introduced.

2.174.4 Usage Examples

The following is output from a traceroute for IPv4 address **192.168.1.1** limited to **3** probes per hop:

```
#traceroute ip 192.168.1.1 probes 3
traceroute to 192.168.1.1 (192.168.1.1), 30 hops max, 38 byte packets
1 102.168.1.1 (192.168.1.1) 0.146 ms 0.149 ms 0.100 ms
```

2.175 veriphy

Use the **veriphy** command to generate a report concerning various cabling states and issues related to the physical condition of an Ethernet cable connected to various ports. Variations of this command include:

veriphy
veriphy interface *<interface>*

2.175.1 Syntax Description

interface *<interface>*	Optional. Specifies that information associated with a specific interface is displayed. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

2.175.2 Default Values

No default values are necessary for this command.

2.175.3 Command History

ASE Release 4.4-41	Command was introduced.

2.175.4 Functional Notes

The VeriPHY feature is only accurate when measuring cables that have a length greater than or equal to 8 meters. It can detect a short in cables shorter than 8 meters, but it will not provide a length measurement to the short.

2.175.5 Usage Examples

The following is a sample veriPHY report generated with this command:

```
#veriphy
Starting VeriPHY - Please wait
Interface               Pair A  Length  Pair B, Length  Pair C  Length  Pair D
Length
----------------------  ------  ------  --------------  ------  ------  ------
-------
GigabitEthernet 1/1     Open    0       Open    0       Open    0       Open
0
GigabitEthernet 1/2     Open    0       Open    0       Open    0       Open
0
GigabitEthernet 1/3     Open    0       Open    0       Open    0       Open
0
GigabitEthernet 1/4     Open    0       Open    0       Open    0       Open
0
GigabitEthernet 1/5     Open    0       Open    0       Open    0       Open
0
GigabitEthernet 1/6     Open    0       Open    0       Open    0       Open
0
GigabitEthernet 1/7     Open    0       Open    0       Open    0       Open
0
```

```
GigabitEthernet 1/8     Open    0       Open    0       Open    0       Open
0
GigabitEthernet 1/9     Short   0       Short   0       Short   0       Short
0
GigabitEthernet 1/10    OK      0       OK      0       OK      0       OK
0
```

3 Global Configuration Mode Command Set

3.1 Scope of this Section

This section outlines the commands available on the ADTRAN Switch Engine (ASE) in the Global Configuration mode. The Global Configuration mode is used to enable and configure the majority of features available on the ASE device.

3.2 Accessing the Global Configuration Mode

To activate the Global Configuration mode, enter the **configure terminal** command at the Enable mode prompt. For example:

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

3.3 Common Commands

The commands listed in Table 3-1 are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the section listed below:

Table 3-1. Common Commands

Sub-Section	Command	See Page …
1.4	do	19
1.5	end	20
1.6	exit	21
1.7	help	22

3.4 Global Configuration Mode Commands

Table 3-2 lists the available commands for the Global Configuration mode.

Table 3-2. Global Configuration Mode Commands

Sub-Section	Command	See Page …
3.5	aaa accounting	253
3.6	aaa authentication login	254
3.7	aaa authorization	256
3.8	access management <id>	257
3.9	access-list ace <ace id> action	259
3.10	access-list ace <ace id> dmac-type	260
3.11	access-list ace <ace id> frame-type	261
3.12	access-list ace <ace id> ingress	263

Table 3-2. Global Configuration Mode Commands (Continued)

Table 3-2. Global Configuration Mode Commands (Continued)

Sub-Section	Command	See Page …
3.45	erps <group> guard <value>	301
3.46	erps <group> holdoff <value>	302
3.47	erps <group> major port0	303
3.48	erps <group> mep port0 sf <index> aps <index> port1 sf <index> aps <index>	304
3.49	erps <group> revertive <time>	305
3.50	erps <group> rpl	306
3.51	erps <group> sub port0	307
3.52	erps <group> topology-change propagate	308
3.53	erps <group> version	309
3.54	erps <group> vlan	310
3.55	green-ethernet eee optimize-for-power	311
3.56	gvrp	312
3.57	hostname <hostname>	314
3.58	interface	315
3.59	ip arp	317
3.60	ip dhcp excluded-address	319
3.61	ip dhcp pool <name>	320
3.62	ip dhcp relay information	321
3.63	ip dhcp server	322
3.64	ip dhcp snooping	323
3.65	ip dns proxy	324
3.66	ip domain name <domain name>	325
3.67	ip helper-address <ipv4 address>	326
3.68	ip http	327
3.69	ip igmp host-proxy	328
3.70	ip igmp snooping	329
3.71	ip igmp ssm-range <ipv4 address>	330
3.72	ip igmp unknown-flooding	331
3.73	ip name-server	332
3.74	ip route	334
3.75	ip routing	335

Table 3-2. Global Configuration Mode Commands (Continued)

Sub-Section	Command	See Page …
3.76	ip source binding interface <interface> <vlan id> <ipv4 address> <mac address>	336
3.77	ip ssh	337
3.78	ip verify source	338
3.79	ipmc profile <name>	339
3.80	ipmc range <name>	340
3.81	ipv6 mld	341
3.82	json notification	342
3.83	lacp system-priority <priority>	344
3.84	line	345
3.85	lldp	346
3.86	lldp med	347
3.87	lldp med location-tlv	348
3.88	lldp med media-vlan-policy	351
3.89	logging	354
3.90	loop-protect	356
3.91	mac address-table	357
3.92	mep <instance> ais	358
3.93	mep <instance> aps <priority>	359
3.94	mep <instance> cc <priority>	360
3.95	mep <instance> ccm-tlv	361
3.96	mep <instance> client domain	362
3.97	mep <instance> dm <priority>	364
3.98	mep <instance> dm	366
3.99	mep <instance> down	367
3.100	mep <instance> lb <priority>	368
3.101	mep <instance> lck	370
3.102	mep <instance> level <level>	371
3.103	mep <instance> link-state-tracking	372
3.104	mep <instance> lm	373
3.105	mep <instance> lm-avail	376
3.106	mep <instance> lm-hli flr-threshold <number> interval <interval>	377

Table 3-2. Global Configuration Mode Commands (Continued)

Sub-Section	Command	See Page …
3.107	mep <instance> lm-notif	378
3.108	mep <instance> lm-sdeg	379
3.109	mep <instance> lt <priority>	380
3.110	mep <instance> meg-id <string>	381
3.111	mep <instance> mep-id <id>	382
3.112	mep <instance> mip	383
3.113	mep <instance> peer-mep-id <id>	385
3.114	mep <instance> performance-monitoring	386
3.115	mep <instance> syslog	387
3.116	mep <instance> tst <priority>	388
3.117	mep <instance> up	390
3.118	mep <instance> vid <vlan id>	391
3.119	mep os-tlv	392
3.120	monitor session	393
3.121	mvr	395
3.122	mvrp	397
3.123	ntp	398
3.124	poe capacitor-detect	399
3.125	poe management mode	400
3.126	poe ping-check	402
3.127	poe profile id	403
3.128	poe supply <value>	404
3.129	privilege <mode> level <level> <command string>	405
3.130	prompt <prompt>	406
3.131	ptp	407
3.132	ptp <instance>	408
3.133	ptp ext	410
3.134	ptp ho-spec	411
3.135	ptp io-pin <number>	412
3.136	ptp tc-internal mode <mode>	413
3.137	ptp system-time	414
3.138	qos map cos-dscp <value> dpl <value> dscp <value>	415

Table 3-2. Global Configuration Mode Commands (Continued)

Table 3-2. Global Configuration Mode Commands (Continued)

Sub-Section	Command	See Page …
3.171	svl fid <fid> vlan <vlan ids>	465
3.172	switchport vlan mapping	466
3.173	tacacs-server	467
3.174	tacacs-server host	468
3.175	thermal-protect grp <id> temperature <value>	469
3.176	udld	470
3.177	upnp	471
3.178	username	472
3.179	vlan <vlan id>	473
3.180	vlan ethertype s-custom-port <type>	474
3.181	vlan protocol eth2	475
3.182	vlan protocol llc <destination> <source> group <name>	476
3.183	vlan protocol snap	477
3.184	voice vlan	478
3.185	web privilege group	479

3.5 aaa accounting

Use the **aaa accounting** command to enable and configure the accounting parameters for use with authentication, authorization, and accounting (AAA) accounting services. Use the **no** form of this command to disable AAA accounting. Variations of this command include:

```
aaa accounting console tacacs exec
aaa accounting ssh tacacs exec
aaa accounting telnet tacacs exec
aaa accounting console tacacs commands <level>
aaa accounting ssh tacacs commands <level>
aaa accounting telnet tacacs commands <level>
```

3.5.1 Syntax Description

console	Specifies the configured accounting parameters are for console connections.
ssh	Specifies the configured accounting parameters are for Secure Shell (SSH) connections.
telnet	Specifies the configured accounting parameters are for telnet connections.
tacacs exec	Specifies that terminal access controller access-control system (TACACS+) servers keep accounting records of AAA executive information.
tacacs commands *<level>*	Specifies that TACACS+ servers keep accounting records of commands accessed that are equal to or above the specified privilege level. Valid range is **0** to **15**.

3.5.2 Default Values

By default, AAA accounting is disabled.

3.5.3 Command History

ASE Release 4.4-41	Command was introduced.

3.5.4 Usage Examples

The following example enables AAA accounting for commands entered from a telnet connection with a privilege level of 10 or higher:

```
(config)#aaa accounting telnet tacacs commands 10
```

3.6 aaa authentication login

Use the **aaa authentication login** command to enable authentication, authorization, and accounting (AAA) login authentication. Use the **no** form of this command to disable AAA authentication. Variations of this command include:

```
aaa authentication login console local
aaa authentication login console radius
aaa authentication login console tacacs
aaa authentication login http local
aaa authentication login http radius
aaa authentication login http tacacs
aaa authentication login ssh local
aaa authentication login ssh radius
aaa authentication login ssh tacacs
aaa authentication login telnet local
aaa authentication login telnet radius
aaa authentication login telnet tacacs
```

3.6.1 Syntax Description

console	Specifies the configured authentication parameters are for console connections.
http	Specifies the configured authentication parameters are for Hypertext Transfer Protocol (HTTP) connections.
ssh	Specifies the configured authentication parameters are for Secure Shell (SSH) connections.
telnet	Specifies the configured authentication parameters are for telnet connections.
local	Specifies using the local user name for authentication. User names must be in the local user name database to use this method.
radius	Specifies that all defined remote authentication dial-in user service (RADIUS) servers are used for authentication. RADIUS servers must be configured to use this method.
tacacs	Specifies that all defined terminal access controller access-control system plus (TACACS+) servers are used for authentication. TACACS+ servers must be configured to use this method.

3.6.2 Default Values

By default, AAA authentication is disabled.

3.6.3 Privilege Level

By default, this command has a privilege level of **15**.

3.6.4 Command History

ASE Release 4.4-41	Command was introduced.

3.6.5 Usage Examples

The following example enables AAA authentication for login on telnet connections using the local user name database for authentication:

```
(config)#aaa authentication login telnet local
```

3.7 aaa authorization

Use the **aaa authorization** command to enable and configure authorization, authentication, and accounting (AAA) authorization parameters. Use the **no** form of this command to disable AAA authorization. Variations of this command include:

```
aaa authorization console tacacs commands <level>
aaa authorization console tacacs commands <level> config-commands
aaa authorization ssh tacacs commands <level>
aaa authorization ssh tacacs commands <level> config-commands
aaa authorization telnet tacacs commands <level>
aaa authorization telnet tacacs commands <level> config-commands
```

3.7.1 Syntax Description

console	Specifies the configured authorization parameters are for console connections.
ssh	Specifies the configured authorization parameters are for Secure Shell (SSH) connections.
telnet	Specifies the configured authorization parameters are for telnet connections.
tacacs commands *<level>*	Specifies that terminal access controller access-control system (TACACS+) servers are used to authorize commands accessed that are equal to or above the specified privilege level. Valid range is **0** to **15**.
config-commands	Optional. Specifies that configuration commands are included in the authorization process.

3.7.2 Default Values

By default, AAA authorization is disabled.

3.7.3 Command History

ASE Release 4.4-41	Command was introduced.

3.7.4 Usage Examples

The following example enables AAA authentication for login on console connections and when commands equal to or above privilege level 8 are entered:

```
(config)#aaa authorization console tacacs commands 8
```

3.8 access management <*id*>

Use the **access management** <*id*> command to enable and configure access management on the ASE device. Use the **no** form of this command to disable the access management feature. Variations of this command include:

```
access management <id>
access management <id> <vlan id> <ipv4 address> all
access management <id> <vlan id> <ipv4 address> snmp
access management <id> <vlan id> <ipv4 address> telnet
access management <id> <vlan id> <ipv4 address> web
access management <id> <vlan id> <ipv6 address> all
access management <id> <vlan id> <ipv6 address> snmp
access management <id> <vlan id> <ipv6 address> telnet
access management <id> <vlan id> <ipv6 address> web
access management <id> <vlan id> <ipv4 address> to <ipv4 address>
```

3.8.1 Syntax Description

<id>	Specifies the ID of the access management entry. Valid range is **1** to **16**.
<vlan id>	Optional. Specifies the virtual local area network (VLAN) instance associated with the access management entry. Valid range is **1** to **4095**.
<ipv4 address>	Optional. Specifies a unicast Internet Protocol version 4 (IPv4) address for access management. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<ipv6 address>	Specifies a unicast Internet Protocol version 6 (IPv6) address for access management. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
all	Optional. Specifies access management is configured for all services on the switch.
snmp	Optional. Specifies that access management is configured for Simple Network Management Protocol (SNMP) services.
telnet	Optional. Specifies that access management is configured for telnet services.
web	Optional. Specifies that access management is configured for web services.
<ipv4 address> **to** *<ipv4 address>*	Optional. Specifies a range of IPv4 addresses used for access management. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

3.8.2 Default Values

By default, access management is not configured.

3.8.3 Privilege Level

By default, this command has a privilege level of **15**.

3.8.4 Command History

ASE Release 4.4-41	Command was introduced.

3.8.5 Usage Examples

The following example enables access management entry ID **1**:

```
(config)#access management 1
Switch access management mode is enabled

W: WEB/HTTPS
S: SNMP
T: TELNET/SSH

Idx VID  Start IP Address                End IP Address                W S T
--- ---  ------------------------------ ------------------------------ - - -
1   1    172.0.0.0                      172.255.255.255                N N Y
```

The following example enables access management by defining management entry ID **5**, associating it with VLAN **125**, and using it for all services associated with IP address **192.168.1.1** :

```
(config)#accesss management 5 125 192.168.1.1 all
```

3.9 access-list ace <*ace id*> action

Use the **access-list ace** <*ace id*> **action** command to specify the action taken when traffic matches a configured access control list (ACL). Use the **no** form of this command to remove the ACL action. Variations of this command include:

```
access-list ace <ace id> action deny
access-list ace <ace id> action permit
```

3.9.1 Syntax Description

<ace id>	Specifies the ACL ID. Valid range is **1** to **128**.
deny	Specifies that traffic matching the ACL is denied entry to the switch.
permit	Specifies that traffic matching the ACL is permitted to pass through the switch normally.

3.9.2 Default Values

By default, no ACLs are configured.

3.9.3 Privilege Level

By default, this command has a privilege level of **15**.

3.9.4 Command History

ASE Release 4.4-41	Command was introduced.

3.9.5 Usage Examples

The following example specifies that traffic matching ACL **75** is permitted:

```
(config)#access-list ace 75 action permit
```

3.10 access-list ace <*ace id*> dmac-type

Use the **access-list ace** <*ace id*> **dmac-type** command to specify the destination media access control (MAC) address type used by an access control list (ACL). Use the **no** form of this command to remove the destination MAC address type from the ACL. Variations of this command include:

```
access-list ace <ace id> dmac-type any
access-list ace <ace id> dmac-type broadcast
access-list ace <ace id> dmac-type multicast
access-list ace <ace id> dmac-type unicast
```

3.10.1 Syntax Description

<ace id>	Specifies the ACL ID. Valid range is **1** to **128**.
any	Specifies that any type of destination MAC is used.
broadcast	Specifies that a broadcast MAC address is used.
multicast	Specifies that a multicast MAC address is used.
unicast	Specifies that a unicast MAC address is used.

3.10.2 Default Values

By default, no ACLs are configured.

3.10.3 Privilege Level

By default, this command has a privilege level of **15**.

3.10.4 Command History

ASE Release 4.4-41	Command was introduced.

3.10.5 Usage Examples

The following example specifies that ACL **75** uses a **unicast** destination MAC address:

```
(config)#access-list ace 75 dmac-type unicast
```

3.11 access-list ace <*ace id*> frame-type

Use the **access-list ace** <*ace id*> **frame-type** command to specify the Ethernet frame types used by an access control list (ACL). Use the **no** form of this command to remove the specified frame type from the ACL. Variations of this command include:

```
access-list ace <ace id> frame-type any
access-list ace <ace id> frame-type arp
access-list ace <ace id> frame-type etype
access-list ace <ace id> frame-type ipv4
access-list ace <ace id> frame-type ipv4-icmp
access-list ace <ace id> frame-type ipv4-tcp
access-list ace <ace id> frame-type ipv4-udp
access-list ace <ace id> frame-type ipv6
access-list ace <ace id> frame-type ipv6-icmp
access-list ace <ace id> frame-type ipv6-tcp
access-list ace <ace id> frame-type ipv6-udp
```

3.11.1 Syntax Description

<ace id>	Specifies the ACL ID. Valid range is **1** to **128**.
any	Specifies that any type of Ethernet frame is used.
arp	Specifies that Address Resolution Protocol (ARP) frames are used.
etype	Specifies that EtherType frames are used.
ipv4	Specifies that Internet Protocol version 4 (IPv4) frames are used.
ipv4-icmp	Specifies that IPv4 Internet Control Message Protocol (ICMP) frames are used.
ipv4-tcp	Specifies that IPv4 Transmission Control Protocol (TCP) frames are used.
ipv4-udp	Specifies that IPv4 User Datagram Protocol (UDP) frames are used.
ipv6	Specifies that Internet Protocol version 6 (IPv6) frames are used.
ipv6-icmp	Specifies that IPv6 ICMP frames are used.
ipv6-tcp	Specifies that IPv6 TCP frames are used.
ipv6-udp	Specifies that IPv6 UDP frames are used.

3.11.2 Default Values

By default, no ACLs are configured.

3.11.3 Privilege Level

By default, this command has a privilege level of **15**.

3.11.4 Command History

ASE Release 4.4-41	Command was introduced.

3.11.5 Usage Examples

The following example configures ACL **75** to use IPv4 frames:

```
(config)#access-list ace 75 frame-type ipv4
```

3.12 access-list ace <*ace id*> ingress

Use the **access-list ace** <*ace id*> **ingress** command to specify a source interface for an access control list (ACL). Use the **no** form of this command to remove the source interface from the ACL. Variations of this command include:

```
access-list ace <ace id> ingress any
access-list ace <ace id> ingress interface <interface>
```

3.12.1 Syntax Description

<ace id>	Specifies the ACL ID. Valid range is **1** to **128**.
any	Specifies any interface as a source interface for the ACL.
interface *<interface>*	Specifies an interface as a source interface for the ACL. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **interface ?** for a complete list of valid interfaces.

3.12.2 Default Values

By default, no ACLs are configured.

3.12.3 Privilege Level

By default, this command has a privilege level of **15**.

3.12.4 Command History

ASE Release 4.4-41	Command was introduced.

3.12.5 Usage Examples

The following example specifies that the GigabitEthernet interface is used as a source interface for ACL **75**:

```
(config)#access-list ace 75 ingress interface GigabitEthernet 1/1
```

3.13 access-list ace <*ace id*> logging

Use the **access-list ace** <*ace id*> **logging** command to enable logging for an access control list (ACL). Use the **no** form of this command to disable logging for the ACL.

3.13.1 Syntax Description

<ace id>	Specifies the ACL ID. Valid range is **1** to **128**.

3.13.2 Default Values

By default, no ACLs are configured.

3.13.3 Privilege Level

By default, this command has a privilege level of **15**.

3.13.4 Command History

ASE Release 4.4-41	Command was introduced.

3.13.5 Usage Examples

The following example enables logging for ACL **75**:

```
(config)#access-list ace 75 logging
```

3.14 access-list ace <*ace id*> mirror

Use the **access-list ace** <*ace id*> **mirror** command to enable mirroring for an access control list (ACL). When mirroring is enabled, traffic matching the ACL is mirrored on a port specified in the mirroring configuration. Use the **no** form of this command to disable mirroring for the ACL.

3.14.1 Syntax Description

<ace id>	Specifies the ACL ID. Valid range is **1** to **128**.

3.14.2 Default Values

By default, no ACLs are configured.

3.14.3 Privilege Level

By default, this command has a privilege level of **15**.

3.14.4 Command History

ASE Release 4.4-41	Command was introduced.

3.14.5 Usage Examples

The following example enables mirroring for ACL **75**:

```
(config)#access-list ace 75 mirror
```

3.15 access-list ace <*ace id*> policy <*policy id*>

Use the **access-list ace** <*ace id*> **policy** <*policy id*> command to associate a configured access control list (ACL) to an access control policy (ACP). Use the **no** form of this command to remove the ACL association with the ACP.

3.15.1 Syntax Description

<ace id>	Specifies the ACL ID. Valid range is **1** to **128**.
<policy id>	Specifies the policy to which the ACL is assigned. Valid range is **0** to **127**.

3.15.2 Default Values

By default, no ACLs are configured or associated with any ACPs.

3.15.3 Privilege Level

By default, this command has a privilege level of **15**.

3.15.4 Command History

ASE Release 4.4-41	Command was introduced.

3.15.5 Usage Examples

The following example specifies that ACL **75** is associated with ACP **50**:

```
(config)#access-list ace 75 policy 50
```

3.16 access-list ace <*ace id*> rate-limiter <*id*>

Use the **access-list ace** <*ace id*> **rate-limiter** <*id*> to specify a rate limiter is assigned to the access control list (ACL). Use the no form of this command to remove the rate limiter from the ACL.

3.16.1 Syntax Description

<ace id>	Specifies the ACL ID. Valid range is **1** to **128**.
<id>	Specifies the rate limiter ID to assign to the ACL. Valid range is **0** to **16**.

3.16.2 Default Values

By default, no ACLs are configured or associated with any ACPs.

3.16.3 Privilege Level

By default, this command has a privilege level of **15**.

3.16.4 Command History

ASE Release 4.4-41	Command was introduced.

3.16.5 Usage Examples

The following example specifies that ACL **75** is assigned rate limiter **10**:

```
(config)#access-list ace 75 rate-limiter 10
```

3.17 access-list ace <*ace id*> redirect <*interface*>

Use the **access-list ace** <*ace id*> **redirect** <*interface*> command to specify that traffic matching a configured access control list (ACL) is redirected to another interface. Use the **no** form of this command to remove the redirect parameter from the ACL configuration.

3.17.1 Syntax Description

<ace id>	Specifies the ACL ID. Valid range is **1** to **128**.
<interface>	Specifies the interface to which to forward matching traffic. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID.

3.17.2 Default Values

By default, no ACLs are configured.

3.17.3 Privilege Level

By default, this command has a privilege level of **15**.

3.17.4 Command History

ASE Release 4.4-41	Command was introduced.

3.17.5 Usage Examples

The following example specifies that traffic matching ACL **75** is forwarded to the GigabitEthernet interface:

```
(config)#access-list ace 75 redirect GigabitEthernet 1/1
```

3.18 access-list ace <*ace id*> shutdown

Use the **access-list ace** <*ace id*> **shutdown** command to specify that when traffic matching the configured access control list (ACL) appears on the port, the port is shutdown. This feature only functions when non-virtual local area network (VLAN) tagged traffic packet length is less than 1518 bytes. Use the **no** form of this command to remove the shutdown feature from the ACL configuration.

3.18.1 Syntax Description

<ace id>	Specifies the ACL ID. Valid range is **1** to **128**.

3.18.2 Default Values

By default, no ACLs are configured.

3.18.3 Privilege Level

By default, this command has a privilege level of **15**.

3.18.4 Command History

ASE Release 4.4-41	Command was introduced.

3.18.5 Usage Examples

The following example specifies that traffic matching ACL **75** causes the port to shutdown:

```
(config)#access-list ace 75 shutdown
```

3.19 access-list ace <*ace id*> tag

Use the **access-list ace** <*ace id*> **tag** command to specify the type of virtual local area network (VLAN) tagged traffic matched by the access control list (ACL). Use the **no** form of this command to remove the tagged traffic criteria from the ACL configuration. Variations of this command include:

```
access-list ace <ace id> tag any
access-list ace <ace id> tag tagged
access-list ace <ace id> tag untagged
```

3.19.1 Syntax Description

<ace id>	Specifies the ACL ID. Valid range is **1** to **128**.
any	Specifies traffic with any type of VLAN tag is matched.
tagged	Specifies only traffic with a VLAN tag is matched.
untagged	Specifies only traffic without a VLAN tag is matched.

3.19.2 Default Values

By default, no ACLs are configured.

3.19.3 Privilege Level

By default, this command has a privilege level of **15**.

3.19.4 Command History

ASE Release 4.4-41	Command was introduced.

3.19.5 Usage Examples

The following example specifies that ACL **75** matches traffic with a VLAN tag only:

```
(config)#access-list ace 75 tag tagged
```

3.20 access-list ace <*ace id*> tag-priority

Use the **access-list ace** <*ace id*> **tag-priority** command to specify the priority of virtual local area network (VLAN) tagged traffic matched by the access control list (ACL). Use the **no** form of this command to remove the tagged traffic criteria from the ACL configuration. Variations of this command include:

```
access-list ace <ace id> tag-priority 0-1
access-list ace <ace id> tag-priority 0-3
access-list ace <ace id> tag-priority 2-3
access-list ace <ace id> tag-priority 4-5
access-list ace <ace id> tag-priority 4-7
access-list ace <ace id> tag-priority 6-7
access-list ace <ace id> tag-priority any
access-list ace <ace id> tag-priority <value>
```

3.20.1 Syntax Description

<ace id>	Specifies the ACL ID. Valid range is **1** to **128**.
0-1	Specifies that the ACL matches VLAN tagged traffic with a priority between **0** and **1**.
0-3	Specifies that the ACL matches VLAN tagged traffic with a priority between **0** and **3**.
2-3	Specifies that the ACL matches VLAN tagged traffic with a priority between **2** and **3**.
4-5	Specifies that the ACL matches VLAN tagged traffic with a priority between **4** and **5**.
4-7	Specifies that the ACL matches VLAN tagged traffic with a priority between **4** and **7**.
6-7	Specifies that the ACL matches VLAN tagged traffic with a priority between **6** and **7**.
any	Specifies that the ACL matches VLAN tagged traffic with any priority value.
<value>	Specifies that the ACL matches VLAN tagged traffic with a specified priority. Valid range is **0** to **7**.

3.20.2 Default Values

By default, no ACLs are configured.

3.20.3 Privilege Level

By default, this command has a privilege level of **15**.

3.20.4 Command History

ASE Release 4.4-41	Command was introduced.

3.20.5 Functional Notes

This command specifies the priority of VLAN tagged traffic that the ACL will match. Specifying the priority for tagged traffic is only necessary when the ACL is configured to match tagged VLAN traffic (refer to the command “access-list ace <ace id> tag” on page 270).

3.20.6 Usage Examples

The following example specifies that ACL **75** matches traffic with a VLAN tag priority of **3**:

```
(config)#access-list ace 75 tag-priority 3
```

3.21 access-list ace <*ace id*> vid

Use the **access-list ace** <*ace id*> **vid** command to specify an allowable virtual local area network (VLAN) for an access control list (ACL). Use the **no** form of this command to remove the VLAN from the ACL configuration. Variations of this command include:

```
access-list ace <ace id> vid any
access-list ace <ace id> vid <vlan id>
```

3.21.1 Syntax Description

<ace id>	Specifies the ACL ID. Valid range is **1** to **128**.
any	Specifies the ACL allows any VLANs.
<vlan id>	Specifies that the ACL allows a particular VLAN ID. Valid range is **1** to **4095**.

3.21.2 Default Values

By default, no ACLs are configured.

3.21.3 Privilege Level

By default, this command has a privilege level of **15**.

3.21.4 Command History

ASE Release 4.4-41	Command was introduced.

3.21.5 Usage Examples

The following example specifies that ACL **75** allows VLAN **125**:

```
(config)#access-list ace 75 vid 125
```

3.22 aggregation mode

Use the **aggregation mode** command to specify the Link Aggregation Group (LAG) and Link Aggregation Control Protocol (LACP) traffic forwarding mode. Use the **no** form of this command to return to the default value. Variations of this command include:

```
aggregation mode dmac
aggregation mode ip
aggregation mode port
aggregation mode smac
```

3.22.1 Syntax Description

dmac	Specifies that destination media access control (MAC) addresses are used by link aggregation in calculating traffic destinations.
ip	Specifies that Internet Protocol (IP) addresses are used by link aggregation in calculating traffic destinations.
port	Specifies that Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port numbers are used by link aggregation in calculating traffic destinations.
smac	Specifies that source MAC addresses are used by link aggregation in calculating traffic destinations.

3.22.2 Default Values

By default, destinations are determined by using IP addresses, port numbers, and source MAC addresses.

3.22.3 Command History

ASE Release 4.4-41	Command was introduced.

3.22.4 Privilege Level

By default, this command has a privilege level of **15**.

3.22.5 Functional Notes

All of the parameters for this command can be used to calculate traffic destinations, and they can be entered in any order.

3.22.6 Usage Examples

The following example specifies that destination MAC addresses will be used by link aggregation in calculating traffic destinations:

```
(config)#aggregation mode dmac
```

3.23 alarm *<alarm name> <alarm expression>*

Use the **alarm** *<alarm name> <alarm expression>* command to enable and configure alarms for the ASE device. Use the **no** form of this command to remove the alarm.

3.23.1 Syntax Description

<alarm name> <alarm expression>	Specifies the alarm name and expression. You can view valid alarm names and expressions by entering the **show alarm** command from the Enable mode prompt (refer to the command "show alarm" on page 96). Each alarm name begins with the word **alarm**, and is limited to **127** characters. Each alarm expression denotes the specific alarm as displayed in the **show alarm** command, entered in a string of no more than **255** characters in length. Enter alarms in the following manner: **`alarm.herlev.switch2.port28 mep.status.instance[2]@Cmeg==false`**

3.23.2 Default Values

By default, no alarms are configured.

3.23.3 Command History

ASE Release 4.4-41	Command was introduced.

3.23.4 Functional Notes

When an alarm is configured, its name is used to specify the alarm hierarchy. The root node is called alarm, meaning that all alarm names must start with **alarm**. Alarm status is inherited in the hierarchy, making it easy for a Network Management System (NMS) to filter alarms.

To configure an alarm, name the alarm and specify it's hierarchy using the format **`alarm.herlev.switch2.port28`**. Entering the **show alarm status** command will display the hierarchy of the alarm name. For example:

```
#show alarm status
alarmName                                          Active  Suppressed  ExposedActive
-------------------------------------------------  ------ ---------- -------------
alarm                                              false    false     false
alarm.herlev                                       false    false     false
alarm.herlev.switch2  alarm.herlev.switch2.port28 false    false     false
```

The alarm expression is determined by the specified alarm sources on the ASE device. Alarm sources are displayed using the **show alarm sources** command, as described *on page 96*. For example, displaying alarm sources that include maintenance entity points (MEPs) will return an alarm source of **`mep.status.instance[2]Cmeg`**. Adding the **`==false`** parameter to the alarm source specifies the alarm is not active.

Once the alarm is configured using the alarm <alarm name> <alarm expression> command, you can view the status of the configured alarm using the show alarm status. If an alarm is triggered, it will return a true value. If you want to suppress an active alarm, enter the **alarm suppress** command as described *on page 30*.

3.23.5 Usage Examples

For example, to configure an alarm for the MEG on port 28 of switch 2, enter the command as follows:

```
(config)#alarm alarm.herlev.switch2.port28 mep.status.instance[2]Cmeg==false
```

3.24 auto-link

Use the **auto-link** command to enable the auto-link feature, to specify the communication method between an ASE device and the n-Command® managed service provider (MSP) server, and to optionally specify the service name prefix of service (SRV) record requests. Communication can be either via Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol over Secure Socket Layer (HTTPS). Use the **no** form of this command to disable auto-link or to return to the default communication method. Variations of this command include:

```
auto-link
auto-link http
auto-link http srv <prefix>
auto-link https
auto-link https srv <prefix>
```

3.24.1 Syntax Description

http	Optional. Specifies that the client use the HTTP posting method.
https	Optional. Specifies that the client use the HTTPS posting method.
srv *<prefix>*	Optional. Specifies the service name prefix of SRV requests.

3.24.2 Default Values

By default, auto-link is disabled. By default, auto-link uses **HTTPS**. By default, if no service name prefix is configured, auto-link uses **_http** for HTTP communication, and **_https** for HTTPS communication.

3.24.3 Command History

ASE Release 4.4-41	Command was introduced.

3.24.4 Usage Examples

The following example enables auto-link:

```
(config)#auto-link
```

The following example specifies that the client use HTTP to communicate with the server:

```
(config)#auto-link http
```

3.25 auto-link penalty <*value*>

Use the **auto-link penalty** <*value*> command to enable and configure a temporary penalty list for auto-link configuration. The temporary penalty list blacklists hosts that cause repeated communication failures. If a server of configured IP address causes a failover event three consecutive times, it is added to the penalty list. Once added to the list, auto-link will not contact the server for a configured number of recontact intervals. Using the **no** form of this command removes the penalty list from the auto-link configuration.

3.25.1 Syntax Description

<value>	Specifies the number of recontact intervals that the server will stay on the penalty list. Valid range is **0** to **65535**. Using a value of **0** disables the penalty feature.

3.25.2 Default Values

By default, the penalty feature is disabled.

3.25.3 Command History

ASE Release 4.4-41	Command was introduced.

3.25.4 Functional Notes

Penalty lists can be based on IP addresses and port numbers. Host IP addresses and port numbers returned from DNS requests, as well as configured IP addresses and port numbers, can be penalized.

3.25.5 Usage Examples

The following example enables recontact interval penalties and specifies that penalized servers remain on the list for **30** recontact intervals:

```
(config)#auto-link penalty 30
```

3.26 auto-link recontact-interval <*value*>

Use the **auto-link recontact-interval** <*value*> command to specify the intervals between contact attempts between the ASE client and the n-Command® managed service provider (MSP) server. Use the **no** form of this command to return to the default value.

3.26.1 Syntax Description

<value>	Specifies the time in seconds between contact attempts. Range is **20** to **604800** seconds. Setting this value to **0** seconds disables the recontact feature.

3.26.2 Default Values

By default, the recontact interval is set to **3600** seconds.

3.26.3 Command History

ASE Release 4.4-41	Command was introduced.

3.26.4 Usage Examples

The following example sets the recontact interval to **7200** seconds:

```
(config)#auto-link recontact-interval 7200
```

3.27 auto-link server <*hostname* | *ip address*>

Use the **auto-link server** command to specify the contact information for the n-Command® managed service provider (MSP) server used by the ASE client. Use the **no** form of this command to remove the server from the client configuration. Variations of this command include:

```
auto-link server primary <hostname | ip address>
auto-link server primary <hostname | ip address> port <port>
auto-link server secondary <hostname | ip address>
auto-link server secondary <hostname | ip address> port <port>
```

3.27.1 Syntax Description

primary	Specifies the primary auto-link server. The primary server must be specified. Only one entry is allowed for the primary server.
secondary	Specifies the secondary auto-link server. Secondary servers are used in auto-link failover situations where the primary server is unavailable. Multiple secondary servers can be configured. The priority of secondary servers is determined by the order in which the servers are configured.
<hostname | ip address>	Specifies the server host name or IP address. IP addresses should be expressed in the decimal dotted notation (for example **10.10.10.1**).
port *<port>*	Optional. Specifies the port number used to communicate with the server. Valid range is **1** to **65535**.

3.27.2 Default Values

By default, no server is configured. When specified, the server uses port **80** for Hypertext Transfer Protocol (HTTP) and port **443** for HTTP secure (HTTPS).

3.27.3 Command History

ASE Release 4.4-41	Command was introduced.

3.27.4 Functional Notes

The host name or the IP address of the server with which the ASE product communicates must be specified for communication to take place. A primary server must be specified, and secondary servers can optionally be configured. Only one entry is allowed for the primary MSP server. To delete the primary MSP server, you must first remove all configured secondary servers.

3.27.5 Usage Examples

The following example specifies the ASE client will communicate with the primary n-Command MSP server at IP address **10.10.10.10**:

```
(config)#auto-link server primary 10.10.10.10
```

3.28 banner

Use the **banner** command to specify messages to be displayed in certain situations. Use the **no** form of this command to delete a previously configured banner. Variations of this command include:

banner exec *<delimiter> <message> <delimiter>*
banner login *<delimiter> <message> <delimiter>*
banner motd *<delimiter> <message> <delimiter>*

3.28.1 Syntax Description

exec	Creates a message to be displayed when any executive-level process takes place.
login	Creates a message to be displayed before the user name and password login prompts.
motd	Creates a message-of-the-day (MOTD) banner.
<delimiter>	Specifies the banner text delimiter. Press **Enter** after the delimiter character to begin input of banner text. After typing the banner message, enter the same delimiter character to end the message.
<message>	Specifies the text message you wish to display.

3.28.2 Default Values

By default, no banners are configured.

3.28.3 Command History

ASE Release 4.4-41	Command was introduced.

3.28.4 Functional Notes

Banners appear in the following order (if configured):

- MOTD banner appears at initial connection.
- Login banner follows the MOTD banner.
- Exec banner appears after successful login.

3.28.5 Usage Examples

The following example configures the system to display a message of the day:

```
(config)#banner motd *The system will be shut down today from 7PM to 11PM*
```

3.29 clock

Use the **clock** command to configure the system software clock for the ASE device. Use the **no** form of this command to disable the system clock. Variations of this command include:

```
clock summer-time <timezone> date <start month>
clock summer-time <timezone> date <start month> <offset>
clock summer-time <timezone> date <start month> <start day> <start year>
   <start time> <end month> <end day> <end year> <end time>
clock summer-time <timezone> date <start month> <start day> <start year>
   <start time> <end month> <end day> <end year> <end time> <offset>
clock summer-time <timezone> recurring <start week>
clock summer-time <timezone> recurring <start week> <offset>
clock summer-time <timezone> recurring <start week> <start weekday> <start month>
   <start time> <end week> <end weekday> <end month> <end time>
clock summer-time <timezone> recurring <start week> <start weekday> <start month>
   <start time> <end week> <end weekday> <end month> <end time> <offset>
clock timezone <timezone> <hours>
clock timezone <timezone> <hours> <minutes> <value>
```

3.29.1 Syntax Description

<timezone>	Specifies the clock's time zone by name. Refer to Section 3.29.5, "Functional Notes" on page 283 for accepted time zone keywords.
summer-time	Configures daylight savings time (DST) settings.
date	Configures the absolute DST settings.
recurring	Configures recurring DST settings.
<start month>	Specifies the month to begin applying DST settings. Valid range is **1** to **12**.
<start day>	Optional. Specifies the day of the month to begin applying DST settings. Valid range is **1** to **31**.
<start year>	Optional. Specifies the year to begin applying DST settings. Valid range is **2000** to **2097**.
<start time>	Optional. Specifies the time to begin applying DST settings. Enter time in *HH:MM* format.
<start week>	Optional. Specifies the week to begin applying recurring DST settings. Valid range is **1** to **5**.
<start weekday>	Optional. Specifies the weekday to begin applying recurring DST settings. Valid range is **1** to **7**.
<end month>	Optional. Specifies the month to cease applying DST settings. Valid range is **1** to **12**.
<end day>	Optional. Specifies the day of the month to cease applying DST settings. Valid range is **1** to **31**.
<end year>	Optional. Specifies the year to cease applying DST settings. Valid range is **2000** to **2097**.
<end time>	Optional. Specifies the time to cease applying DST settings. Enter time in *HH:MM* format.
<end week>	Optional. Specifies the week to cease applying recurring DST settings. Valid range is **1** to **5**.

<end weekday>	Optional. Specifies the weekday to cease applying recurring DST settings. Valid range is **1** to **7**.
<offset>	Optional. Specifies the time offset (in minutes) for DST settings. Valid range is **1** to **1439** minutes.
timezone	Configures the internal clock to the specified time zone.
<hours>	Specifies the time zone offset, in hours, from Coordinated Universal Time (UTC). Valid range is **-23** to **23** hours.
<minutes>	Optional. Specifies the time zone offset, in minutes, from UTC. Valid range is **0** to **59** minutes.
<value>	Optional. Specifies the sub-type of time zone. Valid range is **0** to **9**.

3.29.2 Default Values

No default values are necessary for this command.

3.29.3 Privilege Level

By default, this command has a privilege level of **13**.

3.29.4 Command History

ASE Release 4.4-41	Command was introduced.

3.29.5 Functional Notes

Table 3-3 describes the available time zone keywords to use for defining the *<timezone>* parameter and their hours offset from UTC.

Table 3-3. Timezone Keywords and their UTC Offset Hours

Time zone Keyword	UTC Offset (in hours)	Time zone Keyword	UTC Offset (in hours)
Amsterdam	1	Jerusalem	2
Belgrade	1	Baghdad	3
Brussels	1	Kuwait	3
Sarajevo	1	Moscow	3
West-Africa	1	Nairobi	3
Brisbane	10	Abu-Dhabi	4
Canberra	10	Baku	4
Guam	10	Ekaterinburg	5
Vladivostok	10	Islamabad	5
Auckland	12	Almaty	6
Fiji	12	Astana	6

Table 3-3. Timezone Keywords and their UTC Offset Hours

Time zone Keyword	UTC Offset (in hours)	Time zone Keyword	UTC Offset (in hours)
Athens	2	Sri-Jay	6
Bucharest	2	Bangkok	7
Cairo	2	Kranoyarsk	7
Harare	2	Bejing	8
Helsinki	2	Irkutsk	8
Kuala-Lumpur	8	Perth	8
Taipei	8	Osaka	9
Seoul	9	Yakustsk	9
Adelaide	9:30	Azores	-1
Cape-Verde	-1	Brasilia	-3
Buenos-Aires	-3	Greenland	-3
Atlantic-Time	-4	Caracus	-4
Santiago	-4	Bogota	-5
Eastern-Time	-5	Central-America	-6
Central-Time	-6	Mexico-City	-6
Saskatchewan	-6	Arizona	-7
Mountain-Time	-7		

3.29.6 Usage Examples

The following example configures the internal clock for the Taipei time zone:

```
(config)#clock timezone taipei 8
```

3.30 ddmi

Use the **ddmi** command to enable the discovery and dependency mapping information (DDMI) feature. Use the **no** form of this command to disable DDMI.

3.30.1 Syntax Description

No subcommands.

3.30.2 Default Values

No defaults are necessary for this command.

3.30.3 Command History

ASE Release 4.4-41	Command was introduced.

3.30.4 Usage Examples

The following example enables DDMI:

```
(config)#ddmi
```

3.31 dot1x authentication timer

Use the **dot1x authentication timer** command to configure port-based network access control authentication timer parameters. Use the **no** form of this command to disable the port-based network access control authentication timers. Variations of this command include:

```
dot1x authentication timer inactivity <time>
dot1x authentication timer re-authenticate <time>
```

3.31.1 Syntax Description

inactivity *<time>*	Specifies the time, in seconds, between inspections for activity of successfully authenticated media access control (MAC) addresses. Valid range is **10** to **1000000** seconds.
re-authenticate *<time>*	Specifies the re-authentication timer setting. Valid range is **1** to **3600** seconds.

3.31.2 Default Values

By default, port-based network access control authentication is disabled.

3.31.3 Privilege Level

By default, this command has a privilege level of **15**.

3.31.4 Command History

ASE Release 4.4-41	Command was introduced.

3.31.5 Usage Examples

The following example sets the inactivity timeout for port-based network access control authentication to **2000** seconds:

```
(config)#dot1x authentication timer inactivity 2000
```

3.32 dot1x feature

Use the **dot1x feature** command to enable port-based network access control on the ASE device for a specific feature. Use the **no** form of this command to disable network access control for the feature. Variations of this command include:

```
dot1x feature guest-vlan
dot1x feature radius-qos
dot1x feature radius-vlan
```

3.32.1 Syntax Description

guest-vlan	Enables network access control for the guest virtual local area network (VLAN).
radius-qos	Enables remote authentication dial-in user service (RADIUS)-assigned quality of service (QoS) network access control.
radius-vlan	Enables RADIUS-assigned VLAN network access control.

3.32.2 Default Values

By default, network access control is disabled for all features.

3.32.3 Privilege Level

By default, this command has a privilege level of **15**.

3.32.4 Command History

ASE Release 4.4-41	Command was introduced.

3.32.5 Usage Examples

The following example enables network access control for the guest VLAN:

```
(config)#dot1x feature guest-vlan
```

3.33 dot1x guest-vlan

Use the **dot1x guest-vlan** command to configure network access control parameters for the guest virtual local area network (VLAN). Use the **no** form of this command to return to the default settings. Variations of this command include:

```
dot1x guest-vlan <vlan id>
dot1x guest-vlan supplicant
```

3.33.1 Syntax Description

<vlan id>	Specifies the VLAN ID for the guest VLAN. Valid range is **1** to **4095**.
supplicant	Specifies that the ASE device remembers if an Extensible Authentication Protocol over local area network (LAN) (EAPOL) frame has been received on the port for the lifetime of the port.

3.33.2 Default Values

By default, the guest VLAN does not have network access control enabled. When guest VLAN network access control is enabled, the supplicant feature is disabled.

3.33.3 Privilege Level

By default, this command has a privilege level of **15**.

3.33.4 Command History

ASE Release 4.4-41	Command was introduced.

3.33.5 Functional Notes

Once the switch decides to enter the guest VLAN, it first checks whether the supplicant feature is enabled or disabled. When disabled, the switch enters the guest VLAN only if an EAPOL frame has not been received on the port for the lifetime of the port. If the feature is enabled, the switch considers entering the guest VLAN even if an EAPOL frame has been received on the port.

3.33.6 Usage Examples

The following example specifies that the guest VLAN for network access control is VLAN **175**:

```
(config)#dot1x guest-vlan 175
```

3.34 dot1x max-reauth-req <*number*>

Use the **dot1x max-reauth-req** <*number*> command to specify the number of times a Request Identity Extensible Authentication Protocol over local area network (LAN) (EAPOL) frame is sent in network access control operations without a response before entering a guest virtual local area network (VLAN). Use the **no** form of this command to disable this feature.

3.34.1 Syntax Description

<number>	Specifies the number of times a Request Identity EAPOL frame is sent without a response before entering the guest VLAN. Valid range is **1** to **255**.

3.34.2 Default Values

By default, network access control is disabled.

3.34.3 Privilege Level

By default, this command has a privilege level of **15**.

3.34.4 Command History

ASE Release 4.4-41	Command was introduced.

3.34.5 Usage Examples

The following example specifies that **8** Request Identity frames are sent before entering the guest VLAN:

```
(config)#dot1x max-reauth-req 8
```

3.35 dot1x re-authentication

Use the **dot1x re-authentication** command to enable network access control re-authentication. Use the **no** form of this command to disable the re-authentication feature.

3.35.1 Syntax Description

No subcommands.

3.35.2 Default Values

By default, network access control re-authentication is disabled.

3.35.3 Privilege Level

By default, this command has a privilege level of **15**.

3.35.4 Command History

ASE Release 4.4-41	Command was introduced.

3.35.5 Usage Examples

The following example enables network access control re-authentication:

```
(config)#dot1x re-authentication
```

3.36 dot1x system-auth-control

Use the **dot1x system-auth-control** command to enable the network access server used for network access control. Use the **no** form of this command to disable the network access server.

3.36.1 Syntax Description

No subcommands.

3.36.2 Default Values

By default, the network access server is disabled.

3.36.3 Privilege Level

By default, this command has a privilege level of **15**.

3.36.4 Command History

ASE Release 4.4-41	Command was introduced.

3.36.5 Usage Examples

The following example enables the network access server for use with network access control:

```
(config)#dot1x system-auth-control
```

3.37 dot1x timeout

Use the **dot1x timeout** command to configure the timeout period for network access control. Use the **no** form of this command to disable the network access control timeout settings. Variations of this command include:

```
dot1x timeout tx-period <time>
dot1x timeout tx-period <time> quiet-period <time>
dot1x timeout quiet-period <time>
```

3.37.1 Syntax Description

tx-period *<time>*	Specifies the time between Extensible Authentication Protocol over local area network (LAN) (EAPOL) retransmissions. Valid range is **1** to **65535** seconds.
quiet-period *<time>*	Specifies the time, in seconds, before a media access control (MAC) address that failed authentication can try again. Valid range is **10** to **1000000** seconds.

3.37.2 Default Values

By default, network access control is disabled and the timeout periods are not configured.

3.37.3 Privilege Level

By default, this command has a privilege level of **15**.

3.37.4 Command History

ASE Release 4.4-41	Command was introduced.

3.37.5 Usage Examples

The following example configures the time between MAC address authentication attempts is **20** seconds:

```
(config)#dot1x timeout quiet-period 20
```

3.38 enable

Use the **enable** command to configure Enable mode password parameters. Use the **no** form of this command to remove the Enable mode password configuration. Variations of this command include:

```
enable password level <level> <password>
enable password <password>
enable secret 0 level <level> <password>
enable secret 0 <password>
enable secret 5 level <level> <password>
enable secret 5 <password>
```

3.38.1 Syntax Description

password	Configures the Enable mode password.
level *<level>*	Optional. Specifies the privilege level associated with the password. Valid range is 1 to 15.
<password>	Specifies the clear-text password (unencrypted). Valid passwords cannot exceed 32 characters in length.
secret 0	Specifies that an unencrypted password is used for the privilege level secret.
secret 5	Specifies that an encrypted password is used for the privilege level secret.

3.38.2 Default Values

No default values are necessary for this command.

3.38.3 Command History

ASE Release 4.4-41	Command was introduced.

3.38.4 Usage Examples

The following example creates a password to enter the Enable mode:

```
(config)#enable password OPENSESAME
```

3.39 eps <*instance*> 1plus1

Use the **eps** <*instance*> **1plus1** command to configure an Ethernet Protection Switching (EPS) instance for EPS 1+1 architecture. Use the **no** form of this command to remove the EPS instance configuration. Variations of this command include:

```
eps <instance> 1plus1 bidirectional
eps <instance> 1plus1 unidirectional
eps <instance> 1plus1 unidirectional aps
```

3.39.1 Syntax Description

<instance>	Specifies the EPS instance. Valid range is **1** to **100**.
bidirectional	Specifies this instance uses the EPS 1+1 bidirectional protection.
unidirectional	Specifies this instance uses the EPS 1+1 unidirectional protection.
aps	Optional. Specifies this instance uses EPS 1+1 unidirectional protection with Automatic Protection Switching (APS).

3.39.2 Default Values

By default, EPS is disabled.

3.39.3 Command History

ASE Release 4.4-41	Command was introduced.

3.39.4 Usage Examples

The following example configures EPS instance **10** for EPS 1+1 bidirectional protection:

```
(config)#eps 10 1plus1 bidirectional
```

3.40 eps <*instance*> command

Use the **eps** <*instance*> **command** command to configure various Ethernet Protection Switching (EPS) commands for the EPS instance. Using the **no** form of this command disables the EPS command for the instance. Variations of this command include:

```
eps <instance> command exercise
eps <instance> command forced
eps <instance> command freeze
eps <instance> command lockout
eps <instance> command lockoutlocal
eps <instance> command manualp
eps <instance> command manualw
```

3.40.1 Syntax Description

<instance>	Specifies the EPS instance. Valid range is **1** to **100**.
exercise	Exercises the EPS protocol without affecting traffic. This parameter is only valid when the EPS instance uses bidirectional protection (as specified using the command "eps <instance> 1plus1" on page 294).
forced	Specifies that traffic is forced to switch from normal traffic to protected traffic.
freeze	Specifies that local EPS instances are frozen.
lockout	Specifies that EPS protection is locked out.
lockoutlocal	Specifies that EPS protection is locally locked out.
manualp	Manually switches normal traffic to protected traffic.
manualw	Manually switches normal traffic to working traffic.

3.40.2 Default Values

By default, EPS is not enabled and no EPS instances are configured.

3.40.3 Command History

ASE Release 4.4-41	Command was introduced.

3.40.4 Usage Examples

The following example specifies that EPS instance **10** switches normal traffic to protected traffic:

```
(config)#eps 10 command forced
```

3.41 eps <*instance*> domain

Use the **eps** <*instance*> **domain** command to configure various Ethernet Protection Switching (EPS) domain parameters. Use the **no** form of this command to remove the EPS domain configuration. Variations of this command include:

```
eps <instance> domain port architecture 1for1 work-flow <interface> protect-flow
    <interface>
eps <instance> domain port architecture 1for1 work-flow <interface> protect-flow
    <uint>
eps <instance> domain port architecture 1for1 work-flow <uint> protect-flow
    <interface>
eps <instance> domain port architecture 1for1 work-flow <uint> protect-flow <uint>
eps <instance> domain port architecture 1plus1 work-flow <interface> protect-flow
    <interface>
eps <instance> domain port architecture 1plus1 work-flow <interface> protect-flow
    <uint>
eps <instance> domain port architecture 1plus1 work-flow <uint> protect-flow
    <interface>
eps <instance> domain port architecture 1plus1 work-flow <uint> protect-flow <uint>

eps <instance> domain pw architecture 1for1 work-flow <interface> protect-flow
    <interface>
eps <instance> domain pw architecture 1for1 work-flow <interface> protect-flow
    <uint>
eps <instance> domain pw architecture 1for1 work-flow <uint> protect-flow
    <interface>
eps <instance> domain pw architecture 1for1 work-flow <uint> protect-flow <uint>
eps <instance> domain pw architecture 1plus1 work-flow <interface> protect-flow
    <interface>
eps <instance> domain pw architecture 1plus1 work-flow <interface> protect-flow
    <uint>
eps <instance> domain pw architecture 1plus1 work-flow <uint> protect-flow
    <interface>
eps <instance> domain pw architecture 1plus1 work-flow <uint> protect-flow <uint>
```

3.41.1 Syntax Description

<instance>	Specifies the EPS instance. Valid range is **1** to **100**.
port	Specifies this EPS instance is protecting in the port domain.
pw	Specifies this EPS instance is protecting the Multiprotocol Label Switching-Transport Profile (MPLS-TP) pseudo-wire domain.
architecture 1for1	Specifies the EPS 1 for 1 architecture is used.
architecture 1plus1	Specifies the EPS 1+1 architecture is used.
work-flow	Specifies the working flow instance to which the EPS is related.
protect-flow	Specifies the protecting flow instance to which the EPS is related.
<interface>	Optional. Specifies the interface to which the EPS work flow or protect flow is related. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a

	range of ports, or *<interface type> <id>* for a specific interface ID.
<uint>	Optional. Specifies the protected flow or work flow instance to which the EPS instance is related when not in the port domain. Valid range is **1** to **100**.

3.41.2 Default Values

By default, EPS is not configured.

3.41.3 Command History

ASE Release 4.4-41	Command was introduced.

3.41.4 Usage Examples

The following example specifies the EPS instance **3** is protecting in the port domain with 1 for 1 architecture with a work flow and protected flow for EPS instance 3:

```
(config)#eps 3 domain port architecture 1for1 work-flow 3 protect-flow 3
```

3.42 eps <*instance*> holdoff <*uint*>

Use the **eps** <*instance*> **holdoff** <*uint*> command to configure the Ethernet Protection Switching (EPS) instance hold-off timer. Use the **no** form of this command to return to the default timer setting.

3.42.1 Syntax Description

<instance>	Specifies the EPS instance. Valid range is **1** to **100**.
<uint>	Specifies the hold-off timer value in **100** ms increments. Valid range is **0** to **100** ms, with a maximum value of **10** seconds.

3.42.2 Default Values

By default, the hold-off timer is set to **0** ms.

3.42.3 Command History

ASE Release 4.4-41	Command was introduced.

3.42.4 Usage Example

The following example sets the EPS hold-off timer for EPS instance **3** to **5** seconds:

```
(config)#eps 3 holdoff 5000
```

3.43 eps <*instance*> mep-work <*uint*> mep-protect <*uint*> mep-aps <*uint*>

Use the **eps** <*instance*> **mep-work** command to configure the Ethernet Protection Switching (EPS) instance maintenance endpoint (MEP) work, protection, and Automatic Protection Switching (APS) instances. Use the **no** form of this command to remove the MEP configuration for the EPS instance.

3.43.1 Syntax Description

<instance>	Specifies the EPS instance. Valid range is **1** to **100**.
mep-work *<uint>*	Specifies the working MEP instance number. Valid range is **1** to **100**.
mep-protect *<uint>*	Specifies the protecting MEP instance number. Valid range is **1** to **100**.
mep-aps *<uint>*	Specifies the APS MEP instance. Valid range is **1** to **100**.

3.43.2 Default Values

By default, EPS is not configured for any MEP instances.

3.43.3 Command History

ASE Release 4.4-41	Command was introduced.

3.43.4 Usage Examples

The following example specifies the working, protecting, and APS MEP instances for EPS instance **3**:

```
(config)#eps 3 mep-work 2 mep-protect 4 mep-aps 5
```

3.44 eps <*instance*> revertive

Use the **eps** <*instance*> **revertive** command to configure the Ethernet Protection Switching (EPS) instance wait-to-restore (WTR) value for revertive behavior. Use the **no** form of this command to disable the revertive behavior. Variations of this command include:

```
eps <instance> revertive 10m
eps <instance> revertive 10s
eps <instance> revertive 11m
eps <instance> revertive 11s
eps <instance> revertive 12m
eps <instance> revertive 30s
eps <instance> revertive 5m
eps <instance> revertive 6m
eps <instance> revertive 7m
eps <instance> revertive 8m
eps <instance> revertive 9m
eps <instance> revertive wtr-value <value>
```

3.44.1 Syntax Description

<instance>	Specifies the EPS instance. Valid range is **1** to **100**.
10m	Specifies WTR value is 10 minutes.
10s	Specifies WTR value is 10 seconds.
11m	Specifies WTR value is 11 minutes.
11s	Specifies WTR value is 11 seconds.
12m	Specifies WTR value is 12 minutes.
30s	Specifies WTR value is 30 seconds.
5m	Specifies WTR value is 5 minutes.
6m	Specifies WTR value is 6 minutes.
7m	Specifies WTR value is 7 minutes.
8m	Specifies WTR value is 8 minutes.
9m	Specifies WTR value is 9 minutes.
wtr-value *<value>*	Specifies WTR as a value. Valid range is **1** to **720** seconds.

3.44.2 Default Values

By default, EPS revertive behavior is disabled.

3.44.3 Command History

ASE Release 4.4-41	Command was introduced.

3.44.4 Usage Examples

The following example configures the WTR value as **9m** for EPS instance **3**:

```
(config)#eps 3 revertive 9m
```

3.45 erps <*group*> guard <*value*>

Use the **erps** <*group*> **guard** <*value*> to specify the Ethernet Ring Protection Switching (ERPS) guard time. Use the **no** form of this command to return to the default value.

3.45.1 Syntax Description

<group>	Specifies the ERPS group. Valid range is **1** to **64**.
<value>	Specifies the ERPS guard time for the group in ms. Valid rage is **10** to **2000** ms.

3.45.2 Default Values

By default, the ERPS guard time is set to **10** ms.

3.45.3 Command History

ASE Release 4.4-41	Command was introduced.

3.45.4 Usage Examples

The following example sets the ERPS guard time as **100** ms for ERPS group **2**:

```
(config)#erps 2 guard 100
```

3.46 erps <*group*> holdoff <*value*>

Use the **erps** <*group*> **holdoff** <*value*> command to configure the Ethernet Ring Protection Switching (ERPS) group hold-off timer value. Use the **no** form of this command to return to the default setting.

3.46.1 Syntax Description

<group>	Specifies the ERPS group. Valid range is **1** to **64**.
<value>	Specifies the ERPS hold-off time for the group in ms. Valid rage is **0** to **10000** ms.

3.46.2 Default Values

By default, the ERPS group hold-off timer is set to **0** ms.

3.46.3 Command History

ASE Release 4.4-41	Command was introduced.

3.46.4 Usage Examples

The following example sets the ERPS hold-off time as **1000** ms for ERPS group **2**:

```
(config)#erps 2 holdoff 1000
```

3.47 erps <*group*> major port0

Use the **erps major** <*group*> **port0** command to configure the port interfaces for the major Ethernet Ring Protection Switching (ERPS) group. Use the **no** form of this command to remove the port interfaces from the ERPS group configuration. Variations of this command include:

```
erps <group> major port0 interface <interface> port1 interface <interface>
erps <group> major port0 interface <interface> port1 interface <interface>
    interconnect
```

3.47.1 Syntax Description

<group>	Specifies the ERPS group. Valid range is **1** to **64**.
port0	Specifies the ERPS port 0 interface is being configured.
port1	Specifies the ERPS port 1 interface is being configured.
interface *<interface>*	Specifies the interface to use as the ERPS port 0 or port 1 interface. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **erps** *<group>* **port0 interface ?** for a complete list of valid interfaces.
interconnect	Optional. Specifies that the major ring is interconnected.

3.47.2 Default Values

By default, ERPS is not configured.

3.47.3 Command History

ASE Release 4.4-41	Command was introduced.

3.47.4 Usage Examples

The following example configures the port 0 and port 1 interfaces for the major ERPS group **2**:

```
(config)#erps 2 major port0 interface GigabitEthernet 1/1 port1 interface
    GigabitEthernet 1/2
```

3.48 erps <*group*> mep port0 sf <*index*> aps <*index*> port1 sf <*index*> aps <*index*>

Use the **erps** <*group*> **mep** command to configure the signal fail and Automatic Protection Switching (APS) index for the Ethernet Ring Protection Switching (ERPS) maintenance endpoint (MEP) port 0 and port 1 interfaces. Use the **no** form of this command to remove the MEP port 0 and port 1 values from the ERPS group.

3.48.1 Syntax Description

<group>	Specifies the ERPS group. Valid range is **1** to **64**.
port0	Specifies the ERPS port 0 interface is being configured.
port1	Specifies the ERPS port 1 interface is being configured.
sf *<index>*	Specifies the signal fail index for the MEP. Valid range is **1** to **3124**.
aps *<index>*	Specifies the APS index for the MEP. Valid range is **1** to **3124**.

3.48.2 Default Values

By default, ERPS is not configured.

3.48.3 Command History

ASE Release 4.4-41	Command was introduced.

3.48.4 Usage Examples

The following example specifies the signal fail and APS index for port 0 and port 1 interfaces on the MEP associated with ERPS group **2**:

```
(config)#erps 2 mep port0 sf 200 aps 150 sf 100 aps 151
```

3.49 erps <*group*> revertive <*time*>

Use the **erps** <*group*> **revertive** <*time*> command to configure the time before an Ethernet Ring Protection Switching (ERPS) group is restored. Use the **no** form of this command to return to the default value.

3.49.1 Syntax Description

<group>	Specifies the ERPS group. Valid range is **1** to **64**.
<time>	Specifies the time before the ERPS group is restored. Valid range is **1** to **12** minutes.

3.49.2 Default Values

By default, the restore time for an ERPS group is set to **1** minute.

3.49.3 Command History

ASE Release 4.4-41	Command was introduced.

3.49.4 Usage Examples

The following example configures the restore time for ERPS group **2** as **3** minutes:

```
(config)#erps 2 revertive 3
```

3.50 erps <*group*> rpl

Use the **erps** <*group*> **rpl** command to configure the ring protection link (RPL) parameters for the Ethernet Ring Protection Switching (ERPS) group. Use the **no** form of this command to remove the RPL configuration from the ERPS group. Variations of this command include:

```
erps <group> rpl neighbor port0
erps <group> rpl neighbor port1
erps <group> rpl owner port0
erps <group> rpl owner port1
```

3.50.1 Syntax Description

<*group*>	Specifies the ERPS group. Valid range is **1** to **64**.
neighbor	Specifies the ERPS group operates in a neighbor role.
owner	Specifies the ERPS group operates in an owner roe.
port0	Specifies the role applies to the port 0 interface.
port1	Specifies the role applies to the port 1 interface.

3.50.2 Default Values

By default, no ERPS groups are configured.

3.50.3 Command History

ASE Release 4.4-41	Command was introduced.

3.50.4 Usage Examples

The following example specifies that ERPS group 2 applies the RPL neighbor role to the port 1 interface:

```
(config)#erps 2 rpl neighbor port1
```

3.51 erps <*group*> sub port0

Use the **erps** <*group*> **sub port0** command to configure the Ethernet Ring Protection Switching (ERPS) sub-ring parameters. Use the **no** form of this command to remove the sub-ring configuration. Variations of this command include:

erps *<group>* **sub port0 interface** *<interface>* **interconnect** *<group>* **interface** *<interface>*
erps *<group>* **sub port0 interface** *<interface>* **interconnect** *<group>* **virtual-channel interface** *<interface>* **virtual-channel**

3.51.1 Syntax Description

<group>	Specifies the ERPS group. Valid range is **1** to **64**.
port0	Specifies the ERPS port 0 interface is being configured.
interface *<interface>*	Specifies the interface to use as the ERPS port 0 or port 1 interface. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **erps** *<group>* **sub port0 interface ?** for a complete list of valid interfaces.
interconnect *<group>*	Specifies the major ring to which the sub-ring is interconnected. Valid range is **1** to **64**.
virtual-channel	Optional. Enables the virtual channel for the sub-ring.

3.51.2 Default Values

By default, no ERPS sub-rings are configured.

3.51.3 Command History

ASE Release 4.4-41	Command was introduced.

3.51.4 Usage Examples

The following example specifies that the sub-ring for ERPS group 2 uses the virtual channel:

```
(config)#erps 2 sub port0 interface GigabitEthernet 1/1 interconnect 3 interface
   GigabitEthernet 1/2 virtual-channel
```

3.52 erps <*group*> topology-change propagate

Use the **erps** <*group*> **topology-change propagate** command to enable topology change messages from the Ethernet Ring Protection Switching (ERPS) group. Use the **no** form of this command to disable the feature.

3.52.1 Syntax Description

<group>	Specifies the ERPS group. Valid range is **1** to **64**.

3.52.2 Default Values

By default, topology change messages are not propagated from the ERPS group.

3.52.3 Command History

ASE Release 4.4-41	Command was introduced.

3.52.4 Usage Examples

The following example enables topology change messages for ERPS group 2:

```
(config)#erps 2 topology-change propagate
```

3.53 erps <*group*> version

Use the **erps** <*group*> **version** command to specify which Ethernet Ring Protection Switching (ERPS) version the group uses. Use the **no** form of this command to return to the default setting. Variations of this command include:

erps *<group>* **version 1**
erps *<group>* **version 2**

3.53.1 Syntax Description

<group>	Specifies the ERPS group. Valid range is **1** to **64**.
version 1	Specifies ERPS version 1 is used.
version 2	Specifies ERPS version 2 is used.

3.53.2 Default Values

By default, ERPS version 1 is used.

3.53.3 Command History

ASE Release 4.4-41	Command was introduced.

3.53.4 Usage Examples

The following example specifies that ERSP version 2 is used for ERPS group 2:

```
(config)#erps 2 version 2
```

3.54 erps <*group*> vlan

Use the **erps** <*group*> **vlan** command to configure the virtual local area networks (VLANs) associated with the Ethernet Ring Protection Switching (ERPS) group. Use the **no** form of this command to return to the default settings. Variations of this command include:

```
erps <group> vlan add <vlan ids>
erps <group> vlan remove <vlan ids>
erps <group> vlan none
erps <group> vlan <vlan ids>
```

3.54.1 Syntax Description

<group>	Specifies the ERPS group. Valid range is **1** to **64**.
add	Specifies VLANs to add to the ERPS group.
remove	Specifies VLANs to remove from the ERPS group.
none	Specifies that no VLANs are allowed within the ERPS group.
<vlan ids>	Specifies VLANs to associate with the ERPS group. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

3.54.2 Default Values

By default, all VLANs are allowed within an ERPS group.

3.54.3 Command History

ASE Release 4.4-41	Command was introduced.

3.54.4 Usage Examples

The following example specifies that no VLANs are allowed within the ERPS group 2:

```
(config)#erps 2 vlan none
```

3.55 green-ethernet eee optimize-for-power

Use the **green-ethernet eee optimize-for-power** command to configure power reduction on the ASE device. This command specifies that EEE is optimized for the least power consumption by powering down physical layer links (PHYs) when there is no traffic. Use the **no** form of this command to return to the default setting.

3.55.1 Syntax Description

No subcommands.

3.55.2 Default Values

By default, power reduction on the ASE device is optimized for least traffic latency.

3.55.3 Privilege Level

By default, this command has a privilege level of **15**.

3.55.4 Command History

ASE Release 4.4-41	Command was introduced.

3.55.5 Usage Examples

The following enables power reduction to operate using least power consumption:

```
(config)#green-ethernet eee optimize-for-power
```

3.56 gvrp

Use the **gvrp** command to enable and configure Generic virtual local area network (VLAN) Registration Protocol (GVRP) on the ASE device. Use the **no** form of this command to disable GVRP or return to the default settings. Variations of this command include:

```
gvrp
gvrp max-vlans <number>
gvrp time join-time <value>
gvrp time leave-time <value>
gvrp time leave-all-time <value>
```

3.56.1 Syntax Description

max-vlans *<value>*	Configure the maximum number of VLANs that can be simultaneously supported by GVRP. Valid range is **1** to **4094**.
join-time *<value>*	Configures the GVRP join-timer, which specifies the interval between declarations of new attributes in GVRP protocol data units (PDUs). Valid range is **1** to **20** centiseconds.
leave-time *<value>*	Specifies how long after a leave message is received before a VLAN attribute is deregistered. Valid range is **60** to **300** centiseconds.
leave-all-time *<value>*	Configures the GVRP LeaveAll timer, which specifies how long after a VLAN attribute has been GVRP-enabled before it sends a LeaveAll message. Once the LeaveAll message is sent, the LeaveAll timer starts again. Valid range is **1000** to **5000** centiseconds.

3.56.2 Default Values

By default, GVRP is disabled. When enabled, the maximum number of supported VLANs is 20, the join-timer is set to **20** centiseconds, the leave timer is set to **60** centiseconds, and the LeaveAll timer is set to **1000** centiseconds.

3.56.3 Privilege Level

By default, this command has a privilege level of **15**.

3.56.4 Command History

ASE Release 4.4-41	Command was introduced.

3.56.5 Functional Notes

For GVRP to function correctly, it must be enabled globally on the switch using the gvrp command, and also on the interface using the command “gvrp” on page 504.

When specifying the maximum number of VLANs supported by GVRP, you should specify this number before enabling GVRP on the switch.

Caution should be exercised when adjusting GVRP timers. All GVRP timers across any GVRP-enabled devices on the network must be set to the same value. In addition, any adjustments to the maximum number of VLANs simultaneously controlled by GVRP should be made before enabling GVRP on the switch.

You can enter the timer parameters in any order using this command. You can also configure all timers with a single command by entering the command as follows: **gvrp time join-time 14 leave-all-time 1500 leave-time 70**.

3.56.6 Usage Examples

The following example disables GVRP on the switch (if it has been enabled):

```
(config)#no gvrp
```

The following example specifies the maximum number of supported VLANs for GVRP:

```
(config)#gvrp max-vlans 200
```

The following example configures all the GVRP timers simultaneously:

```
(config)#gvrp time join-time 14 leave-all-time 1500 leave-time 70
```

The following example enables GVRP on the switch:

```
(config)#gvrp
```

3.57 hostname <*hostname*>

Use the **hostname** <*hostname*> command to configure a host name for the system's network. Use the **no** form of this command to remove the host name.

3.57.1 Syntax Description

<hostname>	Specifies the system's network host name. The host name can be any combination of numbers and letters as long as it is not a valid IP address or does not exceed 256 characters.

3.57.2 Default Values

By default, no host name is set for the system's network.

3.57.3 Command History

ASE Release 4.4-41	Command was introduced.

3.57.4 Usage Examples

The following example configures a host name for the ASE device:

```
(config)#hostname MYSYSTEM1
```

3.58 interface

Use the interface command to activate the interface command set for the specified physical or virtual interface on an ASE device. Type **interface ?** for a complete list of valid interface types on the unit. Use the **no** form of this command to delete a configured interface. Variations of this command include:

```
interface *
interface GigabitEthernet <slot/port>
interface 10GigabitEthernet <slot/port>
interface llag <id>
interface vlan <vlan ids>
```

3.58.1 Syntax Description

*****	Specifies all ports on the GigabitEthernet or 10 GigabitEthernet interfaces.
GigabitEthernet	Identifies a 1 GigabitEthernet interface.
10GigabitEthernet	Identifies a 10 GigabitEthernet interface. This option is not available on 8-port ASEs.
<slot/port>	Specifies the slot and port for the GigabitEthernet and 10GigabitEthernet interfaces. For a single port enter the , *<slot/port>*, for a range of ports, enter *<slot/port-slot/port>*. Slot and port number ranges are dependent upon the hardware installed in the unit. Port ranges available for 48-port ASEs are 1/1-49 or 1/1-4. Port ranges available for 24-port ASEs are 1/1-24 or 1/1-2. Port range available for 8-port ASEs is 1/1-10. Type **interface GigabitEthernet ?** or **interface 10GigabitEthernet ?** for information regarding valid ranges.
llag *<id>*	Identifies a Local Link Aggregation (LLAG) interface. Valid range is **1** to **5**.
vlan *<vlan ids>*	Identifies a virtual local area network (VLAN) interface. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

3.58.2 Default Values

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

3.58.3 Command History

ASE Release 4.4-41	Command was introduced.

3.58.4 Usage Examples

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

For a GigabitEthernet interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#
```

For a LLAG interface:

```
(config)#interface llag 2
(config-llag)#
```

For a VLAN interface:

```
(config)#interface vlan 75
(config-if-vlan)#
```

3.59 ip arp

Use the **ip arp** command to enable Internet Protocol version 4 (IPv4) Address Resolution Protocol (ARP) inspection on the ASE device and to configure static ARP table entries. Use the **no** form of this command to disable ARP inspection or remove static ARP entries from the ARP table. Variations of this command include:

```
ip arp inspection
ip arp inspection entry interface <interface> <vlan id> <mac address> <ipv4 address>
ip arp inspection translate
ip arp inspection translate interface <interface> <vlan id> <mac address> <ipv4
   address>
ip arp inspection vlan <vlan ids>
ip arp inspection vlan <vlan ids> logging all
ip arp inspection vlan <vlan ids> logging deny
ip arp inspection vlan <vlan ids> logging permit
```

3.59.1 Syntax Description

entry	Specifies a static entry to add to the ARP table.
translate	Specifies that ARP translates all ARP inspection table entries.
interface *<interface>*	Specifies the interface on which the ARP inspection or translation occurs. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **ip arp inspection entry interface ?** for a complete list of valid interfaces.
<vlan id>	Specifies the virtual local area network (VLAN) on which the ARP inspection or translation occurs. Valid range is **1** to **4095**.
<mac address>	Specifies a valid 48-bit unicast medium access control (MAC) address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
<ipv4 address>	Specifies a valid unicast IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
vlan *<vlan ids>*	Enables ARP inspection on the specified VLANs. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.
logging	Optional. Enables ARP inspection logging for the specified VLAN(s).
all	Specifies that all ARP inspection entries are logged.
deny	Specifies that all ARP inspection denied entries are logged.
permit	Specifies that all ARP inspection permitted entries are logged.

3.59.2 Default Values

No default values are necessary for this command.

3.59.3 Privilege Level

By default, this command has a privilege level of **13**.

3.59.4 Command History

ASE Release 4.4-41 Command was introduced.

3.59.5 Usage Examples

The following example enters the IP address and MAC address into the ARP table that is located on the GigabitEthernet interface within VLAN 150:

```
(config)#ip arp inspection entry interface GigabitEthernet 1/1 150 00:A0:C8:00:00:01
    10.10.10.1
```

3.60 ip dhcp excluded-address

Use the **ip dhcp excluded-address** command to specify IPv4 addresses that cannot be assigned to Dynamic Host Configuration Protocol version 4 (DHCPv4) clients. Use the **no** form of this command to remove a configured IPv4 address restriction. Variations of this command include:

ip dhcp excluded-address *<start ipv4 address>*
ip dhcp excluded-address *<start ipv4 address> <end ipv4 address>*

3.60.1 Syntax Description

<start ipv4 address>	Specifies the lowest IPv4 address in the range OR a single IPv4 address to be excluded.
<end ipv4 address>	Optional. Specifies the highest IPv4 address in the range. This field is not required when specifying a single IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

3.60.2 Default Values

By default, there are no excluded IPv4 addresses.

3.60.3 Privilege Level

By default, this command has a privilege level of **13**.

3.60.4 Command History

ASE Release 4.4-41	Command was introduced.

3.60.5 Usage Examples

The following example excludes an IPv4 address of **172.22.5.100** and the range of IPv4 addresses **172.22.5.200** through **172.22.5.250**:

```
(config)#ip dhcp excluded-address 172.22.5.100
(config)#ip dhcp excluded-address 172.22.5.200 172.22.5.250
```

3.61 ip dhcp pool <*name*>

Use the **ip dhcp pool** <*name*> command to create a Dynamic Host Control Protocol version 4 (DHCPv4) server address pool and enter the pool's configuration mode. The server pool is used to define the information to be assigned to DHCPv4 clients by the DHCPv4 server. The pool chosen to serve a specific client's request is determined by the current pool selection algorithm. Refer to the "DHCPv4 Server Pool Command Set" on page 634 for more information.

3.61.1 Syntax Description

<name>	Specifies the name of the DHCPv4 server address pool using an alphanumeric string (up to 32 characters in length).

3.61.2 Default Values

By default, there are no configured DHCPv4 address pools.

3.61.3 Command History

ASE Release 4.4-41	Command was introduced.

3.61.4 Functional Notes

Use the **ip dhcp pool** command to create multiple DHCPv4 server address pools for various segments of the network. Multiple address pools can be created to service different segments of the network with tailored configurations.

3.61.5 Usage Examples

The following example creates a DHCPv4 server address pool (labeled **SALES**) and enters the DHCPv4 server pool's configuration mode:

```
(config)#ip dhcp pool SALES
(config-dhcp-pool)#
```

3.62 ip dhcp relay information

Use the **ip dhcp relay information** to enable Internet Protocol version 4 (IPv4) Dynamic Host Control Protocol version 4 (DHCPv4) relay information mode (Option 82). Option 82 adds a layer of security to DHCPv4 by preventing DHCPv4 client requests from untrusted devices. In addition, this command can be used to configure a policy for handling DHCPv4 messages received that already contain DHCPv4 relay information. Use the **no** form of this command to disable DHCPv4 Option 82. Variations of this command include:

```
ip dhcp relay information option
ip dhcp relay information policy drop
ip dhcp relay information policy keep
ip dhcp relay information policy replace
```

3.62.1 Syntax Description

option	Enables the DHCPv4 Option 82.
policy	Creates the policy for handling DHCPv4 messages received that already contain DHCPv4 relay information.
drop	Specifies the packet is dropped.
keep	Specifies the DHCPv4 relay information is kept.
replace	Specifies the DHCPv4 relay information is replaced.

3.62.2 Default Values

By default, DHCPv4 relay information mode is disabled.

3.62.3 Privilege Level

By default, this command has a privilege level of **15**.

3.62.4 Command History

ASE Release 4.4-41	Command was introduced.

3.62.5 Usage Examples

The following example enables DHCPv4 relay information mode Option 82:

```
(config)#ip dhcp relay information option
```

3.63 ip dhcp server

Use the **ip dhcp server** command to enable the Internet Protocol version 4 (IPv4) Dynamic Host Control Protocol version 4 (DHCPv4) server on the ASE device. Use the **no** form of this command to disable the DHCPv4 server.

3.63.1 Syntax Description

No subcommands.

3.63.2 Default Values

By default, the DHCPv4 server is disabled.

3.63.3 Privilege Level

By default, this command has a privilege level of **13**.

3.63.4 Command History

ASE Release 4.4-41	Command was introduced.

3.63.5 Usage Examples

The following example enables the DHCPv4 server on the ASE device:

```
(config)#ip dhcp server
```

3.64 ip dhcp snooping

Use the **ip dhcp snooping** command to enable Internet Protocol version 4 (IPv4) Dynamic Host Control Protocol version 4 (DHCPv4) snooping on the ASE device. Use the **no** form of this command to disable DHCPv4 snooping.

3.64.1 Syntax Description

No subcommands.

3.64.2 Default Values

By default, DHCPv4 snooping is disabled.

3.64.3 Privilege Level

By default, this command has a privilege level of **15**.

3.64.4 Command History

ASE Release 4.4-41	Command was introduced.

3.64.5 Usage Examples

The following example enables DHCPv4 snooping:

```
(config)#ip dhcp snooping
```

3.65 ip dns proxy

Use the **ip dns proxy** command to enable domain naming system (DNS) proxy for the ASE device. This enables the device to act as a proxy for other units on the network. Use the **no** form of this command to disable this feature.

3.65.1 Syntax Description

No subcommands.

3.65.2 Default Values

By default, this feature is disabled.

3.65.3 Privilege Level

By default, this command has a privilege level of **15**.

3.65.4 Command History

ASE Release 4.4-41	Command was introduced.

3.65.5 Usage Examples

The following example enables the DNS proxy for the ASE device:

```
(config)#ip dns proxy
```

3.66 ip domain name <*domain name*>

Use the **ip domain name** command to define a default Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6) domain name to be used by the ASE device to resolve host names. Use the **no** form of this command to disable this function. Variations of this command include:

```
ip domain name <domain name>
ip domain name dchp ipv4
ip domain name dhcp ipv6
ip domain name dhcp interface vlan <vlan id>
```

3.66.1 Syntax Description

<domain name>	Specifies the default IPv4 or IPv6 domain name used to resolve unqualified host names. Do not include the initial period that separates the unresolved name from the default domain name.
dhcp ipv4	Specifies the domain naming system (DNS) setting is derived from Dynamic Host Control Protocol version 4 (DHCPv4).
dhcp ipv6	Specifies the DNS settings is derived from DHCP version 6 (DHCPv6).
dhcp interface vlan *<vlan id>*	Specifies the DHCP virtual local are network (VLAN) interface from which to derive DNS settings.Valid range is **1** to **4095**.

3.66.2 Default Values

By default, this feature is disabled. When enabled, DNS settings are derived from DHCPv6.

3.66.3 Command History

ASE Release 4.4-41	Command was introduced.

3.66.4 Usage Examples

The following example defines **adtran** as the default domain name:

```
(config)#ip domain name adtran
```

3.67 ip helper-address <*ipv4 address*>

Use the **ip helper-address** <*ipv4 address*> command to configure the Dynamic Host Control Protocol (DHCP) relay server helper address. Use the **no** form of this command to remove the DHCP relay server helper address.

3.67.1 Syntax Description

<ipv4 address>	Specifies the unicast Internet Protocol version 4 (IPv4) address of the DHCP relay server. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

3.67.2 Default Values

By default, the DHCP relay server does not have a helper address configured.

3.67.3 Privilege Level

By default, this command has a privilege level of **15**.

3.67.4 Command History

ASE Release 4.4-41	Command was introduced.

3.67.5 Usage Examples

The following example specifies an IPv4 helper address for the DHCP relay server:

```
(config)#ip helper-address 172.45.6.99
```

3.68 ip http

Use the **ip http** command to configure Hypertext Transfer Protocol (HTTP) and Secure HTTP (HTTPS) security parameters on the ASE device. Use the **no** form of this command to remove the configured parameters. Variations of this command include:

```
ip http secure-certificate delete
ip http secure-certificate generate
ip http secure-certificate upload <url file>
ip http secure-redirect
ip http secure-server
```

3.68.1 Syntax Description

secure-certificate	Configures the HTTPS certificate.
delete	Deletes the current HTTPS certificate.
generate	Generates a new self-signed Rivest-Shamir-Adleman (RSA) certificate.
upload *<url file>*	Uploads a privacy enhanced mail (PEM) certificate file. Specify the URL file in the format: *<flash:filename>* or *<tftp://server/path-and-filename>*. Valid file name is a text string drawn from the alphabet (**A-Z**, **a-z**), digits (**0-9**), dot (**.**), hyphen (**-**), or underscore (**_**). Maximum file name length is 63 characters. A hyphen cannot be the first character. A file name of only dot (**.**) is not allowed.
secure-redirect	Enables HTTPS web redirection.
secure-server	Enables an HTTPS secure server.

3.68.2 Default Values

By default, HTTP secure settings are disabled.

3.68.3 Privilege Level

By default, this command has a privilege level of **15**.

3.68.4 Command History

ASE Release 4.4-41	Command was introduced.

3.68.5 Usage Examples

The following example enables HTTPS web redirection (when HTTPS is enabled):

```
(config)#ip http secure-redirect
```

3.69 ip igmp host-proxy

Use the **ip igmp host-proxy** command to enable the Internet Group Management Protocol (IGMP) proxy. Use the **no** form of this command to disable the IGMP proxy. Variations of this command include:

```
ip igmp host-proxy
ip igmp host-proxy leave-proxy
```

3.69.1 Syntax Description

leave-proxy	Enables the IGMP proxy leave ability.

3.69.2 Default Values

By default, the IGMP proxy is disabled.

3.69.3 Privilege Level

By default, this command has a privilege level of **15**.

3.69.4 Command History

ASE Release 4.4-41	Command was introduced.

3.69.5 Usage Examples

The following example enables the IGMP proxy:

```
(config)#ip igmp host-proxy
```

3.70 ip igmp snooping

Use the **ip igmp snooping** command to globally enable Internet Group Management Protocol (IGMP) snooping. Use the no form of this command to disable global IGMP snooping. Use the **no** form of this command to disable IGMP snooping. Variations of this command include:

```
ip igmp snooping
ip igmp snooping vlan <vlan ids>
```

3.70.1 Syntax Description

vlan *<vlan ids>*	Optional. Enables IGMP snooping on the specified virtual local area networks (VLANs). You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

3.70.2 Default Values

By default, IGMP snooping is disabled.

3.70.3 Privilege Level

By default, this command has a privilege level of **15**.

3.70.4 Command History

ASE Release 4.4-41	Command was introduced.

3.70.5 Usage Examples

The following example globally enables IGMP snooping:

```
(config)#ip igmp snooping
```

3.71 ip igmp ssm-range <*ipv4 address*>

Use the **ip igmp ssm-range** <*ipv4 address*> command to specify an Internet Protocol version 4 (IPv4) multicast address for Internet Group Management Protocol (IGMP) source specific multicast (SSM) features. Use the no form of this command to remove the IPv4 multicast address.

3.71.1 Syntax Description

<ipv4 address>	Specifies a multicast IPv4 address to use with IGMP snooping SSM. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

3.71.2 Default Values

By default, IGMP does not have SSM addresses configured.

3.71.3 Privilege Level

By default, this command has a privilege level of **15**.

3.71.4 Command History

ASE Release 4.4-41	Command was introduced.

3.71.5 Usage Examples

The following example specifies the IPv4 multicast address to use with IGMP SSM:

```
(config)#ip igmp ssm-range 224.0.0.0
```

3.72 ip igmp unknown-flooding

Use the **ip igmp unknown-flooding** command to enable Internet Group Management Protocol (IGMP) flooding of ports for unregistered Internet Protocol version 4 (IPv4) multicast traffic. Use the **no** form of this command to disable this feature.

3.72.1 Syntax Description

No subcommands.

3.72.2 Default Values

By default, IGMP unknown flooding is disabled.

3.72.3 Privilege Level

By default, this command has a privilege level of **15**.

3.72.4 Command History

ASE Release 4.4-41	Command was introduced.

3.72.5 Usage Examples

The following example enables IGMP unknown flooding:

```
(config)#ip igmp unknown-flooding
```

3.73 ip name-server

Use the **ip name-server** command to designate an address for one or more name servers to use for name-to-address domain naming server (DNS) resolution. Use the **no** form of this command to remove an address. Variations of this command include:

```
ip name-server <preference> <ipv4 address>
ip name-server <preference> <ipv6 address>
ip name-server <preference> dhcp interface vlan <vlan id>
ip name-server <preference> dhcp interface vlan <vlan id> ipv4
ip name-server <preference> dhcp interface vlan <vlan id> ipv6
ip name-server <preference> dhcp ipv4
ip name-server <preference> dhcp ipv6
ip name-server <ipv4 address>
ip name-server <ipv6 address>
ip name-server dhcp interface vlan <vlan id>
ip name-server dhcp interface vlan <vlan id> ipv4
ip name-server dhcp interface vlan <vlan id> ipv6
ip name-server dhcp ipv4
ip name-server dhcp ipv6
```

3.73.1 Syntax Description

<preference>	Optional. Specifies the preference of the DNS server. Valid range is **0** to **3**.
<ipv4 address>	Specifies an Internet Protocol version 4 (IPv4) name server address. IPv4 addresses should be specified in dotted decimal notation (for example, **10.10.10.1**).
<ipv6 address>	Specifies an Internet Protocol version 6 (IPv6) name server address. IPv6 address should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.
dhcp interface vlan *<vlan id>*	Specifies the DHCP virtual local are network (VLAN) interface from which to derive DNS settings. Valid range is **1** to **4095**.
dhcp ipv4	Specifies the domain naming system (DNS) setting is derived from Dynamic Host Control Protocol version 4 (DHCPv4).
dhcp ipv6	Specifies the DNS settings is derived from DHCP version 6 (DHCPv6).

3.73.2 Default Values

By default, no name servers are configured. When configured, server preferences are set to **0** by default. When DHCP is used in conjunction with DNS, settings are derived from DHCPv6.

3.73.3 Privilege Level

By default, this command has a privilege level of **15**.

3.73.4 Command History

ASE Release 4.4-41	Command was introduced.

3.73.5 Usage Examples

The following example specifies IPv4 host **172.34.1.111** the name server:

```
(config)#ip name-server 172.34.1.111
```

3.74 ip route

Use the **ip route** command to add an Internet Protocol version 4 (IPv4) static route to the IPv4 route table. Use the **no** form of this command to remove a configured IPv4 static route. Variations of this command include:

ip route *<ipv4 address> <subnet mask> <ipv4 gateway>*
ip route *<ipv4 address> <subnet mask> <ipv4 gateway> <administrative distance>*

3.74.1 Syntax Description

<ipv4 address>	Specifies the IPv4 network address to add to the route table. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**).
<ipv4 gateway>	Specifies the far-end IPv4 address to use as the gateway address.
<administrative distance>	Optional. Specifies an administrative distance associated with a particular router used to determine the best route when multiple routes to the same destination exist. The lower the administrative distance, the more preferable the route. Range is **1** to **255**.

3.74.2 Default Values

By default, there are no configured routes in the route table.

3.74.3 Privilege Level

By default, this command has a privilege level of **15**.

3.74.4 Command History

ASE Release 4.4-41	Command was introduced.

3.74.5 Usage Examples

The following example adds an IPv4 static route to the **10.220.0.0 255.255.0.0** network through the next-hop router **192.22.45.254**:

```
(config)#ip route 10.220.0.0 255.255.0.0 192.22.45.254
```

3.75 ip routing

Use the **ip routing** command to enable Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) routing on the ASE device. Use the **no** form of this command to disable IP routing.

3.75.1 Syntax Description

No subcommands.

3.75.2 Default Values

By default, IP routing is enabled.

3.75.3 Privilege Level

By default, this command has a privilege level of **15**.

3.75.4 Command History

ASE Release 4.4-41	Command was introduced.

3.75.5 Usage Examples

The following example enables IP routing if it has been disabled:

```
(config)#ip routing
```

3.76 ip source binding interface *<interface> <vlan id> <ipv4 address> <mac address>*

Use the **ip source binding** command to configure the Internet Protocol (IP) source binding entries for the interface. Use the **no** form of this command to remove binding entries.

3.76.1 Syntax Description

<interface>	Specifies the interface to which to bind the source information. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **ip source binding interface ?** for a complete list of valid interfaces.
<vlan id>	Specifies the virtual local area network (VLAN) instance to which the source information is bound. Valid range is **1** to **4095**.
<ipv4 address>	Specifies a valid IPv4 source address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<mac address>	Specifies the source media access control (MAC) address. MAC addresses should be expressed in the following format: XX:XX:XX:XX:XX:XX (for example, **00:A0:C8:00:00:01**).

3.76.2 Default Values

By default, a binding source interface is not defined.

3.76.3 Privilege Level

By default, this command has a privilege level of **13**.

3.76.4 Command History

ASE Release 4.4-41	Command was introduced.

3.76.5 Usage Examples

The following example creates a binding source interface entry for the GigabitEthernet interface, using VLAN **175**, for the IPv4 address **172.5.67.99** and MAC address **00:A0:C8:00:00:01**:

```
(config)#ip source binding interface GigabitEthernet 1/1 175 172.5.67.99
   00:A0:C8:00:00:01
```

3.77 ip ssh

Use the **ip ssh** command to enable Secure Shell (SSH) connections. Use the **no** form of this command to disable SSH.

3.77.1 Syntax Description

No subcommands.

3.77.2 Default Values

By default, SSH connections are disabled.

3.77.3 Privilege Level

By default, this command has a privilege level of **15**.

3.77.4 Command History

ASE Release 4.4-41	Command was introduced.

3.77.5 Usage Examples

The following example enables SSH connections:

```
(config)#ip ssh
```

3.78 ip verify source

Use the **ip verify source** to enable Internet Protocol (IP) source verification. Use the **no** form of this command to disable this feature. Variations of this command include:

```
ip verify source
ip verify source translate
```

3.78.1 Syntax Description

translate	Optional. Enables IP source verification to translate all source entries.

3.78.2 Default Values

By default, IP source verification is disabled.

3.78.3 Privilege Level

By default, this command has a privilege level of **13**.

3.78.4 Command History

ASE Release 4.4-41	Command was introduced.

3.78.5 Usage Examples

The following example enables IP source verification:

```
(config)#ip verify source
```

3.79 ipmc profile <*name*>

Use the **ipmc profile** <*name*> command to create an IPMC profile for Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) multicast configurations. Use the **no** form of this command to remove the IPMC profile.

3.79.1 Syntax Description

<name>	Specifies the name for the IPMC profile. Valid profile names cannot be longer than 16 characters in length.

3.79.2 Default Values

By default, no IPMC profiles are configured.

3.79.3 Command History

ASE Release 4.4-41	Command was introduced.

3.79.4 Functional Notes

The IPMC profile allows permission for certain multicast registrations by providing access authorization using certain configured matching criteria from the profile. Each profile creates a named range, which then is then configured with the rules used for matching multicast addresses for registration. The named ranges are then applied to specific multicast IPv4 and IPv6 addresses to maintain access control for multicast registrations. For more information about applying IPMC named ranges to IPv4 and IPv6 multicast addresses, refer to the command “ipmc range <name>” on page 340. For more information about configuring IPMC profiles, refer to the “IPMC Profile Command Set” on page 655.

3.79.5 Usage Examples

The following example creates the IPMC profile TESTPROFILE and enters the profile’s configuration mode:

```
(config)#ipmc profile TESTPROFILE
(cofnig-ipmc-profile)#
```

3.80 ipmc range <*name*>

Use the **ipmc range** <*name*> command to configure a range of Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) addresses to use with the configured IPMC profile. Use the **no** form of this command to remove the range addresses.

ipmc range *<name> <ipv4 address>*
ipmc range *<name> <ipv6 address>*

3.80.1 Syntax Description

<name>	Specifies the name of the previously created IPMC range to which to apply the IPv4 or IPv6 addresses. Valid range names are no greater than 16 characters in length.
<ipv4 address>	Specifies a valid IPv4 multicast address to be associated with the IPMC range. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<ipv6 address>	Specifies a valid IPv6 multicast address to be associated with the IPMC range. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**). For example, **2001:DB8:1::1**.

3.80.2 Default Values

By default, no IPMC ranges are configured.

3.80.3 Command History

ASE Release 4.4-41	Command was introduced.

3.80.4 Functional Notes

Using this command applies a previously created IPMC range to specific IPv4 and IPv6 multicast addresses. IPMC ranges are created in the IPMC profile configuration. For more information about IPMC profile configuration, refer to the “IPMC Profile Command Set” on page 655.

3.80.5 Usage Examples

The following example applies the IPMC range RANGETEST to the IPv4 multicast address **239.255.255.255**:

```
(config)#ipmc range RANGETEST 239.255.255.255
```

3.81 ipv6 mld

Use the **ipv6 mld** command to configure Internet Protocol version 6 (IPv6) Multicast Listener Discovery (MLD) parameters on the ASE device. Use the **no** form of this command to disable IPv6 MLD. Variations of this command include:

```
ipv6 mld host-proxy
ipv6 mld host-proxy leave-proxy
ipv6 mld snooping
ipv6 mld snooping vlan <vlan ids>
ipv6 mld ssm-range <ipv6 address>
ipv6 mld unknown-flooding
```

3.81.1 Syntax Description

host-proxy	Enables the IPv6 MLD proxy.
leave-proxy	Optional. Enables the IPv6 MLD proxy leave ability.
snooping	Enables IPv6 MLD snooping.
vlan *<vlan ids>*	Optional. Enables IPv6 MLD snooping on the specified virtual local area networks (VLANs). You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.
ssm-range *<ipv6 address>*	Specifies a multicast IPv6 address to use with IPv6 MLD snooping source specific multicast (SSM). IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
unknown-flooding	Enable IPv6 MLD flooding of ports for unregistered IPv6 multicast traffic.

3.81.2 Default Values

By default, IPv6 MLD is disabled.

3.81.3 Privilege Level

By default, this command has a privilege level of **15**.

3.81.4 Command History

ASE Release 4.4-41	Command was introduced.

3.81.5 Usage Examples

The following example enables the IPv6 MLD proxy:

```
(config)#ipv6 mld host-proxy
```

3.82 json notification

Use the **json notification** command to configure JavaScript Object Notation (JSON) remote procedure call (RPC) notifications. Use the **no** form of this command to disable JSON RPC notifications. Variations of this command include:

json notification host *<name>*
json notification listen *<update>*

3.82.1 Syntax Description

host *<name>*	Specifies the notification host for JSON notification request objects and enters the JSON notification host configuration mode. Valid host names are no longer than 32 characters in length.
listen *<update>*	Specifies the JSON RPC notification event subscription for a specific update. Acceptable update parameters are: **acl.status.ace.crossedThreshold.update** **aggregation.status.notification.update** **alarm.status.update** **arpInspection.status.crossedThreshold.update** **ddmi.status.interface.crossedThreshold.update** **ethernetLinkOam.satistics.interfae.criticalL-inkEvent.update** **ip.status.acd.ipv4.update** **ip.status.interface.dhcpClient.update** **ip.status.interface.ipv4.update** **ip.status.interface.ipv6.update** **ip.status.interface.link.update** **ip.status.route.ipv4.update** **ip.status.route.ipv6.update** **mep.status.instance.update** **mep.status.instacePeer.update** **mep.status.lmHli.update** **mep.status.ImNotif.update** **port.status.update** **portSecurity.status.global.notification.update** **portSecurity.status.interface.notification.update** **qos.status.global.update**

3.82.2 Default Values

By default, JSON RPC is disabled.

3.82.3 Command History

ASE Release 4.4-41	Command was introduced.

3.82.4 Usage Examples

The following example specifies a notification host for JSON notification request objects and enters the JSON configuration mode:

```
(config)#json notification host TESTHOST
(config-json-noti-host)#
```

3.83 lacp system-priority <*priority*>

Use the **lacp system-priority** <*priority*> command to specify the priority for the ASE device when connected to other devices using Link Aggregation Control Protocol (LACP). Use the **no** form of this command to return to the default value.

3.83.1 Syntax Description

<*priority*>	Specifies the priority for the ASE device in the LACP connected network. Valid range is **1** to **65535**; it is important to remember that the lower the entered value, the higher the priority.

3.83.2 Default Values

By default, the LACP system priority is set to **32768**.

3.83.3 Privilege Level

By default, this command has a privilege level of **15**.

3.83.4 Command History

ASE Release 4.4-41	Command was introduced.

3.83.5 Usage Examples

The following example changes the system's LACP priority to **1500**:

```
(config)#lacp system-priority 1500
```

3.84 line

Use the **line** command to enter the line configuration for the specified terminal line, console, or virtual terminal (VTY) session. Refer to the "Line Interface Command Set" on page 607 for line configuration commands. Use the **no** form of this command to remove the line configuration. Variations of this command include:

line *<line number>*
line console 0
line vty *<vty number>*

3.84.1 Syntax Description

<line number>	Specifies the line to be configured. Valid range is **0** to **16**.
console 0	Specifies the console line is being configured.
<vty number>	Specifies the virtual terminal to be configured. Valid range is **0** to **15**.

3.84.2 Default Values

By default, no terminal, console, or VTY lines are configured.

3.84.3 Command History

The following example enters the line configuration for the console line:

```
(config)#line console 0
(config-line)#
```

3.85 lldp

Use the **lldp** command to configure global settings that control the way Link Layer Discovery Protocol (LLDP) functions. Use the **no** form of this command to return to the default settings. Variations of this command include:

```
lldp holdtime <time>
lldp reinit <delay>
lldp timer <interval>
lldp transmission-delay <delay>
```

3.85.1 Syntax Description

holdtime *<time>*	Specifies the LLDP hold time, which determines when the neighboring switch discards the LLDP information. The hold time is calculated by multiplying the value set with this parameter and the value set with the **timer** parameter. Valid range is **2** to **10** seconds.
reinit *<delay>*	Specifies the LLDP transmission reinitialization delay. Valid range is **1** to **10** seconds.
timer *<interval>*	Specifies the time between each LLDP frame transmission. This value multiplied with the **holdtime** value determines how long a neighboring switch keeps LLDP information. Valid range is **5** to **32768** seconds.
transmission-delay *<delay>*	Specifies the amount of time to wait before transmitting LLDP frames after the LLDP configuration has changed. Valid range is **1** to **8192** seconds.

3.85.2 Default Values

By default, the hold timer is set to **4** seconds, the reinitialization delay is set to **2** seconds, the LLDP timer is set to **2** seconds, and the transmission delay is set to **30** seconds.

3.85.3 Privilege Level

By default, this command has a privilege level of **15**.

3.85.4 Command History

ASE Release 4.4-41	Command was introduced.

3.85.5 Usage Examples

The following example sets the LLDP timer to **20** seconds:

```
(config)#lldp timer 20
```

3.86 lldp med

Use the **lldp** med command to configure Link Layer Discover Protocol (LLDP) Media Endpoint Discovery (MED) parameters on the ASE device. Use the **no** form of this command to remove the LLDP MED parameters. Variations of this command include:

```
lldp med datum nad83_mllw
lldp med datum nad83_navd88
lldp med datum wsg84
lldp med fast <number>
```

3.86.1 Syntax Description

datum	Specifies that LLDP-MED Datum (geodetic system) type is being specified.
nad83_mllw	Specifies mean lower low water datum 1983.
nad83_navd88	Specifies North American vertical datum 1983.
wsg84	Specifies Word Geodetic System 1984.
fast *<number>*	Specifies the number of times to repeat LLDP frame transmission at fast start. Valid range is **1** to **10**.

3.86.2 Default Values

By default, LLDP-MED is not configured.

3.86.3 Privilege Level

By default, this command has a privilege level of **15**.

3.86.3.1 Command History

ASE Release 4.4-41	Command was introduced.

3.86.4 Usage Examples

The following example specifies the LLDP frame transmissions are repeated **4** times at fast start:

```
(config)#lldp med fast 4
```

3.87 lldp med location-tlv

Use the **lldp med location-tlv** command to configure Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) location type length values (TVLs). Use the **no** form of this command to remove the TVL configuration. Variations of this command include:

```
lldp med location-tlv altitude meters <altitude>
lldp med location-tlv altitude floors <altitude>
lldp med location-tlv civic-addr additional-code <value>
lldp med location-tlv civic-addr additional-info <value>
lldp med location-tlv civic-addr apartment <value>
lldp med location-tlv civic-addr block <value>
lldp med location-tlv civic-addr building <value>
lldp med location-tlv civic-addr city <value>
lldp med location-tlv civic-addr country <value>
lldp med location-tlv civic-addr county <value>
lldp med location-tlv civic-addr district <value>
lldp med location-tlv civic-addr floor <value>
lldp med location-tlv civic-addr house-no <value>
lldp med location-tlv civic-addr house-no-suffix <value>
lldp med location-tlv civic-addr landmark <value>
lldp med location-tlv civic-addr leading-street-direction <value>
lldp med location-tlv civic-addr name <value>
lldp med location-tlv civic-addr p-o-box <value>
lldp med location-tlv civic-addr place-type <value>
lldp med location-tlv civic-addr postal-community-name <value>
lldp med location-tlv civic-addr room-number <value>
lldp med location-tlv civic-addr state <value>
lldp med location-tlv civic-addr street <value>
lldp med location-tlv civic-addr street-suffix <value>
lldp med location-tlv civic-addr trailing-street-suffix <value>
lldp med location-tlv civic-addr zip-code <value>
lldp med location-tlv elin-adddr <value>
lldp med location-tlv latitude north <degrees>
lldp med location-tlv latitude south <degrees>
lldp med location-tlv longitude east <degrees>
lldp med location-tlv longitude west <degrees>
```

3.87.1 Syntax Description

altitude	Specifies the LLDP-MED TVL altitude.
meters *<altitude>*	Specifies the LLDP-MED TVL altitude in meters. Valid range is **-2097151.9** to **2097151.9**.
floors *<altitude>*	Specifies the LLDP-MED TVL altitude in floors. Valid range is **-2097151.9** to **2097151.9**.
civic-addr	Specifies the LLDP-MED TVL civic address and postal information.
additional-code	Specifies an additional address code. For example, **1320300003**.
additional-info	Specifies additional location information. For example, **South Wing**.
apartment	Specifies an apartment unit, in the format *apartment, suite*. For example, **Apt 42**.
block	Specifies a neighborhood block.

building	Specifies a building structure. For example, **Lower Library**.
city	Specifies a city, township, or shi (Japan). For example, **Copenhagen**.
country	Specifies the two-letter ISO 3166 country code in capital ASCII letters. For example, **DK**, **DE**, or **US**.
county	Specifies a county, parish, gun (Japan), or district.
district	Specifies a city division, borough, city district, ward, or chou (Japan).
floor	Specifies a building floor. For example, **4**.
house-no	Specifies a house number. For example, **21**.
house-no-suffix	Specifies a house number suffix. For example, **A, 1/2**.
landmark	Specifies a landmark or vanity address. For example, **Columbia University**.
leading-street-direction	Specifies a leading street direction. For example, **N**.
name	Specifies a resident name or office occupant. For example, **John Doe**.
p-o-box	Specifies a post office (P.O.) box. For example, **12345**.
place-type	Specifies the type of place. For example, **Office**.
postal-community-name	Specifies a postal community name. For example, **Leona**.
room-number	Specifies a room number. For example, **450**.
state	Specifies a national subdivision, such as sate, canton, region, province, or prefecture.
street	Specifies a street name. For example, **Oxford Street**.
street-suffix	Specifies a street suffix. For example, **Ave** or **Platz**.
training-street-suffix	Specifies a trailing street suffix. For example, **SW**.
zip-code	Specifies a postal/zip code. For example, **35806**.
<value>	Specifies the civic address information. Information is limited to **250** characters. The 2 letter country code is not part of the 250 character limitation. In addition, a non-empty civic address location will use 2 extra characters in addition to the civic address location text.
elin-address *<value>*	Specifies the Emergency Location Identification Number (ELIN), in data format, to be used in emergency call configuration to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string that corresponds to the ELIN to be used for emergency calls, as defined by TIA or NENA. For example, **E911**. ELIN identifiers are limited to **25** characters in length.
latitude	Specifies the LLDP-MED TVL latitude.
north *<degrees>*	Specifies a northern latitude in degrees. Valid range is **0.0000** to **90.0000**.
south *<degrees>*	Specifies a southern latitude in degrees. Valid range is **0.0000** to **90.0000**.

longitude	Specifies the LLDP-MED TVL longitude.
east *<degrees>*	Specifies an eastern latitude in degrees. Valid range is **0.0000** to **180.0000**.
west *<degrees>*	Specifies a western latitude in degrees. Valid range is **0.0000** to **180.0000**.

3.87.2 Default Values

By default, LLDP-MED TVL parameters are not configured.

3.87.3 Privilege Level

By default, this command has a privilege level of **15**.

3.87.4 Command History

ASE Release 4.4-41	Command was introduced.

3.87.5 Usage Examples

The following example specifies a P.O. Box for the LLDP-MED TVL:

```
(config)#lldp med location-tlv civic-addr p-o-box 19600
```

3.88 lldp med media-vlan-policy

Use the **lldp med media-vlan policy** command to configure a Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) policy for specifying how particular media traffic should be managed on an interface. Use the **no** form of this command to remove the policy. Variations of this command include:

```
lldp med media-vlan-policy <number> guest-voice tagged <vlan id>
lldp med media-vlan-policy <number> guest-voice tagged <vlan id> dscp <value>
lldp med media-vlan-policy <number> guest-voice tagged <vlan id> l2-priority
   <priority>
lldp med media-vlan-policy <number> guest-voice tagged <vlan id> l2-priority
   <priority> dscp <value>
lldp med media-vlan-policy <number> guest-voice untagged
lldp med media-vlan-policy <number> guest-voice untagged dscp <value>

lldp med media-vlan-policy <number> guest-voice-signaling tagged <vlan id>
lldp med media-vlan-policy <number> guest-voice-signaling tagged <vlan id> dscp
   <value>
lldp med media-vlan-policy <number> guest-voice-signaling tagged <vlan id> l2-
   priority <priority>
lldp med media-vlan-policy <number> guest-voice-signaling tagged <vlan id> l2-
   priority <priority> dscp <value>
lldp med media-vlan-policy <number> guest-voice-signaling untagged
lldp med media-vlan-policy <number> guest-voice-signaling untagged dscp <value>

lldp med media-vlan-policy <number> softphone-voice tagged <vlan id>
lldp med media-vlan-policy <number> softphone-voice tagged <vlan id> dscp <value>
lldp med media-vlan-policy <number> softphone-voice tagged <vlan id> l2-priority
   <priority>
lldp med media-vlan-policy <number> softphone-voice tagged <vlan id> l2-priority
   <priority> dscp <value>
lldp med media-vlan-policy <number> softphone-voice untagged
lldp med media-vlan-policy <number> softphone-voice untagged dscp <value>

lldp med media-vlan-policy <number> streaming-video tagged <vlan id>
lldp med media-vlan-policy <number> streaming-video tagged <vlan id> dscp <value>
lldp med media-vlan-policy <number> streaming-video tagged <vlan id> l2-priority
   <priority>
lldp med media-vlan-policy <number> streaming-video tagged <vlan id> l2-priority
   <priority> dscp <value>
lldp med media-vlan-policy <number> streaming-video untagged
lldp med media-vlan-policy <number> streaming-video untagged dscp <value>

lldp med media-vlan-policy <number> video-conferencing tagged <vlan id>
lldp med media-vlan-policy <number> video-conferencing tagged <vlan id> dscp <value>
lldp med media-vlan-policy <number> video-conferencing tagged <vlan id> l2-priority
   <priority>
lldp med media-vlan-policy <number> video-conferencing tagged <vlan id> l2-priority
   <priority> dscp <value>
lldp med media-vlan-policy <number> video-conferencing untagged
lldp med media-vlan-policy <number> video-conferencing untagged dscp <value>

lldp med media-vlan-policy <number> video-signaling tagged <vlan id>
lldp med media-vlan-policy <number> video-signaling tagged <vlan id> dscp <value>
lldp med media-vlan-policy <number> video-signaling tagged <vlan id> l2-priority
   <priority>
lldp med media-vlan-policy <number> video-signaling tagged <vlan id> l2-priority
   <priority> dscp <value>
```

```
lldp med media-vlan-policy <number> video-signaling untagged
lldp med media-vlan-policy <number> video-signaling untagged dscp <value>

lldp med media-vlan-policy <number> voice tagged <vlan id>
lldp med media-vlan-policy <number> voice tagged <vlan id> dscp <value>
lldp med media-vlan-policy <number> voice tagged <vlan id> l2-priority <priority>
lldp med media-vlan-policy <number> voice tagged <vlan id> l2-priority <priority>
   dscp <value>
lldp med media-vlan-policy <number> voice untagged
lldp med media-vlan-policy <number> voice untagged dscp <value>

lldp med media-vlan-policy <number> voice-signaling tagged <vlan id>
lldp med media-vlan-policy <number> voice-signaling tagged <vlan id> dscp <value>
lldp med media-vlan-policy <number> voice-signaling tagged <vlan id> l2-priority
   <priority>
lldp med media-vlan-policy <number> voice-signaling tagged <vlan id> l2-priority
   <priority> dscp <value>
lldp med media-vlan-policy <number> voice-signaling untagged
lldp med media-vlan-policy <number> voice-signaling untagged dscp <value>
```

3.88.1 Syntax Description

<number>	Specifies the ID number of the policy. Valid range is **0** to **31**.
guest-voice	Creates a policy that applies to guest voice traffic.
guest-voice-signaling	Creates a policy that applies to guest voice signaling.
softphone-voice	Creates a policy that applies to softphone voice traffic.
streaming-video	Creates a policy that applies to streaming video.
video-conferencing	Creates a policy that applies to video conferencing.
video-signaling	Creates a policy that applies to video signaling.
voice	Creates a policy that applies to voice traffic.
voice-signaling	Creates a policy that applies to voice signaling.
tagged *<vlan id>*	Specifies that the policy uses tagged frames from the specified virtual local area network (VLAN). Valid range is **1** to **4095**.
untagged	Specifies that the policy uses untagged frames.
dscp *<value>*	Optional. Specifies the Differentiated Services Code Point (DSCP) value to assign to media traffic in the policy. Valid range is **0** to **63**. If no DSCP value is specified, the value is set to **0**.
l2-priority *<priority>*	Optional. Specifies a Layer 2 priority to assign to media traffic in the policy. Valid range is **0** to **7**. If the Layer 2 priority is not specified, the value is set to **0**.

3.88.2 Default Values

By default, no LLDP-MED media policies are configured.

3.88.3 Privilege Level

By default, this command has a privilege level of **15**.

3.88.4 Command History

ASE Release 4.4-41	Command was introduced.

3.88.5 Usage Examples

The following example configures an LLDP-MED media policy for voice traffic, using tagged frames through VLAN 200:

```
(config)#lldp med media-vlan-policy 5 voice tagged 200
```

3.89 logging

Use the **logging** command to enable and configure system message logging for the ASE device. Use the **no** form of this command to disable the logging feature. Variations of this command include:

```
logging host <hostname | ipv4 address>
logging level error
logging level informational
logging level notice
logging level warning
logging notification listen <name> level error <source>
logging notification listen <name> level informational <source>
logging notification listen <name> level notice <source>
logging notification listen <name> level warning <source>
logging on
```

3.89.1 Syntax Description

<hostname | ipv4 address>	Specifies the host server for logging messages. Host names can be entered as either a fully qualified domain name (FQDN) or as an IP version 4 (IPv4) address in dotted decimal notation (**XX.XX.XX.XX**).
level	Specifies the severity level of the log messages.
error	Specifies error conditions are logged. Error messages are severity level **3**.
informational	Specifies informational messages are logged. Informational messages are severity level **6**.
notice	Specifies notice messages are logged. These messages indicate a significant condition has changed but normal operations continues. Notice messages are severity level **5**.
warning	Specifies warning messages are logged. Warning messages are severity level **4**.
listen *<name>*	Specifies notification messages, tied to a specific listen command name, are logged. Listen command names cannot be more than **127** characters in length.
<source>	Specifies the notification source for notification messages. Source names cannot exceed **255** characters in length.
on	Enables the system message logging feature for all messages.

3.89.2 Default Values

By default, system log messages are disabled.

3.89.3 Privilege Level

By default, this command has a privilege level of **15**.

3.89.4 Command History

ASE Release 4.4-41	Command was introduced.

3.89.5 Usage Examples

The following example specifies that logging is enabled for error messages:

```
(config)#logging level error
```

3.90 loop-protect

Use the **loop-protect** command to enable and configure loop protection on the ASE device. Use the **no** form of this command to disable loop protection. Variations of this command include:

```
loop-protect shutdown-time <time>
loop-protect transmit-time <time>
```

3.90.1 Syntax Description

shutdown-time *<time>*	Specifies the loop protection shutdown interval. Valid range is **0** to **604800** seconds.
transmit-time *<time>*	Specifies the time interval between loop protection transmissions. Valid range is **1** to **10** seconds.

3.90.2 Default Values

By default, loop protection is disabled.

3.90.3 Privilege Level

By default, this command has a privilege level of **15**.

3.90.4 Command History

ASE Release 4.4-41	Command was introduced.

3.90.5 Usage Examples

The following example enables loop protection and specifies the transmit time interval as **5** seconds:

```
(config)#loop-protect transmit-time 5
```

3.91 mac address-table

Use the **mac address-table** command to configure various parameters for the media access control (MAC) address table. Use the **no** form of this command to return to the default values. Variations of this command include:

```
mac address-table aging-time <value>
mac address-table learning vlan <vlan ids>
mac address-table static <mac address> vlan <vlan id>
mac address-table static <mac address> vlan <vlan id> interface <interface>
```

3.91.1 Syntax Description

aging-time *<value>*	Specifies how long before the MAC address table automatically removes a source address entry from the table after it has been inactive. Valid range is **10** to **1000000** seconds, or **0** seconds. Entering **0** disables the automatic aging feature, and all entries remain in the table unless manually deleted.
learning vlan *<vlan ids>*	Enables MAC address learning for virtual local area networks (VLANs), which allows them to automatically learn and add MAC addresses to the MAC address table. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.
static *<mac address>*	Manually adds a MAC address to the MAC address table. MAC addresses should be expressed in the following format **xx:xx:xx:xx:xx:xx** (for example, **00:A0:C8:00:00:01**).
vlan *<vlan id>*	Specifies the VLAN associated with the manually added MAC address. Valid range is **1** to **4095**.
interface *<interface>*	Optional. Specifies the port to which the MAC address is associated. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID.

3.91.2 Default Values

By default, the MAC address table aging time is set to **300** seconds and automatic learning for MAC addresses is enabled for all VLANs.

3.91.3 Privilege Level

By default, this command has a privilege level of **15**.

3.91.4 Command History

ASE Release 4.4-41	Command was introduced.

3.91.5 Usage Examples

The following example disables MAC address learning for VLAN **175**:

```
(config)#mac address-table learning vlan 175
```

3.92 mep <*instance*> ais

Use the **mep** <*instance*> **ais** command to configure alarm indication signal (AIS) parameters for a maintenance entity point (MEP) instance. Use the **no** form of this command to disable the AIS configuration for the MEP instance. Variations of this command include:

```
mep <instance> ais fr1m
mep <instance> ais fr1m protect
mep <instance> ais fr1s
mep <instance> ais fr1s protect
```

3.92.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
fr1m	Specifies an AIS frame rate of 1 frame per minute.
fr1s	Specifies an AIS frame rate of 1 frame per second.
protect	Optional. Specifies AIS is used for protection. In this case, three AIS protocol data units (PDUs) are sent as fast as possible when there is a state change in the MEP.

3.92.2 Default Values

By default, MEP instances are not configured.

3.92.3 Command History

ASE Release 4.4-41	Command was introduced.

3.92.4 Usage Examples

The following example specifies an AIS frame rate of 1 frame per second for MEP instance **100**:

```
(config)#mep 100 ais fr1s
```

3.93 mep <*instance*> aps <*priority*>

Use the **mep** <*instance*> **aps** <*priority*> command to configure the Automatic Protection Switching (APS) parameters for a maintenance entity point (MEP) instance. Use the **no** form of this command to disable APS on the MEP instance. Variations of this command include:

```
mep <instance> aps <priority> laps
mep <instance> aps <priority> uni laps
mep <instance> aps <priority> raps
mep <instance> aps <priority> multi raps
mep <instance> aps <priority> raps octet
```

3.93.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
<priority>	Specifies the APS priority for the MEP instance when using tagged Operation, Administration, and Maintenance (OAM). Valid range is **0** to **7**.
laps	Enables Linear APS (LAPS).
uni	Specifies that the OAM PDU is transmitted with a unicast MAC address. This option is only available when using LAPS.
raps	Enables Ring APS (RAPS).
multi	Specifies that the OAM protocol data unit (PDU) is transmitted with a multicast media access control (MAC) address. This option is only available when using RAPS.
octet	Specifies that only the last octet of the multicast MAC address is transmitted with the OAM PDU. This option is only available when using RAPS.

3.93.2 Default Values

By default, MEP instances are not configured.

3.93.3 Command History

ASE Release 4.4-41	Command was introduced.

3.93.4 Usage Examples

The following example specifies an APS priority of **3** for MEP instance **100** and enables LAPS:

```
(config)#mep 100 aps 3 laps
```

3.94 mep <*instance*> cc <*priority*>

Use the **mep** <*instance*> **cc** <*priority*> command to configure the continuity check parameters for a maintenance entity point (MEP) instance. Use the **no** form of this command to disable APS on the MEP instance. Variations of this command include:

```
mep <instance> cc <priority> fr100s
mep <instance> cc <priority> fr100s rx-only
mep <instance> cc <priority> fr10s
mep <instance> cc <priority> fr10s rx-only
mep <instance> cc <priority> fr1m
mep <instance> cc <priority> fr1m rx-only
mep <instance> cc <priority> fr300s
mep <instance> cc <priority> fr300s rx-only
mep <instance> cc <priority> fr6h
mep <instance> cc <priority> fr6h rx-only
mep <instance> cc <priority> fr6m
mep <instance> cc <priority> fr6m rx-only
```

3.94.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
<priority>	Specifies the continuity check priority for the MEP instance when using tagged Operation, Administration, and Maintenance (OAM). Valid range is **0** to **7**.
fr100s	Specifies the frame rate is 100 frames per second.
fr10s	Specifies the frame rate is 10 frames per second.
fr1m	Specifies the frame rate is 1 frame per minute.
fr300s	Specifies the frame rate is 300 frames per second.
fr6h	Specifies the frame rate is 6 frames per hour.
fr6m	Specifies the frame rate is 6 frames per minute.
rx-only	Optional. Specifies that continuity check message (CCM) transmission and loss of continuity (LOC) detection are not enabled, and only the priority and frame rate parameters are configured.

3.94.2 Default Values

By default, MEP instances are not configured.

3.94.3 Command History

ASE Release 4.4-41	Command was introduced.

3.94.4 Usage Examples

The following example specifies an continuity check priority of **2**, and a frame rate of 10 frames per second for MEP instance **100**:

```
(config)#mep 100 cc 2 fr10s
```

3.95 mep <*instance*> ccm-tlv

Use the **mep** <*instance*> **ccm-tlv** command to specify that type, length, values (TLVs) are included in continuity check messages (CCMs) for the maintenance entity point (MEP) instance. Use the **no** form of this command to disable the feature.

3.95.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.

3.95.2 Default Values

By default, TLVs are not included in CCMs.

3.95.3 Command History

ASE Release 4.4-41	Command was introduced.

3.95.4 Usage Examples

The following example enables TLV inclusion in CCMs for MEP instance **100**:

```
(config)#mep 100 ccm-tlv
```

3.96 mep <*instance*> client domain

Use the **mep** *<instance>* **client domain** command to configure the client flow domain for the maintenance entity point (MEP) instance. Use the **no** form of this command to remove the client flow domain from the MEP instance. Variations of this command include:

```
mep <instance> client domain evc
mep <instance> client domain evc flow <uint> ais-prio <priority>
mep <instance> client domain evc flow <uint> ais-prio ais-highest
mep <instance> client domain evc flow <uint> lck-prio <priority>
mep <instance> client domain evc flow <uint> lck-prio lck-highest
mep <instance> client domain evc flow <uint> level <level>
mep <instance> client domain flow <uint>
mep <instance> client domain flow <uint> ais-prio <priority>
mep <instance> client domain flow <uint> ais-prio ais-highest
mep <instance> client domain flow <uint> lck-prio <priority>
mep <instance> client domain flow <uint> lck-prio lck-highest
mep <instance> client domain flow <uint> level <level>
mep <instance> client domain vlan flow <uint> ais-prio
mep <instance> client domain vlan flow <uint> ais-prio <priority>
mep <instance> client domain vlan flow <uint> ais-prio ais-highest
mep <instance> client domain vlan flow <uint> lck-prio <priority>
mep <instance> client domain vlan flow <uint> lck-prio lck-highest
mep <instance> client domain vlan flow <uint> level <level>
```

3.96.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
evc	Optional. Specifies an Ethernet Virtual Circuit (EVC) client flow.
flow *<uint>*	Specifies the client flow instance number.
vlan	Optional. Specifies a virtual local area network (VLAN) client flow.
ais-prio	Optional. Specifies an alarm indication signal (AIS) injection priority.
<priority>	Specifies the AIS injection priority. Valid range is **0** to **7**.
ais-highest	Requests the highest possible AIS priority.
lck-prio	Optional. Specifies a locked signal (LCK) injection priority.
<priority>	Specifies the LCK injection priority. Valid range is **0** to **7**.
lck-highest	Requests the highest possible LCK priority.
level *<level>*	Optional. Specifies the maintenance endpoint group (MEG) level on the client layer. Valid range is **0** to **7**.

3.96.2 Default Values

By default, MEP client domains are not configured.

3.96.3 Command History

ASE Release 4.4-41	Command was introduced.

3.96.4 Usage Examples

The following specifies the client flow domain **10** for MEP instance **100**, with a client level of **4**:

```
(config)#mep 100 client domain flow 10 level 4
```

3.97 mep <*instance*> dm <*priority*>

Use the **mep** <*instance*> **dm** <*priority*> command to configure the delay measurement priority and direction parameters for the maintenance entity point (MEP) instance. Use the **no** form of this command to remove the delay measurement configurations. Variations of this command include:

```
mep <instance> dm <priority> dual flow interval <interval> last-n <number>
mep <instance> dm <priority> dual flow multi interval <interval> last-n <number>
mep <instance> dm <priority> dual flow uni mep-id <id>
mep <instance> dm <priority> dual flow uni mep-id <id> flow
mep <instance> dm <priority> dual flow uni mep-id <id> interval <interval>
mep <instance> dm <priority> dual flow uni mep-id <id> rdtrp
mep <instance> dm <priority> dual interval <interval> last-n <number>
mep <instance> dm <priority> dual multi flow interval <interval> last-n <number>
mep <instance> dm <priority> dual multi rdtrp interval <interval> last-n <number>
mep <instance> dm <priority> dual rdtrp multi interval <interval> last-n <number>
mep <instance> dm <priority> dual rdtrp uni mep-id <id>
mep <instance> dm <priority> dual rdtrp uni mep-id <id> flow
mep <instance> dm <priority> dual rdtrp uni mep-id <id> interval <interval>
mep <instance> dm <priority> dual rdtrp uni mep-id <id> rdtrp
mep <instance> dm <priority> dual uni mep-id <id>
mep <instance> dm <priority> dual uni mep-id <id> flow
mep <instance> dm <priority> dual uni mep-id <id> interval <interval>
mep <instance> dm <priority> dual uni mep-id <id> rdtrp
```

3.97.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
<priority>	Specifies the delay measurement priority for the MEP instance. Valid range is **0** to **7**.
dual	Specifies a delay measurement based on 1 delay measurement protocol data unit (PDU) transmission.
flow	Specifies the two-way delay is calculated as round trip symmetrical flow delay. When used, the far-end residence time is subtracted.
interval *<interval>*	Specifies the interval between PDU transmissions in 10 microseconds. Minimum value is 10 ms.
last-n *<number>*	Specifies that the specified number of last delay measurements are used to calculate an average delay over the specified number of measurements. Valid range is 10 to 100.
multi	Specifies that the Operation, Administration, and Maintenance (OAM) PDU is transmitted with a multicast media access control (MAC) address.
uni	Specifies that the OAM PDU is transmitted with a unicast MAC address.
mep-id *<id>*	Specifies the peer MEP ID for unicast delay measurement. The MAC address is taken from the peer MEP MAC database.
rdtrp	Specifies that the two-way delay is calculated as round trip delay and the far-end residence time is not subtracted.

3.97.2 Default Values

By default, MEPs are not configured.

3.97.3 Command History

ASE Release 4.4-41	Command was introduced.

3.97.4 Usage Examples

The following example specifies that delay measurement, with a priority of 3, is configured with a unicast MAC address from a peer MEP MAC database for MEP instance 100:

```
(config)#mep 100 dm 3 dual uni mep-id 10 rdtrp
```

3.98 mep <*instance*> dm

Use the **mep** <*instance*> **dm** command to configure delay measurement parameters for the maintenance entity point (MEP) instance. Use the **no** form of this command to disable the MEP instance delay measurement feature. Variations of this command include:

```
mep <instance> dm bin fd <number> threshold <value>
mep <instance> dm bin ifdv <number> threshold <value>
mep <instance> dm ns
mep <instance> dm overflow-reset
mep <instance> dm proprietary
mep <instance> dm synchronized
```

3.98.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
bin	Specifies delay measurement bin configuration.
fd *<number>*	Specifies the number of frame delay (FD) measurement bins. Valid range is **2** to **10**.
ifdv *<number>*	Specifies the number of inter-frame delay variation (IFDV) measurement bins. Valid range is **2** to **10**.
threshold *<value>*	Specifies the threshold at which frame delay measurements are placed in a bin. Valid range is **1** to **50000**.
ns	Specifies delay measurement is calculated in nanoseconds.
overflow-reset	Resets all delay measurement results when the total delay counter overflows.
proprietary	Specifies proprietary delay measurement.
synchronized	Specifies that the near-end and far-end MEPs are synchronized in real time.

3.98.2 Default Values

By default, MEPs are not configured.

3.98.3 Command History

ASE Release 4.4-41	Command was introduced.

3.98.4 Usage Examples

The following example specifies that delay measurement for MEP instance **100** is measured in **nanoseconds**:

```
(config)#mep 100 dm ns
```

3.99 mep <*instance*> down

Use the **mep** <*instance*> **down** command to configure a downstream maintenance entity point (MEP). Use the **no** form of this command to remove the MEP configuration. Variations of this command include:

mep *<instance>* **down domain evc level** *<level>*
mep *<instance>* **down domain evc level** *<level>* **interface** *<interface>*
mep *<instance>* **down domain evc flow** *<uint>* **level** *<level>*
mep *<instance>* **down domain evc flow** *<uint>* **level** *<level>* **interface** *<interface>*
mep *<instance>* **down domain port level** *<level>*
mep *<instance>* **down domain port level** *<level>* **interface** *<interface>*
mep *<instance>* **down domain port flow** *<uint>* **level** *<level>*
mep *<instance>* **down domain port flow** *<uint>* **level** *<level>* **interface** *<interface>*
mep *<instance>* **down domain vlan level** *<level>*
mep *<instance>* **down domain vlan level** *<level>* **interface** *<interface>*
mep *<instance>* **down domain vlan flow** *<uint>* **level** *<level>*
mep *<instance>* **down domain vlan flow** *<uint>* **level** *<level>* **interface** *<interface>*

3.99.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
domain	Specifies the domain of the MEP instance.
evc	Specifies the MEP domain is an Ethernet Virtual Circuit (EVC).
port	Specifies the MEP domain is a port.
vlan	Specifies the MEP domain is a virtual local area network (VLAN).
level *<level>*	Specifies the maintenance endpoint group (MEG) level of the MEP instance. Valid range is **0** to **7**.
flow *<uint>*	Specifies the flow instance number for the MEP. This value must be specified for MEPs that are part of a VLAN, EVC, Multiprotocol Label Switching Transport Profile (MPLS-TP) link, tunnel, LSP, or pseudo-wire domain.
interface *<interface>*	Optional. Specifies the interface with which the MEP is associated. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID.

3.99.2 Default Values

By default, MEPs are not configured.

3.99.3 Command History

ASE Release 4.4-41	Command was introduced.

3.99.4 Usage Examples

The following example specifies that MEP instance **100** is a downstream MEP in an EVC domain with a level of **5**:

```
(config)#mep 100 down domain evc flow 10 level 5
```

3.100 mep <*instance*> lb <*priority*>

Use the **mep** <*instance*> **lb** <*priority*> to configure the loopback settings for a maintenance entity point (MEP) instance. Use the **no** form of this command to remove the loopback configuration from the MEP instance. Variations of this command include:

```
mep <instance> lb <priority> dei uni mac
mep <instance> lb <priority> dei uni mep-id <id>
mep <instance> lb <priority> count <number> dei
mep <instance> lb <priority> count <number> dei uni mac
mep <instance> lb <priority> count <number> dei uni mep-id
mep <instance> lb <priority> multi mac
mep <instance> lb <priority> multi mep-id <id>
mep <instance> lb <priority> count <number> multi
mep <instance> lb <priority> count <number> multi mac
mep <instance> lb <priority> count <number> multi mep-id <id>
```

3.100.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
lb *<priority>*	Specifies the loopback priority for the MEP instance for Operation, Administration, and Management (OAM) tagged traffic. Valid range is **0** to **7**.
dei	Specifies the drop eligible indicator (DEI) for tagged OAM traffic.
uni	Specifies that OAM protocol data units (PDUs) are transmitted with a unicast media access control (MAC) address. The MAC address is taken from a peer MEP MAC database. This value is not used for Multiprotocol Label Switching Transport Profile (MPLS-TP) links.
multi	Specifies that OAM PDUs are transmitted with a multicast MAC address. This value is not used for Multiprotocol Label Switching Transport Profile (MPLS-TP) links.
mac	Specifies that a loopback unicast MAC address is to be used in case of loopback for the maintenance intermediary point (MIP).
mep-id *<id>*	Specifies a MEP ID is used for unicast loopback.
count *<number>*	Optional. Specifies the number of loopback PDUs to send in one loop test. Entering 0 specifies infinitive transmissions. This setting is for hardware-based loopback messages (LBM) and loopback replies (LBR) and requires a versatile OAM endpoint (VOE).

3.100.2 Default Values

By default, MEPs are not configured.

3.100.3 Command History

ASE Release 4.4-41	Command was introduced.

3.100.4 Usage Examples

The following example specifies that MEP instance **100** has a loopback priority of **3**, and transmits OAM PDUs with a multicast MAC address:

```
(config)#mep 100 lb 5 multi mac
```

3.101 mep <*instance*> lck

Use the **mep** <*instance*> **lck** command to specify the lock signal parameters for the maintenance entity point (MEP) instance. Use the **no** form of this command to remove the lock signal parameters from the MEP. Variations of this command include:

mep <*instance*> **lck fr1m**
mep <*instance*> **lck fr1s**

3.101.1 Syntax Description

<*instance*>	Specifies the MEP instance. Valid range is **1** to **3124**.
fr1m	Specifies a frame rate of 1 frame per minute.
fr1s	Specifies a frame rate of 1 frame per second.

3.101.2 Default Values

By default, MEPs are not configured.

3.101.3 Command History

ASE Release 4.4-41	Command was introduced.

3.101.4 Usage Examples

The following example specifies that MEP instance **100** has a lock signal rate of 1 frame per minute:

```
(config)#mep 100 lck fr1m
```

3.102 mep <*instance*> level <*level*>

Use the **mep** <*instance*> **level** <*level*> command to configure the maintenance endpoint group (MEG) level of the maintenance entity point (MEP) instance. Use the **no** form of this command to remove the level from the MEP instance.

3.102.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
<level>	Specifies the MEP level. Valid range is **0** to **7**.

3.102.2 Default Values

By default, MEPs are not configured.

3.102.3 Command History

ASE Release 4.4-41	Command was introduced.

3.102.4 Usage Examples

The following example specifies that MEP instance **100** has a MEG level of **4**:

```
(config)#mep 100 level 4
```

3.103 mep <*instance*> link-state-tracking

Use the **mep** <*instance*> **link-state-tracking** command to enable link state tracking for the maintenance entity point (MEP) instance. Use the **no** form of this command to disable link state tracking for the MEP instance.

3.103.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.

3.103.2 Default Values

By default, MEPs are not configured.

3.103.3 Command History

ASE Release 4.4-41	Command was introduced.

3.103.4 Functional Notes

When link state tracking is enabled on the MEP, local SF or received ‘isDown’ in a continuity check message (CCM) interface status TLV brings down the residence port. Link state tracking is only valid in an upstream MEP, and the CCM rate on that MEP must be set to 1 frame per second or faster.

3.103.5 Usage Examples

The following example enables link state tracking for MEP instance **100**:

```
(config)#mep 100 link-state-tracking
```

3.104 mep <*instance*> lm

Use the **mep** <*instance*> **lm** command to configure loss measurement parameters for a maintenance entity point (MEP) instance. Use the **no** form of this command to remove the loss measurement configuration from the MEP. Variations of this command include:

```
mep <instance> lm <priority> dual
mep <instance> lm <priority> flr <number>
mep <instance> lm <priority> fr100s
mep <instance> lm <priority> fr1s
mep <instance> lm <priority> fr6m
mep <instance> lm <priority> meas <number>
mep <instance> lm <priority> multi
mep <instance> lm <priority> single
mep <instance> lm <priority> size <number>
mep <instance> lm <priority> slm-testid <number>
mep <instance> lm <priority> synthetic
mep <instance> lm <priority> threshold <number>
mep <instance> lm <priority> uni
mep <instance> lm flow-counting
mep <instance> lm oam-counting all
mep <instance> lm oam-counting y1731
mep <instance> lm rx
mep <instance> lm rx synthetic
mep <instance> lm rx synthetic flr <number>
mep <instance> lm rx synthetic flr <number> prio <priority>
mep <instance> lm rx synthetic flr <number> prio <priority> threshold <value>
```

3.104.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
lm *<priority>*	Specifies the loss measurement priority for the MEP instance for Operation, Administration, and Management (OAM) tagged traffic. Valid range is **0** to **7**.
dual	Specifies that dual-ended loss measurement is based on continuity check message (CCM) protocol date units (PDUs).
flr *<number>*	Specifies the frame loss ratio interval in a number of measurement intervals.
fr100s	Specifies the frame rate is 100 frames per second. This value is only valid if the loss measurement type is set to synthetic.
fr10s	Specifies the frame rate is 10 frames per second.
fr1s	Specifies the frame rate is 1 frame per second.
fr6m	Specifies the frame rate is 6 frames per minute. This value is not valid for a dual-ended service frame.
meas *<number>*	This is the 'synthetic' LM measurement interval in milli-seconds. This must be a whole number of the LM PDU transmission interval (inverse 'Frame rate').This is the interval in time where the loss and FLR is calculated based on the counted number of SL OAM PDUs. It is in this interval that the calculated FLR is checked against availability, high loss and degraded FLR threshold. For example, 'Frame rate' = fr100s => 'meas' = N*10 milliseconds or 'Frame rate' = fr10s => 'meas' = N*100 milliseconds. In case of service frame

	based LM this attribute is not used and the measurement interval is always the LM PDU transmission interval.
multi	Specifies that OAM PDUs are transmitted with a multicast media access control (MAC) address.
single	Specifies that single-ended loss measurement is based on loss measurement message (LMM) and loss measurement reply (LMR) PDUs, or, when the loss measurement is set to synthetic, synthetic loss message (SLM) and synthetic loss reply (SLR) PDUs.
size *<number>*	The OAM frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing the OAM PDU - including CRC (four bytes). Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + OAM PDU LENGTH(46) + CRC(4) = 64 bytes. The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC. There are two frame MAX sizes to consider. Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 10240 Bytes. CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 10240 Bytes. Consider that the Peer MEP must be able to handle the selected frame size. Consider that in order to calculate the 'RX rate' a received TST PDU must be copied to CPU. Warning will be given if selected frame size exceeds the CPU RX frame MAX size. Frame MIN Size is 64 Bytes.
slm-testid *<number>*	Specifies a SLM test ID.
synthetic	Specifies synthetic loss measurement is used. Synthetic loss management allows multiple peer MEPs to be configured and measured.
threshold *<number>*	Specifies the frame loss threshold. Valid range is **1** to **100**.
uni	Specifies that OAM PDUs are transmitted with a unicast MAC address. The MAC address is taken from a peer MEP MAC address database. When used with loss measurement, there is only one peer MEP configured and measured.
flow-counting	Specifies that loss measurement is counting service frames per flow.
oam-counting	Specifies loss measurement is counting OAM frames.
all	Specifies loss measurement is counting all OAM frames.
y1731	Specifies loss measurement is counting Y1731 OAM frames.
rx	Enables responses to loss measurement PDUs received from a loss measurement initiator.
synthetic	Optional. Specifies synthetic loss measurement is used. Synthetic loss management allows multiple peer MEPs to be configured and measured.
flr *<number>*	Optional. Specifies the frame loss ratio interval in a number of measurement intervals.
prio *<priority>*	Optional. Specifies the response priority. Valid range is **0** to **7**.

threshold *<number>*	Optional. Specifies the frame loss threshold. Valid range is **1** to **100**.

3.104.2 Default Values

By default, MEPs are not configured. When configured with loss measurement enabled, the frame loss ratio interval is set to **5**, the SLM test ID is set to **0**, and the frame loss threshold is set to **1**.

3.104.3 Command History

ASE Release 4.4-41	Command was introduced.

3.104.4 Usage Examples

The following example enables responses to loss measurement PDUs from a loss measurement initiator for MEP **100**:

```
(config)#mep 100 lm rx
```

3.105 mep <*instance*> lm-avail

Use the **mep** <*instance*> **lm-avail** command to enable loss measurement availability on the maintenance entity point (MEP) instance. Use the **no** form of this command to disable loss measurement availability. Variations of this command include:

mep *<instance>* **lm-avail interval** *<interval>* **flr-threshold** *<number>*
mep <instance> lm-avail maintenance

3.105.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
interval *<interval>*	Specifies the loss measurement availability interval based on the number of measurements. Valid range is **1** to **1000**.
flr-threshold *<number>*	Specifies the frame loss threshold in permille. Valid range is **0** to **1000** permille.
maintenance	Enables the availability maintenance indicator.

3.105.2 Default Values

By default, loss measurement availability is disabled on a configured MEP instance.

3.105.3 Command History

ASE Release 4.4-41	Command was introduced.

3.105.4 Usage Examples

The following example enables loss measurement for maintenance on MEP instance **100**:

```
(config)#mep 100 lm-avail maintenance
```

3.106 mep <*instance*> lm-hli flr-threshold <*number*> interval <*interval*>

Use the **mep** <*instance*> **lm-hli flr-threshold** <*number*> **interval** <*interval*> command to configure loss management high loss interval parameters for a maintenance entity point (MEP) instance. Use the **no** form of this command to disable the high loss interval parameters for the MEP instance.

3.106.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
flr-threshold *<number>*	Specifies the high loss interval frame loss threshold in permille. Valid range is **0** to **1000** permille.
interval *<interval>*	Specifies the high loss interval consecutive interval based on a number of measurements.

3.106.2 Default Values

By default, MEP instances are not configured.

3.106.3 Command History

ASE Release 4.4-41	Command was introduced.

3.106.4 Usage Examples

The following example configures MEP **100** with a high loss interval threshold of **100** permille and an interval of **10**:

```
(config)#mep 100 lm-hli flr-threshold 100 interval 10
```

3.107 mep <*instance*> lm-notif

Use the **mep** <*instance*> **lm-notif** command to enable JSON notification updates for frame loss interval counters on far-end and near-end maintenance entity point (MEP) instances. Use the **no** form of this command to disable JSON notification updates for frame loss on the MEPs. Variations of this command include:

mep *<instance>* **lm-notif los-int-cnt-holddown** *<number>* **los-th-cnt-holddown** *<number>* **hli-cnt-holddown** *<number>*

3.107.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
los-int-cnt-holddown *<number>*	Specifies the hold down timer, in seconds, for JSON notification updates for the near-end MEP frame loss interval count.
los-int-cnt-holddown *<number>*	Specifies the hold down timer, in seconds, for JSON notification updates for the far-end MEP frame loss interval count.
hli-cnt-holddown *<number>*	Specifies the hold down timer for JSON notification updates for near- and far-end MEP high loss interval counts.

3.107.2 Default Values

By default, MEP instances are not configured.

3.107.3 Command History

ASE Release 4.4-41	Command was introduced.

3.107.4 Usage Examples

The following example configures MEP **100** hold down timers for JSON notification updates for both loss and high-loss interval counts:

```
(config)#mep 100 lm-notif los-int-cnt-holddown 10 los-int-cnt-holddown 15 hli-cnt-holddown 20
```

3.108 mep <*instance*> lm-sdeg

Use the **mep** <*instance*> **lm-sdeg** command to configure signal degradation parameters for loss measurement on a maintenance entity point (MEP) instance. Use the **no** form of this command to remove the signal degradation parameters from the MEP. Variations of this command include:

mep <instance> lm-sdeg flr-threshold *<number>* **bad-threshold** *<number>* **good-threshold** *<number>*

3.108.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
flr-threshold *<number>*	Specifies the signal degradation frame loss ratio threshold. Valid range is **0** to **1000** permille.
bad-threshold *<number>*	Specifies the number of consecutive bad interval measurements required to set a signal degraded state.
good-threshold *<number>*	Specifies the number of consecutive good interval measurements required to clear a signal degraded state.

3.108.2 Default Values

By default, MEP instances are not configured.

3.108.3 Command History

ASE Release 4.4-41	Command was introduced.

3.108.4 Usage Examples

The following example configures MEP **100** with a frame loss ratio threshold of **400** permille, **40** consecutive bad interval measurements to count the signal as degraded, and **50** consecutive good interval measurements to count the signal as good:

```
(config)#mep 100 flr-threshold 400 bad-threshold 40 good-threshold 50
```

3.109 mep <*instance*> lt <*priority*>

Use the **mep** <*instance*> **lt** <*priority*> command to configure link trace parameters for a maintenance entity point (MEP) instance. Use the **no** form of this command to disable link trace on the MEP instance. Variations of this command include:

mep *<instance>* **lt** *<priority>* **mac** *<mac address>*
mep *<instance>* **lt** *<priority>* **mep-id** *<id>* **ttl** *<number>*

3.109.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
lt *<priority>*	Specifies the link trace priority for the MEP instance for Operation, Administration, and Management (OAM) tagged traffic. Valid range is **0** to **7**.
mac *<mac address>*	Specifies a link trace target unicast media access control (MAC) address to be used in link trace operations with a maintenance intermediary point (MIP). MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
mep-id *<id>*	Specifies a peer MEP ID to use as a link trace target. Link trace is completed using a unicast MAC address from the peer MEP MAC database. Valid range is **1** to **3124**.
ttl *<number>*	Specifies the time to live (TTL) value for the link trace. Valid range is **0** to **255**.

3.109.2 Default Values

By default, MEP instances are not configured.

3.109.3 Command History

ASE Release 4.4-41	Command was introduced.

3.109.4 Usage Examples

The following example configures MEP instance **100** for a link trace to MEP instance **75**, with a priority of **3** and a TTL value of **10**:

```
(config)#mep 100 lt 3 mep-id 75 ttl 10
```

3.110 mep <*instance*> meg-id <*string*>

Use the **mep** <*instance*> **meg-id** <*string*> command to configure the naming parameters for a maintenance endpoint group (MEG) instance assigned to a maintenance entity point (MEP) instance. Use the **no** form of this command to remove the MEG instance from the MEP. Variations of this command include:

mep *<instance>* **meg-id** *<string>* **ieee**
mep *<instance>* **meg-id** *<string>* **itu**
mep *<instance>* **meg-id** *<string>* **itu-cc**

3.110.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
meg-id *<string>*	Specifies the MEG ID in text string format. String values use either the ITU MEG-ID or the IEEE Short MA format, depending on the selected MEG-ID format (**ieee**, **itu**, or **itu-cc**). ITU strings have a maximum length of **13** characters. ITU-CC strings have a maximum length of **15** characters. IEEE strings have a maximum length of **16** characters.
ieee	Specifies the MEG ID has an IEEE character string format.
itu	Specifies the MEG ID has an ITU format (ICC-UMC).
itu-cc	Specifies the MEG ID has an ITU country code (CC) format (CC-ICC-UMC).

3.110.2 Default Values

By default, no MEGs are associated with any configured MEPs.

3.110.3 Command History

ASE Release 4.4-41	Command was introduced.

3.110.4 Usage Examples

The following example configures a MEG ID with IEEE naming characteristics for MEP **100**:

```
(config)#mep 100 meg-id MEGNAME1 ieee
```

3.111 mep <*instance*> mep-id <*id*>

Use the **mep** <*instance*> **mep-id** <*id*> command to specify a maintenance entity point (MEP) ID for a MEP instance. Use the **no** form of this command to remove the MEP ID from the instance.

3.111.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
mep-id *<id>*	Specifies the MEP ID.

3.111.2 Default Values

By default, no MEP instances are configured.

3.111.3 Command History

ASE Release 4.4-41	Command was introduced.

3.111.4 Usage Examples

The following example configures a MEP ID of **4** for MEP instance **100**:

```
(config)#mep 100 mep-id 4
```

3.112 mep <*instance*> mip

Use the **mep** <*instance*> **mip** command to specify that this maintenance entity point (MEP) instance is a halfway maintenance intermediary point (MIP). Use the no form of this command to remove the MIP configuration from the MEP instance. Variations of this command include:

```
mep <instance> mip down domain evc level <level>
mep <instance> mip down domain evc flow <number> level <level>
mep <instance> mip down domain evc flow <number> level <level> interface <interface>
mep <instance> mip down domain evc level <level> interface <interface>
mep <instance> mip down domain port level <level>
mep <instance> mip down domain port flow <number> level <level>
mep <instance> mip down domain port flow <number> level <level> interface
    <interface>
mep <instance> mip down domain port level <level> interface <interface>
mep <instance> mip down domain vlan level <level>
mep <instance> mip down domain vlan flow <number> level <level>
mep <instance> mip down domain vlan flow <number> level <level> interface
    <interface>
mep <instance> mip down domain vlan level <level> interface <interface>

mep <instance> mip up domain evc level <level> vid <vlan id>
mep <instance> mip up domain evc flow <number> level <level> vid <vlan id>
mep <instance> mip up domain evc flow <number> level <level> interface <interface>
    vid <vlan id>
mep <instance> mip up domain evc level <level> interface <interface> vid <vlan id>
mep <instance> mip up domain port level <level> vid <vlan id>
mep <instance> mip up domain port flow <number> level <level> vid <vlan id>
mep <instance> mip up domain port flow <number> level <level> interface <interface>
    vid <vlan id>
mep <instance> mip up domain port level <level> interface <interface> vid <vlan id>
mep <instance> mip up domain vlan level <level> vid <vlan id>
mep <instance> mip up domain vlan flow <number> level <level> vid <vlan id>
mep <instance> mip up domain vlan flow <number> level <level> interface <interface>
    vid <vlan id>
mep <instance> mip up domain vlan level <level> interface <interface> vid <vlan id>
```

3.112.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
down	Specifies the MEP instance is a halfway MIP downstream.
up	Specifies the MEP instance is a halfway MIP upstream.
domain	Specifies the domain of the MEP instance.
evc	Specifies the MEP domain is an Ethernet Virtual Circuit (EVC).
port	Specifies the MEP domain is a port.
vlan	Specifies the MEP domain is a virtual local area network (VLAN).
level *<level>*	Specifies the maintenance endpoint group (MEG) level of the MEP instance. Valid range is **0** to **7**.
flow *<uint>*	Optional. Specifies the flow instance number for the MEP. This value must be specified for MEPs that are part of a VLAN, EVC, Multiprotocol Label Switching Transport Profile (MPLS-TP) link, tunnel, LSP, or pseudo-wire domain.

interface *<interface>*	Optional. Specifies the interface with which the MEP is associated. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID.
vid *<vlan id>*	Specifies the VLAN ID for an upstream MEP. Valid range is **1** to **4095**.

3.112.2 Default Values

By default, no MEP instances are configured.

3.112.3 Command History

ASE Release 4.4-41	Command was introduced.

3.112.4 Usage Examples

The following example configures the MEP instance **100** as a downstream MIP in a port domain with a MEG level of **4**:

```
(config)#mep 100 mip domain port level 4
```

3.113 mep <*instance*> peer-mep-id <*id*>

Use the **mep** <*instance*> **peer-mep-id** <*id*> command to configure the maintenance entity point (MEP) as a peer MEP instance. Use the **no** form of this command to remove this MEP as a peer. Variations of this command include:

```
mep <instance> peer-mep-id <id>
mep <instance> peer-mep-id <id> mac <mac address>
```

3.113.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
peer-mep-id *<id>*	Specifies the peer MEP ID.
mac *<mac address>*	Optional. Specifies a unicast media access control (MAC) address is used in communication with other MEPs. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).

3.113.2 Default Values

By default, no MEP instances are configured.

3.113.3 Command History

ASE Release 4.4-41	Command was introduced.

3.113.4 Usage Examples

The following example configures MEP instance **100** as a peer MEP with an ID of **10**:

```
(config)#mep 100 peer-mep-id 10
```

3.114 mep <*instance*> performance-monitoring

Use the **mep** <*instance*> **performance-monitoring** command to enable performance monitoring on the maintenance entity point (MEP) instance. Use the **no** form of this command to disable the feature.

3.114.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.

3.114.2 Default Values

By default, performance monitoring is disabled on the MEP instance.

3.114.3 Command History

ASE Release 4.4-41	Command was introduced.

3.114.4 Usage Examples

The following example enables performance monitoring on MEP instance **100**:

```
(config)#mep 100 performance-monitoring
```

3.115 mep <*instance*> syslog

Use the **mep** *<instance>* **syslog** command to enable syslog on the maintenance entity point (MEP) instance. Use the **no** form of this command to disable syslog on the MEP instance.

3.115.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.

3.115.2 Default Values

By default, syslog is disabled on the MEP instance.

3.115.3 Command History

ASE Release 4.4-41	Command was introduced.

3.115.4 Usage Examples

The following example enables syslog on MEP instance **100**:

```
(config)#mep 100 syslog
```

3.116 mep <*instance*> tst <*priority*>

Use the **mep** <*instance*> **tst** <*priority*> command to configure signal test parameters for a maintenance entity point (MEP) instance. Use the **no** form of this command to disable the signal test on the MEP instance. Variations of this command include:

```
mep <instance> tst <priority> dei mep-id <id> all-one
mep <instance> tst <priority> dei mep-id <id> all-zero
mep <instance> tst <priority> dei mep-id <id> one-zero
mep <instance> tst <priority> dei mep-id <id> rate <value> size <size>
mep <instance> tst <priority> dei mep-id <id> sequence
mep <instance> tst <priority> mep-id <id> all-one
mep <instance> tst <priority> mep-id <id> all-zero
mep <instance> tst <priority> mep-id <id> one-zero
mep <instance> tst <priority> mep-id <id> rate <value> size <size>
mep <instance> tst <priority> mep-id <id> sequence
mep <instance> tst rx
mep <instance> tst tx
```

3.116.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
<priority>	Specifies the signal test priority for the MEP instance for Operation, Administration, and Management (OAM) tagged traffic. Valid range is **0** to **7**.
dei	Optional. Specifies the drop eligibility indicator (DEI) is used for OAM tagged traffic.
mep-id *<id>*	Specifies a peer MEP ID to use as a link trace target. Link trace is completed using a unicast MAC address from the peer MEP MAC database. Valid range is **1** to **3124**.
all-one	Specifies the test pattern is set to all ones.
all-zero	Specifies the test pattern is set to all zeros.
one-zero	Specifies the test pattern alternates ones and zeros (**10101010**).
rate *<value>*	Specifies the test frame transmission bit rate in megabits per second (Mbps). This is the bit rate of a standard frame without any encapsulation. If 1 Mbps rate is selected in a EVC MEP, the added tag will give a higher bit rate on the wire. Rate limit is **400** Mbps.
rx	Specifies a received test signal.
sequence	Enables the sequence number in test protocol data unit (PDU) messages.
size *<size>*	Specifies the test frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing TST OAM PDU - including CRC (four bytes). For example, when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes. The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC. There are two frame MAX sizes to consider: the switch RX frame MAX size, which is the MAX frame size (all inclusive) accepted on the switch

	port of 10240 Bytes, and the CPU RX frame MAX size, which is the MAX frame size (all inclusive) possible to copy to CPU of 10240 Bytes. Consider that the Peer MEP must be able to handle the selected frame size. Consider that in order to calculate the 'RX rate' a received TST PDU must be copied to CPU. Warning will be given if selected frame size exceeds the CPU RX frame MAX size. Frame MIN Size is 64 Bytes.
tx	Specifies a transmission test signal.

3.116.2 Default Values

By default, signal tests are not configured for MEP instances.

3.116.3 Command History

ASE Release 4.4-41	Command was introduced.

3.116.4 Usage Examples

The following example enables a test signal transmission from MEP instance **100**:

```
(config)#mep 100 tst tx
```

3.117 mep <*instance*> up

Use the **mep** <*instance*> **up** command to configure an upstream maintenance entity point (MEP). Use the **no** form of this command to remove the MEP configuration. Variations of this command include:

```
mep <instance> up domain evc level <level>
mep <instance> up domain evc level <level> interface <interface>
mep <instance> up domain evc flow <uint> level <level>
mep <instance> up domain evc flow <uint> level <level> interface <interface>
mep <instance> up domain port level <level>
mep <instance> up domain port level <level> interface <interface>
mep <instance> up domain port flow <uint> level <level>
mep <instance> up domain port flow <uint> level <level> interface <interface>
mep <instance> up domain vlan level <level>
mep <instance> up domain vlan level <level> interface <interface>
mep <instance> up domain vlan flow <uint> level <level>
mep <instance> up domain vlan flow <uint> level <level> interface <interface>
```

3.117.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
domain	Specifies the domain of the MEP instance.
evc	Specifies the MEP domain is an Ethernet Virtual Circuit (EVC).
port	Specifies the MEP domain is a port.
vlan	Specifies the MEP domain is a virtual local area network (VLAN).
level *<level>*	Specifies the maintenance endpoint group (MEG) level of the MEP instance. Valid range is **0** to **7**.
flow *<uint>*	Specifies the flow instance number for the MEP. This value must be specified for MEPs that are part of a VLAN, EVC, Multiprotocol Label Switching Transport Profile (MPLS-TP) link, tunnel, LSP, or pseudo-wire domain.
interface *<interface>*	Optional. Specifies the interface with which the MEP is associated. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID.

3.117.2 Default Values

By default, MEPs are not configured.

3.117.3 Command History

ASE Release 4.4-41	Command was introduced.

3.117.4 Usage Examples

The following example specifies that MEP instance **100** is an upstream MEP in an EVC domain with a level of **5**:

```
(config)#mep 100 up domain evc level 5
```

3.118 mep <*instance*> vid <*vlan id*>

Use the **mep** <*instance*> **vid** <*vlan id*> command to associate a virtual local area network (VLAN) with a maintenance entity point (MEP) instance. Use the **no** form of this command to remove the VLAN from the MEP.

3.118.1 Syntax Description

<instance>	Specifies the MEP instance. Valid range is **1** to **3124**.
vid *<vlan id>*	Specifies the VLAN ID for the MEP. Valid range is **1** to **4095**.

3.118.2 Default Values

By default, MEPs are not configured.

3.118.3 Command History

ASE Release 4.4-41	Command was introduced.

3.118.4 Usage Examples

The following example specifies that MEP instance **100** is associated with VLAN **175**:

```
(config)#mep 100 vid 175
```

3.119 mep os-tlv

Use the **mep os-tlv** command to specify the organization-specific time, length, value (OS-TLV) for the maintenance entity point (MEP). Use the **no** form of this command to remove the OS-TLV value. Variations of this command include:

mep os-tlv oui *<oui>* **sub-type** *<type>* **value** *<value>*

3.119.1 Syntax Description

oui *<oui>*	Specifies the organizationally unique identifier. Valid range is **0** to **0xFFFFFF**.
sub-type *<type>*	Specifies the sub-type in a one octet value. Valid range is **0** to **0xFF**.
value *<value>*	Specifies the value in a one octet value. Valid range is **0** to **0xFF**.

3.119.2 Default Values

By default, MEPs are not configured.

3.119.3 Command History

ASE Release 4.4-41	Command was introduced.

3.119.4 Usage Examples

The following example specifies th OS-TLV information for the MEP:

```
(config)#mep os-tlv oui 0 sub-type 0 value 0
```

3.120 monitor session

Use the **monitor session** command to enable and configure a traffic mirroring session. Use the **no** form of this command to remove the traffic mirroring session. Variations of this command include:

```
monitor session <session id>
monitor session <session id> destination interface <interface>
monitor session <session id> destination remote vlan <vlan id> reflector-port
    <interface>
monitor session <session id> source cpu both
monitor session <session id> source cpu rx
monitor session <session id> source cpu tx
monitor session <session id> source interface <interface>
monitor session <session id> source interface <interface> both
monitor session <session id> source interface <interface> rx
monitor session <session id> source interface <interface> tx
monitor session <session id> source remote vlan <vlan id>
monitor session <session id> source vlan <vlan id>
```

3.120.1 Syntax Description

<session id>	Specifies the mirroring session for configuration. Valid range depends on the ASE switch model. For an 8-port ASE switch, the range is **1** to **5**.
destination	Specifies a mirroring destination for the session.
source	Specifies a mirroring source for the session.
interface *<interface>*	Specifies the source or destination interface for the mirroring session. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID.
remote vlan *<vlan id>*	Specifies the virtual local area network (VLAN) to use for sending remote mirror traffic. Valid range is **1** to **4095**.
reflector-port *<interface>*	Creates the reflector port for remote mirroring. The reflector port directs the mirrored traffic to the mirroring VLAN. This setting is only used when configuring remote mirroring. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID.
vlan *<vlan id>*	Specifies a source VLAN for VLAN-based mirroring. This option is only available for local mirroring. Valid range is **1** to **4095**.
cpu	Specifies the mirroring source is the CPU.
both	Specifies that both received and transmitted traffic is mirrored.
rx	Specifies that traffic received on the port or CPU is mirrored.
tx	Specifies that traffic transmitted from the port or CPU is mirrored.

3.120.2 Default Values

By default, no mirroring sessions are configured. When configured, VLAN-based mirroring uses VLAN **200**.

3.120.3 Command History

ASE Release 4.4-41	Command was introduced.

3.120.4 Usage Examples

The following example specifies the GigabitEthernet 1/1 interface as a source port for a local mirroring session monitoring transmitted traffic:

```
(config)#monitor session 1 source interface GigabitEthernet 1/1 tx
```

3.121 mvr

Use the **mvr** command to enable and configure multicast virtual local area network (VLAN) registration (MVR) parameters on the ASE device. Use the **no** form of this command to disable MVR or remove the configuration. Variations of this command include:

```
mvr name <name> channel <name>
mvr name <name> election
mvr name <name> frame priority <priority>
mvr name <name> frame tagged
mvr name <name> igmp-address <ipv4 address>
mvr name <name> last-member-query-interval <number>
mvr name <name> mode compatible
mvr name <name> mode dynamic

mvr vlan <vlan ids> channel <name>
mvr vlan <vlan ids> name <name> channel <name>
mvr vlan <vlan ids> election
mvr vlan <vlan ids> name <name> election
mvr vlan <vlan ids> frame priority <priority>
mvr vlan <vlan ids> name <name> frame priority <priority>
mvr vlan <vlan ids> frame tagged
mvr vlan <vlan ids> name <name> frame tagged
mvr vlan <vlan ids> igmp-address <ipv4 address>
mvr vlan <vlan ids> name <name> igmp-address <ipv4 address>
mvr vlan <vlan ids> last-member-query-interval <number>
mvr vlan <vlan ids> name <name> last-member-query-interval <number>
mvr vlan <vlan ids> mode compatible
mvr vlan <vlan ids> name <name> mode compatible
mvr vlan <vlan ids> mode dynamic
mvr vlan <vlan ids> name <name> mode dynamic
```

3.121.1 Syntax Description

name *<name>*	Specifies the MVR multicast VLAN name. Valid names are no more than 16 characters in length.
vlan *<vlan ids>*	Specifies the MVR multicast VLANs. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.
channel *<name>*	Specifies the MVR channel configuration profile name. Valid names are no more than 16 characters in length.
election	Specifies that the MVR instance acts as an Internet Group Management Protocol (IGMP) querier to join querier elections.
frame	Specifies the MVR control frame for transmissions.
priority *<priority>*	Specifies a class of service (CoS) priority. Valid range is 0 to 7.
tagged	Specifies that tagged IGMP/MLD frames are sent.
igmp-address *<ipv4 address>*	Specifies a unicast IPv4 address is used for the MVR address in IGMP. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

last-member-query-interval *<number>*	Specifies the last member query interval in tenths of seconds. Valid range is **0** to **31744** tenths of a second.
mode	Specifies the MVR mode of operation.
compatible	Specifies MVR operates in compatible mode.
dynamic	Specifies MVR operates in dynamic mode.

3.121.2 Default Values

By default, MVR is disabled.

3.121.3 Privilege Level

By default, this command has a privilege level of **15**.

3.121.4 Command History

ASE Release 4.4-41	Command was introduced.

3.121.5 Usage Examples

The following example configures MVR for VLAN **175** in dynamic mode:

```
(config)#mvr vlan 175 name VLANNAME1 mode dynamic
```

3.122 mvrp

Use the **mvrp** command to enable and configure Multiple virtual local area network (VLAN) Registration Protocol (MVRP) on the ASE device. Use the **no** form of this command to disable MVRP. Variations of this command include:

```
mvrp
mvrp managed vlan <vlan id>
mvrp managed vlan add <vlan id>
mvrp managed vlan all
mvrp managed vlan except <vlan id>
mvrp managed vlan none
mvrp managed vlan remove <vlan id>
```

3.122.1 Syntax Description

managed vlan	Optional. Specifies the VLANs to be managed by MVRP.
add	Optional. Adds a VLAN ID to the managed VLANs list.
all	Optional. Specifies that all VLANs are managed by MVRP.
except	Optional. Specifies a VLAN ID that is not to be managed by MVRP.
none	Optional. Specifies that no VLANs are manged by MVRP.
remove	Optional. Removes the VLAN ID from the managed VLANs list.
<vlan id>	Optional. Specifies the VLAN ID to be managed by MVRP, or be added, removed, or exempted from the managed VLAN list. Valid range is **1** to **4095**.

3.122.2 Default Values

By default, MVRP is disabled.

3.122.3 Command History

ASE Release 4.4-41	Command was introduced.

3.122.4 Usage Example

The following example enables MVRP on the ASE device:

```
(config)#mvrp
```

3.123 ntp

Use the **ntp** command to enable and configure the Network Time Protocol (NTP) parameters on the ASE device. Use the **no** form of this command to remove the NTP configuration. Variations of this command include:

```
ntp
ntp server <number> ip-address <domain name>
ntp server <number> ip-address <ipv4 address>
ntp server <number> ip-address <ipv6 address>
```

3.123.1 Syntax Description

server *<number>*	Specifies the NTP server number. Valid range is 1 to 5.
ip-address *<domain name>*	Specifies the domain name of the NTP server.
ip-address *<ipv4 address>*	Specifies an Internet Protocol version 4 (IPv4) unicast address for the NTP server. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
ip-address *<ipv6 address>*	Specifies an IPv6 unicast address for the NTP server. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.

3.123.2 Default Values

By default, NTP is disabled.

3.123.3 Privilege Level

By default, this command has a privilege level of **13**.

3.123.4 Command History

ASE Release 4.4-41	Command was introduced.

3.123.5 Usage Examples

The following example enables NTP:

```
(config)#ntp
```

3.124 poe capacitor-detect

Use the **poe capacitor-detect** to enable Power over Ethernet (POE) capacitor detection. his feature is used for PoE detection in legacy products that do not meet PoE or PoE+ IEEE standards. Use the **no** form of this command to disable this feature.

3.124.1 Syntax Description

No subcommands.

3.124.2 Default Values

By default, capacitor detection is disabled.

3.124.3 Command History

ASE Release 4.4-41	Command was introduced.

3.124.4 Usage Examples

The following example enables POE capacitor detection:

```
(config)#poe capacitor-detect
```

3.125 poe management mode

Use the **poe management mode** command to configure the power management behavior for Pover over Ethernet (POE) configurations. Power management is configured by specifying how the reserved power is determined (by class, allocation, or Link Layer Discover Protocol (LLDP)) and specifying the power management mode (actual consumption or reserved power). Use the **no** form of this command to disable POE. Variations of this command include:

```
poe management mode allocation-consumption
poe management mode allocation-reserved-power
poe management mode class-consumption
poe management mode class-reserved-power
poe management mode lldp-consumption
poe management mode lldp-reserved-power
```

3.125.1 Syntax Description

allocation-consumption	Specifies that power management is completed by shutting down ports whose actual power usage exceeds their allocated power.
allocation-reserved-power	Specifies that power management is completed by shutting down ports whose power usage exceeds the amount of power reserved on the port.
class-consumption	Specifies that the class of powered device (PD) on the port determines which ports are shut down if actual power usage exceeds the power allocated for the specific class.
class-reserved-power	Specifies that the class of PD on the port determines which ports are shut down if power usage exceeds the amount of power reserved on the port for the PD class.
lldp-consumption	Specifies that the power assigned to a port is determined by LLDP, and that power management is completed by shutting down ports whose actual power usage exceeds the power allocated by LLDP.
lldp-reserved-power	Specifies that the power assigned to a port is determined by LLDP, and that power management is completed by shutting down ports whose power usage exceeds the amount of power reserved on the port by LLDP.

3.125.2 Default Values

By default, POE is enabled.

3.125.3 Privilege Level

By default, this command has a privilege level of **15**.

3.125.4 Command History

ASE Release 4.4-41	Command was introduced.

3.125.5 Usage Examples

The following example specifies that POE power management uses allocation consumption:

```
(config)#poe management mode allocation-consumption
```

3.126 poe ping-check

Use the **poe ping-check** command to enable or disable Power Over Ethernet (POE) ping checking. Variations of this command include:

```
poe ping-check disable
poe ping-check enable
```

3.126.1 Syntax Description

disable	Disables the POE ping check.
enable	Enables the POE ping check.

3.126.2 Default Values

By default, POE ping check is disabled.

3.126.3 Command History

ASE Release 4.4-41	Command was introduced.

3.126.4 Usage Examples

The following example enables POE ping check:

```
(config)#poe ping-check enable
```

3.127 poe profile id

Use the **poe profile id** command to configure and apply a Power over Ethernet (POE) schedule to a port to automate when the port is enabled or disabled. Use the **no** form of this command to remove the POE profile. Variations of this command include:

poe profile id *<id>* **name** *<name>*
poe profile id *<id> <day> <start hour> <start minute> <end hour> <end minute>*

3.127.1 Syntax Description

<id>	Specifies a numerical ID for the POE schedule profile. Valid ID range is **1** to **16**.
name *<name>*	Specifies the name of the POE scheduling profile. Profile names are limited to **32** characters in length.
<day>	Specifies the day of the week (**Mon**, **Tue**, **Wed**, **Thr**, **Fri**, **Sat**, or **Sun**) on which to employ the PoE schedule.
<start hour>	Specifies the start hour for the schedule. Valid range is **0** to **23**.
<start minute>	Specifies the start time (in minutes) for the schedule. Valid minute range is **0** to **55**, and must be entered in multiples of **5**.
<end hour>	Specifies the end hour for the schedule. Valid range is **0** to **23**.
<end minute>	Specifies the end time (in minutes) for the schedule. Valid minute range is **0** to **55**, and must be entered in multiples of **5**.

3.127.2 Default Values

By default, no POE schedules are configured.

3.127.3 Privilege Level

By default, this command has a privilege level of **15**.

3.127.4 Command History

ASE Release 4.4-41	Command was introduced.

3.127.5 Usage Examples

The following example creates a POE schedule profile with an ID of **1**, that enables PoE on the port on Mondays, from **8:30** am to **12:30** pm, enter the command as follows:

```
(config)#poe profile id 1 Mon 8 30 12 30
```

3.128 poe supply <*value*>

Use the **poe supply** <*value*> command to specify the power supply's deliverable power. In order to manage the powered devices (PDs), the ASE needs to know the maximum amount of power the power supply can deliver. This value is not automatically detected and must be specified. Typically, the configured power supply value is less than the actual power that the power supply can deliver in order to prevent the power supply from being exceeded when the PDs are turned on.

3.128.1 Syntax Description

<value>	Specifies the deliverable power. Valid range, in Watts, varies by hardware.

3.128.2 Default Values

No default values are necessary for this command.

3.128.3 Privilege Level

By default, this command has a privilege level of **15**.

3.128.4 Command History

ASE Release 4.4-41	Command was introduced.

3.128.5 Usage Examples

Enter the command as follows to specify a maximum power of 150 Watts for the power supply:

```
(config)#poe supply 150
```

3.129 privilege <*mode*> level <*level*> <*command string*>

Use the **privilege** <*mode*> **level** <*level*> <*command string*> command to assigned a privilege level to specific commands. The exact command mode name is required to identify the correct commands or command string.

3.129.1 Syntax Description

<mode>	Specifies the exact command mode name to which the command or command string belongs.
level *<level>*	Specifies the privilege level to be applied to the commands. Valid range is **0** through **15**.
<command string>	Optional. Specifies the command string to which the privilege level is to be applied. This can include the full command string or partial command string. Maximum string length is **128** characters.

3.129.2 Default Values

By default, commands in Basic mode are set to a **0** privilege level, and the admin user is set at level **15** by default, the highest possible privilege level.

3.129.3 Command History

ASE Release 4.4-41	Command was introduced.

3.129.4 Usage Examples

The following example sets the privilege level to **15** for the **ip address** command in the virtual local area network (VLAN) interface configuration mode:

```
(config)#privilege if-vlan level 15 ip address
```

3.130 prompt <*prompt*>

Use the **prompt** <*prompt*> command to configure the prompt display on the ASE device. Use the **no** form of this command to remove the configured prompt.

3.130.1 Syntax Description

<prompt>	Specifies the prompt with a maximum of 32 characters. Refer to the "Functional Notes" below for prompt variable information.

3.130.2 Default Values

By default, no prompt is configured.

3.130.3 Command History

ASE Release 4.4-41	Command was introduced.

3.130.4 Functional Notes

Prompts, when being configured, must be proceeded by the percent sign (**%**). Prompts can be entered with variables. The following variables are used for prompt configuration:

- **%h** signifies a host name as the prompt
- **%%** signifies a percent sign
- **%s** signifies a space
- **%t** signifies a tab
- **%D** signifies the date
- **%T** signifies the time
- **%Z** signifies the date and time

3.130.5 Usage Examples

The following example configures the prompt with the ASE host name, and date and time:

```
(config)#prompt %h%s%Z
```

3.131 ptp

Use the **ptp** command to enable Precision Time Protocol (PTP) on the ASE device. Use the **no** form of this command to disable PTP.

3.131.1 Syntax Description

No subcommands.

3.131.2 Default Values

By default, PTP is disabled.

3.131.3 Command History

ASE Release 4.4-41	Command was introduced.

3.131.4 Usage Examples

The following example enables PTP:

```
(config)#ptp
```

3.132 ptp <*instance*>

Use the **ptp** <*instance*> command to configure the Precision Time Protocol (PTP) parameters for specific clock instances on the ASE device. Use the **no** form of this command to remove the clock instance configuration. Variations of this command include:

```
ptp <instance> afi-announce
ptp <instance> afi-sync
ptp <instance> clk sync <threshold> ap <number>
ptp <instance> domain <number>
ptp <instance> filter-type aci-basic-phase
ptp <instance> filter-type aci-basic-phase-low
ptp <instance> filter-type aci-basic-phase-low-synce
ptp <instance> filter-type aci-basic-phase-synce
ptp <instance> filter-type aci-bc-full-on-path-freq
```

3.132.1 Syntax Description

<instance>	Specifies the clock instance to configure. Valid range is **0** to **3**.
afi-announce	Enables automatic frame injection of PTP announce frames.
afi-sync	Enables automatic frame injection of PTP sync frames.
clk	Specifies the PTP slave clock configuration.
sync *<threshold>*	Configures the PTP slave clock to the “clock in SyncE locked” setting by defining the threshold at which the slave clock is offset from the master clock when the offset increment/decrement mode is defined. Valid range is **1** to **1000** nanoseconds.
ap *<number>*	Specifies the offset increment/decrement mode for the SyncE threshold. Valid range is **1** to **40**.
domain *<number>*	Specifies the PTP clock domain. Valid range is **0** to **127**.
filter-type	Specifies the PTP filter type.
aci-basic-phase	Specifies the ACI basic phase filter.
aci-basic-phase-low	Specifies the ACI basic low phase filter.
aci-basic-phase-low-synce	Specifies the ACI basic low phase filter in conjunction with SyncE.
aci-basic-phase-synce	Specifies the ACI basic phase filter in conjunction with SyncE.
aci-bc-full-on-path-freq	Specifies the ACI BC full-on-path frequency filter.

3.132.2 Default Values

By default, PTP clock instances are not configured.

3.132.3 Command History

ASE Release 4.4-41	Command was introduced.

3.132.4 Usage Examples

The following example configures PTP clock instance **2** for the PTP domain **10**:

```
(config)#ptp 2 domain 10
```

3.133 ptp ext

Use the **ptp ext** command to configure the Precision Time Protocol (PTP) external clock parameters. Use the **no** form of this command to remove the external clock configuration. Variations of this command include:

```
ptp ext auto
ptp ext ext <frequency>
ptp ext input
ptp ext ltc
ptp ext out-in
ptp ext output
```

3.133.1 Syntax Description

auto	Specifies the clock control is automatically determined based on the PTP profile and hardware resources.
ext *<frequecy>*	Specifies the external clock's frequency output. Valid range is **1** to **25000000** Hz.
input	Enables 1PPS input for the clock.
ltc	Specifies the local time controller (LTC) provides frequency control for the external clock.
out-in	Enables 1PPS output and input for the clock (Jaguar1 only).
output	Enables 1PPS output for the clock.

3.133.2 Default Values

By default, the external PTP clock is not configured.

3.133.3 Command History

ASE Release 4.4-41	Command was introduced.

3.133.4 Usage Examples

The following example specifies the PTP external clock control is automatically determined:

```
(config)#ptp ext auto
```

3.134 ptp ho-spec

Use the **ptp ho-spec** command to specify the holdover parameters for G8275 Precision Time Protocol (PTP) clocks. Use the **no** form of this command to remove the holdover configurations. Variations of this command include:

```
ptp ho-spec cat1 <time>
ptp ho-spec cat2 <time>
ptp ho-spec cat3 <time>
```

3.134.1 Syntax Description

cat1	Specifies the cat1 time is being configured.
cat2	Specifies the cat2 time is being configured.
cat3	Specifies the cat3 time is being configured.
<time>	Specifies the time in seconds. Valid range is **0** to **999999999** seconds.

3.134.2 Default Values

By default, the G8275 PTP clock is not configured.

3.134.3 Command History

ASE Release 4.4-41	Command was introduced.

3.134.4 Usage Examples

The following example specifies the **cat1** holdover time for the G8275 PTP clock is **2500** seconds:

```
(config)#ptp ho-spec cat1 2500
```

3.135 ptp io-pin <*number*>

Use the **ptp io-pin** <*instance*> command to configure or display the input and output configuration of the Precision Time Protocol (PTP) clock. Use the **no** form of this command to remove the input or output clock configuration. Variations of this command include:

```
ptp io-pin <number> domain <number>
ptp io-pin <number> freq <frequency>
ptp io-pin <number> interface <interface>
ptp io-pin <number> load
ptp io-pin <number> pps-output
ptp io-pin <number> save
ptp io-pin <number> waveform-output
```

3.135.1 Syntax Description

<number>	Specifies a pin number. Valid range is **0** to **3**.
domain *<number>*	Specifies a PTP domain to associate with this pin. Valid range is **0** to **2**.
freq *<frequency>*	Specifies the clock frequency for waveform output. Valid range is **1** to **25000000** Hz.
interface *<interface>*	Specifies the PTP slave clock interface. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID.
load	Specifies the input and output configuration to load. Configuration loading occurs with the next 1pps input.
pps-output	Specifies the input and output is set to 1-pps output.
save	Specifies the input and output pin configuration is saved. Saving occurs with the next 1pps input.
waveform-output	Specifies the input and output is set to the waveform clock output.

3.135.2 Default Values

By default, no PTP clock pins are configured.

3.135.3 Command History

ASE Release 4.4-41	Command was introduced.

3.135.4 Usage Examples

The following example specifies PTP clock pin **2** is assigned to PTP domain **1**:

```
(config)#ptp io-pin 2 domain 1
```

3.136 ptp tc-internal mode <*mode*>

Use the **ptp tc-internal mode** <*mode*> command to specify the internal Precision Time Protocol (PTP) clock mode. Use the **no** form of this command to remove the internal clock configuration.

3.136.1 Syntax Description

<mode>	Specifies the internal clock mode. Valid range is **0** to **3**. Entering **0** indicates **MODE_30BIT**, **1** indicates **MODE_32BIT**, **2** indicates **MODE_44BIT**, and **3** indicates **MODE48_BIT**.

3.136.2 Default Values

By default, the internal clock mode is not set.

3.136.3 Command History

ASE Release 4.4-41	Command was introduced.

3.136.4 Usage Examples

The following example specifies the PTP internal clock is in 48 BIT mode:

```
(config)#ptp tc-internal mode 3
```

3.137 ptp system-time

Use the **ptp system-time** command to enable synchronization between the Precision Time Protocol (PTP) time and the ASE system time. Use the **no** form of this command to disable this feature. Variations of this command include:

```
ptp system-time get
ptp system-time set
```

3.137.1 Syntax Description

get	Specifies the PTP time is retrieved from the system time.
set	Specifies the system time is updated from the PTP time.

3.137.2 Default Values

By default, synchronization between PTP time and system time is disabled.

3.137.3 Command History

ASE Release 4.4-41	Command was introduced.

3.137.4 Usage Examples

The following example specifies that PTP time is retrieved from the system time:

```
(config)#ptp system-time get
```

3.138 qos map cos-dscp <*value*> dpl <*value*> dscp <*value*>

Use the **qos map cos-dscp** command to map Class of Service (CoS) values to Differentiated Service Code Points (DSCP) values for Quality of Service (QoS) configurations. This command can be entered as many times as necessary to map as many CoS values to DSCP values as needed. Use the **no** form of this command to remove the CoS to DSCP mapping.

3.138.1 Syntax Description

cos-dscp *<value>*	Specifies the CoS class value to be mapped to the DSCP value. Valid range is **0** to **7**, and can be entered as a single class value or as a range.
dpl *<value>*	Defines the drop precedence level (DPL) value associated with the CoS class; valid range is **0** to **3**, and can be entered as a single value or as a range.
dscp *<value>*	Specifies the DSCP value to be associated with the specified CoS class. Valid range is **0** to **63**.

3.138.2 Default Values

By default, no CoS values are mapped to DSCP values for QoS.

3.138.3 Privilege Level

By default, this command has a privilege level of **15**.

3.138.4 Command History

ASE Release 4.4-41	Command was introduced.

3.138.5 Functional Notes

CoS values can be mapped to DSCP values for use with DSCP-based QoS. When this option is configured, traffic coming into the switch is automatically classified by its CoS and DPL value, and then assigned a corresponding DSCP value. The DSCP value can then be used to classify, remark, or rewrite traffic as it moves through the ASE device. For more information about QoS configuration in the ASE device, refer to the *Configuring QoS in ASE* configuration guide, available online at https://supportcommunity.adtran.com.

3.138.6 Usage Examples

To configure the CoS to DSCP map to associate the DSCP value **10** with the CoS class **5**, enter the command as follows:

```
(config)#qos map cos-dscp 5 dpl 2 dscp 10
```

3.139 qos map dscp-classify *<dscp value>*

Use the **qos map dscp-classify** command to specify that particular Differentiated Service Code Points (DSCP) values are classified as trustworthy and can be used by other Quality of Service (QoS) processes (ingress traffic classification and egress traffic rewriting). Enter the command as many times as necessary to classify as many DSCP values as necessary. Use the **no** form of this command to remove the DSCP value from the DSCP classification table.

3.139.1 Syntax Description

<dscp value>	Specifies the DSCP value to classify as trustworthy. Valid range is **0** to **63**.

3.139.2 Default Values

By default, no DSCP values are classified as trustworthy for QoS.

3.139.3 Privilege Level

By default, this command has a privilege level of **15**.

3.139.4 Command History

ASE Release 4.4-41	Command was introduced.

3.139.5 Functional Notes

DSCP classification is used for additional classification of ingress traffic on the port, as well as rewriting DSCP values on egress traffic. By default, DSCP classification is disabled, indicating that no DSCP classification is completed for ingress traffic and is not applied to egress traffic. When DSCP classification is enabled on the port, specific, trusted DSCP values are configured as “classified,” and can be used to further classify ingress traffic or to rewrite egress traffic. DSCP values are configured as trusted and classified using the globally-configured DSCP Classify Map. For more information about QoS configuration in the ASE device, refer to the *Configuring QoS in ASE* configuration guide, available online at https://supportcommunity.adtran.com.

3.139.6 Usage Examples

To globally configure DSCP classification of specific DSCP values for use with other QoS features, such as best effort (**0**) or assured forwarding (**10**) DSCP values, enter the command as follows:

```
(config)#qos map dscp-classify 0
(config)#qos map dscp-classify 10
```

3.140 qos map dscp-cos <*value*> cos <*value*> dpl <*value*>

Use the **qos map dscp-cos** command to map Differentiated Service Code Points (DSCP) values to Class of Service (CoS) values for Quality of Service (QoS) configurations. This command can be entered as many times as necessary to map as many DSCP values to CoS values as needed. Use the **no** form of this command to remove the DSCP to CoS mapping.

3.140.1 Syntax Description

dscp-cos *<value>*	Specifies the DSCP value being mapped to the CoS class value. Valid range is **0** to **63**.
cos *<value>*	defines the CoS class value that you are associating with the specified DSCP value; valid range is **0** to **7**, and can be entered as a single value or as a range.
dpl *<value>*	Defines the drop precedence level (DPL) value associated with the CoS class; valid range is **0** to **3**, and can be entered as a single value or as a range.

3.140.2 Default Values

By default, no DSCP values are mapped to CoS values for QoS.

3.140.3 Privilege Level

By default, this command has a privilege level of **15**.

3.140.4 Command History

ASE Release 4.4-41	Command was introduced.

3.140.5 Functional Notes

DSCP values can be mapped to CoS values for use with DSCP-based QoS. When this option is configured, traffic coming into the switch is automatically classified by its DSCP value and then assigned corresponding CoS and DPL values. The CoS and DPL values can then be used to classify, remark, or rewrite traffic as it moves through the ASE device. For more information about QoS configuration in the ASE device, refer to the *Configuring QoS in ASE* configuration guide, available online at https://supportcommunity.adtran.com.

3.140.6 Usage Examples

To configure the DSCP to CoS map to associate the DSCP value **10** with the CoS class **5**, enter the command as follows:

```
(config)#qos map dscp-cos 10 cos 5 dpl 2
```

3.141 qos map dscp-egress-translation <*dscp value*> to <*dscp value*>

Use the **qos map dscp-egress-translation** command to specify Differentiated Service Code Points (DSCP) values for egress translation. Quality of Service (QoS) configuration uses the values specified in the DSCP egress translation map to remap the DSCP values of egress traffic on the port. Use the **no** form of this command remove the specific DSCP value from DSCP translation.

3.141.1 Syntax Description

<dscp value>	Specifies the DSCP value to be mapped or the DSCP value to which another value is mapped. Valid range is **0** to **63**.

3.141.2 Default Values

By default, no DSCP egress translation values are mapped.

3.141.3 Privilege Level

By default, this command has a privilege level of **15**.

3.141.4 Command History

ASE Release 4.4-41	Command was introduced.

3.141.5 Usage Examples

To configure specific DSCP values to be used for remapping egress traffic, enter the command as follows:

```
(config)#qos map dscp-egress-translation 34 to 14
(config)#qos map dscp-egress-translation 10 to 0
```

3.142 qos map dscp-ingress-translation *<dscp value>* to *<dscp value>*

Use the **qos map dscp-ingress-translation** command to specify Differentiated Service Code Points (DSCP) values for ingress translation. Quality of Service (QoS) configuration uses the values specified in the DSCP ingress translation map to remap the DSCP values of ingress traffic on the port. Use the **no** form of this command remove the specific DSCP value from DSCP translation.

3.142.1 Syntax Description

<dscp value>	Specifies the DSCP value to be mapped or the DSCP value to which another value is mapped. Valid range is **0** to **63**.

3.142.2 Default Values

By default, no DSCP ingress translation values are mapped.

3.142.3 Privilege Level

By default, this command has a privilege level of **15**.

3.142.4 Command History

ASE Release 4.4-41	Command was introduced.

3.142.5 Usage Examples

To configure specific DSCP values to be used for remapping ingress traffic, enter the command as follows:

```
(config)#qos map dscp-ingress-translation 34 to 14
(config)#qos map dscp-ingress-translation 10 to 0
```

3.143 qos map egress *<map id>*

Use the **qos map egress** *<map id>* command to create an egress Quality of Service (QoS) map, assigns it an ID, and enters the map's configuration mode. Use the **no** form of this command to remove the egress map configuration.

3.143.1 Syntax Description

<map id>	Specifies the egress map ID. Valid range is **0** to **255**.

3.143.2 Default Values

By default, no QoS egress maps are configured.

3.143.3 Privilege Level

By default, this command has a privilege level of **15**.

3.143.4 Command History

ASE Release 4.4-41	Command was introduced.

3.143.5 Functional Notes

Several parameters are available for configuration once you have entered the QoS egress map's configuration mode. These commands are detailed in the "QoS Egress Map Command Set" on page 668.

3.143.6 Usage Examples

To create a new QoS egress map, with an ID of **75**, enter the command as follows:

```
(config)#qos map egress 75
(config-qos-map-egress)#
```

3.144 qos map ingress <*map id*>

Use the **qos map ingress** <*map id*> command to create an ingress Quality of Service (QoS) map, assigns it an ID, and enters the map's configuration mode. Use the **no** form of this command to remove the ingress map configuration.

3.144.1 Syntax Description

<map id>	Specifies the ingress map ID. Valid range is **0** to **255**.

3.144.2 Default Values

By default, no QoS ingress maps are configured.

3.144.3 Privilege Level

By default, this command has a privilege level of **15**.

3.144.4 Command History

ASE Release 4.4-41	Command was introduced.

3.144.5 Functional Notes

Several parameters are available for configuration once you have entered the QoS ingress map's configuration mode. These commands are detailed in the "QoS Ingress Map Command Set" on page 677.

3.144.6 Usage Examples

To create a new QoS ingress map, with an ID of **100**, enter the command as follows:

```
(config)#qos map egress 100
(config-qos-map-ingress)#
```

3.145 qos qce <*ace id*>

Use the **qos qce** <*ace id*> command to configure Quality of Service (QoS) control lists (QCLs). QCLs can be used to configure flexible classification for Layer 2, 3, and 4 network traffic, and can perform reclassification of traffic based on Class of Service (CoS), Drop Precedence Level (DPL), Priority Code Point (PCP), Drop Eligibility Indicator (DEI), Differentiated Service Code Points (DSCP), and access control list (ACL) values. The QCL is comprised of various QoS control entries (QCEs), which are applied on a per-port basis, and can specify source and destination media access control (MAC) addresses, traffic types, virtual local area network (VLAN) IDs, PCP values, and frame types that receive certain classifications if the incoming traffic matches the QCE criteria. Use the **no** version of this command to remove the specified QCE from the ASE device configuration. Variations of this command include:

qos qce *<qce id>* **[refresh | update** *<qce id>***] [action** *<action>***]** [*<matching criteria>*] [*<qce operation>*]

3.145.1 Syntax Description

<ace id>	Specifies the ID number of the QoS control list entry. Valid range is **1** to **256**. When used alone, it creates the QCE with the specified ID number.
refresh	Refreshes the QCE tables in hardware.
update *<qce id>*	Specifies that a previously configured QCE is being updated or edited. Valid range is **1** to **256**.
action *<action>*	Enables CoS, DPL, DSCP, ingress map, PCP-DEI, and policy classification for traffic that matches the QCE matching criteria. Refer to "Functional Notes" on page 423 for specific parameters used as QCE actions.
<matching criteria>	Specifies the key values that are compared to the values included in incoming traffic packets and frames. Refer to "Functional Notes" on page 423 for specific parameters used as matching criteria.
<qce operation>	Specifies the location of the QCE in the QCE list and can apply the QCE to an interface. Refer to Refer to "Functional Notes" on page 423 for specific parameters used as QCE operations.

3.145.2 Default Values

By default, no QCEs or QCLs are configured.

3.145.3 Privilege Level

By default, this command has a privilege level of **15**.

3.145.4 Command History

ASE Release 4.4-41	Command was introduced.

3.145.5 Functional Notes

The following paragraphs describe the available parameters for defining QCE actions, matching criteria, and operations. For more information about QoS configuration in the ASE device, refer to the *Configuring QoS in ASE* configuration guide, available online at https://supportcommunity.adtran.com.

QCE Actions

After entering the **action** keyword in the QCE configuration command, you can specify one of the following *<action>* parameters:

- **cos [***<value>* **| default]**: Configures CoS class actions. Specifying *<value>* assigns a single CoS class ID. Valid range is **0** to **7**. Using the **default** parameter specifies that matching traffic keeps the existing setting.
- **dpl [***<value>* **| default]**: Configures DPL actions. Specifying *<value>* assigns a single DPL value. Valid range is **0** to **3**. Using the **default** parameter specifies that matching traffic keeps the existing setting.
- **dscp [***<value>* **| default]**: Configures DSCP actions. Specifying *<value>* assigns a single DSCP value. Valid range is **0** to **63**. Using the **default** parameter specifies that matching traffic keeps the existing setting.
- **ingress-map [***<map id>* **| default]**: Assigns a QoS ingress map to the incoming traffic. Specifying *<map id>* assigns a single ingress map to the traffic. Valid range is **0** to **127**. Using the **default** parameter specifies that matching traffic keeps the existing ingress map setting.
- **pcp-dei [***<pcp value> <dei value>* **| default]**: Configures PCP and DEI actions. Using the *<pcp value> <dei value>* parameter assigns a new PCP value (range is **0** to **7**) and DEI value (range is **0** to **1**. Using the **default** parameter specifies that matching traffic keeps the existing setting.
- **policy [***<acl id>* **| default]**: Assigns an ACL to the incoming traffic. Specifying *<acl id>* assigns a single ACL to the traffic. Valid range is **0** to **127**. Using the **default** parameter specifies that matching traffic keeps the existing ACL setting.

Each of these *<action>* can be entered multiple times, and in any order. The following is an example of configuring QCE **5** with a CoS action:

```
(config)#qos qce 5 action cos 2
```

After specifying an *<action>* parameter for the QCE, you can begin specifying the QCE *<matching criteria>* parameters.

Matching Criteria

QCE matching criteria are specified key values that are compared to the values included in incoming traffic packets and frames. Multiple types of matching criteria can be used in a single QCE entry, and can be entered in any order. The same *<matching criteria>* parameters are available in almost every area of the QCE configuration.

Table 3-4 on page 3-424 below displays the *<matching criteria>* parameters available in QCE configuration, listing the criteria keywords, the additional configurable parameters for each keyword, and a description of the matching action they perform.

Table 3-4. Available Parameters for QCE *<matching criteria>*

Keyword	Parameters	Description
<action>	Refer to "Functional Notes" on page 423	Actions can be included after a specified matching criteria is defined, without having to use the **action** keyword.
dmac	**[***<mac_address>* **| any | broadcast | multicast | unicast]**	Configures traffic matching based on destination MAC address. Enter *<mac_address>* in the **xx-xx-xx-xx-xx-xx** format. The **any** keyword indicates any destination MAC address matches. The **broadcast**, **multicast**, and **unicast** keywords indicate broadcast, multicast, or unicast destination MAC addresses match, respectively.
frame-type	**[any | etype | ipv4 | ipv6 | llc | snap]** **Note**: Each of these parameters has additional configuration for matching parameters. Refer to "Functional Notes" on page 423.	Configures traffic matching based on the specific frame type. The **any** keyword specifies any frame type is matched. The **etype** keyword specifies the Ether type of frame to match. The **ipv4** keyword specifies that IPv4 packets are matched.The **ipv6** keyword specifies that IPv6 packets are matched. The **llc** keyword specifies that LLC frames are matched. The **snap** keyword indicates that SNAP frames are matched.
inner-tag	**dei [***<value>* **| default]** **pcp [***<value>* **| default]** **type [any | c-tagged | s-tagged | tagged | untagged]** **vid [***<id>* **| any]**	Configures traffic matching based on the inner tag of the traffic. The **dei** *<value>* parameter specifies the DEI value; valid range is **0** to **1**. The **pcp** *<value>* parameter specifies the PCP value; valid range is **0** to **7**. The **default** keyword indicates the existing DEI or PCP value is used for matching. The **any** keyword indicates any type of tag or VLAN ID matches. The **c-tagged**, **s-tagged**, **tagged,** and **untagged** keywords indicate C-tagged, S-tagged, tagged, or untagged traffic matches, respectively. The **vid** *<id>* parameter specifies the VLAN ID, or ID range, of the inner tag to use for matching.
smac	**[***<mac_address>* **| any]**	Configures traffic matching based on source MAC address. Enter *<mac_address>* in the **xx-xx-xx-xx-xx-xx** format. The **any** keyword indicates any source MAC address matches.
tag	**dei [***<value>* **| default]** **pcp [***<value>* **| default]** **type [any | c-tagged | s-tagged | tagged | untagged]** **vid [***<id>* **| any]**	Configures traffic matching based on the tag of the traffic. The **dei** *<value>* parameter specifies the DEI value; valid range is **0** to **1**. The **pcp** *<value>* parameter specifies the PCP value; valid range is **0** to **7**. The **default** keyword indicates the existing DEI or PCP value is used for matching. The **any** keyword indicates any type of tag or VLAN ID matches. The **c-tagged**, **s-tagged**, **tagged,** and **untagged** keywords indicate C-tagged, S-tagged, tagged, or untagged traffic matches, respectively. The **vid** *<id>* parameter specifies the VLAN ID tag, or ID range, to use for matching.

Each of these *<matching criteria>* parameters can be entered multiple times, and in any order. The following is an example of configuring QCE **5** with a CoS action, and matching based on destination MAC addresses and VLAN ID tags:

```
(config)#qos qce 5 action cos 2 dmac any tag vid 100
```

Frame-Type Matching Criteria

The **frame-type** matching criteria for QCEs includes several additional parameters and configuration options. The frame types available to use as matching criteria include specific Ethernet frames, IPv4 and IPv6 packets, LLC frames, and SNAP frames. You can specify additional parameters for each of these options to use as matching criteria for the QCE. The command syntax for specifying matching criteria by frame type appears as follows:

```
(config)#qos qce <qce id> frame-type [any | etype | ipv4 | ipv6 | llc | snap]
```

The syntax of the **frame-type** keywords, and their additional parameters, are defined below:

- **any**: Specifies that matching occurs for traffic of any frame type.
- **etype** *<value>*: Specifies the EtherType frame used for traffic matching. Valid *<value>* ranges are **0x600** to **0x7ff**, **0x801** to **0x86dc**, **0x86de** to **0xfff**.
- **ipv4**: Specifies IPv4 information is used for traffic matching. This frame type has additional configuration parameters for specific IPv4 criteria to use for matching purposes. Refer to Table 3-5 on page 3-426.
- **ipv6**: Specifies IPv6 information is used for traffic matching. This frame type has additional configuration parameters for specific IPv6 criteria to use for matching purposes. Refer to Table 3-5 on page 3-426.
- **llc**: Specifies LLC frame information is used for traffic matching. This frame type has additional configuration parameters for specific LLC frame types to use for matching purposes. Refer to Table 3-6 on page 3-427.
- **snap** [*<value>* | **any**]: Specifies SNAP frame information is used for traffic matching. Valid *<value>* range is **0** to **0xfff**. The **any** keyword indicates matching occurs for any SNAP frame.

The following tables display the additional configurable parameters for the IPv4, IPv6, and LLC frame types. These additional parameters are configured after entering the frame type keyword, and can be followed by specifying additional *<actions>*, *<matching criteria>*, or *<qce operations>* parameters.

Table 3-5. Additional Parameters for IPv4 and IPv6 Frame Type *<matching criteria>*

Keyword	Parameters	Description
dip	[*<ipv4 address>* *<subnet mask>* | **any**] [*<ipv6 address>* | **any**]	Configures traffic matching based on destination IP address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). IPv4 subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**). IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**. The **any** keyword indicates any destination IP address matches.
dport	[*<port>* | **any**]	Configures traffic matching based on UDP/TCP destination port. Valid *<port>* range is **0** to **65535**. The **any** keyword indicates any destination TCP or UDP port matches.
fragment (Note: Applies to **ipv4** only)	[**any** | **no** | **yes**]	Configures traffic matching based on IPv4 packet fragments. The **any** keyword indicates any IPv4 packet fragment matches. The **no** keyword indicates matches occur only on non-fragmented IPv4 traffic. The **yes** keyword indicates matches occur on IPv4 fragments.
proto	[*<number>* | **any** | **tcp** | **udp**]	Configures traffic matching based on IP protocol. The *<number>* parameter indicates a specific protocol number. Valid range is **0** to **255**. The **any** keyword indicates any IP protocol matches. The **tcp** keyword indicates matches occur on TCP protocol packets. The **udp** keyword indicates matches occur on UDP protocol packets.
sip	[*<ipv4 address>* *<subnet mask>* | **any**] [*<ipv6 address>* | **any**]	Configures traffic matching based on source IP address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). IPv4 subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**). IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**. The **any** keyword indicates any source IP address matches.
sport	[*<port>* | **any**]	Configures traffic matching based on UDP/TCP source port. Valid *<port>* range is **0** to **65535**. The **any** keyword indicates any source TCP or UDP port matches.
<action>	Refer to **"Functional Notes"** on page 423	Actions can be specified after entering the additional IPv4 or IPv6 traffic matching specifications, without having to use the **action** keyword.
<matching criteria>	Refer to "Functional Notes" on page 423	Additional matching criteria can be specified after entering the additional IPv4 or IPv6 traffic matching specifications.
<qce operations>	Refer to "Functional Notes" on page 423	QCE operations can be specified after entering the additional IPv4 or IPv6 traffic matching specifications.

Table 3-6. Additional Parameters for LLC Frame Type *<matching criteria>*

Keyword	Parameters	Description
control	[*<value>* | **any**]	Configures traffic matching based on LLC control bytes. The <value> parameter specifies a single control byte; valid range is **0** to **0xff**. The **any** keyword indicates any LLC control byte matches.
dsap	[*<value>* | **any**]	Configures traffic matching based on LLC destination SAP bytes. The <value> parameter specifies a single destination SAP byte; valid range is **0** to **0xff**. The **any** keyword indicates any LLC destination SAP byte matches.
ssap	[*<value>* | **any**]	Configures traffic matching based on LLC source SAP bytes. The <value> parameter specifies a single source SAP byte; valid range is **0** to **0xff**. The **any** keyword indicates any LLC source SAP byte matches.
<action>	Refer to **"Functional Notes"** on page 423	Actions can be specified after entering the additional LLC traffic matching specifications, without having to use the **action** keyword.
<matching criteria>	Refer to "Functional Notes" on page 423	Additional matching criteria can be specified after entering the additional LLC traffic matching specifications.
<qce operations>	Refer to "Functional Notes" on page 423	QCE operations can be specified after entering the additional LLC traffic matching specifications.

QCE Operations

QCE operations are values that act on the QCE entry itself, to specify the location of the QCE entry. This parameter is configured by entering one (or more) of the following keywords and their parameters:

- **interface** *<interface>*: Associates the QCE with an interface. The *<interface>* parameter is specified in the format **GigabitEthernet** *<slot/port>* or **10GigabitEthernet** *<slot/port>*.
- **last**: Specifies this QCE is placed at the end of the list of configured QCEs.
- **next** *<qce id>*: Specifies this QCE is placed in the QCE list before the specified QCE ID. Valid *<qce id>* range is **1** to **256**.

To configure a QCE (**5**), that applies CoS and DSCP values to IPv4 traffic with a destination TCP port of **443**, and appears last in the QCE list, enter the command as follows:

```
(config)#qos qce 5 action cos 2 dscp 10 frame-type ipv4 dport 443 last
```

To associate the QCE with an interface, enter the command as follows:

```
(config)#qos qce 5 interface GigabitEthernet 1/1
```

3.145.6 Usage Examples

The following is an example of configuring QCE **5** with a CoS action, and matching based on destination MAC addresses and VLAN ID tags:

```
(config)#qos qce 5 action cos 2 dmac any tag vid 100
```

To configure a QCE (**5**), that applies CoS and DSCP values to IPv4 traffic with a destination TCP port of **443**, and appears last in the QCE list, enter the command as follows:

```
(config)#qos qce 5 action cos 2 dscp 10 frame-type ipv4 dport 443 last
```

To associate the QCE with an interface, enter the command as follows:

```
(config)#qos qce 5 interface GigabitEthernet 1/1
```

3.146 qos storm

Use the **qos storm** command to configure global Quality of Service (QoS) storm policers. Use the **no** form of this command to remove the storm policer configuration. Variations of this command include:

```
qos storm broadcast <rate>
qos storm broadcast <rate> fps
qos storm broadcast <rate> kbps
qos storm broadcast <rate> kfps
qos storm broadcast <rate> mbps

qos storm multicast <rate>
qos storm multicast <rate> fps
qos storm multicast <rate> kbps
qos storm multicast <rate> kfps
qos storm multicast <rate> mbps

qos storm unicast <rate>
qos storm unicast <rate> fps
qos storm unicast <rate> kbps
qos storm unicast <rate> kfps
qos storm unicast <rate> mbps
```

3.146.1 Syntax Description

broadcast	Specifies that the policer is applied to broadcast traffic.
multicast	Specifies that the policer is applied to multicast traffic.
unicast	Specifies that the policer is applied to unicast traffic.
<rate>	Specifies the rate limit of the policer. Valid range is **1** to **13128147**.
fps	Optional. Specifies the rate unit for the policer in frames per second.
kbps	Optional. Specifies the rate unit for the policer in kilobits per second.
kfps	Optional. Specifies the rate unit for the policer in kiloframes per second.
mbps	Optional. Specifies the rate unit for the policer in Megabits per second.

3.146.2 Default Values

By default, global storm policers are not configured. When configured, the global storm policer is set to a rate limit **10 fps**.

3.146.3 Privilege Level

By default, this command has a privilege level of **15**.

3.146.4 Command History

ASE Release 4.4-41	Command was introduced.

3.146.5 Functional Notes

You can optionally choose to configure global-level storm policers on the ASE device to aid in QoS functionality. Global storm policers apply to the entire switch, and can be used to restrict the amount of flooded frames, those without previously-learned source MAC addresses, from entering the device. Global policers can be configured to limit unicast, multicast, or broadcast packets. For more information about QoS configuration in the ASE device, refer to the *Configuring QoS in ASE* configuration guide, available online at https://supportcommunity.adtran.com.

3.146.6 Usage Examples

To configure the QoS global storm policer to limit unicast traffic, enter the command as follows:

```
(config)#qos storm unicast 100 mbps
```

3.147 qos wred group

Use the **qos wred group** command to configure a Weighted Random Early Detection (WRED) group for Quality of Service (QoS) queues on the ASE device. Use the **no** form of this command to remove the WRED group. Variations of this command include:

```
qos wred group <group id> queue <queue> dpl <value> min-fl <number> max <number>
qos wred group <group id> queue <queue> dpl <value> min-fl <number> max <number>
    fill-level
```

3.147.1 Syntax Description

<group id>	Creates the WRED group that will be associated with the queue. Valid range is **1** to **3**.
queue *<queue>*	Specifies the queue associated with the WRED group. Valid range is **0** to **7**, and can be entered as a specific queue, or a range of queues.
dpl *<value>*	Associates a drop probability level with the queue, and is used by default as the fill maximum value for the queue. Valid range is **1** to **3**.
min-fl *<number>*	Specifies the minimum fill level (in percent) of the queue. Valid range is **0** to **100** percent.
max *<number>*	Specifies the maximum threshold (in percent) for the queue. Valid range is **1** to **100** percent.
fill-level	Optional. Specifies that packets are not dropped until the fill-level of the queue is reached, rather than when the drop probability percentage is reached.

3.147.2 Default Values

By default, no QoS WRED groups are configured. When they are configured, the queue uses the drop probability setting to determine when packets begin to drop from the queue.

3.147.3 Privilege Level

By default, this command has a privilege level of **15**.

3.147.4 Command History

ASE Release 4.4-41	Command was introduced.

3.147.5 Usage Examples

To configure a WRED group with an ID of **2**, for queue **3** with a DPL value of **2** and a minimum fill percentage of **75** percent and a maximum drop probability of **95**, enter the command as follows:

```
(config)#qos wred group 2 queue 3 dpl 2 min-fl 75 max 95
```

3.148 radius-server attribute

Use the **radius-server attribute** command to configure the network access server (NAS) attributes for the remote authentication dial-in user service (RADIUS) server used by the ASE device. Use the **no** form of this command to remove the RADIUS server attribute configuration. Variations of this command include:

```
radius-server attribute 32 <id>
radius-server attribute 4 <ipv4 address>
radius-server attribute 95 <ipv6 address>
```

3.148.1 Syntax Description

32 *<id>*	Specifies the NAS 32 attribute and the accompanying NAS identifier. Identifiers are between 1 and 253 characters in length.
4 *<ipv4 address>*	Specifies the NAS 4 attribute and the accompanying unicast Internet Protocol version 4 (IPv4) address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
95 *<ipv6 address>*	Specifies the NAS 95 attribute and the accompanying unicast IPv6 address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.

3.148.2 Default Values

By default, the RADIUS server is not configured.

3.148.3 Privilege Level

By default, this command has a privilege level of **15**.

3.148.4 Command History

ASE Release 4.4-41	Command was introduced.

3.148.5 Usage Examples

The following example configures the NAS attribute **4** for the RADIUS server:

```
(config)#radius-server attribute 4 10.10.2.1
```

3.149 radius-server deadtime <*value*>

Use the **radius-server deadtime** <*value*> command to specify the time to wait (in minutes) before attempting to reconnect to a remote authentication dial-in user service (RADIUS) server that has timed out. Use the **no** form of this command to return to the default setting.

3.149.1 Syntax Description

<value>	Specifies the time to wait (in minutes) before attempting to reconnect to a RADIUS server that has timed out. Valid range is **1** to **1440** minutes.

3.149.2 Default Values

By default, the RADIUS server deadtime is set to **1** minute.

3.149.3 Privilege Level

By default, this command has a privilege level of **15**.

3.149.4 Command History

ASE Release 4.4-41	Command was introduced.

3.149.5 Usage Examples

The following example configures the RADIUS deadtime to **100** minutes:

```
(config)#radius-server deadtime 100
```

3.150 radius-server host

Use the **radius-server host** command to specify the parameters for a remote authentication dial-in user service (RADIUS) server. Use the **no** form of this command to return to the default settings. Variations of this command include:

```
radius-server host <hostname | ip address>
radius-server host <hostname | ip address> acct-port <port>
radius-server host <hostname | ip address> auth-port <port>
radius-server host <hostname | ip address> key encrypted <key>
radius-server host <hostname | ip address> key unencrypted <key>
radius-server host <hostname | ip address> retransmit <number>
radius-server host <hostname | ip address> timeout <value>
```

3.150.1 Syntax Description

<hostname | ip address>	Specifies the server to configure. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). If a host name is used, a domain naming system (DNS) server should be learned by the ASE device using Dynamic Host Configuration Protocol (DHCP), Point-to-Point Protocol (PPP), or specified in the Global Configuration mode with the command “hostname <hostname>” on page 314.
acct-port *<port>*	Specifies the User Datagram Protocol (UDP) port used by the AAA accounting server. Port range is **0** to **65535**.
auth-port *<port>*	Specifies the UDP port used by the AAA authentication server. The port range is **0** to **65535**. Entering **0** disables authentication.
key encrypted *<key>*	Specifies the key used by the RADIUS server is an encrypted key. This command overrides the global RADIUS key setting (set with the command “radius-server” on page 436). This command must be entered last in the command line because everything after the **key** parameter is read as the new key.
key unencrypted *<key>*	Specifies the key used by the RADIUS server is an unencrypted key. This command overrides the global RADIUS key setting (set with the command “radius-server” on page 436). This command must be entered last in the command line because everything after the **key** parameter is read as the new key.
retransmit *<number>*	Specifies the number of connection attempts made to the server. Attempt range is **1** to **1000**.
timeout *<value>*	Specifies the time to wait (in seconds) for this server to reply to requests. Range is **1** to **1000** seconds.

3.150.2 Default Values

By default, **acct-port** is set to **1813** and **auth-port** is set to **1812**. By default, the key, retransmit and timeout values are the values set by the command “radius-server” on page 436.

3.150.3 Privilege Level

By default, this command has a privilege level of **15**.

3.150.4 Command History

ASE Release 4.4-41	Command was introduced.

3.150.5 Functional Notes

At a minimum, the address (IP or host name) of the server must be given. The other parameters can be entered in any order (except the **key** parameter) and, if the parameters are not specified, they will take default values or fall back on the global RADIUS server's default settings (set using the command "radius-server" on page 436).

3.150.6 Usage Examples

The following example specifies that the RADIUS server at IP address **10.10.10.2** uses the global key setting (left unspecified), a timeout value of **10** seconds, the default authorization port (left unspecified), and a retransmit number of **5**:

```
(config)#radius-server host 10.10.10.2 retransmit 5 timeout 10
```

3.151 radius-server

Use the **radius-server** command to configure several remote authentication dial-in user service (RADIUS) parameters for all RADIUS servers on the network. Most of these global settings can be overridden on a per-server basis (using the command "radius-server host" on page 434). Use the **no** form of this command to return to the default setting. Variations of this command include:

```
radius-server key encrypted <key>
radius-server key unencrypted <key>
radius-server retransmit <number>
radius-server timeout <value>
```

3.151.1 Syntax Description

key encrypted *<key>*	Specifies the encrypted key shared by all RADIUS servers. This is a global setting; however, it can be overridden on a per-server basis.
key unencrypted *<key>*	Specifies the unencrypted key shared by all RADIUS servers. This is a global setting; however, it can be overridden on a per-server basis.
retransmit *<number>*	Specifies the number of connection attempts to a RADIUS server. Attempt range is **1** to **1000**. This is a global setting; however, it can be overridden on a per-server basis.
timeout *<value>*	Specifies the amount of time (in seconds) that RADIUS servers have to respond to a request. Time range is **1** to **1000** seconds. This is a global setting; however, it can be overridden on a per-server basis.

3.151.2 Default Values

By default, there is no key set, the retry is set for **1** attempt, and the timeout value is set to **5** seconds.

3.151.3 Privilege Level

By default, this command has a privilege level of **15**.

3.151.4 Command History

ASE Release 4.4-41	Command was introduced.

3.151.5 Usage Examples

The following example shows a typical configuration of these parameters:

```
(config)#radius-server key unencrypted mysecretkey
(config)#radius-server retransmit 4
(config)#radius-server timeout 2
```

3.152 rmon alarm

Use the **rmon alarm** command to configure remote monitoring alarm parameters. Use the **no** form of this command to disable remote monitoring alarms. Variations of this command include:

rmon alarm *<id>* **ifInOctets** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]**
rmon alarm *<id>* **ifInOctets** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] both**
rmon alarm *<id>* **ifInOctets** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] falling**
rmon alarm *<id>* **ifInOctets** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] rising**
rmon alarm *<id>* **ifInOctets** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]**
rmon alarm *<id>* **ifInOctets** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] both**
rmon alarm *<id>* **iflinOctets** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] falling**
rmon alarm *<id>* **ifInOctets** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] rising**

rmon alarm *<id>* **ifInUncastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]**
rmon alarm *<id>* **ifInUncastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] both**
rmon alarm *<id>* **ifInUncastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] falling**
rmon alarm *<id>* **ifInUncastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] rising**
rmon alarm *<id>* **ifInUncastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]**
rmon alarm *<id>* **ifInUncastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] both**
rmon alarm *<id>* **ifInUncastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] falling**
rmon alarm *<id>* **ifInUncastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] rising**

rmon alarm *<id>* **ifInNUncastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]**
rmon alarm *<id>* **ifInNUncastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] both**
rmon alarm *<id>* **ifInNUncastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] falling**
rmon alarm *<id>* **ifInNUncastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] rising**
rmon alarm *<id>* **ifInNUncastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]**
rmon alarm *<id>* **ifInNUncastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] both**
rmon alarm *<id>* **ifInNUncastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] falling**

rmon alarm *<id>* **ifInNUncastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] rising**

rmon alarm *<id>* **ifInDiscards** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]**
rmon alarm *<id>* **ifInDiscards** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] both**
rmon alarm *<id>* **ifInDiscards** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] falling**
rmon alarm *<id>* **ifInDiscards** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] rising**
rmon alarm *<id>* **ifInDiscards** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]**
rmon alarm *<id>* **ifInDiscards** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] both**
rmon alarm *<id>* **ifInDiscards** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] falling**
rmon alarm *<id>* **ifInDiscards** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] rising**

rmon alarm *<id>* **ifInErrors** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]**
rmon alarm *<id>* **ifInErrors** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] both**
rmon alarm *<id>* **ifInErrors** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] falling**
rmon alarm *<id>* **ifInErrors** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] rising**
rmon alarm *<id>* **ifInErrors** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]**
rmon alarm *<id>* **ifInErrors** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] both**
rmon alarm *<id>* **ifInErrors** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] falling**
rmon alarm *<id>* **ifInErrors** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] rising**

rmon alarm *<id>* **ifInUnkownProtos** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]**
rmon alarm *<id>* **ifInUnkownProtos** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] both**
rmon alarm *<id>* **ifInUnkownProtos** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] falling**
rmon alarm *<id>* **ifInUnkownProtos** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] rising**
rmon alarm *<id>* **ifInUnkownProtos** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]**
rmon alarm *<id>* **ifInUnkownProtos** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] both**
rmon alarm *<id>* **ifInUnkownProtos** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] falling**
rmon alarm *<id>* **ifInUnkownProtos** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] rising**

rmon alarm *<id>* **ifOutOctets** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]**
rmon alarm *<id>* **ifOutOctets** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] both**
rmon alarm *<id>* **ifOutOctets** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] falling**
rmon alarm *<id>* **ifOutOctets** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] rising**
rmon alarm *<id>* **ifOutOctets** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]**
rmon alarm *<id>* **ifOutOctets** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] both**
rmon alarm *<id>* **ifOutOctets** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] falling**
rmon alarm *<id>* **ifOutOctets** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] rising**

rmon alarm *<id>* **ifOutUcastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]**
rmon alarm *<id>* **ifOutUcastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] both**
rmon alarm *<id>* **ifOutUcastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] falling**
rmon alarm *<id>* **ifOutUcastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] rising**
rmon alarm *<id>* **ifOutUcastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]**
rmon alarm *<id>* **ifOutUcastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] both**
rmon alarm *<id>* **ifOutUcastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] falling**
rmon alarm *<id>* **ifOutUcastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] rising**

rmon alarm *<id>* **ifOutNUcastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]**
rmon alarm *<id>* **ifOutNUcastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] both**
rmon alarm *<id>* **ifOutNUcastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] falling**
rmon alarm *<id>* **ifOutNUcastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***] rising**
rmon alarm *<id>* **ifOutNUcastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]**
rmon alarm *<id>* **ifOutNUcastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] both**
rmon alarm *<id>* **ifOutNUcastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] falling**
rmon alarm *<id>* **ifOutNUcastPkts** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***] rising**

rmon alarm *<id>* **ifOutDiscards** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]**

rmon alarm *<id>* **ifOutDiscards** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]** **both**
rmon alarm *<id>* **ifOutDiscards** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]** **falling**
rmon alarm *<id>* **ifOutDiscards** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]** **rising**
rmon alarm *<id>* **ifOutDiscards** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]**
rmon alarm *<id>* **ifOutDiscards** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]** **both**
rmon alarm *<id>* **ifOutDiscards** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]** **falling**
rmon alarm *<id>* **ifOutDiscards** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]** **rising**

rmon alarm *<id>* **ifOutErros** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]**
rmon alarm *<id>* **ifOutErros** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]** **both**
rmon alarm *<id>* **ifOutErros** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]** **falling**
rmon alarm *<id>* **ifOutErros** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]** **rising**
rmon alarm *<id>* **ifOutErros** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]**
rmon alarm *<id>* **ifOutErros** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]** **both**
rmon alarm *<id>* **ifOutErros** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]** **falling**
rmon alarm *<id>* **ifOutErros** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]** **rising**

rmon alarm *<id>* **ifOutUnkownProtos** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]**
rmon alarm *<id>* **ifOutUnkownProtos** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]** **both**
rmon alarm *<id>* **ifOutUnkownProtos** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]** **falling**
rmon alarm *<id>* **ifOutUnkownProtos** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event> <falling threshold>* **[***<falling event>***]** **rising**
rmon alarm *<id>* **ifOutUnkownProtos** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]**
rmon alarm *<id>* **ifOutUnkownProtos** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]** **both**
rmon alarm *<id>* **ifOutUnkownProtos** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]** **falling**
rmon alarm *<id>* **ifOutUnkownProtos** *<index> <interval>* **[absolute | delta] rising-threshold** *<value> <rising event>* **falling-threshold** *<value>* **[***<falling event>***]** **rising**

3.152.1 Syntax Description

<id>	Specifies the alarm entry ID. Valid range is **1** to **65535**.
ifInOctets	Specifies an alarm for the total number of octets received on the interface, including framing characters.

ifInUcastPkts	Specifies an alarm for the number of unicast packets delivered to a higher-layer protocol.
ifInNUcastPkts	Specifies an alarm for the number of broadcast and multicast packets delivered to a higher-layer protocol.
ifInDiscards	Specifies an alarm for the number of inbound packets that are discarded even if the packets are normal.
ifInErrors	Specifies an alarm for the number of inbound packets that contained errors, thus preventing them from being deliverable to a higher-layer protocol.
ifInUnknownProtos	Specifies an alarm for the number of the inbound packets that were discarded because of an unknown or unsupported protocol.
ifOutOctets	Specifies an alarm for the total number of octets transmitted from the interface, including framing characters.
ifOutUcastPkts	Specifies an alarm for the number of unicast packets requested to be transmitted from the interface.
ifOutNUcastPkts	Specifies an alarm for the number of broadcast and multicast packets requested to be transmitted from the interface.
ifOutDiscards	Specifies an alarm for the number of outbound packets that are discarded even if the packets are normal.
ifOutErrors	Specifies an alarm for the number of outbound packets that contained errors, thus preventing them from being transmitted.
ifOutUnknownProtos	Specifies an alarm for the number of the outbound packets that were discarded because of an unknown or unsupported protocol.
<index>	Specifies the interface index.
<interval>	Specifies the sample interval. Valid range is **1** to **2147483647**.
absolute	Specifies that each sample is tested directly.
delta	Specifies that the delta between each sample is tested.
rising-threshold *<value>*	Specifies the rising threshold value. Valid range is **-214748367** to **2147483647**.
<rising event>	Specifies the event to fire when the rising threshold value is surpassed. Valid range is **0** to **65535**.
falling-threshold *<value>*	Specifies the falling threshold value. Valid range is **-214748367** to **2147483647**.
<falling event>	Optional. Specifies the event to fire when the falling threshold value is surpassed. Valid range is **0** to **65535**.
both	Optional. Specifies alarms are trigged when the first value is larger than the rising threshold or less than the falling threshold.
falling	Optional. Specifies alarms are triggered when the first value is less than the falling threshold.

rising	Optional. Specifies alarms are triggered when the first value is larger than the rising threshold.

3.152.2 Default Values

By default, no remote monitoring alarms are configured. When configured, the default behavior is to trigger an alarms when the first value is larger than the rising threshold or less than the falling threshold.

3.152.3 Privilege Level

By default, this command has a privilege level of **15**.

3.152.4 Command History

ASE Release 4.4-41	Command was introduced.

3.152.5 Usage Examples

The following example configures a remote monitoring alarm for inbound errors:

```
(config)#rmon alarm 10000 ifInErrors 6 9999 absolute rising-threshold 0 falling-
    threshold 0 both
```

3.153 rmon event

Use the **rmon event** command to configure remote monitoring event parameters. Use the **no** form of this command to disable remote monitoring events. Variations of this command include:

```
rmon event <id> log
rmon event <id> trap
rmon event <id> description <text>
```

3.153.1 Syntax Description

<id>	Specifies the even ID. Valid range is **1** to **65535**.
log	Specifies a remote monitoring log is generated when an event occurs.
trap	Specifies a Simple Network Monitoring Protocol (SNMP) trap is generated when an event occurs.
description *<text>*	Specifies a description for the event. Descriptions have a maximum length of **127** characters.

3.153.2 Default Values

By default, no remote monitoring events are configured.

3.153.3 Privilege Level

By default, this command has a privilege level of **15**.

3.153.4 Command History

ASE Release 4.4-41	Command was introduced.

3.153.5 Usage Examples

The following example specifies a log is generated when a remote monitoring event occurs:

```
(config)#rmon event 100 log
```

3.154 sflow

Use the **sflow** command to configure statistics flow (sflow) parameters on the ASE device. Use the **no** form of this command to disable the sflow feature. Variations of this command include:

```
sflow agent-ip ipv4 <ipv4 address>
sflow agent-ip ipv6 <ipv6 address>
sflow collector-address <domain name>
sflow collector-address <ipv4 address>
sflow collector-address <ipv6 address>
sflow collector-port <number>
sflow max-datagram-size <value>
sflow timeout <value>
```

3.154.1 Syntax Description

agent-ip	Specifies the IP address associated with the sflow agent. This address is used as the agent address in User Datagram Protocol (UDP) messages.
ipv4 *<ipv4 address>*	Specifies the agent address is an Internet Protocol version 4 (IPv4) address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
ipv6 *<ipv6 address>*	Specifies the agent address is an Internet Protocol version 6 (IPv6) address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
collector-address	Specifies the address of the sflow collector.
<domain name>	Specifies the domain name of the sflow collector.
<ipv4 address>	Specifies the IPv4 address of the sflow collector. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<ipv6 address>	Specifies the IPv6 address of the sflow collector. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
collector-port *<number>*	Specifies the UDP port of the sflow collector. Valid range is **1** to **65535**.
max-datagram-size *<value>*	Specifies the maximum datagram size for collection. Valid range is **200** to **1468** bytes.
timeout *<value>*	Specifies the timeout for the sflow collector. The ASE device decrements the timeout once per second until it reaches zero. Before it reaches zero, the collector receives traffic samples. Once the timeout reaches zero, the receiver and its configuration revert to the default values. Valid range is **0** to **2147483647** seconds.

3.154.2 Default Values

By default, sflow is disabled. When enabled, the agent IP address is set to an IPv4 loopback address.

3.154.3 Privilege Level

By default, this command has a privilege level of **15**.

3.154.4 Command History

ASE Release 4.4-41	Command was introduced.

3.154.5 Usage Examples

The following example configures the sflow agent address, collector port, frame size collected, and timeout values:

```
(config)#sflow agent-ip ipv4 192.168.1.2
(config)#sflow collector-port 3
(config)#sflow max-datagram-size 333
(config)#sflow timeout 3333
```

3.155 snmp-server access

Use the **snmp-server access** command to configure Simple Network Management Protocol (SNMP) access security parameters. Use the **no** form of this command to remove the SNMP server access configuration. Variations of this command include:

```
snmp-server access <name> model any level auth
snmp-server access <name> model any level auth read <name>
snmp-server access <name> model any level auth write <name>
snmp-server access <name> model any level noauth
snmp-server access <name> model any level noauth read <name>
snmp-server access <name> model any level noauth write <name>
snmp-server access <name> model any level priv
snmp-server access <name> model any level priv read <name>
snmp-server access <name> model any level priv write <name>

snmp-server access <name> model v1 level auth
snmp-server access <name> model v1 level auth read <name>
snmp-server access <name> model v1 level auth write <name>
snmp-server access <name> model v1 level noauth
snmp-server access <name> model v1 level noauth read <name>
snmp-server access <name> model v1 level noauth write <name>
snmp-server access <name> model v1 level priv
snmp-server access <name> model v1 level priv read <name>
snmp-server access <name> model v1 level priv write <name>

snmp-server access <name> model v2c level auth
snmp-server access <name> model v2c level auth read <name>
snmp-server access <name> model v2c level auth write <name>
snmp-server access <name> model v2c level noauth
snmp-server access <name> model v2c level noauth read <name>
snmp-server access <name> model v2c level noauth write <name>
snmp-server access <name> model v2c level priv
snmp-server access <name> model v2c level priv read <name>
snmp-server access <name> model v2c level priv write <name>

snmp-server access <name> model v3 level auth
snmp-server access <name> model v3 level auth read <name>
snmp-server access <name> model v3 level auth write <name>
snmp-server access <name> model v3 level noauth
snmp-server access <name> model v3 level noauth read <name>
snmp-server access <name> model v3 level noauth write <name>
snmp-server access <name> model v3 level priv
snmp-server access <name> model v3 level priv read <name>
snmp-server access <name> model v3 level priv write <name>
```

3.155.1 Syntax Description

<name>	Specifies the SNMP group name. Valid names cannot exceed 32 characters in length.
model	Specifies the SNMP security model to be used for access security.
any	Specifies that **any** SNMP security model is accepted.
v1	Specifies that the SNMP **v1** security model is used.
v2c	Specifies that the SNMP **v2c** security model is used.
v3	Specifies that the SNMP **v3** security model is used.

level	Specifies the SNMP security level for the SNMP group.
auth	Specifies the authNoPriv security level for the SNMP group.
noauth	Specifies the noAuthNoPriv security level for the SNMP group.
priv	Specifies the authPriv security level for the SNMP group.
read *<name>*	Optional. Specifies a read view for the group. Read view names cannot exceed **32** characters in length.
write *<name>*	Optional. Specifies a write view for the group. Write view names cannot exceed **32** characters in length.

3.155.2 Default Values

By default, SNMP is not configured.

3.155.3 Privilege Level

By default, this command has a privilege level of **15**.

3.155.4 Command History

ASE Release 4.4-41	Command was introduced.

3.155.5 Usage Examples

The following example configures the SNMP group TEXT with the v2c security model, no authorization, and a write group:

```
(config)#snmp-server access TEXT model v2c level noauth write TEXT2
```

3.156 snmp-sever community

Use the **snmp-server community** command specify a community string to control access to the Simple Network Management Protocol (SNMP) information. Use the **no** form of this command to remove a specified community. Variations of this command include:

```
snmp-server community <name>
snmp-server community <name> encrypted <secret>
snmp-server community <name> ip-range <ipv4 address> <subnet mask>
snmp-server community <name> ipv6-range <ipv6 address>
```

3.156.1 Syntax Description

<name>	Specifies the community string (a password to grant SNMP access).
encrypted *<secret>*	Optional. Specifies an encrypted community secret. Valid secrets have between **96** and **160** characters.
ip-range	Specifies an Internet Protocol version 4 (IPv4) address range for the community.
<ipv4 address>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**).
ipv6-range	Specifies an IPv6 address range for the community.
<ipv6 address>	Specifies an IPv6 address. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.

3.156.2 Default Values

By default, SNMP is not configured.

3.156.3 Privilege Level

By default, this command has a privilege level of **15**.

3.156.4 Command History

ASE Release 4.4-41	Command was introduced.

3.156.5 Usage Examples

The following example configures the SNMP community:

```
(config)#snmp-server community COMMUNITY1 ip-range 192.168.1.0 255.255.255.0
```

3.157 snmp-server contact <*string*>

Use the **snmp-server contact** <*string*> command to specify Simple Network Management Protocol (SNMP) server contact information. Use the **no** form of this command to remove a configured contact.

3.157.1 Syntax Description

<string>	Populates the sysContact string using an alphanumeric string of no more than **255** characters.

3.157.2 Default Values

By default, SNMP is not configured.

3.157.3 Privilege Level

By default, this command has a privilege level of **15**.

3.157.4 Command History

ASE Release 4.4-41	Command was introduced.

3.157.5 Usage Examples

The following example configures the SNMP server contact:

```
(config)#snmp-server contact CONTACTSNMPSERVER
```

3.158 snmp-server engine-id local <*id*>

Use the **snmp-server engine-id local** <*id*> command to change the default and manually set the Simple Network Management Protocol (SNMP) version 3 (v3) engine ID for the local machine. Use the **no** form of this command to return to the default engine ID.

3.158.1 Syntax Description

<*id*>	Defines the engine ID for the system. Engine IDs are the 12-octet hexadecimal representation (**24** characters using **0** through **9** and/or **a** through **f**) defining a system on the management domain.

3.158.2 Default Values

By default, the local SNMP-server engine ID is **8000029803xxxxxxxxxxxx** (where the string of Xs represents the system medium access control (MAC) address).

3.158.3 Privilege Level

By default, this command has a privilege level of **13**.

3.158.4 Command History

ASE Release 4.4-41	Command was introduced.

3.158.5 Functional Notes

SNMP v3 requires unique engine IDs for all systems in the management domain. Use the default engine ID when possible to ensure the uniqueness of the numbers. Problems can occur on a management network that contains duplicate engine IDs.

3.158.6 Usage Examples

The following example configures the SNMP server contact:

```
(config)#snmp-server engine-id local 1234567890
```

3.159 snmp-server host <*name*>

Use the **snmp-server host** <*name*> command to enable the Simple Network Management Protocol (SNMP) host and enter the SNMP Server Host configuration mode. Use the **no** form of this command to remove the SNMP host.

3.159.1 Syntax Description

<name>	Specifies the SNMP host name. Valid names cannot exceed 32 characters in length.

3.159.2 Default Values

By default, SNMP is not configured.

3.159.3 Privilege Level

By default, this command has a privilege level of **15**.

3.159.4 Command History

ASE Release 4.4-41	Command was introduced.

3.159.5 Usage Examples

The following example configures the SNMP server host name and enters the SNMP Server Host configuration mode:

```
(config)#snmp-server host SERVERHOST1
(config-snmps-host)#
```

3.160 snmp-server location <*string*>

Use the **snmp-server location** <*string*> command to specify the Simple Network Management Protocol (SNMP) server location. Use the no form of this command to remove the SNMP server location.

3.160.1 Syntax Description

<string>	Specifies the SNMP server location in a text string of no more than 255 characters.

3.160.2 Default Values

By default, SNMP is not configured.

3.160.3 Privilege Level

By default, this command has a privilege level of **15**.

3.160.4 Command History

ASE Release 4.4-41	Command was introduced.

3.160.5 Usage Examples

The following example specifies the SNMP server location:

```
(config)#snmp-server location FIRSTFLOOR
```

3.161 snmp-server security-to-group

Use the **snmp-server security-to-group** command to configure the Simple Network Management Protocol (SNMP) server security settings for contact with the SNMP group. Use the **no** form of this command to remove the security setting. Variations of this command include:

```
snmp-server security-to-group model v1 name <name> group <name>
snmp-server security-to-group model v2c name <name> group <name>
snmp-server security-to-group model v3 name <name> group <name>
```

3.161.1 Syntax Description

v1	Specifies the SNMP v1 security model is used.
v2c	Specifies the SNMP v2c security model is used.
v3	Specifies the SNMP v3 security model is used.
name *<name>*	Specifies the security user name. Valid names cannot exceed 32 characters in length.
group *<name>*	Specifies the security group name. Valid names cannot exceed 32 characters in length.

3.161.2 Default Values

By default, SNMP is not configured.

3.161.3 Privilege Level

By default, this command has a privilege level of **15**.

3.161.4 Command History

ASE Release 4.4-41	Command was introduced.

3.161.5 Usage Examples

The following example specifies the SNMP server security parameters for contact with the SNMP group:

```
(config)#snmp-server security-to-group model v3 name USERNAME1 group GROUPNAME1
```

3.162 snmp-server trap

Use the **snmp-server trap** command to enable and configure Simple Network Management Protocol (SNMP) trap source parameters. Use the **no** form of this command to remove the trap source information. Variations of this command include:

```
snmp-server trap <trap>
snmp-server trap <trap> <OID>
snmp-server trap <trap> <OID> exclude
snmp-server trap <trap> <OID> include
snmp-server trap <trap> id <id>
```

3.162.1 Syntax Description

<trap>	Specifies the SNMP trap to enable. Refer to "Functional Notes" below for supported traps.
<OID>	Specifies the object identifier (OID) to use as an index filter.
exclude	Optional. Excludes the specified filter type.
include	Optional. Includes the specified filter type.
id *<id>*	Specifies a specific filter ID. Valid range is **0** to **127**.

3.162.2 Default Values

By default, SNMP is not configured.

3.162.3 Privilege Level

By default, this command has a privilege level of **15**.

3.162.4 Command History

ASE Release 4.4-41	Command was introduced.

3.162.5 Functional Notes

The following are supported SNMP traps:

- **authenticationFialure**
- **coldStart**
- **entConfigChange**
- **fallingAlarm**
- **linkDown**
- **linkUp**
- **lldpRemTablesChange**
- **newRoot**
- **risingALarm**
- **topologyChange**
- **warmStart**

3.162.6 Usage Examples

The following example enables the **entConfigChange** SNMP trap using filter **33**:

```
(config)#snmp-server trap entConfigChange id 33
```

3.163 snmp-server user

Use the **snmp-server user** command to configure Simple Network Management Protocol (SNMP) users to control access to SNMP information. Use the **no** form of this command to remove a user from the specified SNMP server group. Variations of this command include:

```
snmp-server user <username> engine-id <id>
snmp-server user <username> engine-id <id> md5 <password>
snmp-server user <username> engine-id <id> md5 <password> priv aes
snmp-server user <username> engine-id <id> md5 <password> priv des
snmp-server user <username> engine-id <id> md5 encrypted <password>
snmp-server user <username> engine-id <id> md5 encrypted <password> priv aes
snmp-server user <username> engine-id <id> md5 encrypted <password> priv des
```

3.163.1 Syntax Description

<username>	Specifies the name of the user.
<id>	Defines the engine ID for the system. Engine IDs are the 12-octet hexadecimal representation (**24** characters using **0** through **9** and/or **a** through **f**) defining a system on the management domain.
md5 *<password>*	Optional. Uses the HMAC-MD5-96 authentication level and a password string to build the key for the authentication level.
md5 encrypted *<password>*	Optional. Uses the HMAC-MD5-96 authentication level and an encrypted password string to build the key for the authentication level.
priv aes	Optional. Specifies that 28-bit Advanced Encryption Standard (AES) is used.
priv des	Optional. Specifies that 56-bit Data Encryption Standard (DES) is used.

3.163.2 Default Values

By default, SNMP is not configured.

3.163.3 Privilege Level

By default, this command has a privilege level of **15**.

3.163.4 Command History

ASE Release 4.4-41	Command was introduced.

3.163.5 Functional Notes

SNMP user security is used exclusively with SNMP version 3 (SNMPv3).

3.163.6 Usage Examples

The following example configures a user for the SNMPv3 server:

```
(config)#snmp-server user USERNAME engine-id 1234567890 md5 PASSWORD
```

3.164 snmp-server view

Use the **snmp-server view** command to view Simple Network Management Protocol (SNMP) management information base (MIB) objects and their configuration. Variations of this command include:

snmp-server view *<name>* *<OID>* **exclude**
snmp-server view *<name>* *<OID>* **include**

3.164.1 Syntax Description

<name>	Specifies the name of the MIB to view. MIB names cannot exceed 32 characters in length.
<OID>	Specifies the MIB's object identifier (OID). OIDs cannot exceed 255 characters in length.
exclude	Displays the view of all MIBs except the specified MIB.
include	Limits the view to only the specified MIB information.

3.164.2 Default Values

No defaults are necessary for this command.

3.164.3 Privilege Level

By default, this command has a privilege level of **15**.

3.164.4 Command History

ASE Release 4.4-41	Command was introduced.

3.164.5 Usage Examples

The following example specifies a MIB to view:

```
(config)#snmp-server view MIBNAME 20 include
```

3.165 spanning-tree aggregation

Use the spanning-tree aggregation command to enter the Spanning Tree Protocol (STP) aggregation group configuration mode.

3.165.1 Syntax Description

No subcommands.

3.165.2 Default Values

By default, STP is disabled and no aggregation groups are configured.

3.165.3 Command History

ASE Release 4.4-41	Command was introduced.

3.165.4 Functional Notes

Using this command enters the STP Aggregated Group configuration mode, which contains the same spanning tree configuration commands as an individual port interface.

3.165.5 Usage Examples

The following example enters the STP aggregation group configuration mode:

```
(config)#spanning-tree aggregation
(config-stp-aggr)#
```

3.166 spanning-tree edge

Use the **spanning-tree edge** command to specify whether the ports are used as edge ports, regardless of any spanning tree detection. Use the **no** form of this command to return edge port detection to the default setting. Variations of this command include:

```
spanning-tree edge bpdu-filter
spanning-tree edge bpdu-guard
```

3.166.1 Syntax Description

bpdu-filter	Enables Bridge Protocol Data Unit (BPDU) filtering on all edge ports within the spanning tree instance. This setting prevents the ports from transmitting or receiving BPDU messages.
bpdu-guard	Enables BPDU guarding on all edge ports within the spanning tree instance. This setting prevents the ports from receiving BPDU messages.

3.166.2 Default Values

By default, both BPDU filtering and BPDU guarding are disabled.

3.166.3 Privilege Level

By default, this command has a privilege level of **15**.

3.166.4 Command History

ASE Release 4.4-41	Command was introduced.

3.166.5 Usage Examples

The following example enables BPDU guarding for all edge ports in the spanning tree instance:

```
(config)#spanning-tree edge bpdu-guard
```

3.167 spanning-tree mode

Use the **spanning-tree mode** command to enable and specify the type of spanning tree protocol to use on the ASE device. Use the **no** form of this command to disable spanning tree. Variations of this command include:

```
spanning-tree mode mstp
spanning-tree mode rstp
spanning-tree mode stp
```

3.167.1 Syntax Description

mstp	Specifies Multiple Spanning Tree Protocol (MSTP).
rstp	Specifies Rapid Spanning Tree Protocol (RSTP).
stp	Specifies Spanning Tree Protocol (STP).

3.167.2 Default Values

By default, spanning tree is disabled.

3.167.3 Privilege Level

By default, this command has a privilege level of **15**.

3.167.4 Command History

ASE Release 4.4-41	Command was introduced.

3.167.5 Usage Examples

The following example enables RSTP on the ASE device:

```
(config)#spanning-tree mode rstp
```

3.168 spanning-tree mst

Use the **spanning-tree mst** command to configure Multiple Spanning Tree Protocol (MSTP) instance (MSTI) parameters on the ASE device. Use the **no** form of this command to remove the MIST configuration or return to the default setting. Variations of this command include:

```
spanning-tree mst <instance> priority <priority>
spanning-tree mst <instance> vlan <vlan ids>
spanning-tree mst forward-time <value>
spanning-tree mst hello-time <value>
spanning-tree mst max-age <value>
spanning-tree mst max-hops <number>
spanning-tree mst name <name> revision <number>
```

3.168.1 Syntax Description

mst *<instance>*	Specifies the bridge instance for which priority is being configured. Valid range is **0** to **7**, with **0** being the common and internal spanning tree (CIST) instance, and **1** through **7** being **MSTI1** through **MSTI7**, respectively.
priority *<priority>*	Specifies the priority for the bridge instance. This priority is used by the protocol to determine which switch is the root bridge, and the priorities of the other switches connected to the instance. Valid range is **0** to **61440**, in multiples of **4096**.
vlan *<vlan ids>*	Specifies which virtual local area networks (VLANs) are mapped to the MSTI instance. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.
forward-time *<value>*	Specifies the time that ports spend in the Listening and Learning states, before moving to the Forwarding state. Valid range is **4** to **30** seconds.
hello-time *<value>*	Specifies the interval between Bridge Protocol Data Unit (BPDU) messages sent by the bridge. Valid range is **1** to **10** seconds.
max-age *<value>*	Specifies how long a port saves the configuration information delivered to it in BPDU messages. Valid range is **6** to **40** seconds. The maximum age timer must be configured to be less than or equal to two times the forward delay timer.
max-hops *<number>*	Specifies the number of hops a BPDU message can travel before being discarded and before the port information included in the message is no longer valid. Valid range is **6** to **40** hops.
name *<name>* **revision** *<number>*	Configures the MSTP region name and revision number. MSTP region names and revision numbers are carried in BPDU messages throughout the network and must be identical on all switches within the MSTP region. Configuration names are specified as ASCII strings with a maximum length of 32 characters, and are case-sensitive. Valid range for revision numbers is **1** to **65535**.

3.168.2 Default Values

By default, MSTP is disabled. When enabled, the priority is set to **16384**, the forward timer is set to **15** seconds, the hello timer is set to **2** seconds, the maximum age timer is set to **20** seconds, the maximum hops are set to **20**, and the revision number is **0**.

3.168.3 Privilege Level

By default, this command has a privilege level of **15**.

3.168.4 Command History

ASE Release 4.4-41	Command was introduced.

3.168.5 Usage Examples

To specify an MSTP region name and revision number, enter the command as follows:

```
(config)#spanning-tree mst name REGION1 revision 10
```

3.169 spanning-tree recovery interval <*interval*>

Use the **spanning-tree recovery interval** command to enable the ports in the spanning tree instance to automatically recover from errors. When enabled, the port will automatically recover from being disabled by an error after an allotted timeout period. Use the **no** form of this command to disable the automatic recovery feature.

3.169.1 Syntax Description

<interval>	Specifies the timeout period before the port automatically recovers. Valid range is **30** to **86400** seconds.

3.169.2 Default Values

By default, automatic recovery is disabled.

3.169.3 Privilege Level

By default, this command has a privilege level of **15**.

3.169.4 Command History

ASE Release 4.4-41	Command was introduced.

3.169.5 Usage Examples

The following example specifies ports within the spanning tree instance recover after **120** seconds:

```
(config)#spanning-tree recovery interval 120
```

3.170 spanning-tree hold-count <*value*>

Use the **spanning-tree hold-count** command to specify the maximum number of transmitted Bridge Protocol Data Unit (BPDU) messages sent by the spanning tree bridge per second. Use the **no** form of this command to return to the default value.

3.170.1 Syntax Description

<value>	Specifies the maximum number of BPDU messages transmitted per second. Valid range is **1** to **10** messages.

3.170.2 Default Values

By default, a maximum of **6** BPDUs can be sent per second.

3.170.3 Privilege Level

By default, this command has a privilege level of **15**.

3.170.4 Command History

ASE Release 4.4-41	Command was introduced.

3.170.5 Usage Examples

To change the maximum transmitted number of BPDUs per second, enter the command as follows:

```
(config)#spanning-tree transmit hold-count 3
```

3.171 svl fid <*fid*> vlan <*vlan ids*>

Use the **svl fid** <*fid*> **vlan** <*vlan ids*> command to enable shared virtual local area network (VLAN) learning (SVL) and specify which VLANs are associated with each filter ID. Use the **no** form of this command to disable SVL on the ASE device.

3.171.1 Syntax Description

fid *<fid>*	Specifies the filter ID to associate with the specified VLAN(s). Valid range is **1** to **4095**.
vlan *<vlan ids>*	Specifies the VLAN(s) to associate with the filter ID. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

3.171.2 Default Values

By default, SVL is disabled.

3.171.3 Command History

ASE Release 4.4-41	Command was introduced.

3.171.4 Usage Examples

The following example enables SVL and specifies that VLANs **3** through **75** are associated with filter ID **1**:

```
(config)#svl fid 1 vlan 3-75
```

3.172 switchport vlan mapping

Use the **switchport vlan mapping** command to configure virtual local area network (VLAN) translation characteristics on the ASE device. Use the **no** form of this command to remove the VLAN translation. Variations of this command include:

```
switchport vlan mapping <id> both <vlan id> <translated vlan id>
switchport vlan mapping <id> egress <vlan id> <translated vlan id>
switchport vlan mapping <id> ingress <vlan id> <translated vlan id>
```

3.172.1 Syntax Description

<id>	Specifies the group ID. Valid range is **1** to **53**.
both	Specifies bi-directional VLAN translation.
egress	Specifies egress-only VLAN translation.
ingress	Specifies ingress-only VLAN translation.
<vlan id>	Specifies the VLAN ID to translate. Valid range is **1** to **4095**.
<translated vlan id>	Specifies the translated VLAN ID. Valid range is **1** to **4095**.

3.172.2 Default Values

By default, VLAN translation is not configured.

3.172.3 Command History

ASE Release 4.4-41	Command was introduced.

3.172.4 Usage Examples

The following example specifies that VLAN ID **175** is translated to VLAN **75** on ingress:

```
(config)#switchport vlan mapping 10 ingress 175 75
```

3.173 tacacs-server

Use the **tacacs-server** command to configure several terminal access controller access-control system plus (TACACS+) parameters for all TACACS+ servers on the network. Most of these global settings can be overridden on a per-server basis (using the command "tacacs-server host" on page 468). Use the **no** form of this command to return to the default setting. Variations of this command include the following:

```
tacacs-server deadtime <valtacacs-server key <key>
tacacs-server key encrypted <key>
tacacs-server key unencrypted <key>
tacacs-server timeout <value>
```

3.173.1 Syntax Description

deadtime *<value>*	Specifies the time interval to wait before ceasing to use a TACACS+ server that doesn't respond. Valid range is **1** to **1440** minutes.
key encrypted *<key>*	Specifies the encryption key used by all TACACS+ servers. This is a global setting; however, it can be overridden on a per-server basis. Encrypted keys are between **96** and **224** characters in length.
key unencrypted *<key>*	Specifies an unencrypted key used by all TACACS+ servers. This is a global setting; however, it can be overridden on a per-server basis. Unencrypted keys are between **1** and **63** characters in length.
timeout *<value>*	Specifies the time (in seconds) that the ASE device will wait for the server's reply before declaring an error. The time range is **1** to **1000** seconds. This is a global setting; however, it can be overridden on a per-server basis.

3.173.2 Default Values

By default, there is no key specified for TACACS+ servers and the TACACS+ server timeout is set to **5** seconds.

3.173.3 Privilege Level

By default, this command has a privilege level of **15**.

3.173.4 Command History

ASE Release 4.4-41	Command was introduced.

3.173.5 Usage Examples

The following example specifies the TACACS+ server timeout value as **30** seconds:

```
(config)#tacacs-server timeout 30
```

3.174 tacacs-server host

Use the **tacacs-server host** command to specify the parameters for a terminal access controller access-control system plus (TACACS+) server. Use the **no** form of this command to return to the default settings. Variations of this command include:

```
tacacs-server host <hostname> | <ip address>
tacacs-server host <hostname> | <ip address> key encrypted <key>
tacacs-server host <hostname> | <ip address> key unencrypted <key>
tacacs-server host <hostname> | <ip address> port <port>
tacacs-server host <hostname> | <ip address> timeout <value>
```

3.174.1 Syntax Description

<hostname> **|** *<ip address>*	Specifies the server to configure. IP addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). If a host name is used, a domain naming system (DNS) server should be learned by the ASE device using Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol (PPP).
key encrypted *<key>*	Specifies the encryption key used by the TACACS+ server. This command overrides the global TACACS+ key setting (set with the command "tacacs-server" on page 467). This command must be entered last in the command line because everything after the **key** parameter is read as the new key.
key unencrypted *<key>*	Specifies an unencrypted key used by the TACACS+ server. This command overrides the global TACACS+ key setting (set with the command "tacacs-server" on page 467). This command must be entered last in the command line because everything after the **key** parameter is read as the new key.
port *<port>*	Specifies the Transmission Control Protocol (TCP) port used by the TACACS+ server. Range is **0** to **65535**.
timeout *<value>*	Specifies the time to wait (in seconds) for the server to reply to requests. Range is **1** to **1000** seconds.

3.174.2 Default Values

By default, the TACACS+ server uses TCP port **49**. By default, the key and timeout values are the values set by the command "tacacs-server" on page 467.

3.174.3 Privilege Level

By default, this command has a privilege level of **15**.

3.174.4 Command History

ASE Release 4.4-41	Command was introduced.

3.174.5 Usage Examples

The following example specifies a timeout value of **30** seconds for the TACACS+ server at IP address **192.168.1.2**:

```
(config)#tacacs-server host 192.168.1.2 timeout 30
```

3.175 thermal-protect grp <*id*> temperature <*value*>

Use the **thermal-protect grp** <*id*> **temperature** <*value*> command to configure the thermal protection settings on the ASE device. Use the **no** form of this command to disable thermal protection.

3.175.1 Syntax Description

grp *<id>*	Specifies the group to which ports are mapped. All ports associated with this group will shutdown if the temperature exceeds the set limit. Valid range is **0** to **3**.
temperature *<value>*	Specifies the temperature at which to shut down ports associated with the protection group. Valid range is **0** to **255** degrees Celsius.

3.175.2 Default Values

By default, thermal protection is disabled.

3.175.3 Privilege Level

By default, this command has a privilege level of **15**.

3.175.4 Command History

ASE Release 4.4-41	Command was introduced.

3.175.5 Functional Notes

Ports are assigned a thermal protection group using the **thermal-protect grp** <*id*> command from the interface's configuration mode.

3.175.6 Usage Examples

The following example configures a thermal protection group **3**, that will shutdown ports once the temperature reaches **100** degrees Celsius:

```
(config)#thermal-protect grp 3 temperature 100
```

3.176 udld

Use the **udld** command to configure Unidirectional Link Detection (UDLD) parameters on the ASE device. Use the **no** form of this command to disable this feature. Variations of this command include:

```
udld aggressive
udld enable
udld message time-interval <value>
```

3.176.1 Syntax Description

aggressive	Enables UDLD in aggressive mode on all fiber optic ports.
enable	Enables UDLD in normal mode on all fiber optic ports.
time-interval *<value>*	Specifies the amount of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. Valid range is **7** to **90** seconds.

3.176.2 Default Values

By default, UDLD is disabled. When enabled, the message time interval is set to **7** seconds.

3.176.3 Command History

ASE Release 4.4-41	Command was introduced.

3.176.4 Usage Examples

The following example enables UDLD in normal mode on all fiber optic ports:

```
(config)#udld enable
```

3.177 upnp

Use the **upnp** command to enable and configure the Universal Plug and Play (UPNP) parameters of the ASE device. Use the **no** form of this command to disable UPNP. Variations of this command include:

```
upnp
upnp advertising-duration <value>
upnp ip-addressing-mode dynamic
upnp ip-addressing-mode static
upnp static interface vlan <vlan id>
```

3.177.1 Syntax Description

advertising-duration *<value>*	Specifies the UPNP advertising duration. Valid range is **100** to **86400**.
ip-addressing-mode	Specifies the UPNP IP addressing mode.
dynamic	Specifies that IP addresses are determined dynamically.
static	Specifies that a virtual local area network (VLAN) interface is statically added to use for UPNP addressing.
interface vlan *<vlan id>*	Specifies a VLAN interface to use for static IP addressing. Valid range is **1** to **4095**.

3.177.2 Default Values

By default, UPNP is disabled.

3.177.3 Privilege Level

By default, this command has a privilege level of **15**.

3.177.4 Command History

ASE Release 4.4-41	Command was introduced.

3.177.5 Usage Examples

The following example enables UPNP and specifies the advertising duration:

```
(config)#upnp
(config)#upnp advertising-duration 188
```

3.178 username

Use the **username** command to configure a username and password for authentication. Use the **no** form of this command to remove the user authentication configuration. Variations of this command include:

```
username <name> privilege <level> password encrypted <password>
username <name> privilege <level> password none
username <name> privilege <level> password unencrypted <password>
```

3.178.1 Syntax Description

<name>	Specifies the user name to add to the system. Names can be up to **31** characters in length, and can include letters, numbers, and underscore.
privilege *<level>*	Specifies the privilege level for the user. Valid range is **0** to **15** (15 being administrator level).
password	Specifies the user password
encrypted *<password>*	Specifies an encrypted password.
none	Specifies no password is assigned.
unencrypted *<password>*	Specifies an unencrypted password.

3.178.2 Default Values

No default values are necessary for this command.

3.178.3 Privilege Level

By default, this command has a privilege level of **15**.

3.178.4 Command History

ASE Release 4.4-41	Command was introduced.

3.178.5 Functional Notes

The ASE switches are designed to always encrypt a password. Even if a password is specified as unencrypted with this command, the configuration stored in the switch will always have the encrypted password shown.

3.178.6 Usage Examples

The following example configures a user with administrative privileges:

```
(config)#username MIGHTYADMIN privilege 15 password unencrypted SPECIAL
```

3.179 vlan <*vlan id*>

Use the **vlan** <*vlan id*> command to enable a virtual local area network (VLAN) on the ASE device, and enter the VLAN name configuration mode. Use the **no** form of this command to disable the VLAN.

Once you have entered the **vlan** <*vlan id*> command, you can then specify the name of the VLAN using the **name** <*name*> command from the VLAN configuration mode prompt. Use the no form of this command to remove the VLAN name.

3.179.1 Syntax Description

<vlan id>	Specifies the VLAN to enable on the switch. Valid range is **1** to **4095**.
name *<name>*	Specifies the name of the VLAN. Names cannot exceed 32 characters in length. This parameter is entered after entering the **vlan** <*vlan id*> command.

3.179.2 Default Values

By default, only VLAN **0** is enabled on the switch.

3.179.3 Privilege Level

By default, this command has a privilege level of **13**.

3.179.4 Command History

ASE Release 4.4-41	Command was introduced.

3.179.5 Usage Examples

The following example enables VLAN **175** on the switch, and names the VLAN **MYVLAN**:

```
(config)#vlan 175
(config-vlan)#name MYVLAN
```

3.180 vlan ethertype s-custom-port <*type*>

Use the **vlan ethertype s-custom-port** <*type*> command to specify the Ethertype port setting for virtual local area network (VLAN) ports that are configured in hybrid mode with an S-Custom-Port type setting. Use the **no** form of this command to return the port's Ethertype setting to the default value.

3.180.1 Syntax Description

<type>	Specifies the Ethertype used by port to classify incoming VLAN traffic. Valid range is **0x0600** to **0xffff**.

3.180.2 Default Values

By default, when a VLAN hybrid port is set to S-Custom-Port, the type value is **0x88A8**.

3.180.3 Privilege Level

By default, this command has a privilege level of **13**.

3.180.4 Command History

ASE Release 4.4-41	Command was introduced.

3.180.5 Usage Examples

The following example specifies an Ethertype of **0x0600** for hybrid ports using S-Custom-Port mode:

```
(config)#vlan ethertype s-custom-port 0x0600
```

3.181 vlan protocol eth2

Use the **vlan protocol eth2** command to configure virtual local area network (VLAN) ETH2 protocol parameters. Use the **no** form of this command to remove the ETH2 protocol parameters from the VLAN configuration. Variations of this command include:

```
vlan protocol eth2 <type> group <name>
vlan protocol eth2 arp group <name>
vlan protocol eth2 at group <name>
vlan protocol eth2 ip group <name>
vlan protocol eth2 ipx group <name>
```

3.181.1 Syntax Description

<type>	Specifies the Ethertype. Valid range is **0x600** to **0xFFFF**.
arp	Specifies the Ethertype Address Resolution Protocol (ARP).
at	Specifies the Ethertype AppleTalk (AT).
ip	Specifies the Ethertype Internet Protocol (IP).
ipx	Specifies the Ethertype Internetwork Packet Exchange (IPX).
group *<name>*	Specifies the protocol-based VLAN group. Valid names are **1** to **16** characters in length.

3.181.2 Default Values

By default, no VLAN protocol parameters are configured.

3.181.3 Privilege Level

By default, this command has a privilege level of **13**.

3.181.4 Command History

ASE Release 4.4-41	Command was introduced.

3.181.5 Usage Examples

The following example specifies that VLANs use the IP protocol for group DATA:

```
(config)#vlan protocol eth2 ip group DATA
```

3.182 vlan protocol llc *<destination>* *<source>* group *<name>*

Use the **vlan protocol llc** command to configure virtual local area network (VLAN) Link Layer Control (LLC) protocol parameters. Use the **no** form of this command to remove the LLC protocol parameters from the VLAN configuration.

3.182.1 Syntax Description

<destination>	Specifies the destination service access point. Valid range is **0x00** to **0xFF**.
<source>	Specifies the source service access point. Valid range is **0x00** to **0xFF**.
group *<name>*	Specifies the protocol-based VLAN group. Valid names are **1** to **16** characters in length.

3.182.2 Default Values

By default, no VLAN protocol parameters are configured.

3.182.3 Command History

ASE Release 4.4-41	Command was introduced.

3.182.4 Usage Examples

The following example specifies the LLC parameters for VLAN group DATA:

```
(config)#vlan protocol llc 0x01 0x02 group DATA
```

3.183 vlan protocol snap

Use the **vlan protocol snap** command to configure virtual local area network (VLAN) Subnet Access Protocol (SNAP) parameters. Use the **no** form of this command to remove the SNAP parameters from the VLAN configuration. Variations of this command include:

```
vlan protocol snap <OUI> <protocol id> group <name>
vlan protocol snap rfc-1042 <protocol id> group <name>
vlan protocol snap snap-8021h <protocol id> group <name>
```

3.183.1 Syntax Description

<OUI>	Specifies the SNAP object identifier. Valid range is **0x0** to **0xffffff**.
<protocol id>	Specifies the protocol ID. Valid range is **0x0** to **0xFFFF**.
rfc-1042	Specifies the SNAP object identifier is RFC 1042.
snap-8021h	Specifies the SNAP object identifier is 8021h.
group *<name>*	Specifies the protocol-based VLAN group. Valid names are **1** to **16** characters in length.

3.183.2 Default Values

By default, no VLAN protocol parameters are configured.

3.183.3 Command History

ASE Release 4.4-41	Command was introduced.

3.183.4 Usage Examples

The following example specifies the SNAP parameters for VLAN group DATA:

```
(config)#vlan protocol snap rfc-1042 0x600 group DATA
```

3.184 voice vlan

Use the **voice vlan** command to enable and configure voice virtual local area network (VLAN) parameters on the ASE device. Use the **no** form of this command to remove the voice VLAN configuration. Variations of this command include:

```
voice vlan
voice vlan aging-time <value>
voice vlan oui <OUI>
voice vlan oui <OUI> description <text>
voice vlan vid <vlan id>
voice vlan vid class <value>
```

3.184.1 Syntax Description

aging-time *<value>*	Specifies the secure learning aging time for the VLAN. Valid range is **10** to **10000000** seconds.
oui *<OUI>*	Specifies a Voice over IP (VoIP) device to manually add to the VLAN object identifier (OUI) table. Enter OUI addresses as a 24-bit number in the format **00:00:00**.
description *<text>*	Optional. Specifies a 32-character description associated with the device.
<vlan id>	Specifies the VLAN ID for the voice VLAN. Valid range is **1** to **4095**.
class *<value>*	Specifies the class of service (CoS) value for the voice traffic on the VLAN. Valid range is **0** to **7**.

3.184.2 Default Values

By default, the voice VLAN is set to VLAN ID **1000**, with a CoS value of **7**, and an aging time of **86400** seconds. In addition, by default OUIs of VoIP devices are added to the OUI table automatically.

3.184.3 Privilege Level

By default, this command has a privilege level of **15**.

3.184.4 Command History

ASE Release 4.4-41	Command was introduced.

3.184.5 Usage Examples

The following example adds a VoIP device to the VLAN OUI table:

```
(config)#voice vlan oui 00:0A:C8 description ADTRAN IP phone
```

3.185 web privilege group

Use the **web privilege group** command to configure web privilege group access parameters for the ASE device. Use the **no** form of this command to disable the web privilege group. Variations of this command include:

```
web privilege group <group> level <level>
web privilege group <group> level configRoPriv <level>
web privilege group <group> level configRwPriv <level>
web privilege group <group> level statusRoPriv <level>
web privilege group <group> level statusRwPriv <level>
```

3.185.1 Syntax Description

group *<group>*	Specifies the web privilege group. Refer to "Functional Notes" below for supported privilege group name keywords.
level *<level>*	Specifies the privilege level for the group. Valid range is **0** to **15**, with 15 being administrator privilege level.
configRoPriv	Optional. Specifies the group has read-only privileges.
configRwPriv	Optional. Specifies the group has read-write privileges.
statusRoPriv	Optional. Specifies the group has read-only privileges for statistical information.
statusRwPriv	Optional. Specifies the group has read-write privileges for statistical information.

3.185.2 Default Values

By default, no web privilege groups are configured.

3.185.3 Privilege Level

By default, this command has a privilege level of **15**.

3.185.4 Command History

ASE Release 4.4-41	Command was introduced.

3.185.5 Functional Notes

Table 3-7 outlines the supported group name keywords for web privilege groups.

Table 3-7. Web Privilege Group Name Keywords

Keyword Syntax			
AUTOLINK	IP	Private_VLANs	sFlow
Aggregation	IPMC_Snooping	QoS	uFDMA_AIL
Alarm	LACP	RMirror	uFDMA_CIL
DDMI	LLDP	Security(access)	
DHCP	Loop_Protect	Security(network)	
DHCPv6_Client	MAC_Table	Spanning_Tree	

Table 3-7. Web Privilege Group Name Keywords (Continued)

Keyword Syntax		
Debug	MEP	System
Diagnostics	MRP	UDLD
EPS	MVR	UPnP
ERPS	Miscellaneous	VCL
ETH_LINK_OAM	NTP	VLAN_Translation
FRR	POE	VLANs
Firmware	PTP	Voice_VLAN
Green_Ethernet	Ports	XXRP

3.185.6 Usage Examples

The following example configures web privilege access parameters for the DDMI group with read-only privileges:

```
(config)#web privilege group DDMI level configRoPriv 3
```

ASE Command Reference Guide

Volume 2: Interface Configuration Command Sets

1 GigabitEthernet Interface Command Set

1.1 Scope of this Section

This section outlines the commands available from the GigabitEthernet interface configuration mode on the ADTRAN Switch Engine (ASE) device. In this command mode, you can manage the configuration of various Gigabit Ethernet features supported by the ASE device on a per-port basis.

There are two types of GigabitEthernet interface supported on the ASE device:

- 1 GigabitEthernet interfaces
- 10 GigabitEthernet interfaces

NOTE
Not all ASE platforms have both GigabitEthernet interfaces available. To see if your unit has this capability, type **`show interfaces`** at the Enable mode prompt.

1.2 Accessing the Interface Configuration Mode

To activate the 1 GigabitEthernet Interface Configuration mode, enter the **interface GigabitEthernet** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface GigabitEthernet 1/1
(config-if)#
```

To activate the 10 GigabitEthernet Interface Configuration mode, enter the **interface 10GigabitEthernet** command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface 10GigabitEthernet 1/1
(config-if)#
```

1.3 Common Commands

The commands listed in Table 1-1 are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the section listed below:

Table 1-1. Common Commands

Sub-Section	Command	See Page …
1.4	do	19
1.5	end	20
1.6	exit	21
1.7	help	22

1.4 Gigabit Ethernet Interface Configuration Commands

Table 1-2 lists the commands available from the GigabitEthernet interfaces.

Table 1-2. GigabitEthernet Interface Commands

Sub-Section	Command	See Page …
1.5	access-list action	487
1.6	access-list logging	488
1.7	access-list mirror	489
1.8	access-list policy <id>	490
1.9	access-list port-state	491
1.10	access-list rate-limiter <id>	492
1.11	access-list redirect interface <interface>	493
1.12	access-list shutdown	494
1.13	aggregation group <group id> mode	495
1.14	dot1x	496
1.15	dot1x port-control	497
1.16	duplex	498
1.17	excessive-restart	500
1.18	flowcontrol	501
1.19	frame-length-check	502
1.20	green-ethernet	503
1.21	gvrp	504
1.22	ip arp inspection	505
1.23	ip dhcp snooping trust	506
1.24	ip igmp snooping	507
1.25	ip verify source	508
1.26	ipv6 mld snooping	509
1.27	lacp	510
1.28	link-oam	511
1.29	link-oam link-monitor	512
1.30	link-oam mib-retrieval supported	514
1.31	link-oam mode	515
1.32	link-oam remote-loopback supported	516
1.33	link-oam variable-retrieve	517

Table 1-2. GigabitEthernet Interface Commands (Continued)

Sub-Section	Command	See Page …
1.34	lldp cdp-aware	518
1.35	lldp med media-vlan policy-list <policies>	519
1.36	lldp med transmit-tlv	520
1.38	lldp receive	522
1.39	lldp tlv-select	523
1.40	lldp transmit	524
1.41	lldp trap	525
1.42	loop-protect	526
1.43	mac address-table learning	527
1.44	media-type	528
1.45	mrp periodic	529
1.46	mrp timers	530
1.47	mtu <size>	531
1.48	mvr immediate-leave	532
1.49	mvr name <name> type	533
1.50	mvr vlan <vlan ids> type	534
1.51	mvrp	535
1.52	poe delay-mode	536
1.53	poe delay-time <time>	537
1.54	poe failure-action	538
1.55	poe interval-time <time>	539
1.56	poe mode	540
1.57	poe ping-ip-addr <ipv4 address>	541
1.58	poe ping-retry-time <number>	542
1.59	poe port-profile name <name>	543
1.60	poe power limit <value>	544
1.61	poe priority	545
1.62	poe reboot-time <value>	546
1.63	poe startup-time <value>	547
1.64	port-security	548
1.65	port-security maximum <number>	549
1.66	port-security maximum-violation <number>	550

Table 1-2. GigabitEthernet Interface Commands (Continued)

Table 1-2. GigabitEthernet Interface Commands (Continued)

Sub-Section	Command	See Page …
1.96	speed	584
1.97	switchport access vlan <vlan id>	585
1.98	switchport forbidden vlan	586
1.99	switchport hybrid	587
1.100	switchport hybrid allowed vlan	589
1.101	switchport hybrid native vlan <vlan id>	591
1.102	switchport hybrid port-type	592
1.103	switchport mode	594
1.104	switchport trunk allowed vlan	595
1.105	switchport trunk native vlan <vlan id>	597
1.106	switchport trunk vlan tag native	598
1.107	switchport vlan ip-subnet <ipv4 address> <subnet mask> vlan <vlan id>	599
1.108	switchport vlan mac <mac address> vlan <vlan id>	600
1.109	switchport vlan mapping <group id>	601
1.110	switchport vlan protocol group <name> vlan <vlan id>	602
1.111	switchport voice vlan	603
1.112	thermal-protect grp <group id>	605
1.113	udld port	606

1.5 access-list action

Use the **access-list action** command to specify whether access control lists (ACLs) applied to the interface permit or deny traffic. Use the **no** form of this command to disable the ACL action. Variations of this command include:

```
access-list action deny
access-list action permit
```

1.5.1 Syntax Description

deny	Specifies that ACLs deny traffic on the interface that match the ACL criteria.
permit	Specifies that ACLs permit traffic on the interface that match the ACL criteria.

1.5.2 Default Values

By default, no ACLs are configured.

1.5.3 Privilege Level

By default, this command has a privilege level of **15**.

1.5.4 Command History

ASE Release 4.4-41	Command was introduced.

1.5.5 Usage Examples

The following example specifies that traffic matching the ACL criteria is permitted on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#access-list permit
```

1.6 access-list logging

Use the **access-list logging** command to enable logging for packets matching the access control list (ACL) criteria on the interface. Use the **no** form of this command to disable this feature.

1.6.1 Syntax Description

No subcommands.

1.6.2 Default Values

By default, this feature is disabled.

1.6.3 Privilege Level

By default, this command has a privilege level of **15**.

1.6.4 Command History

ASE Release 4.4-41	Command was introduced.

1.6.5 Functional Notes

The logging feature only functions when the length of packets being logged is less than 1518, without virtual local area network (VLAN) tags, and when the system log memory size and logging rate are limited.

1.6.6 Usage Examples

The following example enables the packet logging feature for ACLs:

```
(config)#interface GigabitEthernet 1/1
(config-if)#access-list logging
```

1.7 access-list mirror

Use the **access-list mirror** command to send packets matching the applied access control list (ACL) to a destination mirror port. Use the **no** form of this command to disable this feature.

1.7.1 Syntax Description

No subcommands.

1.7.2 Default Values

By default, the mirroring feature is disabled for ACLs.

1.7.3 Privilege Level

By default, this command has a privilege level of **15**.

1.7.4 Command History

ASE Release 4.4-41	Command was introduced.

1.7.5 Usage Examples

The following example enables mirroring for packets matching applied ACL criteria:

```
(config)#interface GigabitEthernet 1/1
(config-if)#access-list mirror
```

1.8 access-list policy <*id*>

Use the **access-list policy** <*id*> to apply an access control list (ACL) to the interface. Use the **no** form of this command to remove the ACL from the interface.

1.8.1 Syntax Description

<*id*>	Specifies the ID of the ACL to apply to the interface. Valid range is **0** to **127**.

1.8.2 Default Values

By default, no ACLs are applied to the interface.

1.8.3 Privilege Level

By default, this command has a privilege level of **15**.

1.8.4 Command History

ASE Release 4.4-41	Command was introduced.

1.8.5 Usage Examples

The following example applies the ACL **5** to the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#access-list policy 5
```

1.9 access-list port-state

Use the **access-list port-state** command to enable an interface after it has been shutdown due to an access control list (ACL).

1.9.1 Syntax Description

No subcommands.

1.9.2 Default Values

By default, ports remain shutdown after being shutdown due to an ACL.

1.9.3 Privilege Level

By default, this command has a privilege level of **15**.

1.9.4 Command History

ASE Release 4.4-41	Command was introduced.

1.9.5 Usage Examples

The following example enables the interface after it has been shutdown by an ACL:

```
(config)#interface GigabitEthernet 1/1
(config-if)#access-list port-state
```

1.10 access-list rate-limiter <*id*>

Use the **access-list rate-limiter** <*id*> command to apply a configured access control list (ACL) rate limiter to the interface. Use the **no** form of this command to remove the rate limiter.

1.10.1 Syntax Description

<*id*>	Specifies the ID of the previously configured rate limiter. Valid range is **1** to **16**.

1.10.2 Default Values

By default, rate limiters are not applied to the interface.

1.10.3 Privilege Level

By default, this command has a privilege level of **15**.

1.10.4 Command History

ASE Release 4.4-41	Command was introduced.

1.10.5 Usage Examples

The following example applies rate limiter **10** to the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#access-list rate-limiter 10
```

1.11 access-list redirect interface <*interface*>

Use the **access-list redirect** command to redirect packets matching an access control list (ACL) applied on the interface to another interface. Use the **no** form of this command to disable this feature.

1.11.1 Syntax Description

interface *<interface>*	Optional. Specifies the interface to which matching packets are redirected. Specify an interface in one of the following formats: *<interface type> <slot/port>* for a single port, *<interface type> <slot/port-slot/port>* for a range of ports, or *<interface type> <id>* for a specific interface ID. Enter **access-list redirect interface ?** for a complete list of valid interfaces.

1.11.2 Default Values

By default, the redirect feature is disabled.

1.11.3 Privilege Level

By default, this command has a privilege level of **15**.

1.11.4 Command History

ASE Release 4.4-41	Command was introduced.

1.11.5 Usage Examples

The following example redirects packets matching the applied ACL to the **10GigabitEthernet** interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#access-list redirect 10GigabitEthernet 1/2
```

1.12 access-list shutdown

Use the **access-list shutdown** command to shutdown the port from which traffic matching an applied access control list (ACL) was sent. Use the **no** form of this command to disable this feature.

1.12.1 Syntax Description

No subcommands.

1.12.2 Default Values

By default, this feature is disabled.

1.12.3 Privilege Level

By default, this command has a privilege level of **15**.

1.12.4 Command History

ASE Release 4.4-41	Command was introduced.

1.12.5 Usage Examples

The following example enables the ACL shutdown feature:

```
(config)#interface GigabitEthernet 1/1
(config-if)#access-list shutdown
```

1.13 aggregation group <*group id*> mode

Use the **aggregation group** <*group id*> **mode** command to create a Link Aggregation Control Protocol (LACP) group on the interface. Use the **no** form of this command to remove the LACP group. Variations of this command include:

```
aggregation group <group id> mode active
aggregation group <group id> mode on
aggregation group <group id> mode passive
```

1.13.1 Syntax Description

<group id>	Specifies the LACP group ID. Valid range depends on the ASE switch model. For an 8-port ASE switch, the range is **1** to **5**.
active	Specifies that the LACP group is in active mode, indicating ports transmit LACP frames to connected devices no matter the mode of the connected group.
on	Specifies that this is a Link Aggregation Group (LAG) group, using static mode and thus always on, and that LACP is not employed.
passive	Specifies that the LACP group is in passive mode, indicating ports transmit LACP frames to connected devices only when they receive LACP frames first.

1.13.2 Default Values

By default, no LACP or LAG groups are configured.

1.13.3 Privilege Level

By default, this command has a privilege level of **15**.

1.13.4 Command History

ASE Release 4.4-41	Command was introduced.

1.13.5 Usage Examples

The following example creates LACP group **3** and places it in **active** mode:

```
(config)#interface GigabitEthernet 1/1
(config-if)#aggregation group 3 mode active
```

1.14 dot1x

Use the **dot1x** command to configure port-based authentication (802.1x) parameters for the interface. Use the **no** form of this command to disable this feature. Variations of this command include:

```
dot1x guest-vlan
dot1x radius-qos
dot1x radius-vlan
dot1x re-authenticate
```

1.14.1 Syntax Description

guest-vlan	Enables the use of a guest virtual local area network (VLAN) on the interface.
radius-qos	Specifies that the Quality of Service (QoS) value for the interface is assigned by a Remote Authentication Dial-In User Service (RADIUS) server.
radius-vlan	Specifies that the VLAN associated with the interface is assigned by a RADIUS server.
re-authenticate	Restarts the 802.1x authentication process on the interface.

1.14.2 Default Values

By default, 802.1x is disabled on the interface.

1.14.3 Privilege Level

By default, this command has a privilege level of **15**.

1.14.4 Command History

ASE Release 4.4-41	Command was introduced.

1.14.5 Usage Examples

The following example restarts the 802.1x authentication process on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#dot1x re-authenticate
```

1.15 dot1x port-control

Use the **dot1x port-control** command to configure the port authentication process applied to the interface. Use the **no** form of this command to disable port-based authentication. Variations of this command include:

```
dot1x port-control auto
dot1x port-control force-authorized
dot1x port-control force-unauthorized
dot1x port-control mac-based
dot1x port-control multi
dot1x port-control single
```

1.15.1 Syntax Description

auto	Enables 802.1x authentication for all host types (single and multiple).
force-authorized	Specifies that access to the interface is always allowed.
force-unauthorized	Specifies that access to the interface is never allowed.
mac-based	Specifies that the ASE switch authenticates clients requesting port access based on media access control (MAC) address.
multi	Enables 802.1x authentication for multiple hosts.
single	Enables 802.1x authentication for single hosts.

1.15.2 Default Values

By default, 802.1x authentication is disabled on the interface.

1.15.3 Privilege Level

By default, this command has a privilege level of **15**.

1.15.4 Command History

ASE Release 4.4-41	Command was introduced.

1.15.5 Usage Examples

The following example enables 802.1x port authentication for all host types on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#dot1x port-control auto
```

1.16 duplex

Use the **duplex** command to specify the duplex operation of the interface. Use the **no** form of this command to return to the default setting. Variations of this command include:

```
duplex auto
duplex auto full
duplex auto half
duplex full
duplex half
```

1.16.1 Syntax Description

auto	Specifies that the interface operates at either full- or half-duplex, depending on the device to which the interface is connected.
full	Optional. Specifies that although the interface duplex mode is automatically determined, it advertises itself as operating in full-duplex mode.
half	Optional. Specifies that although the interface duplex mode is automatically determined, it advertises itself as operating in half-duplex mode.
full	Specifies the interface operates in full-duplex mode. This allows the interface to send and receive traffic simultaneously.
half	Specifies the interface operates in halfduplex mode. This setting allows the interface to either send or receive at any given moment, but not simultaneously.

1.16.2 Default Values

By default, the interface operates in half-duplex mode.

1.16.3 Privilege Level

By default, this command has a privilege level of **15**.

1.16.4 Command History

ASE Release 4.4-41	Command was introduced.

1.16.5 Functional Notes

Half-duplex Ethernet is the traditional form of Ethernet that employs the carrier sense multiple access/collision detect (CSMA/CD) protocol to allow two or more hosts to share a common transmission medium while providing mechanisms to avoid collisions. A host on a half-duplex link must “listen” on the link and only transmit when there is an idle period. Packets transmitted on the link are broadcast (so it will be “heard” by all hosts on the network). In the event of a collision (two hosts transmitting at once), a message is sent to inform all hosts of the collision and a backoff algorithm is implemented. The backoff algorithm requires the station to remain silent for a random period of time before attempting another transmission. This sequence is repeated until a successful data transmission occurs.

Full-duplex Ethernet is a variety of Ethernet technology currently being standardized by the IEEE. Because there is no official standard, vendors are free to implement their independent versions of full-duplex operation. Therefore, it is not safe to assume that one vendor's equipment will work with another.

Devices at each end of a full-duplex link have the ability to send and receive data simultaneously over the link. Theoretically, this simultaneous action can provide twice the bandwidth of normal (half-duplex) Ethernet. To deploy full-duplex Ethernet, each end of the link must only connect to a single device (a workstation or a switched hub port). With only two devices on a full-duplex link, there is no need to use the medium access control mechanism (to share the signal channel with multiple stations) and listen for other transmissions or collisions before sending data

1.16.6 Usage Examples

The following example specifies that the interface operates in full-duplex mode:

```
(config)#interface GigabitEthernet 1/1
(config-if)#duplex full
```

1.17 excessive-restart

Use the **excessive-restart** command to restart the backoff algorithm used to avoid collisions (two hosts transmitting at once) when interfaces are in half duplex mode. Using the **no** form of this commands specifies the algorithm continues until a successful data transmission occurs without a collision.

1.17.1 Syntax Description

No subcommands.

1.17.2 Default Values

By default, this feature is disabled and the interface will continue attempting transmissions until one is successful.

1.17.3 Privilege Level

By default, this command has a privilege level of **15**.

1.17.4 Command History

ASE Release 4.4-41	Command was introduced.

1.17.5 Functional Notes

A host on a half-duplex link must “listen” on the link and only transmit when there is an idle period. Packets transmitted on the link are broadcast (so it will be “heard” by all hosts on the network). In the event of a collision (two hosts transmitting at once), a message is sent to inform all hosts of the collision and a backoff algorithm is implemented. The backoff algorithm requires the station to remain silent for a random period of time before attempting another transmission. This sequence is repeated until a successful data transmission occurs.

Using the **excessive-restart** command restarts the backoff algorithm after **16** collisions.

1.17.6 Usage Examples

Enter the command as follows to specify the half-duplex backoff algorithm is restarted after 16 collisions:

```
(config)#interface GigabitEthernet 1/1
(config-if)#excessive-restart
```

1.18 flowcontrol

Use the **flowcontrol** command to enable or disable flow control for the interface. If flow control is enabled, the unit will honor pause frames. Variations of this command include:

```
flowcontrol off
flowcontrol on
```

1.18.1 Syntax Description

off	Disables flow control on the interface.
on	Enables flow control on the interface.

1.18.2 Default Values

By default, flow control is disabled on the interface.

1.18.3 Privilege Level

By default, this command has a privilege level of **15**.

1.18.4 Command History

ASE Release 4.4-41	Command was introduced.

1.18.5 Usage Examples

The following example enables flow control on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#flowcontrol on
```

1.19 frame-length-check

Use the **frame-length-check** command to specify that the interface drops packets whose EtherType or Length fields do not match the packet's payload size. Use the **no** form of this command to disable this feature.

1.19.1 Syntax Description

No subcommands.

1.19.2 Default Values

By default, this feature is disabled.

1.19.3 Command History

ASE Release 4.4-41	Command was introduced.

1.19.4 Usage Examples

The following example enables the frame checking feature on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#frame-length-check
```

1.20 green-ethernet

Use the **green-ethernet** command to configure Ethernet power reduction settings on the interface. Use the **no** form of this command to disable the Ethernet power reduction feature. Variations of this command include:

```
green-ethernet eee
green-ethernet eee urgent-queues <interface range>
green-ethernet energy-detect
green-ethernet short-reach
```

1.20.1 Syntax Description

eee	Enables energy efficient Ethernet (EEE) and specifies the interface is powered down when there is no traffic.
urgent-queues *<interface range>*	Optional. Enables the EEE urgent queue on the specified EEE interface. An urgent queue indicates that latency is kept to a minimum for traffic going to that queue. When enabled, EEE power savings are reduced. Specify an EEE interface range in the format *<slot/port>* for a single port, *<slot/port-slot/port>* for a range of ports, or *<id>* for a specific interface ID.
energy-detect	Enables power savings for interfaces not connected to a link partner.
short-reach	Enables power savings for interfaces connected to a link partner with a short cable.

1.20.2 Default Values

By default, Ethernet power reduction is disabled on the interface.

1.20.3 Privilege Level

By default, this command has a privilege level of **15**.

1.20.4 Command History

ASE Release 4.4-41	Command was introduced.

1.20.5 Usage Examples

The following example enables EEE on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#green-ethernet eee
```

1.21 gvrp

Use the **gvrp** command to enable Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) on the interface. Use the **no** form of this command to disable the feature on the interface.

1.21.1 Syntax Description

No subcommands.

1.21.2 Default Values

By default, GVRP is disabled on the interface.

1.21.3 Privilege Level

By default, this command has a privilege level of **15**.

1.21.4 Command History

ASE Release 4.4-41	Command was introduced.

1.21.5 Usage Examples

The following example enables GVRP on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#gvrp
```

1.22 ip arp inspection

Use the **ip arp inspection** command to configure Address Resolution Protocol (ARP) inspection parameters on the interface. Use the **no** form of this command to disable ARP inspection. Variations of this command include:

```
ip arp inspection check-vlan
ip arp inspection logging all
ip arp inspection logging deny
ip arp inspection logging permit
ip arp inspection trust
```

1.22.1 Syntax Description

check-vlan	Enables ARP inspection for virtual local area network (VLAN) configurations.
logging	Enables ARP inspection of logging configuration.
all	Specifies ARP inspects all logging entries.
deny	Specifies ARP inspects all denied log entries.
permit	Specifies ARP inspects all permitted log entries.
trust	Enables ARP inspection for trusted configurations.

1.22.2 Default Values

By default, ARP inspection is disabled.

1.22.3 Privilege Level

By default, this command has a privilege level of **13**.

1.22.4 Command History

ASE Release 4.4-41	Command was introduced.

1.22.5 Usage Examples

The following example enables ARP inspection for VLAN configurations:

```
(config)#interface GigabitEthernet 1/1
(config-if)#ip arp inspection check-vlan
```

1.23 ip dhcp snooping trust

Use the **ip dhcp snooping trust** to enable Dynamic Host Control Protocol (DHCP) snooping of trust configurations on the interface. Use the **no** form of this command to disable this feature.

1.23.1 Syntax Description

No subcommands.

1.23.2 Default Values

By default, this feature is disabled.

1.23.3 Privilege Level

By default, this command has a privilege level of **15**.

1.23.4 Command History

ASE Release 4.4-41	Command was introduced.

1.23.5 Usage Examples

The following example enables DHCP snooping of trust configurations on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#ip dhcp snooping trust
```

1.24 ip igmp snooping

Use the **ip igmp snooping** command to enable and configure Internet Group Management Protocol (IGMP) parameters on the interface. Use the **no** form of this command to disable IGMP on the interface. Variables that may be used with this command to further define the IGMP configuration include:

```
ip igmp snooping filter <profile>
ip igmp snooping immediate-leave
ip igmp snooping max-groups <number>
ip igmp snooping mrouter
```

1.24.1 Syntax Description

filter *<profile>*	Applies an access control list (ACL) to IGMP multicast group registrations. Profiles are specified by a name of no more than 16 characters in length.
immediate-leave	Enables IGMP immediate leave parameters on the interface.
max-groups *<number>*	Specifies the maximum number of IGMP groups that can be registered. Valid range is **1** to **10**.
mrouter	Enables IGMP multicast router support on the interface.

1.24.2 Default Values

By default, IGMP is disabled on the interface.

1.24.3 Privilege Level

By default, this command has a privilege level of **15**.

1.24.4 Command History

ASE Release 4.4-41	Command was introduced.

1.24.5 Usage Examples

The following example enables IGMP multicast router support on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#ip igmp snooping mrouter
```

1.25 ip verify source

Use the **ip verify source** command to enable command Internet Protocol (IP) source verification on the interface. Use the **no** form of this command to disable the feature. Variations of this command include:

```
ip verify source
ip verify source limit <number>
```

1.25.1 Syntax Description

limit *<source>*	Optional. Specifies a limit of the number of sources to verify. Valid range is **0** to **2**.

1.25.2 Default Values

By default, this feature is disabled.

1.25.3 Privilege Level

By default, this command has a privilege level of **13**.

1.25.4 Command History

ASE Release 4.4-41	Command was introduced.

1.25.5 Usage Examples

The following example enables IP source verification on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#ip verify source
```

1.26 ipv6 mld snooping

Use the **ipv6 mld snooping** command to enable and configure Internet Protocol version 6 (IPv6) Multicast Listener Discovery (MLD) parameters on the interface. Use the **no** form of this command to disable MLD on the interface. Variables that may be used with this command to further define the MLD configuration include:

```
ipv6 mld snooping filter <profile>
ipv6 mld snooping immediate-leave
ipv6 mld snooping max-groups <number>
ipv6 mld snooping mrouter
```

1.26.1 Syntax Description

filter *<profile>*	Applies an access control list (ACL) to MLD multicast group registrations. Profiles are specified by a name of no more than 16 characters in length.
immediate-leave	Enables MLD immediate leave parameters on the interface.
max-groups *<number>*	Specifies the maximum number of MLD groups that can be registered. Valid range is **1** to **10**.
mrouter	Enables MLD multicast router support on the interface.

1.26.2 Default Values

By default, MLD is disabled on the interface.

1.26.3 Command History

ASE Release 4.4-41	Command was introduced.

1.26.4 Usage Examples

The following example enables MLD multicast router support on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#ipv6 mld snooping mrouter
```

1.27 lacp

Use the **lacp** command to enable Link Aggregation Control Protocol (LACP) on the interface. Use the **no** form of this command to disable LACP. Variations of this command include:

```
lacp
lacp port-priority <priority>
lacp timeout fast
lacp timeout slow
```

1.27.1 Syntax Description

<priority>	Optional. Specifies the priority for the port within the LACP group. Valid range is **1** to **65535**
timeout	Specifies the period between LACP messages on the port.
fast	Specifies that LACP messages are sent every second.
slow	Specifies that LACP messages are sent every **30** seconds.

1.27.2 Default Values

By default, LACP is disabled on the interface. When enabled, the LACP port priority is set to **32768** and LACP messages are send every second (**fast**).

1.27.3 Privilege Level

By default, this command has a privilege level of **15**.

1.27.4 Command History

ASE Release 4.4-41	Command was introduced.

1.27.5 Usage Examples

The following example specifies the priority for the port within the LACP group as **2500**:

```
(config)#interface GigabitEthernet 1/1
(config-if)#lacp port-priority 2500
```

1.28 link-oam

Use the **link-oam** command to enable Ethernet Link Operations, Administration, and Management (OAM) on the interface. Use the **no** form of this command to disable the feature.

1.28.1 Syntax Description

No subcommands.

1.28.2 Default Values

By default, this feature is disabled.

1.28.3 Command History

ASE Release 4.4-41	Command was introduced.

1.28.4 Usage Examples

The following example enables Ethernet Link OAM on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#link-oam
```

1.29 link-oam link-monitor

Use the **link-oam link-monitor** command to enable and configure Ethernet Link Operations, Administration, and Management (OAM) link monitoring on the interface. Use the **no** form of this command to disable the feature. Variables that may be used with this command to further define the OAM link monitoring configuration include:

```
link-oam link-monitor frame threshold <number>
link-oam link-monitor frame threshold <number> window <time>
link-oam link-monitor frame window <time>
link-oam link-monitor frame window <time> threshold <number>
link-oam link-monitor frame-seconds threshold <number>
link-oam link-monitor frame-seconds threshold <number> window <time>
link-oam link-monitor frame-seconds window <time>
link-oam link-monitor frame-seconds window <time> threshold <number>
link-oam link-monitor supported
link-oam link-monitor symbol-period threshold <number>
link-oam link-monitor symbol-period threshold <number> window <time>
link-oam link-monitor symbol-period window <time>
link-oam link-monitor symbol-period window <time> threshold <number>
```

1.29.1 Syntax Description

frame	Configures link monitoring frame error event parameters.
threshold *<number>*	Specifies the number of errors allowed, within a specific time frame, before a frame error event is trigged. Valid range is **0** to **4294967295** frames.
window *<time>*	Specifies the time frame within which a certain number of errors are allowed before a frame error event is triggered. Valid range is **1** to **60** seconds.
frame-seconds	Configures the allowable frame errors by frames per second for link monitoring.
threshold *<number>*	Specifies the number of errors allowed by frames per second, within a specific time frame, before a frame error event is trigged. Valid range is **0** to **65535** frames.
window *<time>*	Specifies the time frame within which a certain number of errors are allowed before a frame error event is triggered. Valid range is **10** to **900** seconds.
supported	Enables OAM link monitoring on the interface.
symbol-period	Configures link monitoring error symbol link event parameters.
threshold *<number>*	Specifies the number of error symbols allowed, within a specific time frame, before an error symbol event is trigged. Valid range is **0** to **4294967295** frames.
window *<time>*	Specifies the time frame within which a certain number of error symbols are allowed before an error symbol event is triggered. Valid range is **1** to **60** seconds.

1.29.2 Default Values

By default, link OAM link monitoring is disabled.

1.29.3 Command History

ASE Release 4.4-41	Command was introduced.

1.29.4 Usage Examples

The following example enables Ethernet Link OAM link monitoring on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#link-oam link-monitor supported
```

1.30 link-oam mib-retrieval supported

Use the **link-oam mib-retrieval supported** command to enable Ethernet Link Operations, Administration, and Management (OAM) management information base (MIB) retrieval support. Use the **no** form of this command to disable the feature.

1.30.1 Syntax Description

No subcommands.

1.30.2 Default Values

By default, MIB retrieval is disabled for OAM configurations.

1.30.3 Command History

ASE Release 4.4-41	Command was introduced.

1.30.4 Usage Examples

The following example enables MIB retrieval for OAM link monitoring:

```
(config)#interface GigabitEthernet 1/1
(config-if)#link-oam mib-retrieval supported
```

1.31 link-oam mode

Use the **link-oam mode** command to specify the mode in which Ethernet Link Operations, Administration, and Management (OAM) operates on the interface. Use the **no** form of this command to disable the Link OAM mode. Variations of this command include:

```
link-oam mode active
link-oam mode passive
```

1.31.1 Syntax Description

active	Specifies the interface operates in OAM active mode. In this mode, the interface discovers and monitors connected links.
passive	Specifies the interface operates in OAM passive mode. In this mode, the interface waits for connected links to initiate the discovery process.

1.31.2 Default Values

By default, link OAM is disabled on the interface.

1.31.3 Command History

ASE Release 4.4-41	Command was introduced.

1.31.4 Usage Examples

The following example specifies the interface operates in OAM active mode:

```
(config)#interface GigabitEthernet 1/1
(config-if)#link-oam mode active
```

1.32 link-oam remote-loopback supported

Use the **link-oam remote-loopback supported** command to enable Ethernet Link Operations, Administration, and Management (OAM) remote loopback functionality on the interface. Use the **no** form of this command to disable this feature.

1.32.1 Syntax Description

No subcommands.

1.32.2 Default Values

By default, this feature is disabled.

1.32.3 Command History

ASE Release 4.4-41	Command was introduced.

1.32.4 Usage Examples

The following example enables remote loopback for OAM on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#link-oam remote-loopback supported
```

1.33 link-oam variable-retrieve

Use the **link-oam variable-retrieve** command to specify whether Ethernet Link Operations, Administration, and Management (OAM) retrieves local information when retrieving management information base (MIB) information. Use the **no** form of this command to disable OAM variable retrieval. Variations of this command include:

```
link-oam variable-retrieve local-info
```

1.33.1 Syntax Description

local-info	Specifies that OAM retrieves local MIB information.

1.33.2 Default Values

By default, OAM does not retrieve MIB information.

1.33.3 Command History

ASE Release 4.4-41	Command was introduced.

1.33.4 Usage Examples

The following example enables OAM to retrieve local MIB information:

```
(config)#interface GigabitEthernet 1/1
(config-if)#link-oam variable-retrieve local-info
```

1.34 lldp cdp-aware

Use the **lldp cdp-aware** command to specify that the interface is Cisco Discovery Protocol (CDP) aware and able to add CDP information to the Link Layer Discovery Protocol (LLDP) neighbor table. Use the **no** form of this command to disable this feature.

1.34.1 Syntax Description

No subcommands.

1.34.2 Default Values

By default, this feature is disabled.

1.34.3 Privilege Level

By default, this command has a privilege level of **15**.

1.34.4 Command History

ASE Release 4.4-41	Command was introduced.

1.34.5 Usage Examples

The following example enables CDP awareness on the interface for use with LLDP:

```
(config)#interface GigabitEthernet 1/1
(config-if)#lldp cdp-aware
```

1.35 lldp med media-vlan policy-list *<policies>*

Use the **lldp med media-vlan policy-list** command to assign access control lists (ACLs) to the virtual local area network (VLAN) used for Link Layer Discover Protocol (LLDP) Media Endpoint Discovery (MED) purposes. Use the **no** form of this command to remove the policy from the LLDP-MED configuration.

1.35.1 Syntax Description

<policies>	Specifies ACLs to add to the LLDP configuration for controlling media VLAN traffic. You can enter a single ACL ID, or several IDs separated by commas, or a range of IDs separated by a hyphen.

1.35.2 Default Values

By default, no ACLs are associated with LLDP.

1.35.3 Privilege Level

By default, this command has a privilege level of **15**.

1.35.4 Command History

ASE Release 4.4-41	Command was introduced.

1.35.5 Usage Examples

The following example applies ACL **31** to the LLDP-MED VLAN on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#lldp med media-vlan policy-list 31
```

1.36 lldp med transmit-tlv

Use the **lldp med transmit-tlv** command to enable Link Layer Discovery Protocol (LLDP) Media Endpoint Detection (MED) type length value (TLV) transmissions from the interface. Use the **no** form of this command to disable TLV transmissions. Variations of this command include:

```
lldp med transmit-tlv
lldp med transmit-tlv capabilities
lldp med transmit-tlv location
lldp med transmit-tlv network-policy
lldp med transmit-tlv poe
```

1.36.1 Syntax Description

capabilities	Optional. Enables capability TLV transmissions on the interface.
location	Optional. Enables location TLV transmissions on the interface.
network-policy	Optional. Enables network policy TLV transmissions on the interface.
poe	Optional. Enables Power over Ethernet (PoE) TLV transmissions on the interface.

1.36.2 Default Values

By default, TLV transmissions are disabled on the interface.

1.36.3 Privilege Level

By default, this command has a privilege level of **15**.

1.36.4 Command History

ASE Release 4.4-41	Command was introduced.

1.36.5 Functional Notes

The optional parameters of this command, **capabilities**, **location**, **network-policy**, and **poe**, can be entered in any order and within a single command. For example, to enable the **capabilities**, **location**, and **poe** TLV transmissions, enter the command as follows:

```
(config)#interface GigabitEthernet 1/1
(config-if)#lldp med transmit-tlv capabilities location poe
```

1.36.6 Usage Examples

The following example enables LLDP-MED TLV transmissions on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#lldp med transmit-tlv
```

1.37 lldp med type

Use the **lldp med type** command to specify whether the interface functions as a Link Layer Discovery Protocol (LLDP) Media Endpoint Discovery (MED) connectivity or endpoint device. Use the **no** form of this command to disable LLDP MED on the interface.

```
lldp med type connectivity
lldp med type end-point
```

1.37.1 Syntax Description

connectivity	Specifies the interface functions as a network connectivity device within the LLDP-MED configuration.
end-point	Specifies the interface functions as an endpoint device within the LLDP-MED configuration.

1.37.2 Default Values

By default, LLDP-MED is disabled on the interface.

1.37.3 Command History

ASE Release 4.4-41	Command was introduced.

1.37.4 Functional Notes

This command is used to specify that the interface functions as either network connectivity device, or as an endpoint device, within the LLDP-MED configuration. A network connectivity device initializes LLDP-MED TLV transmissions only when it discovers an endpoint device as a link partner. An endpoint device, however, begins sending LLDP-MED TLV transmissions at once.

1.37.5 Usage Examples

The following example specifies the interface is an LLDP-MED network connectivity device:

```
(config)#interface GigabitEthernet 1/1
(config-if)#lldp med type connectivity
```

1.38 lldp receive

Use the **lldp receive** command to enable the decoding of received Link Layer Discovery Protocol (LLDP) packets on the interface. Use the **no** form of this command to disable this feature.

1.38.1 Syntax Description

No subcommands.

1.38.2 Default Values

By default, this feature is disabled.

1.38.3 Privilege Level

By default, this command has a privilege level of **15**.

1.38.4 Command History

ASE Release 4.4-41	Command was introduced.

1.38.5 Usage Examples

The following example enables the decoding of received LLDP packets on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#lldp receive
```

1.39 lldp tlv-select

Use the **lldp tlv-select** command to specify which optional Link Layer Discover Protocol (LLDP) type length value (TLV) transmissions are sent from the interface. Use the **no** form of this command to disable optional LLDP TLV transmissions. Variations of this command include:

```
lldp tlv-select management-address
lldp tlv-select port-description
lldp tlv-select system-capabilities
lldp tlv-select system-description
lldp tlv-select system-name
```

1.39.1 Syntax Description

management-address	Specifies that management address TLV transmissions are sent from the interface.
port-description	Specifies that port description TLV transmissions are sent from the interface.
system-capabilities	Specifies that system capability TLV transmissions are sent from the interface.
system-description	Specifies that system description TLV transmissions are sent from the interface.
system-name	Specifies that system name TLV transmissions are sent from the interface.

1.39.2 Default Values

By default, no optional LLDP TLV transmissions are sent.

1.39.3 Privilege Level

By default, this command has a privilege level of **15**.

1.39.4 Command History

ASE Release 4.4-41	Command was introduced.

1.39.5 Usage Examples

The following example enables system name TLV transmissions on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#lldp tlv-select system-name
```

1.40 lldp transmit

Use the **lldp transmit** command to enable the transmission of Link Layer Discovery Protocol (LLDP) packets on the interface. Use the **no** form of this command to disable LLDP packet transmission.

1.40.1 Syntax Description

No subcommands.

1.40.2 Default Values

By default, LLDP is disabled.

1.40.3 Privilege Level

By default, this command has a privilege level of **15**.

1.40.4 Command History

ASE Release 4.4-41	Command was introduced.

1.40.5 Usage Examples

The following example enables LLDP transmissions on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#lldp transmit
```

1.41 lldp trap

Use the **lldp trap** command to specify that when the Link Layer Discover Protocol (LLDP) neighbor table is updated a Simple Network Management Protocol (SNMP) trap is sent. Use the **no** form of this command to disable this feature.

1.41.1 Syntax Description

No subcommands.

1.41.2 Default Values

By default, SNMP traps are not sent when the LLDP neighbor table is updated.

1.41.3 Privilege Level

By default, this command has a privilege level of **15**.

1.41.4 Command History

ASE Release 4.4-41	Command was introduced.

1.41.5 Usage Examples

The following example enables LLDP to send SNMP traps when the LLDP neighbor table is updated:

```
(config)#interface GigabitEthernet 1/1
(config-if)#lldp trap
```

1.42 loop-protect

Use the **loop-protect** command to enable and configure loop protection parameters on the interface. Use the **no** form of this command to disable loop protections.Variations of this command include:

```
loop-protect
loop-protect action log
loop-protect action log shutdown
loop-protect action shutdown
loop-protect action shutdown log
loop-protect tx-mode
```

1.42.1 Syntax Description

action	Optional. Specifies an action to take when a loop is detected.
log	Optional. Specifies that a log is generated when a loop is detected. This can be used in conjunction with the **shutdown** parameter.
shutdown	Optional. Specifies that the port shuts down when a loop is detected. This can be used in conjunction with the **log** parameter.
tx-mode	Optional. Specifies that the interface actively generates protocol data units (PDUs).

1.42.2 Default Values

By default, loop protection is disabled.

1.42.3 Privilege Level

By default, this command has a privilege level of **15**.

1.42.4 Command History

ASE Release 4.4-41	Command was introduced.

1.42.5 Usage Examples

The following example enables loop protection, and specifies that a log is generated and the interface shuts down when a loop is detected:

```
(config)#interface GigabitEthernet 1/1
(config-if)#loop-protect log shutdown
```

1.43 mac address-table learning

Use the **mac address-table learning** command to enable or disable the automatic learning of source Media Access Control (MAC) addresses on the port. Use the **no** form of this command to disable this feature. Variations of this command include:

```
mac address-table learning
mac address-table learning secure
```

1.43.1 Syntax Description

secure	Optional. Specifies that secure MAC addresses are learned by the switch and added to the MAC address table.

1.43.2 Default Values

By default, the automatic learning of MAC addresses is enabled. However, the learning of secure MAC addresses is disabled.

1.43.3 Command History

ASE Release 4.4-41	Command was introduced.

1.43.4 Usage Examples

To enable the dynamic addition of secure MAC addresses on the port, if it has been disabled, enter the command as follows:

```
(config)#interface GigabitEthernet 1/1
(config-if)#mac address-table learning secure
```

1.44 media-type

Use the **media-type** command to enable the media type connected to the interface. Use the **no** form of this command to disable the media type. Variations of this command include:

```
media-type dual
media-type rj45
media-type sfp
```

1.44.1 Syntax Description

dual	Specifies the interface is a dual media interface, supporting both copper and fiber connections.
rj45	Specifies the interface supports only copper connections.
sfp	Specifies the interface supports only fiber connections.

1.44.2 Default Values

By default, no media type is specified.

1.44.3 Privilege Level

By default, this command has a privilege level of **15**.

1.44.4 Command History

ASE Release 4.4-41	Command was introduced.

1.44.5 Usage Examples

The following example specifies the interface supports both copper and fiber connections:

```
(config)#interface GigabitEthernet 1/10
(config-if)#media-type dual
```

1.45 mrp periodic

Use the **mrp periodic** command to enable periodic Multiple Registration Protocol (MRP) transmissions on the interface. Use the **no** form of this command to disable MRP periodic transmissions on the interface.

1.45.1 Syntax Description

No subcommands.

1.45.2 Default Values

By default, MRP is disabled.

1.45.3 Command History

ASE Release 4.4-41	Command was introduced.

1.45.4 Usage Examples

The following example enables MRP transmissions on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#mrp periodic
```

1.46 mrp timers

Use the **mrp timers** command to configure Multiple Registration Protocol (MRP) timers on a per-port basis. Use the **no** form of this command to return to the default settings. Variations of this command include:

```
mrp timers default
mrp timers join-time <value>
mrp timers leave-all-time <value>
mrp timers leave-time <value>
```

1.46.1 Syntax Description

default	Sets all MRP timers to their default values.
join-time *<value>*	Configures the Join timer, which controls when protocol data unit (PDU) messages are sent. Valid range is **1** to **20** centiseconds.
leave-all-time *<value>*	Configures the LeaveAll timer, which controls the frequency with which interfaces generate deregistration requests. Valid range is **1000** to **5000** centiseconds.
leave-time *<value>*	Configures the Leave timer, which controls when a virtual local area network (VLAN) is deregistered, after it initializes a deregistration request, while also allowing enough time for connected devices to keep the registration alive while the request is being made. This value should always be set to be larger than the join timer value. Valid range is **60** to **300** centiseconds.

1.46.2 Default Values

By default the Join timer is set to **20** centiseconds, the LeaveAll timer is set to **1000** centiseconds, and the Leave timer is set to **60** centiseconds.

1.46.3 Command History

ASE Release 4.4-41	Command was introduced.

1.46.4 Functional Notes

You can enter the **join-time**, **leave-all-time**, and **leave-time** parameters of this command in any order, and in a single command if necessary.

1.46.5 Usage Examples

To configure all three timers at once, enter the command as follows:

```
(config)#interface GigabitEthernet 1/1
(config-if)#mrp timers leave-all-time 2000 join-time 10 leave-time 100
```

1.47 mtu <*size*>

Use the **mtu** <*size*> command to set the maximum transmission unit (MTU) size for the interface and allow Ethernet frames larger than 1518 bytes (known as jumbo frames) to pass. Use the **no** form of this command to return to the default setting.

1.47.1 Syntax Description

<size>	Specifies the maximum allowed frame size in bytes. Valid range is **1518** to **10240** bytes.

1.47.2 Default Values

By default, the MTU size is set to **1518** bytes.

1.47.3 Privilege Level

By default, this command has a privilege level of **15**.

1.47.4 Command History

ASE Release 4.4-41	Command was introduced.

1.47.5 Usage Examples

The following example sets the MTU size at **3600** bytes for the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#mtu 3600
```

1.48 mvr immediate-leave

Use the **mvr immediate-leave** command to enable the Multicast Virtual local area network (VLAN) Registration (MVR) immediate leave feature. This feature allows receiver ports to be removed from MVR membership as soon as they generate a leave message. Use the **no** form of this command to disable this feature.

1.48.1 Syntax Description

No subcommands.

1.48.2 Default Values

By default, this feature is disabled.

1.48.3 Privilege Level

By default, this command has a privilege level of **15**.

1.48.4 Command History

ASE Release 4.4-41	Command was introduced.

1.48.5 Functional Notes

This feature should only be enabled on receiver ports that are only connected to a single other receiver device.

1.48.6 Usage Examples

The following example enables the MVR immediate leave feature on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#mvr immediate-leave
```

1.49 mvr name <*name*> type

Use the **mvr name** <*name*> **type** command to define the role of the port in the Multicast Virtual local area network (VLAN) Registration (MVR) multicast VLAN. Use the **no** form of this command to remove the multicast VLAN from the port. Variations of this command include the following:

```
mvr name <name> type receiver
mvr name <name> type source
```

1.49.1 Syntax Description

<*name*>	Specifies the multicast VLAN name. Valid names are a maximum of **16** characters in length.
type receiver	Specifies the port associated with the named VLAN as a receiver port for MVR.
type source	Specifies the port associated with the named VLAN as a source port for MVR.

1.49.2 Default Values

By default, no multicast VLANs are associated with an interface.

1.49.3 Privilege Level

By default, this command has a privilege level of **15**.

1.49.4 Command History

ASE Release 4.4-41	Command was introduced.

1.49.5 Usage Examples

The following example specifies the VLAN MYVLAN1 on the interface as a source for MVR operations:

```
(config)#interface GigabitEthernet 1/1
(config-if)#mvr name MYVLAN1 type source
```

1.50 mvr vlan <*vlan ids*> type

Use the **mvr vlan** <*vlan ids*> **type** command to define the role of the port in the Multicast Virtual local area network (VLAN) Registration (MVR) VLANs. Use the **no** form of this command to remove the VLANs from the port. Variations of this command include:

```
mvr name <vlan ids> type receiver
mvr name <vlan ids> type source
```

1.50.1 Syntax Description

<vlan ids>	Specifies the VLANs to associate with the MVR port role. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.
type receiver	Specifies the port associated with the specified VLANs as a receiver port for MVR.
type source	Specifies the port associated with the specified VLANs as a source port for MVR.

1.50.2 Default Values

By default, no VLANs are associated with an interface MVR role.

1.50.3 Privilege Level

By default, this command has a privilege level of **15**.

1.50.4 Command History

ASE Release 4.4-41	Command was introduced.

1.50.5 Usage Examples

The following example specifies the VLAN 100 on the interface as a source for MVR operations:

```
(config)#interface GigabitEthernet 1/1
(config-if)#mvr vlan 100 type source
```

1.51 mvrp

Use the **mvrp** command to enable Multiple Virtual local area network (VLAN) Registration Protocol (MVRP) on the interface. Use the **no** form of this command to disable MVRP.

1.51.1 Syntax Description

No subcommands.

1.51.2 Default Values

By default, MVRP is disabled.

1.51.3 Command History

ASE Release 4.4-41	Command was introduced.

1.51.4 Usage Examples

The following example enables MVRP on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#mvrp
```

1.52 poe delay-mode

Use the **poe delay-mode** command to enable the Power over Ethernet (PoE) time delay feature on the interface. Use the **no** form of this command to disable this feature.

1.52.1 Syntax Description

No subcommands.

1.52.2 Default Values

By default, the PoE time delay is disabled.

1.52.3 Privilege Level

By default, this command has a privilege level of **15**.

1.52.4 Command History

ASE Release 4.4-41	Command was introduced.

1.52.5 Functional Notes

Before enabling the PoE time delay on the interface, first configure the delay time on the interface using the command “poe delay-time <time>” on page 537.

1.52.6 Usage Examples

The following example enables the PoE delay feature on the interface and specifies a delay time of **100** seconds:

```
(config)#interface GigabitEthernet 1/1
(config-if)#poe delay-time 100
(config-if)#poe delay-mode
```

1.53 poe delay-time <*time*>

Use the **poe delay-time** <*time*> command to specify the timed delay for the Power over Ethernet (PoE) port. Use the **no** form of this command to return to the default setting.

1.53.1 Syntax Description

<time>	Specifies the time delay in seconds. Valid range is **0** to **300** seconds.

1.53.2 Default Values

By default, the PoE time delay is not configured (**0** seconds).

1.53.3 Privilege Level

By default, this command has a privilege level of **15**.

1.53.4 Command History

ASE Release 4.4-41	Command was introduced.

1.53.5 Functional Notes

Once the PoE delay time is specified with this command, you must also enable the PoE delay using the command “poe delay-mode” on page 536.

1.53.6 Usage Examples

The following example configures a PoE delay time of **100** seconds and enables the PoE delay:

```
(config)#interface GigabitEthernet 1/1
(config-if)#poe delay-time 100
(config-if)#poe delay-mode
```

1.54 poe failure-action

Use the **poe failure-action** command to specify the action taken if Power over Ethernet (PoE) discovers a failure while automatically checking for failures. Use the **no** form of this command to return to the default setting. Variations of this command include:

```
poe failure-action nothing
poe failure-action reboot-Remote-PD
```

1.54.1 Syntax Description

nothing	Specifies no action is taken if PoE discovers a failure.
reboot-Remote-PD	Specifies PoE reboots the remote powered device if a failure is detected.

1.54.2 Default Values

By default, PoE takes no action if a failure is detected (**nothing**).

1.54.3 Privilege Level

By default, this command has a privilege level of **15**.

1.54.4 Command History

ASE Release 4.4-41	Command was introduced.

1.54.5 Functional Notes

This command determines the action taken when PoE discovers a failure. When configuring PoE to automatically check for failures, you can also specify the interval at which PoE checks for failures using the command “poe interval-time <time>” on page 539.

1.54.6 Usage Examples

The following example specifies that PoE should reboot the remotely connected powered device when a failure is discovered:

```
(config)#interface GigabitEthernet 1/1
(config-if)#poe failure-action reboot-Remote-PD
```

1.55 poe interval-time <*time*>

Use the **poe interval-time** <*time*> command to specify the interval at which Power over Ethernet (PoE) checks for failures. Use the **no** form of this command to return to the default setting.

1.55.1 Syntax Description

<time>	Specifies the interval (in seconds) between PoE checks for failures. Valid range is **10** to **120** seconds.

1.55.2 Default Values

By default, PoE checks for failures every **10** seconds.

1.55.3 Privilege Level

By default, this command has a privilege level of **15**.

1.55.4 Command History

ASE Release 4.4-41	Command was introduced.

1.55.5 Functional Notes

This command specifies the interval between PoE checks for failures. To specify the action taken when PoE discovers a failure, use the command “poe failure-action” on page 538.

1.55.6 Usage Examples

The following example specifies that PoE checks for failures every **75** seconds:

```
(config)#interface GigabitEthernet 1/1
(config-if)#poe interval-time 75
```

1.56 poe mode

Use the **poe mode** command to enable Power over Ethernet (PoE) on the interface and specify which PoE mode it supports (PoE+ or standard PoE). Use the **no** form of this command to disable PoE on the interface. Variations of this command include:

```
poe mode plus
poe mode standard
```

1.56.1 Syntax Description

plus	Specifies that the port uses PoE+, and will have a maximum power value of **30 W**.
standard	Specifies that the port uses PoE, and will have a maximum power value of **15.4 W**.

1.56.2 Default Values

By default, PoE+ is enabled.

1.56.3 Privilege Level

By default, this command has a privilege level of **15**.

1.56.4 Command History

ASE Release 4.4-41	Command was introduced.

1.56.5 Usage Examples

The following example enables PoE+ on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#poe mode plus
```

1.57 poe ping-ip-addr <*ipv4 address*>

Use the **poe ping-ip-addr** <*ipv4 address*> to enable Power over Ethernet (PoE) to ping a connected powered device.

1.57.1 Syntax Description

<ipv4 address>	Specifies the IPv4 address to ping. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

1.57.2 Default Values

No default values are necessary for this command.

1.57.3 Privilege Level

By default, this command has a privilege level of **15**.

1.57.4 Command History

ASE Release 4.4-41	Command was introduced.

1.57.5 Functional Notes

In addition to specifying the IPv4 address for PoE to ping using this command, you can also specify the how many times the ping action is repeated using the command “poe ping-retry-time <number>” on page 542.

1.57.6 Usage Examples

The following example specifies that PoE pings a powered device at the IPv4 address **192.22.72.101**:

```
(config)#interface GigabitEthernet 1/1
(config-if)#poe ping-ip-addr 192.22.72.101
```

1.58 poe ping-retry-time <*number*>

Use the **poe ping-retry-time** <*number*> command to specify how many times Power over Ethernet (PoE) will attempt to ping a connected powered device.

1.58.1 Syntax Description

<*number*>	Specifies the number of times PoE will attempt to ping an IPv4 address. Valid range is **1** to **5**.

1.58.2 Default Values

By default, the PoE ping action is not configured.

1.58.3 Privilege Level

By default, this command has a privilege level of **15**.

1.58.4 Command History

ASE Release 4.4-41	Command was introduced.

1.58.5 Functional Notes

This command specifies how many times to attempt to connect to a powered device using the ping functionality. For this command to have any effect, you must first configure a PoE ping action using the command “poe ping-ip-addr <ipv4 address>” on page 541.

1.58.6 Usage Examples

The following example specifies a PoE ping retry attempt of **3** to the IPv4 address **192.22.72.101**:

```
(config)#interface GigabitEthernet 1/1
(config-if)#poe ping-ip-addr 192.22.72.101
(config-if)#poe ping-retry-time 3
```

1.59 poe port-profile name <*name*>

Use the **poe port-profile name** <*name*> to apply a created Power over Ethernet (PoE) schedule to the interface. Use the no form of this command to disable the PoE scheduling feature.

1.59.1 Syntax Description

<*name*>	Specifies the name of the previously created PoE scheduling profile. Profile names are limited to **32** characters in length.

1.59.2 Default Values

By default, no PoE schedules are configured.

1.59.3 Privilege Level

By default, this command has a privilege level of **15**.

1.59.4 Command History

ASE Release 4.4-41	Command was introduced.

1.59.5 Functional Notes

This command applies a previously created PoE scheduling profile to the interface. PoE scheduling profiles are configured using the command “poe profile id” on page 403.

1.59.6 Usage Examples

To apply the PoE schedule profile with the profile ID of **1** to the port, enter the command as follows:

```
(config)#interface GigabitEthernet 1/1
(config-if)#poe port-profile name 1
```

1.60 poe power limit <*value*>

Use the **poe power limit** <*value*> command to specify the maximum power allotted to the port for Power over Ethernet (PoE) and power management. Using the **no** form of this command returns the power limit to the default setting.

1.60.1 Syntax Description

<value>	Specifies the port's maximum power. Valid range is **0** to **15.4** Watts for ports using standard PoE, and **0** to **30.0** Watts for ports using PoE+.

1.60.2 Default Values

By default, ports using standard PoE have a power limit of **15.4** Watts, and ports using PoE+ have a power limit of **30.0** Watts.

1.60.3 Privilege Level

By default, this command has a privilege level of **15**.

1.60.4 Command History

ASE Release 4.4-41	Command was introduced.

1.60.5 Functional Notes

Power management is configured by specifying how the reserved power is determined (by class, allocation, or Link Layer Discover Protocol (LLDP)), specifying the power management mode (actual consumption or reserved power), and optionally enabling capacitor detection mode. To configure how PoE determines reserved power, refer to the command "poe management mode" on page 400.

When power management is completed by verifying power allocation to a port, it takes into account the maximum power (in Watts) specified for the port. This is the maximum power specified using this command (**poe power limit**).

1.60.6 Usage Examples

The following example specifies the maximum power for the interface as **10.2** Watts:

```
(config)#interface GigabitEthernet 1/1
(config-if)#poe power limit 10.2
```

1.61 poe priority

Use the **poe priority** command to specify the port's Power over Ethernet (PoE) priority setting. Use the **no** form of this command to return to the default setting. Variations of this command include:

```
poe priority critical
poe priority high
poe priority low
```

1.61.1 Syntax Description

critical	Assigns a critical priority to the port.
high	Assigns a high priority to the port.
low	Assigns a low priority to the port.

1.61.2 Default Values

By default, all PoE ports have the same priority.

1.61.3 Privilege Level

By default, this command has a privilege level of **15**.

1.61.4 Command History

ASE Release 4.4-41	Command was introduced.

1.61.5 Functional Notes

You can assign each port one of three priorities—low, high, or critical. The lowest priority port is shut down when a remote device requires more power than the power supply can deliver. If port priorities are equal, the highest numbered port is shut down (default behavior).

1.61.6 Usage Examples

The following example specifies the port is a high priority PoE port:

```
(config)#interface GigabitEthernet 1/1
(config-if)#poe priority high
```

1.62 poe reboot-time <*value*>

Use the **poe reboot-time** <*value*> command to specify how long it takes Power over Ethernet (PoE) to reboot a connected powered device should it fail. Use the **no** form of this command to disable automatic reboots from PoE failures.

1.62.1 Syntax Description

<value>	Specifies the time (in seconds) before PoE reboots a connected device. Valid range is **3** to **120** seconds.

1.62.2 Default Values

By default, PoE does not automatically reboot failed powered devices.

1.62.3 Privilege Level

By default, this command has a privilege level of **15**.

1.62.4 Command History

ASE Release 4.4-41	Command was introduced.

1.62.5 Usage Examples

The following example specifies that PoE reboots a failed device after **10** seconds:

```
(config)#interface GigabitEthernet 1/1
(config-if)#poe reboot-time 10
```

1.63 poe startup-time <*value*>

Use the **poe startup-time** <*value*> to specify how long after a Power over Ethernet (PoE) port becomes active to begin automatically checking for PoE failures. Use the **no** form of this command to return to the default value.

1.63.1 Syntax Description

<value>	Specifies the time (in seconds) before PoE begins checking for failures. Valid range is **30** to **600** seconds.

1.63.2 Default Values

By default, PoE begins automatically checking for failures after **30** seconds.

1.63.3 Privilege Level

By default, this command has a privilege level of **15**.

1.63.4 Command History

ASE Release 4.4-41	Command was introduced.

1.63.5 Usage Examples

The following example specifies that PoE begins checking for failures after **75** seconds:

```
(config)#interface GigabitEthernet 1/1
(config-if)#poe startup-time 75
```

1.64 port-security

Use the **port-security** command to enable port security on the interface. When enabled, port security specifies how many Media Access Control (MAC) addresses can be learned on the interface, and what actions are taken if this limit is exceeded. Use the **no** form of this command to disable port security.

1.64.1 Syntax Description

No subcommands.

1.64.2 Default Values

By default, port security is disabled.

1.64.3 Privilege Level

By default, this command has a privilege level of **15**.

1.64.4 Command History

ASE Release 4.4-41	Command was introduced.

1.64.5 Functional Notes

To specify the maximum number of MAC addresses that can be learned on the interface, use the command “port-security maximum <number>” on page 549. To configure the action taken when this limit is exceeded, use the command “port-security violation” on page 551.

1.64.6 Usage Examples

The following example enables port security on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#port-security
```

1.65 port-security maximum <*number*>

Use the **port-security maximum** <*number*> command to specify the maximum number of Media Access Control (MAC) addresses that can be learned on the interface. Use the **no** form of this command to return to the default setting.

1.65.1 Syntax Description

<*number*>	Specifies the maximum number of MAC addresses that can be learned. Valid range is **0** to **1023**.

1.65.2 Default Values

By default, a maximum of **1023** MAC addresses can be learned on the interface.

1.65.3 Privilege Level

By default, this command has a privilege level of **15**.

1.65.4 Command History

ASE Release 4.4-41	Command was introduced.

1.65.5 Usage Examples

The following example specifies that **800** MAC addresses can be learned on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#port-security maximum 800
```

1.66 port-security maximum-violation <*number*>

Use the **port-security maximum-violation** <*number*> command to specify the maximum number of Media Access Control (MAC) addresses that can be learned on the interface once the interface is placed in restricted mode due to a violation (using the command "port-security violation" on page 551). Use the **no** form of this command to return to the default setting.

1.66.1 Syntax Description

<*number*>	Specifies the maximum number of MAC addresses that can be learned on the interface once it has been placed in restricted mode due to a violation. Valid range is **1** to **1023**.

1.66.2 Default Values

By default, an interface can learn up to **1023** MAC addresses.

1.66.3 Privilege Level

By default, this command has a privilege level of **15**.

1.66.4 Command History

ASE Release 4.4-41	Command was introduced.

1.66.5 Usage Examples

The following example specifies that only **100** MAC addresses can be learned once the interface is placed in restricted mode due to a violation:

```
(config)#interface GigabitEthernet 1/1
(config-if)#port-security maximum-violation 100
```

1.67 port-security violation

Use the **port-security violation** command to specify the action taken when the number of learned Media Access Control (MAC) addresses on the interface exceeds the limit specifies using the command “port-security maximum <number>” on page 549. Use the **no** form of this command to return to the default setting. Variations of this command include:

```
port-security violation protect
port-security violation restrict
port-security violation shutdown
```

1.67.1 Syntax Description

protect	Specifies that no action is taken when the interface MAC address limit is exceeded.
restrict	Specifies that the interface continues to record MAC addresses learned in excess of the specified limit.
shutdown	Specifies that the port is shutdown once the MAC address limit is exceeded.

1.67.2 Default Values

By default, no action is taken when MAC address limits are exceeded on the interface.

1.67.3 Privilege Level

By default, this command has a privilege level of **15**.

1.67.4 Command History

ASE Release 4.4-41	Command was introduced.

1.67.5 Usage Examples

The following example specifies that the port is shutdown once the MAC address limit is exceeded on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#port-security violation shutdown
```

1.68 priority-flowcontrol prio <*value*>

Use the **priority-flowcontrol prio** <*value*> to configure priority flow control settings on the interface. Use the **no** form of this command to disable the flow control feature.

1.68.1 Syntax Description

<value> Specifies the priority. Valid range is **0** to **7**.

1.68.2 Default Values

By default, flow control is disabled.

1.68.3 Privilege Level

By default, this command has a privilege level of **15**.

1.68.4 Command History

ASE Release 4.4-41 Command was introduced.

1.68.5 Usage Examples

The following example specifies a flow control priority of **3** for the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#priority-flowcontrol prio 3
```

1.69 ptp

Use the **ptp** command to enable Precision Time Protocol (PTP) on the interface. Use the **no** form of this command to disable PTP on the interface.

1.69.1 Syntax Description

No subcommands.

1.69.2 Default Values

By default, PTP is disabled on the interface.

1.69.3 Command History

ASE Release 4.4-41	Command was introduced.

1.69.4 Usage Examples

The following example enables PTP on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#ptp
```

1.70 ptp <*instance*>

Use the **ptp** <*instance*> command to create a Precision Time Protocol (PTP) clock instance and configure PTP parameters for that instance. Use the **no** form of this command to remove the PTP clock instance from the interface's configuration. Variations of this command include:

```
ptp <instance>
ptp <instance> announce interval <interval>
ptp <instance> announce interval <interval> timeout <number>
ptp <instance> announce timeout <number>
ptp <instance> announce timeout <number> interval <interval>
ptp <instance> delay-asymmetry <time>
ptp <instance> delay-mechanism e2e
ptp <instance> delay-mechanism p2p
ptp <instance> delay-req interval <interval>
ptp <instance> egress-latency <time>
ptp <instance> ingress-latency <time>
ptp <instance> internal
ptp <instance> localpriority <value>
ptp <instance> mcast-dest default
ptp <instance> mcast-dest link-local
ptp <instance> not-slave
ptp <instance> sync-interval <interval>
ptp <instance> two-step false
ptp <instance> two-step true
```

1.70.1 Syntax Description

<*instance*>	Specifies the PTP clock instance. Valid range is **0** to **3**.
announce interval <*interval*>	Specifies the interval at which PTP announcements are sent. Valid range is **-3** to **4**.
announce timeout <*interval*>	Specifies the PTP announcement timeout interval. Valid range is **1** to **10**. This timeout interval is created by multiplying the value entered here by the specified interval value.
delay-asymmetry <*time*>	Optional. Specifies the path delay for asymmetrical paths. Valid range is **-100000** to **100000** nanoseconds.
delay-mechanism e2e	Optional. Specifies the mechanism that determines a path delay is an end-to-end mechanism.
delay-mechanism p2p	Optional. Specifies the mechanism that determines a path delay is a peer-to-peer mechanism.
delay-req interval <*interval*>	Optional. Specifies the interval between PTP Pdelay_req messages. Valid range is **-7** to **5**.
egress-latency <*time*>	Optional. Specifies the port egress latency. Valid range is **-100000** to **100000** nanoseconds.
ingress-latency <*time*>	Optional. Specifies the port ingress latency. Valid range is **-100000** to **100000** nanoseconds.
internal	Optional. Specifies that this clock instance is an internal interface.

localpriority *<value>*	Optional. Specifies the local priority for the interface in accordance with the G8275.1 BMC algorithm. Valid range is **1** to **255**, with **1** being the highest priority.
mcast-dest default	Optional. Specifies that the type of multicast destination address used on the interface is the default destination address.
mcast-dest link-local	Optional. Specifies that the type of multicast destination address used on the interface is a link-local destination address.
not-slave	Optional. Specifies this clock instance is not a slave clock, in accordance with the G8275.1 BMC algorithm.
sync-interval *<interval>*	Optional. Specifies the interval at which PTP sends synchronization messages. Valid range is **-7** to **4**.
two-step false	Optional. Specifies that the two-step override value for the interface is false.
two-step true	Optional. Specifies that the two-step override value for the interface is true.

1.70.2 Default Values

By default, no PTP clock instance is configured.

1.70.3 Command History

ASE Release 4.4-41	Command was introduced.

1.70.4 Usage Examples

The following example creates PTP clock instance **1**, and specifies that it is not a slave clock:

```
(config)#interface GigabitEthernet 1/1
(config-if)#ptp 1 not-slave
```

1.71 pvlan

Use the **pvlan** command to configure private virtual local area network (VLAN) parameters for the interface. Use the **no** form of this command to remove the private VLAN configuration from the interface. Variations of this command include:

```
pvlan <vlan ids>
pvlan isolation
```

1.71.1 Syntax Description

<vlan ids>	Specifies the private VLANs associated with the interface. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.
isolation	Specifies the interface is isolated within the private VLAN. This setting indicates devices connected to the interface cannot communicate with each other.

1.71.2 Default Values

By default, no private VLANs are configured.

1.71.3 Privilege Level

By default, this command has a privilege level of **13**.

1.71.4 Command History

ASE Release 4.4-41	Command was introduced.

1.71.5 Functional Notes

VLANs must be previously configured before they can be specified as a private VLAN.

1.71.6 Usage Examples

The following example specifies VLANs **100**, **110**, and **120** are private VLANs associated with the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#pvlan 100,110,120
```

1.72 qos class <*id*>

Use the **qos class** <*id*> command to configure the Quality of Service (QoS) Class of Service (CoS) ID for the interface. Use the **no** form of this command to return the CoS ID to the default value.

1.72.1 Syntax Description

<*id*>	Specifies the CoS ID for the interface. Valid range **0** to **7**.

1.72.2 Default Values

By default, the CoS ID for the interface is **0**.

1.72.3 Privilege Level

By default, this command has a privilege level of **15**.

1.72.4 Command History

ASE Release 4.4-41	Command was introduced.

1.72.5 Usage Examples

The following example specifies a QoS CoS ID of **3** for the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#qos class 3
```

1.73 qos cos <*value*>

Use the **qos cos** <*value*> command to configure the Quality of Service (QoS) Class of Service (CoS) classification for the interface. Use the **no** form of this command to return to the default value.

1.73.1 Syntax Description

<value>	Specifies the CoS classification for the interface. Valid range is **0** to **7**.

1.73.2 Default Values

By default, the QoS CoS classification for the interface is **0**.

1.73.3 Privilege Level

By default, this command has a privilege level of **15**.

1.73.4 Command History

ASE Release 4.4-41	Command was introduced.

1.73.5 Functional Notes

The CoS classification entered on the interface applies to all incoming traffic on the interface, and can only be overwritten by a QoS control list entry (QCE) applied to the interface.

1.73.6 Usage Examples

The following example specifies a CoS classification of **2** for the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#qos cos 2
```

1.74 qos dei <*value*>

Use the **qos dei** <*value*> command to specify the Quality of Service (QoS) drop eligibility indicator (DEI) values assigned to incoming traffic on the interface. Use the **no** form of this command to return to the default setting.

1.74.1 Syntax Description

<value>	Specifies the DEI value assigned to incoming traffic. Valid range is **0** or **1**.

1.74.2 Default Values

By default, a DEI value of **0** is assigned to incoming traffic.

1.74.3 Privilege Level

By default, this command has a privilege level of **15**.

1.74.4 Command History

ASE Release 4.4-41	Command was introduced.

1.74.5 Usage Examples

The following example assigns a DEI value of **1** to incoming traffic on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#qos dei 1
```

1.75 qos dpl <*value*>

Use the **qos dpl** <*value*> command to assign Quality of Service (QoS) drop precedence level (DPL) values to incoming traffic on the interface. Use the **no** form of this command to return to the default setting.

1.75.1 Syntax Description

<value>	Specifies the DPL value to assign to incoming traffic. Valid range is **0** to **3**.

1.75.2 Default Values

By default, a DPL value of **0** is assigned to incoming traffic on the interface.

1.75.3 Privilege Level

By default, this command has a privilege level of **15**.

1.75.4 Command History

ASE Release 4.4-41	Command was introduced.

1.75.5 Usage Examples

The following example assigns a DPL value of **3** to ingress traffic on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#qos dpl 3
```

1.76 qos dscp-classify

Use the **qos dscp-classify** command to enable Quality of Service (QoS) Differentiated Service Code Points (DSCP) classification for ingress traffic on the interface. Use the **no** form of this command to disable DSCP classification. Variations of this command include:

```
qos dscp-classify any
qos dscp-classify selected
qos dscp-classify zero
```

1.76.1 Syntax Description

any	Specifies that incoming traffic is always classified to a new DSCP value.
selected	Specifies that incoming traffic of a specific DSCP value is classified to a new DSCP value only if DSCP classification is enabled for that specific DSCP value in the global DSCP classify map (refer to command “qos map dscp-classify <dscp value>” on page 416).
zero	Specifies that incoming traffic is classified to a new DSCP value if the current DSCP value is zero.

1.76.2 Default Values

By default, DSCP classification is disabled.

1.76.3 Privilege Level

By default, this command has a privilege level of **15**.

1.76.4 Command History

ASE Release 4.4-41	Command was introduced.

1.76.5 Usage Examples

The following example specifies that all incoming traffic is assigned a new DSCP value when it enters the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#qos dscp-classify any
```

1.77 qos dscp-remark

Use the **qos dscp-remark** command to enable Quality of Service (QoS) Differentiated Service Code Points (DSCP) rewriting and remapping of egress traffic on the interface. Use the **no** form of this command to disable this feature. Variations of this command include:

```
qos dscp-remark remap
qos dscp-remark rewrite
```

1.77.1 Syntax Description

remap	Specifies that the DSCP field of egress traffic is rewritten using classified DSCP values that have been mapped through the global DSCP egress translation map (refer to command "qos map dscp-egress-translation <dscp value> to <dscp value>" on page 418).
rewrite	Specifies that the DSCP field of egress traffic is rewritten with a classified DSCP value without any DSCP translation.

1.77.2 Default Values

By default, DSCP rewriting and remapping features are disabled.

1.77.3 Privilege Level

By default, this command has a privilege level of **15**.

1.77.4 Command History

ASE Release 4.4-41	Command was introduced.

1.77.5 Usage Examples

The following example enables DSCP to rewrite egress traffic based on the global DSCP egress translation map settings:

```
(config)#interface GigabitEthernet 1/1
(config-if)#qos dscp-remark remap
```

1.78 qos dscp-translate

Use the **qos dscp-translate** command to enable Quality of Service (QoS) Differentiated Service Code Points (DSCP) translation for incoming traffic on the interface. Use the **no** form of this command to disable this feature.

1.78.1 Syntax Description

No subcommands.

1.78.2 Default Values

By default, DSCP translation is disabled.

1.78.3 Privilege Level

By default, this command has a privilege level of **15**.

1.78.4 Command History

ASE Release 4.4-41	Command was introduced.

1.78.5 Usage Examples

The following example enables DSCP translation for ingress traffic on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#qos dscp-translate
```

1.79 qos egress-map <*map id*>

Use the **qos egress-map** <*map id*> command to apply a previously configured Quality of Service (QoS) egress map to egress traffic on the interface. Use the **no** form of this command to remove the map from the interface.

1.79.1 Syntax Description

<map id>	Specifies the ID of the previously created QoS egress map to associate with the interface. Valid range is **0** to **255**.

1.79.2 Default Values

By default, no QoS egress maps are configured or applied to the interface.

1.79.3 Privilege Level

By default, this command has a privilege level of **15**.

1.79.4 Command History

ASE Release 4.4-41	Command was introduced.

1.79.5 Functional Notes

Egress maps are used to control the rewriting of packets at egress, where Priority Code Points (PCP), drop eligibility indicator (DEI), and Differentiated Service Code Points (DSCP) values can be updated based on their classified key values. Egress maps are configured by specifying which part of the packet is used for matching (Class of Service (CoS) ID, CoS ID-drop precedence level (DPL), DSCP, or DSCP-DPL), enabling the rewriting actions taken once the packet information is processed, and specifying which new values are mapped to the packet information. Refer to the commands outlined in "QoS Egress Map Command Set" on page 668 for more information about configuring QoS egress maps.

1.79.6 Usage Examples

The following example applies the previously created QoS egress map **10** to egress traffic on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#qos egress-map 10
```

1.80 qos ingress-map <*map id*>

Use the **qos ingress-map** <*map id*> command to apply a previously configured Quality of Service (QoS) ingress map to ingress traffic on the interface. Use the **no** form of this command to remove the map from the interface.

1.80.1 Syntax Description

<map id>	Specifies the ID of the previously created QoS ingress map to associate with the interface. Valid range is **0** to **127**.

1.80.2 Default Values

By default, no QoS ingress maps are configured or applied to the interface.

1.80.3 Privilege Level

By default, this command has a privilege level of **15**.

1.80.4 Command History

ASE Release 4.4-41	Command was introduced.

1.80.5 Functional Notes

Ingress maps are used by QoS as a method for further classifying incoming traffic based on key values in the packet or frame header. Refer to the commands outlined in “QoS Ingress Map Command Set” on page 677 for more information about configuring QoS ingress maps.

1.80.6 Usage Examples

The following example applies the previously created QoS ingress map **50** to ingress traffic on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#qos ingress-map 50
```

1.81 qos map

Use the **qos map** command to enable Quality of Service (QoS) tag mapping for incoming traffic on the interface and specify how incoming tagged frames on the virtual local area network (VLAN)-aware interface are handled. Use the **no** form of this command to disable the tag mapping feature. Variations of this command include:

qos map cos-tag cos *<value>* **dpl** *<value>* **pcp** *<value>* **dei** *<value>*
qos map tag-cos pcp *<value>* **dei** *<value>* **cos** *<value>* **dpl** *<value>*

1.81.1 Syntax Description

cos-tag	Configures the mapping parameters for Class of Service (CoS)-to-tag configurations by specifying the CoS and drop precedence level (DPL) values to map to the specified Priority Code Points (PCP) and drop eligibility indicator (DEI) parameters.
cos *<value>*	Specifies the CoS value you are mapping: valid range is **0** to **7** and can consist of a specific CoS class value or a range.
dpl *<value>*	Specifies the DPL level you are mapping; valid range is **0** to **3**.
pcp *<value>*	Specifies the PCP value to which you are mapping the specified CoS and DPL values; valid range is **0** to **7**.
dei *<value>*	Specifies the DEI value to which you are mapping the specified CoS and DPL values; valid range is **0** to **1**.
tag-cos	Configures the mapping parameters for Tag-to-CoS configurations by specifying the PCP and DEI values to map to the specified CoS and DPL parameters.
pcp *<value>*	Specifies the PCP value you are mapping; valid range is **0** to **7** and can consist of a specific value or a range.
dei *<value>*	Specifies the DEI value you are mapping; valid range is **0** to **1**.
cos *<value>*	Specifies the CoS value to which you are mapping the PCP and DEI values, and has a valid range **0** to **7**.
dpl *<value>*	Specifies the DPL level to which you are mapping the PCP and DEI values; valid range is **0** to **3**.

1.81.2 Default Values

By default, this feature is disabled, which indicates that the default CoS and DPL values are used for tagged frames.

1.81.3 Privilege Level

By default, this command has a privilege level of **15**.

1.81.4 Command History

ASE Release 4.4-41	Command was introduced.

1.81.5 Usage Examples

To configure Cos-to-tag mapping of CoS **5** and DPL **1** to PCP **3** and DEI **0**, enter the command as follows:

```
(config)#interface GigabitEthernet 1/1
(config-if)#qos map cos-tag cos 5 dpl 1 pcp 3 dei 0
```

To configure Tag-to-CoS mapping of PCP **6** and DEI **0** to CoS **3** and DPL **1**, enter the command as follows:

```
(config)#interface GigabitEthernet 1/1
(config-if)#qos map tag-cos pcp 6 dei 0 cos 3 dpl 1
```

1.82 qos pcp <*value*>

Use the **qos pcp** <*value*> command to assign Quality of Service (QoS) Priority Code Point (PCP) values to all incoming traffic on the interface. Use the **no** form of this command to disable this feature and allow all incoming traffic to be associated with the default PCP value.

1.82.1 Syntax Description

<value>	Specifies the PCP value to assign. Valid range is **0** to **7**.

1.82.2 Default Values

By default, all frames are classified using the default PCP value unless the port is VLAN-aware and the frame is tagged, in which case the PCP value given in the frame tag is used.

1.82.3 Privilege Level

By default, this command has a privilege level of **15**.

1.82.4 Command History

ASE Release 4.4-41	Command was introduced.

1.82.5 Usage Examples

The following example specifies that incoming traffic is classified using the PCP value **3**:

```
(config)#interface GigabitEthernet 1/1
(config-if)#qos pcp 3
```

1.83 qos policer

Use the **qos policer** command to enable and configure a Quality of Service (QoS) policer on the interface. The policer serves to additionally classify the ingress traffic on the interface. Use the **no** form of this command to disable the QoS policer. Variations of this command include:

```
qos policer <rate>
qos policer <rate> flowcontrol
qos policer <rate> flowcontrol fps
qos policer <rate> flowcontrol kbps
qos policer <rate> flowcontrol kfps
qos policer <rate> flowcontrol mbps
qos policer <rate> fps
qos policer <rate> kbps
qos policer <rate> kfps
qos policer <rate> mbps
```

1.83.1 Syntax Description

<rate>	Specifies the traffic rate for the policer. The specified rate is internally rounded up to the nearest value supported by the policer. Valid range is **1** to **13128147**.
flowcontrol	Optional. Enables flow control for the interface, which specifies that the policer does not discard Transmission Control Protocol (TCP) traffic paused frames, but rather continues to send them.
fps	Optional. Specifies the rate unit for the policer as frames per second.
kbps	Optional. Specifies the rate unit for the policer as kilobits per second.
kfps	Optional. Specifies the rate unit for the policer as kiloframes per second.
mbps	Optional. Specifies the rate unit for the policer as Megabits per second.

1.83.2 Default Values

By default, a QoS policer is not configured on the interface. When the policer is configured, its default traffic rate is **500 kbps**.

1.83.3 Privilege Level

By default, this command has a privilege level of **15**.

1.83.4 Command History

ASE Release 4.4-41	Command was introduced.

1.83.5 Usage Examples

The following example enables the QoS policer on the interface with the default traffic rate parameters:

```
(config)#interface GigabitEthernet 1/1
(config-if)#qos policer 10000
```

1.84 qos queue-policer

Use the **qos queue-policer** command to configure a Quality of Service (QoS) queue policer on the interface, thus limiting the bandwidth of received frames that exceeds configured rates for the interface. Use the **no** form of this command to return to the QoS queue policer to the default setting. Variations of this command include:

qos queue-policer queue *<queue>* *<rate>* **kbps**
qos queue-policer queue *<queue>* *<rate>* **mbps**

1.84.1 Syntax Description

<queue>	Specifies the queue for which you are configuring the policer. Valid range is **0** to **7**, and can be entered as a single queue or a range of queues.
<rate>	Specifies the traffic rate for the policer. Valid range is **1** to **13128147**.
kbps	Specifies the traffic rate unit as kilobits per second.
mbps	Specifies the traffic rate unit as Megabits per second.

1.84.2 Default Values

By default, QoS queue policers limit bandwidth at a rate of **500 kbps**.

1.84.3 Privilege Level

By default, this command has a privilege level of **15**.

1.84.4 Command History

ASE Release 4.4-41	Command was introduced.

1.84.5 Usage Examples

The following example configures a QoS policer for queue **2** with the traffic rate settings of **1500 mbps**:

```
(config)#interface GigabitEthernet 1/1
(config-if)#qos queue-policer queue 2 1500 mbps
```

1.85 qos queue-shaper

Use the **qos queue-shaper** command to configure Quality of Service (QoS) traffic shapers on a per-queue basis to control bandwidth usage and traffic flow parameters for egress traffic on the ASE device. Use the **no** form of this command to return the queue shaper to the default setting. Variations of this command include:

```
qos queue-shaper queue <queue> <rate> kbps rate-type data
qos queue-shaper queue <queue> <rate> kbps rate-type line
qos queue-shaper queue <queue> <rate> mbps rate-type data
qos queue-shaper queue <queue> <rate> mbps rate-type line
```

1.85.1 Syntax Description

<queue>	Specifies the queue for which the shaper is being configured. Valid range is **0** to **7**, and can be entered as a single queue or a range of queues.
<rate>	Specifies the traffic rate for the shaper. Valid range is **1** to **13107100**.
kbps	Specifies the traffic rate unit as kilobits per second.
mbps	Specifies the traffic rate unit as Megabits per second.
rate-type data	Specifies that the data rate is being shaped with the queue shaper.
rate-type line	Specifies that the line rate is being shaped with the queue shaper.

1.85.2 Default Values

By default, all queue shapers are configured with a rate of **500 kbps**.

1.85.3 Privilege Level

By default, this command has a privilege level of **15**.

1.85.4 Command History

ASE Release 4.4-41	Command was introduced.

1.85.5 Usage Examples

The following example configures a queue shaper for queue **3** with a **data** shaper rate of **1500 mbps**:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos queue-shaper queue 3 1500 mbps rate-type data
```

1.86 qos shaper <*rate*>

Use the **qos shaper** <*rate*> command to configure Quality of Service (QoS) shapers on the interface to aid in bandwidth allocation for egress traffic. Use the **no** form of this command to return the shaper to the default values. Variations of this command include:

```
qos shaper <rate>
qos shaper <rate> kbps
qos shaper <rate> kbps rate-type data
qos shaper <rate> kbps rate-type line
qos shaper <rate> mbps
qos shaper <rate> mbps rate-type data
qos shaper <rate> mbps rate-type line
```

1.86.1 Syntax Description

<rate>	Specifies the traffic rate for the shaper. Valid range is **1** to **13107100**.
kbps	Specifies the traffic rate unit as kilobits per second.
mbps	Specifies the traffic rate unit as Megabits per second.
rate-type data	Specifies that the data rate is being shaped with the shaper.
rate-type line	Specifies that the line rate is being shaped with the shaper.

1.86.2 Default Values

By default, all shapers are configured with a rate of **500 kbps**.

1.86.3 Privilege Level

By default, this command has a privilege level of **15**.

1.86.4 Command History

ASE Release 4.4-41	Command was introduced.

1.86.5 Usage Examples

The following example configures a shaper for the interface with a **data** shaper rate of **1500 mbps**:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos shaper 1500 mbps rate-type data
```

1.87 qos tag-remark

Use the **qos tag-remark** command to enable Quality of Service (QoS) tag remarking on egress traffic at the interface level. This feature can apply mapped definitions for Class of Service and drop precedence level (CoS/DPL) values to Priority Code Point and drop eligibility indicator (PCP/DEI) values, or the configured default PCP and DEI values defined on the interface can be applied. Use the **no** form of this command to disable QoS tag remarking. Variations of this command include:

```
qos tag-remark mapped
qos tag-remark pcp <value> dei <value>
```

1.87.1 Syntax Description

mapped	Specifies that tag remarking occurs using previously mapped CoS/DPL to PCP/DEI values (as set by the command "qos map" on page 566).
pcp *<value>* **dei** *<value>*	Specifies that tag remarking occurs using default PCP and DEI settings that are set with this command. Valid range of PCP values is **0** to **7**, and valid range of DEI values is **0** to **1**.

1.87.2 Default Values

By default, QoS tag remarking of egress traffic is disabled.

1.87.3 Privilege Level

By default, this command has a privilege level of **15**.

1.87.4 Command History

ASE Release 4.4-41	Command was introduced.

1.87.5 Usage Examples

To configure QoS tag remarking to use newly specified PCP and DEI values, enter the command as follows:

```
(config)#interface GigabitEthernet 1/1
(config-if)#qos tag-remark pcp 4 dei 0
```

To configure QoS tag remarking to use previously mapped tag values, enter the command as follows:

```
(config)#interface GigabitEthernet 1/1
(config-if)#qos tag-remark mapped
```

1.88 qos trust

Use the **qos trust** command to enable trust for Differentiated Service Code Points (DSCP) and virtual local area network (VLAN) tagged traffic. Trust must be enabled to configure DSCP-based Quality of Service (QoS). Use the **no** form of this command to disable QoS trust on the interface, and therefore DSCP-based QoS. Variations of this command include:

```
qos trust dscp
qos trust tag
```

1.88.1 Syntax Description

dscp	Specifies that DSCP values defined in the DSCP to CoS map are trusted, and can be used for DSCP-based QoS.
tag	Specifies that traffic tagged with VLAN IDs defined in the CoS to DSCP map are trusted, and can be used for DSCP-based QoS.

1.88.2 Default Values

By default, QoS trust and DSCP-based QoS are disabled.

1.88.3 Privilege Level

By default, this command has a privilege level of **15**.

1.88.4 Command History

ASE Release 4.4-41	Command was introduced.

1.88.5 Usage Examples

To enable trust on the interface for incoming traffic with associated DSCP values, enter the command as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos trust dscp
```

1.89 qos wred-group <*group id*>

Use the **qos wred-group** <*group id*> command to assign a Weighted Random Early Detection (WRED) group to the interface for Quality of Service (QoS) traffic management. Use the **no** form of this command to remove the WRED group from the interface. Variations of this command include:

qos wred-group *<group id>*

1.89.1 Syntax Description

<group id>	Specifies the previously configured WRED group to assign to the interface. Valid range is **1** to **3**.

1.89.2 Default Values

By default, no WRED group is assigned to the interface.

1.89.3 Privilege Level

By default, this command has a privilege level of **15**.

1.89.4 Command History

ASE Release 4.4-41	Command was introduced.

1.89.5 Functional Notes

QoS WRED groups are configured at the Global level. Refer to the command “qos wred group” on page 431 for information about WRED group configuration.

1.89.6 Usage Examples

The following example applies the previously configured WRED group **2** to the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#qos wred-group 2
```

1.90 qos wrr <*Q# weight*>

Use the **qos wrr** <*Q# weight*> command to configure Quality of Service (QoS) Deficit Weighted Round Robin (DWRR) scheduling for egress traffic from the interface. DWRR scheduling is based on the weights configured for each queue associated with the interface. Use the **no** form of this command to remove the weight associated with the queue.

1.90.1 Syntax Description

<Q# weight>	This parameter assigns a weight, from **1** to **100**, to each queue (**0** through **7**), where each queue is represented as <*Q# weight*> (for example, queue **0** is <*Q0 weight*> and queue **7** is <*Q7 weight*>). The higher the weight assigned to the queue, the higher the priority of the queue. Each queue is assigned a weight in order (refer to the "Functional Notes" below).

1.90.2 Default Values

By default, egress traffic is scheduled using strict priority, not DWRR.

1.90.3 Privilege Level

By default, this command has a privilege level of **15**.

1.90.4 Command History

ASE Release 4.4-41	Command was introduced.

1.90.5 Functional Notes

With this command, each queue (**0** to **7**) can be assigned a weight. Each queue is configured in numerical order using this command in the format **qos wrr** *<Q0 weight> <Q1 weight> <Q2 weight> <Q3 weight> <Q4 weight> <Q5 weight> <Q6 weight> <Q7 weight>*. With this configuration you must specify the queue weights in order; you cannot configure a weight for queue **5** without first specifying weights for queues **0** through **4**.

1.90.6 Usage Examples

To configure the DWRR scheduling on the egress interface, by specifying a that queue **0** has higher priority than queues **1** or **2**, enter the command as follows:

```
(config)#interface GigabitEthernet 1/1
(config-if)#qos wrr 10 6 2
```

1.91 rmon collection

Use the **rmon collection** command to configure remote monitoring collection parameters on the interface. Use the **no** form of this command to return to the default collection settings. Variations of this command include:

```
rmon collection history <id> buckets <number>
rmon collection history <id> buckets <number> interval <interval>
rmon collection history <id> interval <interval>
rmon collection history <id> interval <interval> buckets <number>
rmon collection stats <id>
```

1.91.1 Syntax Description

history *<id>*	Specifies a collection history entry ID. Valid range is **1** to **65535**.
buckets *<number>*	Specifies the requested buckets of intervals. Valid range is **1** to **65535**.
interval *<interval>*	Specifies the interval at which to sample data for each bucket. Valid range is **1** to **3600** seconds.
stats *<id>*	Specifies the statistics entry ID. Valid range is **1** to **65535**.

1.91.2 Default Values

By default, remote monitoring collection uses **50** buckets and a sampling interval of **1800** seconds.

1.91.3 Privilege Level

By default, this command has a privilege level of **15**.

1.91.4 Command History

ASE Release 4.4-41	Command was introduced.

1.91.5 Usage Examples

The following example configures the remote monitoring collection rate for the history entry **100**:

```
(config)#interface GigabitEthernet 1/1
(config-if)#rmon collection history 100 buckets 75 interval 120
```

1.92 sflow

Use the **sflow** command to enable and configure the Sflow parameters on the interface. Use the **no** form of this command to disable Sflow functionality. Variations of this command include:

```
sflow
sflow counter-poll-interval <interval>
sflow max-sampling-size <size>
sflow sampling-rate <rate>
```

1.92.1 Syntax Description

counter-poll-interval *<interval>*	Optional. Configures the interval between counter poll samples. Valid range is **1** to **3600** seconds.
max-sampling-size *<size>*	Optional. Specifies the maximum number of bytes to transmit per flow sample. Valid range is **14** to **200** bytes.
sampling-rate *<rate>*	Optional. Specifies the statistical sampling rate. Valid range is **1** to **4294967295**.

1.92.2 Default Values

By default, the Sflow feature is disabled.

1.92.3 Privilege Level

By default, this command has a privilege level of **15**.

1.92.4 Command History

ASE Release 4.4-41	Command was introduced.

1.92.5 Functional Notes

When configuring the maximum sample size, the maximum size should be set roughly 100 bytes larger than the maximum supported packet header size allowed on the interface. This allows any size frame to be accommodated in the Sflow sample.

The sample rate is specified as N to sample 1/Nth of the packets in monitored flows. There are no restrictions on the sample rate value, but the ASE device will adjust it to the closes possible sampling rate.

1.92.6 Usage Examples

The following example enables Sflow on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#sflow
```

1.93 shutdown

Use the **shutdown** command to disable the interface. Use the **no** form of this command to enable the interface.

1.93.1 Syntax Description

No subcommands.

1.93.2 Default Values

Interfaces are enabled by default.

1.93.3 Privilege Level

By default, this command has a privilege level of **15**.

1.93.4 Command History

ASE Release 4.4-41	Command was introduced.

1.93.5 Usage Examples

The following example disables the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#shutdown
```

1.94 spanning-tree

Use the **spanning-tree** command to enable and configure various Spanning Tree Protocol (STP) parameters on the interface. Use the **no** form of this command to disable spanning tree features, or return specific parameters to the default settings. Variations of this command include:

```
spanning-tree
spanning-tree auto-edge
spanning-tree bpdu-guard
spanning-tree edge
spanning-tree link-type auto
spanning-tree link-type point-to-point
spanning-tree link-type shared
spanning-tree restricted-role
spanning-tree restricted-tcn
```

1.94.1 Syntax Description

auto-edge	Specifies that spanning tree automatically determines if the interface is an edge port.
bpdu-guard	Enables Bridge Protocol Data Unit (BPDU) guarding on the interface.
edge	Specifies that the interface is an edge port, no matter what spanning tree may automatically detect.
link-type	Configures the link type between connected ports used by spanning tree.
auto	Specifies that the switch automatically determines the link type based on the interface's duplex mode (full-duplex interfaces are treated as point-to-point connected interfaces, and half-duplex interfaces are treated as shared connection interfaces).
point-to-point	Specifies the interface are linked through a point-to-point connection.
shared	Specifies the interfaces are linked through a shared connection.
restricted-role	Restricts the spanning tree role of the interface.
restricted-tcn	Disables topology change notification (TCN) messages on the interface.

1.94.2 Default Values

By default, STP is disabled. When STP is enabled, the **auto-edge** parameter is also enabled, and the link type is set to **auto**, but all other STP features are disabled.

1.94.3 Privilege Level

By default, this command has a privilege level of **15**.

1.94.4 Command History

ASE Release 4.4-41	Command was introduced.

1.94.5 Functional Notes

When BPDU guarding is enabled, it prevents the interface from receiving BPDU messages, and causes the port to shut down if it does receive valid BPDU messages.

By default, the switch automatically determines the STP link type based on the interface's duplex mode (full-duplex interfaces are treated as point-to-point connected ports, and half-duplex interfaces are treated as shared connection ports)

When STP restricted role is enabled on the interface, it specifies that the port is not selected as the root port for the Command and Internal Spanning Tree (CIST) (or any Multiple Spanning Tree Instance (MSTI)), even if it has the lowest cost or higher priority, although it does not keep the port from being selected as an alternative once the root port has been determined. Enabling this feature can be beneficial by preventing external bridges from influencing the active topology of the spanning tree instance; however, when enabled this feature can also cause a lack of spanning tree connectivity.

When TCN restriction is enabled, the interface does not propagate TCNs to other ports in the spanning tree instance. Enabling this feature can prevent a device outside the core region of the network from causing address flushing in the core region; however, when enabled it can also cause temporary loss of connectivity if any modifications to the network topology result in perpetuating incorrect topology information from the port.

1.94.6 Usage Examples

The following example enables STP on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#spanning-tree
```

1.95 spanning-tree mst <*instance*>

Use the **spanning-tree mst** <*instance*> command to configure Multiple Spanning Tree Protocol (MSTP) and Multiple Spanning Tree instance (MSTI) port parameters on the interface. Use the **no** form of this command to return to the default settings. Variations of this command include:

```
spanning-tree mst <instance> cost <number>
spanning-tree mst <instance> cost auto
spanning-tree mst <instance> port-priority <number>
```

1.95.1 Syntax Description

mst *<instance>*	Specifies the spanning tree instance for which the port path cost is being configured. Valid range is **0** to **7**, with **0** being the Common and Internal Spanning Tree (CIST) instance, and **1** through **7** being **MSTI1** through **MSTI7**, respectively.
cost *<number>*	Defines a specific cost for the port's path. Valid path cost range is **1** to **200000000**.
cost auto	Specifies that the spanning tree protocol automatically determines the cost of the path from the port to the root bridge.
port-priority *<number>*	Specifies the priority for the port. Valid range is **0** to **240**, in multiples of **16**.

1.95.2 Default Values

By default, the MSTP port cost is determined automatically, and the port's priority is set to **128**.

1.95.3 Privilege Level

By default, this command has a privilege level of **15**.

1.95.4 Command History

ASE Release 4.4-41	Command was introduced.

1.95.5 Functional Notes

The path cost is used by MSTP to determine which port to put in a forwarding state should a loop occur in the network. Lower costs values can be assigned interfaces that should be selected by spanning tree first, and higher costs can be assigned to interfaces that should be selected last. If all ports have the same path cost, spanning tree selects the interface with the lowest number should a loop occur.

The port's priority is also used by spanning tree to determine which port to put in a forwarding state should a loop occur in the network. Higher priority is assigned to ports with a lower numerical priority value.

1.95.6 Usage Examples

The following example specifies a cost of **3500** for the MSTI **2**:

```
(config)#interface GigabitEthernet 1/1
(config-if)#spanning-tree mst 2 cost 3500
```

1.96 speed

Use the **speed** command to specify the interface speed. Use the **no** form of this command to return to the default setting. Variations of this command include:

```
speed 10
speed 100
speed 1000
speed auto
speed auto 10
speed auto 100
speed auto 1000
```

1.96.1 Syntax Description

10	Specifies the interface speed is 10 Mbps. When paired with the auto keyword, it indicates the advertised speed of the interface is 10 Mbps.
100	Specifies the interface speed is 100 Mbps. When paired with the auto keyword, it indicates the advertised speed of the interface is 100 Mbps.
1000	Specifies the interface speed is 1 Gbps. When paired with the auto keyword, it indicates the advertised speed of the interface is 1 Gbps.
auto	Specifies that the interface speed is automatically determined.

1.96.2 Default Values

By default, the interface speed is automatically determined.

1.96.3 Privilege Level

By default, this command has a privilege level of **15**.

1.96.4 Command History

ASE Release 4.4-41	Command was introduced.

1.96.5 Usage Examples

The following example specifies the interface speed is automatically determined, but that its advertised speed is **100** Mbps:

```
(config)#interface GigabitEthernet 1/1
(config-if)#speed auto 100
```

1.97 switchport access vlan <*vlan id*>

Use the **switchport access vlan** <*vlan id*> command to associate a virtual local area network (VLAN) with an access port. Use the **no** form of this command to remove the port from the VLAN.

1.97.1 Syntax Description

<vlan id>	Specifies the VLAN to associate with the access port. Valid range is **1** to **4095**.

1.97.2 Default Values

By default, the port is not associated with any VLAN.

1.97.3 Privilege Level

By default, this command has a privilege level of **13**.

1.97.4 Command History

ASE Release 4.4-41	Command was introduced.

1.97.5 Functional Notes

This command applies only to ports in **access** mode. Port modes can be configured as access, hybrid, or trunk port modes using the command “switchport mode” on page 594.

1.97.6 Usage Examples

The following example associates the access port with VLAN **100**:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport access vlan 100
```

1.98 switchport forbidden vlan

Use the switchport forbidden vlan command to specify on which virtual local area networks (VLANs) the port cannot transmit traffic. Variations of this command include:

switchport forbidden vlan add *<vlan ids>*
switchport forbidden vlan remove *<vlan ids>*

1.98.1 Syntax Description

add *<vlan ids>*	Specifies the VLANs to add to the port's forbidden list.You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.
remove *<vlan ids>*	Specifies the VLANs to remove from the port's forbidden list.You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

1.98.2 Default Values

By default, no VLANs are forbidden.

1.98.3 Privilege Level

By default, this command has a privilege level of **15**.

1.98.4 Command History

ASE Release 4.4-41	Command was introduced.

1.98.5 Functional Notes

This command can be used to specify forbidden VLANs for all three port modes: access, hybrid, and trunk port modes. Port modes are specified using the command "switchport mode" on page 594.

1.98.6 Usage Examples

The following example adds VLANs 3, 5, and 100 to the forbidden VLAN list for the access port:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport forbidden add 3,5,100
```

1.99 switchport hybrid

Use the **switchport hybrid** command to configure the virtual local area network (VLAN) settings for a port in hybrid mode. Use the **no** form of this command to return to the default VLAN settings. Variations of this command include:

```
switchport hybrid acceptable-frame-type all
switchport hybrid acceptable-frame-type tagged
switchport hybrid acceptable-frame-type untagged
switchport hybrid egress-tag all
switchport hybrid egress-tag none
switchport hybrid ingress-filtering
switchport hybrid native vlan <vlan id>
```

1.99.1 Syntax Description

acceptable-frame-type	Specifies the types of frames accepted on the port.
all	Specifies that both tagged and untagged frame types are allowed.
tagged	Specifies that only tagged ingress frames are accepted and all others are discarded.
untagged	Specifies that only untagged ingress frames are accepted and all others are discarded.
egress-tag	Specifies the VLAN tagging behavior for egress traffic.
all	Specifies that all egress traffic is transmitted with a tag, whether it is classified as part of the port's VLAN or not.
none	Specifies that all egress traffic is transmitted without a tag, whether it is classified as part of the port's VLAN or not.
ingress-filtering	Enables ingress filtering, which indicates that incoming traffic for a VLAN of which the port is not a member is discarded.
native vlan *<vlan id>*	Specifies the native VLAN for the hybrid port. Valid ID range is **1** to **4095**.

1.99.2 Default Values

- By default, hybrid ports accept all ingress frame types.
- By default, egress tagging behavior for hybrid ports is that traffic associated with the port's VLAN is transmitted untagged at egress, and any traffic not associated with the port's VLAN is transmitted with its relevant tag.
- By default, ingress filtering is disabled for hybrid ports.
- By default, the default VLAN (VLAN **1**) is the native VLAN for all ports.

1.99.3 Privilege Level

By default, this command has a privilege level of **13**.

1.99.4 Command History

ASE Release 4.4-41	Command was introduced.

1.99.5 Functional Notes

This command applies only to ports in **hybrid** mode. Port modes can be configured as access, hybrid, or trunk port modes using the command “switchport mode” on page 594.

1.99.6 Usage Examples

The following example specifies the acceptable frame type for the interface as untagged frames:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport hybrid acceptable-frame-type untagged
```

The following example specifies that all egress traffic for the interface is transmitted without a tag:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport hybrid egress-tag none
```

The following example enables ingress filtering on the interface so that ingress traffic for a VLAN of which the interface is a member is dropped:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport hybrid ingress-filtering
```

The following example specifies a native VLAN for the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport hybrid native vlan 100
```

1.100 switchport hybrid allowed vlan

Use the **switchport hybrid allowed vlan** command to specify of which virtual local area networks (VLANs) the hybrid port is allowed to become a member. Use the **no** form of this command to return to the default setting. Variations of this command include:

```
switchport hybrid allowed vlan <vlan ids>
switchport hybrid allowed vlan add <vlan ids>
switchport hybrid allowed vlan all
switchport hybrid allowed vlan except <vlan ids>
switchport hybrid allowed vlan none
switchport hybrid allowed vlan remove <vlan ids>
```

1.100.1 Syntax Description

<vlan ids>	Specifies the allowed VLANs for the port. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.
add *<vlan ids>*	Specifies the VLANs being added to the allowed VLAN list for the port. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.
all	Specifies all configured VLANs are allowed for the port.
except *<vlan ids>*	Specifies that all VLANs are allowed for the port, except for the specified VLANs. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.
none	Specifies that no VLANs are allowed for the port.
remove *<vlan ids>*	Specifies the VLANs being removed from the allowed VLAN list for the port. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

1.100.2 Default Values

By default, all ports are allowed to become members of all available VLANs.

1.100.3 Privilege Level

By default, this command has a privilege level of **13**.

1.100.4 Command History

ASE Release 4.4-41	Command was introduced.

1.100.5 Functional Notes

This command applies only to ports in **hybrid** mode. Port modes can be configured as access, hybrid, or trunk port modes using the command “switchport mode” on page 594.

1.100.6 Usage Examples

The following example specifies that all VLANs are allowed for the hybrid port except VLANs **2**, **10**, and **150**:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport hybrid allowed vlan except 2,10,150
```

1.101 switchport hybrid native vlan <*vlan id*>

Use the **switchport hybrid native vlan** <*vlan id*> command to associate the port with a non-default virtual local area network (VLAN) instance. Use the **no** form of this command to return to the default setting.

1.101.1 Syntax Description

<vlan id>	Specifies the VLAN to associate with the port. Valid range is **1** to **4095**.

1.101.2 Default Values

By default, each port is associated with the default VLAN (**VLAN 1**).

1.101.3 Privilege Level

By default, this command has a privilege level of **13**.

1.101.4 Command History

ASE Release 4.4-41	Command was introduced.

1.101.5 Usage Examples

The following example specifies that the port is associated with VLAN **130** as its native VLAN:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport hybrid native vlan 130
```

1.102 switchport hybrid port-type

Use the **switchport hybrid port-type** command to specify whether the virtual local area network (VLAN) tag protocol ID (TPID) of ingress traffic on the port is used to classify the incoming frames to a particular VLAN. Use the **no** form of this command to return to the default setting. Variations of this command include:

```
switchport hybrid port-type c-port
switchport hybrid port-type s-custom-port
switchport hybrid port-type s-port
switchport hybrid port-type unaware
```

1.102.1 Syntax Description

c-port	Specifies that all ingress frames with a VLAN tag TPID of 0x8100 are classified to the VLAN ID embedded in the tag. If a frame is untagged, or has a priority tag, the frame is classified to the VLAN associated with the port. With this setting, any egress frames that must be tagged are tagged with a C-tag.
s-custom-port	Specifies that all ingress frames with a VLAN tag TPID of 0x8100, or a value equal to the Ethertype configured for S-Custom-Ports (using the command “vlan ethertype s-custom-port <type>” on page 474), are classified to the VLAN ID embedded in the tag. If a frame is untagged, or has a priority tag, the frame is classified to the VLAN associated with the port. With this setting, any egress frames that must be tagged are tagged with the custom S-tag.
s-port	Specifies that all ingress frames with a VLAN tag TPID of 0x8100 or 0x88A8 are classified to the VLAN ID embedded in the tag. If a frame is untagged, or has a priority tag, the frame is classified to the VLAN associated with the port. With this setting, any egress frames that must be tagged are tagged with an S-tag.
unaware	Specifies that all ingress frames (whether carrying a VLAN tag or not) are classified to the VLAN associated with the port.

1.102.2 Default Values

By default, ports in hybrid mode are set to **unaware**. Ports in access or trunk mode are set to **c-port**, and cannot be changed.

1.102.3 Privilege Level

By default, this command has a privilege level of **13**.

1.102.4 Command History

ASE Release 4.4-41	Command was introduced.

1.102.5 Usage Examples

The following example configures the port type for VLAN ports in hybrid mode as **c-port**:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport hybrid port-type c-port
```

1.103 switchport mode

Use the **switchport mode** command to specify the port mode for virtual local area network (VLAN) port configuration. Use the **no** form of this command to return to the default setting. Variations of this command include:

```
switchport mode access
switchport mode hybrid
switchport mode trunk
```

1.103.1 Syntax Description

access	Specifies the port is an access port.
hybrid	Specifies the port is a hybrid port.
trunk	Specifies the port is a trunk port.

1.103.2 Default Values

By default, each port is an access port, unless otherwise specified.

1.103.3 Privilege Level

By default, this command has a privilege level of **13**.

1.103.4 Command History

ASE Release 4.4-41	Command was introduced.

1.103.5 Usage Examples

The following example configures the port as a trunk port:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport mode trunk
```

1.104 switchport trunk allowed vlan

Use the **switchport trunk allowed vlan** command to specify of which virtual local area networks (VLANs) the trunk port is allowed to become a member. Use the **no** form of this command to return to the default setting. Variations of this command include:

```
switchport trunk allowed vlan <vlan ids>
switchport trunk allowed vlan add <vlan ids>
switchport trunk allowed vlan all
switchport trunk allowed vlan except <vlan ids>
switchport trunk allowed vlan none
switchport trunk allowed vlan remove <vlan ids>
```

1.104.1 Syntax Description

<vlan ids>	Specifies the allowed VLANs for the port. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.
add *<vlan ids>*	Specifies the VLANs being added to the allowed VLAN list for the port. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.
all	Specifies all configured VLANs are allowed for the port.
except *<vlan ids>*	Specifies that all VLANs are allowed for the port, except for the specified VLANs. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.
none	Specifies that no VLANs are allowed for the port.
remove *<vlan ids>*	Specifies the VLANs being removed from the allowed VLAN list for the port. You can enter a single VLAN ID, or several IDs separated by commas, or a range of IDs separated by a hyphen. Valid range is **1** to **4095**.

1.104.2 Default Values

By default, all ports are allowed to become members of all available VLANs.

1.104.3 Privilege Level

By default, this command has a privilege level of **13**.

1.104.4 Command History

ASE Release 4.4-41	Command was introduced.

1.104.5 Functional Notes

This command applies only to ports in **trunk** mode. Port modes can be configured as access, hybrid, or trunk port modes using the command “switchport mode” on page 594.

1.104.6 Usage Examples

The following example specifies that all VLANs are allowed for the trunk port except VLANs **2**, **10**, and **150**:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport trunk allowed vlan except 2,10,150
```

1.105 switchport trunk native vlan <*vlan id*>

Use the **switchport trunk native vlan** <*vlan id*> command to associate the port with a non-default virtual local area network (VLAN) instance. Use the **no** form of this command to return to the default setting.

1.105.1 Syntax Description

<vlan id>	Specifies the VLAN to associate with the port. Valid range is **1** to **4095**.

1.105.2 Default Values

By default, each port is associated with the default VLAN (**VLAN 1**).

1.105.3 Privilege Level

By default, this command has a privilege level of **13**.

1.105.4 Command History

ASE Release 4.4-41	Command was introduced.

1.105.5 Usage Examples

The following example specifies that the port is associated with VLAN **130** as its native VLAN:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport trunk native vlan 130
```

1.106 switchport trunk vlan tag native

Use the **switchport trunk vlan tag native** command to change the virtual local area network (VLAN) tagging behavior of egress traffic on the port. This command specifies that traffic classified as part of the port's VLAN is tagged upon egress, in addition to the traffic that is already tagged because it is not part of the port's VLAN. In effect, all traffic is tagged upon egress when this command is issued. Use the **no** form of this command to return to the default setting.

1.106.1 Syntax Description

No subcommands.

1.106.2 Default Values

By default, only traffic not associated with the port VLAN is tagged upon egress.

1.106.3 Privilege Level

By default, this command has a privilege level of **13**.

1.106.4 Command History

ASE Release 4.4-41	Command was introduced.

1.106.5 Usage Examples

The following example specifies that traffic associated with the port's VLAN is tagged upon egress:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport trunk vlan tag native
```

1.107 switchport vlan ip-subnet *<ipv4 address> <subnet mask>* vlan *<vlan id>*

Use the **switchport vlan ip-subnet** *<ipv4 address> <subnet mask>* command to configure a source Internet Protocol version 4 (IPv4) address for virtual local area network (VLAN) control list (VCL) parameters on the interface. Use the **no** form of this command to remove address from the VCL configuration.

1.107.1 Syntax Description

<ipv4 address>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**).
vlan *<vlan id>*	Specifies the VLAN to which the IPv4 address is mapped. Valid range is **1** to **4095**.

1.107.2 Default Values

By default, no VCL configurations exist.

1.107.3 Privilege Level

By default, this command has a privilege level of **13**.

1.107.4 Command History

ASE Release 4.4-41	Command was introduced.

1.107.5 Usage Examples

The following example specifies the source IPv4 address **192.22.72.101 255.255.255.252** is used for VCL operations on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport vlan ip-subnet 192.22.72.101/255.255.255.252 vlan
   200
```

1.108 switchport vlan mac <*mac address*> vlan <*vlan id*>

Use the **switchport vlan mac** <*mac address*> **vlan** <*vlan id*> command to configure mapping for a specific unicast Media Access Control (MAC) address to a specific virtual local area network (VLAN) instance on the interface. Use the **no** form of this command to remove the MAC address-to-VLAN instance mapping.

1.108.1 Syntax Description

<mac address>	Specifies a unicast MAC address to map to the VLAN instance. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
<vlan id>	Specifies the VLAN to which the MAC address is mapped. Valid range is **1** to **4095**.

1.108.2 Default Values

By default, no MAC address-to-VLAN instance mapping is configured.

1.108.3 Privilege Level

By default, this command has a privilege level of **13**.

1.108.4 Command History

ASE Release 4.4-41	Command was introduced.

1.108.5 Usage Examples

The following example configures the MAC address **00:A0:C8:00:00:01** to be mapped to VLAN **175**:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport vlan mac 00:A0:C8:00:00:01 vlan 175
```

1.109 switchport vlan mapping <*group id*>

Use the **switchport vlan mapping** <*group id*> command to map a virtual local area network (VLAN) instance to a particular group on the interface. Use the **no** form of this command to remove the mapping configuration.

1.109.1 Syntax Description

<group id>	Specifies the group to which the VLAN is mapped. Valid range is **1** to **10**.

1.109.2 Default Values

By default, no VLAN mapping is configured.

1.109.3 Privilege Level

By default, this command has a privilege level of **13**.

1.109.4 Command History

ASE Release 4.4-41	Command was introduced.

1.109.5 Usage Examples

The following example specifies that the VLAN associated with the interface is mapped to group **4**:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport vlan mapping 4
```

1.110 switchport vlan protocol group <*name*> vlan <*vlan id*>

Use the **switchport vlan protocol group** <*name*> **vlan** <*vlan id*> command to associate a protocol group with a specific virtual local area network (VLAN) instance on the interface. Use the **no** form of this command to remove the group-to-VLAN mapping configuration.

1.110.1 Syntax Description

<name>	Specifies the protocol group to map to the VLAN instance. Valid group names are **1** to **16** characters in length.
<vlan id>	Specifies the VLAN to which the group is mapped. Valid range is **1** to **4095**.

1.110.2 Default Values

By default, no protocol groups are configured or mapped to VLAN instances.

1.110.3 Privilege Level

By default, this command has a privilege level of **13**.

1.110.4 Command History

ASE Release 4.4-41	Command was introduced.

1.110.5 Usage Examples

The following example maps the protocol group **GROUP1** to VLAN **175**:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport vlan protocol group GROUP1 vlan 175
```

1.111 switchport voice vlan

Use the **switchport voice vlan** command to configure voice virtual local area network (VLAN) parameters on the interface. Use the **no** form of this command to return to the default voice VLAN settings. Variations of this command include:

```
switchport voice vlan discovery-protocol both
switchport voice vlan discovery-protocol lldp
switchport voice vlan discovery-protocol oui
switchport voice vlan mode auto
switchport voice vlan mode disable
switchport voice vlan mode force
switchport voice vlan security
```

1.111.1 Syntax Description

discovery-protocol	Specifies the protocol used to discover Voice over IP (VoIP) devices connected to the interface.
both	Specifies that both Link Layer Discovery Protocol (LLDP) and the device's Object Unique Identifier (OUI) are used to discover VoIP devices.
lldp	Specifies that only LLDP is used to discover VoIP devices.
oui	Specifies that only the OUI is used to discover VoIP devices.
mode	Specifies how the port behaves when VoIP devices are connected.
auto	Specifies that when VoIP devices connect to the port, they are automatically detected and the port automatically joins the voice VLAN.
disable	Specifies that the port is not a member of the voice VLAN and does not automatically detect VoIP devices.
force	Specifies that the port is forced to join the voice VLAN, regardless of connected devices or voice traffic.
security	Enables port security for voice VLANs on the interface.

1.111.2 Default Values

By default, the interface voice VLAN mode is disabled, the device's OUI is used to discover connected VoIP devices, and port security is enabled.

1.111.3 Privilege Level

By default, this command has a privilege level of **15**.

1.111.4 Command History

ASE Release 4.4-41	Command was introduced.

1.111.5 Usage Examples

The following example specifies that LLDP is used to discover VoIP devices on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#switchport voice vlan discovery-protocol lldp
```

1.112 thermal-protect grp <*group id*>

Use the **thermal-protect grp** <*group id*> command to enable thermal protection and configure a thermal protection group for the interface. Use the **no** form of this command to remove the group from the interface's configuration.

1.112.1 Syntax Description

<group id>	Specifies the thermal protection group ID. Valid range is **0** to **3**.

1.112.2 Default Values

By default, thermal protection is disabled and no thermal protection groups are configured.

1.112.3 Privilege Level

By default, this command has a privilege level of **15**.

1.112.4 Command History

ASE Release 4.4-41	Command was introduced.

1.112.5 Usage Examples

The following example enables thermal protection and creates thermal protection group **2** on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#thermal-protect grp 2
```

1.113 udld port

Use the **udld port** command to enable Unidirectional Link Detection (UDLD) on the interface and to configure various UDLD parameters. Use the **no** form of this command to disable the UDLD feature. Variations of this command include:

```
udld port
udld port aggressive
udld port aggressive message time-interval <interval>
udld port message time-interval <interval>
udld port message time-interval <interval> aggressive
```

1.113.1 Syntax Description

aggressive	Optional. Specifies that UDLD operates in aggressive mode.
message time-interval *<interval>*	Optional. Specifies the period of time between UDLD probe messages on ports that are in the advertisement phase of UDLD operation and are determined to be bidirectional. Valid range is **7** to **90** seconds.

1.113.2 Default Values

By default, UDLD is disabled. When enabled, UDLD probe messages are sent every **7** seconds.

1.113.3 Command History

ASE Release 4.4-41	Command was introduced.

1.113.4 Usage Examples

The following example enables UDLD in aggressive mode on the interface:

```
(config)#interface GigabitEthernet 1/1
(config-if)#udld port
```

2 Line Interface Command Set

2.1 Scope of this Section

This section outlines the commands available to configure the Line interface on the ADTRAN Switch Engine (ASE). The Line Terminal Interface command set allows you to configure the terminal connection parameters for the ASE device.

2.2 Accessing the Line Interface Configuration Mode

The Line interface is accessed using the **line** command from the Global Configuration mode prompt. This command enters the line's configuration mode. To enter the line's configuration mode, enter the command as follows:

```
#configure terminal
(config)#line 5
(config-line)#
```

2.3 Common Commands

The commands listed in Table 2-1 are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the section listed below:

Table 2-1. Common Commands

Sub-Section	Command	See Page …
1.4	do	19
1.5	end	20
1.6	exit	21
1.7	help	22

2.4 Line Interface Configuration Commands

Table 2-2 lists the commands available from the Line interface configuration mode.

Table 2-2. Line Interface Configuration Commands

Sub-Section	Command	See Page …
2.5	editing	609
2.6	exec-banner	610
2.7	exec-timeout <minutes> <seconds>	611
2.8	history size <size>	612
2.9	length <number>	613
2.10	location <description>	614

Table 2-2. Line Interface Configuration Commands (Continued)

Sub-Section	Command	See Page …
2.11	motd-banner	615
2.12	privilege level <level>	616
2.13	width <number>	617

2.5 editing

Use the **editing** command to enable command line editing for the specified line. Use the **no** form of this command to disable line editing.

2.5.1 Syntax Description

No subcommands.

2.5.2 Default Values

By default, line editing is disabled.

2.5.3 Command History

ASE Release 4.4-41	Command was introduced.

2.5.4 Usage Examples

The following example enables line editing for line **5**:

```
(config)#line 5
(config-line)#editing
```

2.6 exec-banner

Use the **exec-banner** command to enable the display of the executive banner on the line. Use the **no** form of this command to disable the banner display.

2.6.1 Syntax Description

No subcommands.

2.6.2 Default Values

By default, the executive banner is not displayed.

2.6.3 Command History

ASE Release 4.4-41	Command was introduced.

2.6.4 Usage Example

The following example enables the executive banner display on line 5:

```
(config)#line 5
(config-line)#exec-banner
```

2.7 exec-timeout <*minutes*> <*seconds*>

Use the **exec-timeout** <*minutes*> <*seconds*> command to specify the executive timeout for the line. Use the **no** form of this command to remove the timeout value.

2.7.1 Syntax Description

<minutes>	Specifies the executive timeout in minutes. Valid range is **0** to **1440** minutes.
<seconds>	Specifies the executive timeout in seconds. Valid range is **0** to **3660** seconds.

2.7.2 Default Values

By default, the executive timeout is not configured.

2.7.3 Command History

ASE Release 4.4-41	Command was introduced.

2.7.4 Usage Examples

The following example specifies an executive timeout of **5** minutes and **30** seconds for line **5**:

```
(config)#line 5
(config-line)#exec-timeout 5 30
```

2.8 history size <*size*>

Use the **history size** <*size*> command to specify the number of commands stored in the history buffer for the line. Use the **no** form of this command to return to the default setting.

2.8.1 Syntax Description

<size>	Specifies the number of commands stored in the history buffer. Valid range is **0** to **32**. When set to **0**, the history buffer is disabled.

2.8.2 Default Values

By default, the history buffer stores **0** commands.

2.8.3 Command History

ASE Release 4.4-41	Command was introduced.

2.8.4 Usage Examples

The following example specifies that **20** commands are stored in the history buffer for line **5**:

```
(config)#line 5
(config-line)#history size 20
```

2.9 length <*number*>

Use the **length** <*number*> command to specify how many lines are displayed in the terminal screen. Use the **no** form of this command to disable this setting.

2.9.1 Syntax Description

<*number*>	Specifies the number of lines displayed on the terminal screen. Valid range is 3 to 512. Entering a value of 0 indicates there is no pausing in lines displayed.

2.9.2 Default Values

By default, a length is not specified.

2.9.3 Command History

ASE Release 4.4-41	Command was introduced.

2.9.4 Usage Examples

The following example specifies a length of **40** lines for the display associated with line **5**:

```
(config)#line 5
(config-line)#length 40
```

2.10 location <*description*>

Use the **location** <*description*> command to specify a description for the terminal line location. Use the **no** form of this command to remove the specified description. Variations of this command include:

```
location <description>
location <description> <description>
location <description> <description> <description>
```

2.10.1 Syntax Description

<description>	Specifies a description of the terminal line location using an alphanumeric string (up to **32** characters in length). You can optionally specify up to **3** descriptions for a single location.

2.10.2 Default Values

By default, no location description is specified.

2.10.3 Command History

ASE Release 4.4-41	Command was introduced.

2.10.4 Usage Examples

The following example specifies a location description for line **5**:

```
(config)#line 5
(config-line)#location REMOTEOFFICE 6THFLOOR
```

2.11 motd-banner

Use the **motd-banner** command to enable the message-of-the-day banner on the line. Use the **no** form of this command to disable the banner display.

2.11.1 Syntax Description

No subcommands.

2.11.2 Default Values

By default, the message-of-the-day banner is disabled.

2.11.3 Command History

ASE Release 4.4-41	Command was introduced.

2.11.4 Usage Examples

The following example enables the message-of-the-day banner display on line **5**:

```
(config)#line 5
(config-line)#motd-banner
```

2.12 privilege level <*level*>

Use the **privilege level** <*level*> command to specify the default privilege level for the line. Use the **no** form of this command to remove the privilege level.

2.12.1 Syntax Description

<level>	Specifies the privilege level to be applied to the line. Valid range is **0** to **15**, with **15** being administrator privilege level.

2.12.2 Default Values

By default, a privilege level is not set for the line.

2.12.3 Command History

ASE Release 4.4-41	Command was introduced.

2.12.4 Usage Examples

The following example specifies a privilege level of **7** for line **5**:

```
(config)#line 5
(config-line)#privilege level 7
```

2.13 width <*number*>

Use the **width** <*number*> command to specify the width of the display terminal for the line. Use the **no** form of this command to remove the width configuration.

2.13.1 Syntax Description

<*number*>	Specifies the number of characters allowed in the display width. Valid range is **40** to **512** characters. Setting this value to **0** specifies an unlimited width for the display screen.

2.13.2 Default Values

By default, the display width is not limited.

2.13.3 Command History

ASE Release 4.4-41	Command was introduced.

2.13.4 Usage Examples

The following example specifies a display width of **100** characters for line **5**:

```
(config)#line 5
(config-line)#width 100
```

3 Local Link Aggregation Interface Command Set

3.1 Scope of this Section

This section outlines the commands available from the Local Link Aggregation (LLAG) interface configuration mode on the ADTRAN Switch Engine (ASE) device. In this command mode, you can manage the configuration of Link Aggregation Control Protocol (LACP) on a per-port basis.

3.2 Accessing the Interface Configuration Mode

To activate the LLAG Interface Configuration mode, enter the **interface llag** *<group id>* command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface llag 3
(config-llag)#
```

3.3 Common Commands

The commands listed in Table 3-1 are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the section listed below:

Table 3-1. Common Commands

Sub-Section	Command	See Page …
1.4	do	19
1.5	end	20
1.6	exit	21
1.7	help	22

3.4 LLAG Interface Configuration Commands

Table 3-2 lists the commands available from the LLAG interface.

Table 3-2. LLAG Interface Commands

Sub-Section	Command	See Page …
3.5	lacp failover	619
3.6	lacp max-bundle <value>	620

3.5 lacp failover

Use the **lacp failover** command to enable revertive mode for a Link Aggregation Control Protocol (LACP) group. Use the **no** form of this command to return to the default value. Variations of this command include:

```
lacp failover non-revertive
lacp failover revertive
```

3.5.1 Syntax Description

non-revertive	Specifies the LACP group cannot switch between links should a better link become available or if a currently used link becomes unavailable.
revertive	Specifies the LACP group can switch between links should a better link become available or if a currently used link becomes unavailable.

3.5.2 Default Values

By default, LACP groups have revertive mode enabled.

3.5.3 Command History

ASE Release 4.4-41	Command was introduced.

3.5.4 Usage Examples

The following example disables revertive mode for LACP group 3:

```
(config)#interface llag 3
(config-llag)#lacp failover non-revertive
```

3.6 lacp max-bundle <*value*>

Use the **lacp max-bundle** <*value*> command to specify the maximum number of bundles supported in the Link Aggregation Control Protocol (LACP) group. Use the **no** form of this command to return to the default setting.

3.6.1 Syntax Description

<value>	Specifies the maximum number of bundles supported by the LACP group. Valid range is determined by the number of LACP groups available on the ASE device. For example, if **5** LACP groups are available, the maximum bundle is **10**.

3.6.2 Default Value

By default, the number of LACP groups available on the ASE device is determined by the number of ports supported on the device divided by two. For example, if the ASE device has 48 ports, then 24 LACP groups are supported.

3.6.3 Command History

ASE Release 4.4-41	Command was introduced.

3.6.4 Functional Notes

The number of members allowed in an LACP group can be restricted by setting the maximum bundle to a number less than the number of group members. Additional members of the group become standby ports and do not forward any frames, unless an active member of the group becomes disabled, in which case the standby member of the highest priority becomes active and takes over frame transmission (as long as the group has revertive mode enabled using the command “lacp failover” on page 619).

You can achieve one to one active and standby behavior on a LACP group by creating a single group with two associated ports, and specifying the **max-bundle** value as **1**. In this case, the LACP group port with the higher priority actively forwards traffic, while the lower priority port is in standby mode. If the active port goes down for any reason, the standby port takes over and begins forwarding traffic. For this to function correctly, the LACP group must have revertive mode enabled (using the command “lacp failover” on page 619).

3.6.5 Usage Examples

The following example configures the maximum number of members allowed in the LACP group as **3**:

```
(config)#interface llag 3
(config-llag)#lacp max-bundle 3
```

4 VLAN Interface Command Set

4.1 Scope of this Section

This section outlines the commands available from the Virtual Local Area Network (VLAN) interface configuration mode on the ADTRAN Switch Engine (ASE) device. In this command mode, you can configure the Internet Protocol parameters for ports within the specified VLAN.

4.2 Accessing the Interface Configuration Mode

To activate the VLAN Interface Configuration mode, enter the **interface vlan** <*vlan id*> command at the Global Configuration mode prompt. For example:

```
>enable
#configure terminal
(config)#interface vlan 5
(config-if-vlan)#
```

4.3 Common Commands

The commands listed in Table 4-1 are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the section listed below:

Table 4-1. Common Commands

Sub-Section	Command	See Page …
1.4	do	19
1.5	end	20
1.6	exit	21
1.7	help	22

4.4 VLAN Interface Configuration Commands

Table 4-2 lists the commands available from the VLAN interface.

Table 4-2. VLAN Interface Commands

Sub-Section	Command	See Page …
4.5	ip address <ipv4 address> <subnet mask>	622
4.6	ip address dhcp	623
4.7	ip dhcp server	626
4.8	ip igmp snooping	627
4.9	ipv6 address <ipv6 address/prefix-length>	629
4.10	ipv6 address dhcp	630
4.11	ipv6 mld snooping	631

4.5 ip address *<ipv4 address> <subnet mask>*

Use the **ip address** command to define an Internet Protocol version 4 (IPv4) address on the specified interface (only one primary address is allowed). Use the **no** form of this command to remove a configured IPv4 address.

4.5.1 Syntax Description

<ipv4 address>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**).

4.5.2 Default Values

By default, no IP addresses are assigned.

4.5.3 Privilege Level

By default, this command has a privilege level of **15**.

4.5.4 Command History

ASE Release 4.4-41	Command was introduced.

4.5.5 Usage Examples

The following example configures an IPv4 address of **192.22.72.101 255.255.255.252**:

```
(config)#interface vlan 5
(config-if-vlan)#ip address 192.22.72.101 255.255.255.252
```

4.6 ip address dhcp

Use the **ip address dhcp** command to use Dynamic Host Configuration Protocol (DHCP) to obtain an address on the interface. Use the **no** form of this command to remove a configured IP address (using DHCP) and disable DHCP operation on the interface. Variables that may be used with this command to further define the DHCP configuration include:

```
ip address dhcp
ip address dhcp client-id [<interface> | ascii <string> | hex <string>]
ip address dhcp client-id [<interface> | ascii <string> | hex <string>] fallback
    <ipv4 address> <subnet mask>
ip address dhcp client-id [<interface> | ascii <string> | hex <string>] fallback
    <ipv4 address> <subnet mask> hostname <string>
ip address dhcp client-id [<interface> | ascii <string> | hex <string>] fallback
    <ipv4 address> <subnet mask> timeout <value>
ip address dhcp client-id [<interface> | ascii <string> | hex <string>] fallback
    <ipv4 address> <subnet mask> timeout <value> hostname <string>

ip address dhcp fallback <ipv4 address> <subnet mask>
ip address dhcp fallback <ipv4 address> <subnet mask> client-id [<interface> | ascii
    <string> | hex <string>]
ip address dhcp fallback <ipv4 address> <subnet mask> client-id [<interface> | ascii
    <string> | hex <string>] hostname <string>
ip address dhcp fallback <ipv4 address> <subnet mask> hostname <string> client-id
    [<interface> | ascii <string> | hex <string>]
ip address dhcp fallback <ipv4 address> <subnet mask> timeout <value>
ip address dhcp fallback <ipv4 address> <subnet mask> timeout <value> client-id
    [<interface> | ascii <string> | hex <string>]
ip address dhcp fallback <ipv4 address> <subnet mask> timeout <value> client-id
    [<interface> | ascii <string> | hex <string>] hostname <string>
ip address dhcp fallback <ipv4 address> <subnet mask> timeout <value> hostname
    <string>
ip address dhcp fallback <ipv4 address> <subnet mask> timeout <value> hostname
    <string> client-id [<interface> | ascii <string> | hex <string>]

ip address dhcp hostname <string>
ip address dhcp hostname <string> client-id [<interface> | ascii <string> | hex
    <string>]
ip address dhcp hostname <string> client-id [<interface> | ascii <string> | hex
    <string>] fallback <ipv4 address> <subnet mask>
ip address dhcp hostname <string> client-id [<interface> | ascii <string> | hex
    <string>] fallback <ipv4 address> <subnet mask> timeout <value>
```

4.6.1 Syntax Description

client-id — Optional. Specifies the client identifier used when obtaining an IP address from a DHCP server.

<interface> — Specifies an interface, thus defining the client identifier as the hexadecimal medium access control (MAC) address of the specified interface (including a hexadecimal number added to the front of the MAC address to identify the media type).

For example, specifying the **client-id GigabitEthernet 1/1** (where the GigabitEthernet interface has a MAC address of d217.0491.1150) defines the client identifier as **01:d2:17:04:91:11:50**.

ascii *<string>*	Specifies a custom client identifier using a text string. Text strings are limited to 32 characters in length.
hex *<string>*	Specifies a custom client identifier using a hexadecimal string. Hexadecimal strings are limited to 64 characters and should be entered in the format **0f:ff:ff:ff:ff:51:04:99:a1**.
fallback	Specifies the DHCP fallback address.
<ipv4 address>	Specifies the fallback IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the fallback IPv4 address subnet mask. Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**).
timeout *<value>*	Optional. Specifies the DHCP fallback timeout value. Valid range is **0** to **4294967295** seconds; default value is **60** seconds.
hostname *<name>*	Specifies a domain name (to override the global router name) to use as the name in the DHCP option 12 field. A valid name consist of a sequence of domain labels separated by '.', each name starting and ending with an alphanumeric character and possibly also containing '-' characters. The length of a name must be 63 characters or less.

4.6.2 Default Values

By default, the host name is the name configured using the Global Configuration **hostname** command and the DHCP fallback timeout is set to **60** seconds.

4.6.3 Privilege Level

By default, this command has a privilege level of **15**.

4.6.4 Command History

ASE Release 4.4-41	Command was introduced.

4.6.5 Functional Notes

DHCP allows interfaces to acquire a dynamically assigned IP address from a configured DHCP server on the network. Many service providers require the use of DHCP when connecting to their services. Using DHCP reduces the number of dedicated IP addresses the ISP must obtain. Consult your ISP to determine the proper values for the **client-id** and **hostname** fields.

In addition, with this command, you can enter the **client-id**, **fallback**, and **hostname** parameters in any order.

4.6.6 Usage Examples

The following example specifies the DHCP fallback time of **100** seconds for IP address **192.22.72.101 255.255.255.252**:

```
(config)#interface vlan 5
(config-if-vlan)#ip address dchp fallback 192.22.72.101 255.255.255.252 timeout 100
```

4.7 ip dhcp server

Use the **ip dhcp server** command to enable Dynamic Host Control Protocol (DHCP) on the interface, and allow the interface to receive IP addresses from the DHCP server. Use the **no** form of this command to disable DHCP on the interface.

4.7.1 Syntax Description

No subcommands.

4.7.2 Default Values

By default, DHCP is disabled on the interface.

4.7.3 Privilege Level

By default, this command has a privilege level of **13**.

4.7.4 Command History

ASE Release 4.4-41	Command was introduced.

4.7.5 Usage Examples

The following example enables DHCP on the interface:

```
(config)#interface vlan 5
(config-if-vlan)#ip dhcp server
```

4.8 ip igmp snooping

Use the **ip igmp snooping** command to enable and configure Internet Group Management Protocol (IGMP) parameters on the interface. Use the **no** form of this command to disable IGMP on the interface. Variables that may be used with this command to further define the IGMP configuration include:

```
ip igmp snooping
ip igmp snooping compatibility [auto | v1 | v2 | v3]
ip igmp snooping last-member-query-interval <time>
ip igmp snooping priority <value>
ip igmp snooping querier address <ipv4 address>
ip igmp snooping query-interval <time>
ip igmp snooping query-max-response-time <time>
ip igmp snooping robustness-variable <number>
ip igmp snooping unsolicited-report-interval <time>
```

4.8.1 Syntax Description

compatibility	Optional. Specifies the IGMP version compatible with the interface.
auto	Specifies the interface is compatible with IGMP version 1, 2, and 3.
v1	Specifies the interface is only compatible with IGMP version 1.
v2	Specifies the interface is only compatible with IGMP version 2.
v3	Specifies the interface is only compatible with IGMP version 3.
last-member-query-interval *<time>*	Optional. Specifies the last member query interval. Valid range is **0** to **31744** in tenths of seconds.
priority *<value>*	Optional. Specifies the interface class of service (CoS) priority. Valid range is **0** to **7**.
querier	Optional. Configures the IGMP Querier.
address *<ipv4 address>*	Specifies a unicast IPv4 address for the IGMP querier. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
query-interval *<time>*	Optional. Specifies the query interval in seconds. Valid range is **1** to **31744** seconds.
query-max-response-time *<time>*	Optional. Specifies the query response interval. Valid range is **0** to **31744** tenths of a second.
robustness-variable *<number>*	Optional. Specifies the packet loss tolerance count. Valid range is **1** to **255**.
unsolicited-report-interval *<time>*	Optional. Specifies the unsolicited report interval in seconds. Valid range is **0** to **31744** seconds.

4.8.2 Default Values

By default, IGMP is disabled on the interface.

4.8.3 Privilege Level

By default, this command has a privilege level of **15**.

4.8.4 Command History

ASE Release 4.4-41	Command was introduced.

4.8.5 Usage Examples

The following example enables IGMP on the interface:

```
(config)#interface vlan 5
(config-if-vlan)#ip igmp snooping
```

4.9 ipv6 address *<ipv6 address/prefix-length>*

Use the **ipv6 address** command to assign a unicast Internet Protocol version 6 (IPv6) address to the interface and enable IPv6 processing on the interface. Use the **no** form of this command to remove the IPv6 address from the interface.

4.9.1 Syntax Description

<ipv6 address/prefix-length>	Specifies the IPv6 unicast address to add to the interface. IPv6 prefixes should be expressed in colon hexadecimal format (**X:X::X/<Z>**). For example, **2001:DB8:3F::/64**. The prefix length (**<Z>**) is an integer with a value between **0** and **128**.

4.9.2 Default Values

By default, no IPv6 address is configured on the interface and IPv6 processing is not enabled on the interface.

4.9.3 Command History

ASE Release 4.4-41	Command was introduced.

4.9.4 Functional Notes

The IPv6 unicast address can be a global unicast address or a unique local address, but it cannot be a link-local IPv6 address (**FE80::**).

The address created by this command is a manually configured IPv6 address, which must have all parts (prefix and host bits) specified.

Using the **no** form of this command with a specified IPv6 address removes only that IPv6 address from the interface. Using the **no** form of this command without a specified IPv6 address removes all manually configured IPv6 addresses from the interface.

4.9.5 Usage Examples

The following example adds a unicast IPv6 address to the interface and enables IPv6 processing on the interface:

```
(config)#interface vlan 5
(config-if-vlan)#ipv6 address 2001:DB8::/32
```

4.10 ipv6 address dhcp

Use the **ipv6 address dhcp** command to enable Dynamic Host Control Protocol for Internet Protocol version 6 (DHCPv6) on the interface, place the interface in DHCPv6 client mode, and configure the address parameters of the DHCPv6 client. Use the **no** form of this command to disable the DHCPv6 client on the interface. Variations of this command include:

```
ipv6 address dhcp
ipv6 address dhcp rapid-commit
```

4.10.1 Syntax Description

rapid-commit	Optional. Allows the client to request the use of a two message DHCPv6 address exchange instead of the normal four message exchange. This option should not be used if more than one DHCPv6 server is available to clients on the network being served.

4.10.2 Default Values

By default, DHCPv6 client mode is not enabled on the interface.

4.10.3 Usage Examples

The following example enables DHCPv6 on the interface:

```
(config)#interface vlan 5
(config-if-vlan)#ipv6 address dhcp
```

4.11 ipv6 mld snooping

Use the **ipv6 mld snooping** command to enable and configure Internet Protocol version 6 (IPv6) Multicast Listener Discovery (MLD) parameters on the interface. Use the **no** form of this command to disable MLD on the interface. Variables that may be used with this command to further define the MLD configuration include:

```
ipv6 mld snooping
ipv6 mld snooping compatibility [auto | v1 | v2]
ipv6 mld snooping last-member-query-interval <time>
ipv6 mld snooping priority <value>
ipv6 mld snooping querier election
ipv6 mld snooping query-interval <time>
ipv6 mld snooping query-max-response-time <time>
ipv6 mld snooping robustness-variable <number>
ipv6 mld snooping unsolicited-report-interval <time>
```

4.11.1 Syntax Description

compatibility	Optional. Specifies the MLD version compatible with the interface.
auto	Specifies the interface is compatible with MLD version 1, 2, and 3.
v1	Specifies the interface is only compatible with MLD version 1.
v2	Specifies the interface is only compatible with MLD version 2.
last-member-query-interval *<time>*	Optional. Specifies the last member query interval. Valid range is **0** to **31744** in tenths of seconds.
priority *<value>*	Optional. Specifies the interface class of service (CoS) priority. Valid range is **0** to **7**.
querier election	Optional. Specifies that the interface acts an MLD querier and joins the querier elections.
query-interval *<time>*	Optional. Specifies the query interval in seconds. Valid range is **1** to **31744** seconds.
query-max-response-time *<time>*	Optional. Specifies the query response interval. Valid range is **0** to **31744** tenths of a second.
robustness-variable *<number>*	Optional. Specifies the packet loss tolerance count. Valid range is **1** to **255**.
unsolicited-report-interval *<time>*	Optional. Specifies the unsolicited report interval in seconds. Valid range is **0** to **31744** seconds.

4.11.2 Default Values

By default, MLD is disabled on the interface.

4.11.3 Privilege Level

By default, this command has a privilege level of **15**.

4.11.4 Command History

ASE Release 4.4-41	Command was introduced.

4.11.5 Usage Examples

The following example enables MLD on the interface:

```
(config)#interface vlan 5
(config-if-vlan)#ipv6 mld snooping
```

ASE Command Reference Guide

Volume 3: Protocol and Services Command Sets

1 DHCPv4 Server Pool Command Set

1.1 Scope of this Section

This section outlines the commands available to configure the Internet Protocol version 4 (IPv4) Dynamic Host Control Protocol (DHCPv4) server pool on the ADTRAN Switch Engine (ASE). The server pool is used to define the information to be assigned to clients by the DHCPv4 server. The pool chosen to serve a specific client's request is determined by the current pool selection algorithm.

1.2 Accessing the DHCP Server Pool Configuration Mode

The DHCPv4 server pool is created using the **ip dhcp pool** command from the Global Configuration mode prompt. This command creates the DHCPv4 server pool and enters the pool's configuration mode. To create a DHCPv4 server pool, and enter the pool's configuration mode, enter the command as follows:

```
#configure terminal
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#
```

1.3 Common Commands

The commands listed in Table 1-1 are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the section listed below:

Table 1-1. Common Commands

Sub-Section	Command	See Page …
1.4	do	19
1.5	end	20
1.6	exit	21
1.7	help	22

1.4 DHCPv4 Server Pool Configuration Commands

Table 1-2 lists the commands available from the DHCPv4 Server Pool configuration mode.

Table 1-2. DHCPv4 Server Pool Commands

Sub-Section	Command	See Page …
1.5	broadcast <ipv4 address>	636
1.6	client-identifier	637
1.7	client-name <name>	638
1.8	default-router	639
1.9	dns-server	640

Table 1-2. DHCPv4 Server Pool Commands (Continued)

Sub-Section	Command	See Page …
1.10	domain-name <name>	641
1.11	hardware-address <mac address>	642
1.12	host <ipv4 address> <subnet mask>	643
1.13	lease	644
1.14	netbios-name-server	645
1.15	netbios-node-type	646
1.16	netbios-scope <identifier>	647
1.17	network <ipv4 address> <subnet mask>	648
1.18	nis-domain-name <name>	649
1.19	nis-server	650
1.20	ntp-server <ipv4 address>	651
1.21	option <number>	652
1.22	vendor class-identifier <string> specific-info <value>	654

1.5 broadcast <*ipv4 address*>

Use the **broadcast** <*ipv4 address*> command to specify the broadcast Internet Protocol version 4 (IPv4) address in use on the Dynamic Host Control Protocol (DHCP) client subnet. Use the **no** form of this command to remove the broadcast address.

1.5.1 Syntax Description

<ipv4 address>	Specifies a valid IPv4 address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

1.5.2 Default Values

By default, the DHCPv4 server pool is not configured and the client broadcast address is not specified.

1.5.3 Privilege Level

By default, this command has a privilege level of **13**.

1.5.4 Command History

ASE Release 4.4-41	Command was introduced.

1.5.5 Usage Examples

The following example specifies a broadcast address of **192.22.4.253** for the client subnet:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#broadcast 192.22.4.253
```

1.6 client-identifier

Use the **client-identifier** command to specify a unique identifier for a Dynamic Host Configuration Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove a configured client identifier. Variations of this command include:

client-identifier mac-address *<mac address>*
client-identifier name *<name>*

1.6.1 Syntax Description

mac-address *<mac address>*	Specifies a valid 48-bit medium access control (MAC) address as the client identifier. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).
name *<name>*	Specifies a name to use as the client identifier. Names are specified in an alphanumeric format of no more than 128 characters.

1.6.2 Default Values

No default values are necessary for this command.

1.6.3 Privilege Level

By default, this command has a privilege level of **13**.

1.6.4 Command History

ASE Release 4.4-41	Command was introduced.

1.6.5 Usage Example

The following example specifies a MAC address for the DHCPv4 client identifier:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#client-identifier mac-address 01:d2:17:04:91:11:50
```

1.7 client-name <*name*>

Use the **client-name** <*name*> command o specify the name of a Dynamic Host Configuration Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove the configured client name.

1.7.1 Syntax Description

<*name*>	Identifies the DHCPv4 client (example is **client1**) using an alphanumeric string (up to 32 characters in length).

1.7.2 Default Values

By default, there are no specified client names.

1.7.3 Privilege Level

By default, this command has a privilege level of **13**.

1.7.4 Command History

ASE Release 4.4-41	Command was introduced.

1.7.5 Usage Examples

The following example specifies a client name of **MYCLIENT**:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#client-name MYCLIENT
```

1.8 default-router

Use the **default-router** command to specify the default primary and secondary routers to use for the Dynamic Host Configuration Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove the configured router. Variations of this command include:

```
default-router <ipv4 address>
default-router <ipv4 address> <secondary>
```

1.8.1 Syntax Description

<ipv4 address>	Specifies the unicast Internet Protocol version 4 (IPv4) address of the preferred router on the client's subnet. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<secondary>	Optional. Specifies the IPv4 address of the second preferred router on the client's subnet. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

1.8.2 Default Values

By default, there are no specified default routers.

1.8.3 Privilege Level

By default, this command has a privilege level of **13**.

1.8.4 Command History

ASE Release 4.4-41	Command was introduced.

1.8.5 Functional Notes

When specifying a router to use as the primary/secondary preferred router, verify that the listed router is on the same subnet as the DHCPv4 client. The ASE device allows a designation for two routers, listed in order of precedence.

1.8.6 Usage Examples

The following example configures a default router with address **192.22.4.253** and a secondary router with address **192.22.4.254**:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#default-router 192.22.4.253 192.22.4.254
```

1.9 dns-server

Use the **dns-server** command to specify the default Internet Protocol version 4 (IPv4) domain naming system (DNS) servers (up to four servers) to use for the Dynamic Host Configuration Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove the configured IPv4 DNS server. Variations of this command include:

```
dns-server <ipv4 address>
dns-server <ipv4 address> <second>
dns-server <ipv4 address> <second> <third>
dns-server <ipv4 address> <second> <third> <fourth>
```

1.9.1 Syntax Description

<ipv4 address>	Specifies the IPv4 address of the preferred DNS server on the network. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<second>	Optional. Specifies the IPv4 address of the second preferred DNS server on the network.
<third>	Optional. Specifies the IPv4 address of the third preferred DNS server on the network.
<fourth>	Optional. Specifies the IPv4 address of the fourth preferred DNS server on the network.

1.9.2 Default Values

By default, there are no specified default DNS servers.

1.9.3 Privilege Level

By default, this command has a privilege level of **13**.

1.9.4 Command History

ASE Release 4.4-41	Command was introduced.

1.9.5 Usage Examples

The following example specifies a default IPv4 DNS server with address **192.72.3.254** and a secondary DNS server with address **192.100.4.253**:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#dns-server 192.72.3.254 192.100.4.253
```

1.10 domain-name <*name*>

Use the **domain-name** <*name*> command to specify the domain name for the Dynamic Host Configuration Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove the configured domain name.

1.10.1 Syntax Description

<*name*>	Identifies the DHCPv4 client (e.g., **adtran.com**) using an alphanumeric string (up to **128** characters in length).

1.10.2 Default Values

By default, there are no specified domain names.

1.10.3 Privilege Level

By default, this command has a privilege level of **13**.

1.10.4 Command History

ASE Release 4.4-41	Command was introduced.

1.10.5 Usage Examples

The following example specifies a domain name of **adtran.com**:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#domain-name adtran.com
```

1.11 hardware-address <*mac address*>

Use the **hardware-address** <*mac address*> command to specify the hardware address of a Dynamic Host Configuration Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove the specified address.

1.11.1 Syntax Description

<mac address>	Specifies a valid 48-bit medium access control (MAC) address. MAC addresses should be expressed in the following format xx:xx:xx:xx:xx:xx (for example, **00:A0:C8:00:00:01**).

1.11.2 Default Values

No default value is necessary for this command.

1.11.3 Privilege Level

By default, this command has a privilege level of **13**.

1.11.4 Command History

ASE Release 4.4-41	Command was introduced.

1.11.5 Usage Examples

The following example specifies a client with a MAC address of **ae:11:54:60:99:10**:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#hardware-address ae:11:54:60:99:10
```

1.12 host *<ipv4 address> <subnet mask>*

Use the **host** *<ipv4 address> <subnet mask>* command to specify the Internet Protocol version 4 (IPv4) address and subnet mask for a manual binding to a Dynamic Host Configuration Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove the configured client address.

1.12.1 Syntax Description

<ipv4 address>	Specifies a valid IPv4 address for a manual binding with a DHCPv4 client. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**).

1.12.2 Default Values

By default, there are no specified host addresses.

1.12.3 Privilege Level

By default, this command has a privilege level of **13**.

1.12.4 Command History

ASE Release 4.4-41	Command was introduced.

1.12.5 Usage Examples

The following example specifies a client with IPv4 address **12.200.5.99** and a 21-bit subnet mask:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp)#host 12.200.5.99 255.255.248.0
```

1.13 lease

Use the **lease** command to specify the duration of the lease for an Internet Protocol version 4 (IPv4) address assigned to a Dynamic Host Configuration Protocol version 4 (DHCPv4) client. Use the **no** form of this command to return to the default lease value. Variations of this command include:

```
lease <days>
lease <days> <hours>
lease <days> <hours> <minutes>
```

1.13.1 Syntax Description

<days>	Specifies the duration of the IPv4 address lease in days. Valid range is **0** to **365** days.
<hours>	Optional. Specifies the number of hours in a lease. You may only enter a value in the hours field if the days field is specified. Valid range is **0** to **23** hours.
<minutes>	Optional. Specifies the number of minutes in a lease. You may only enter a value in the minutes field if the days and hours fields are specified. Valid range is **0** to **59** minutes.

1.13.2 Default Values

By default, an IPv4 address lease is **1** day.

1.13.3 Privilege Level

By default, this command has a privilege level of **13**.

1.13.4 Command History

ASE Release 4.4-41	Command was introduced.

1.13.5 Usage Examples

The following example specifies a lease of **2** days:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#lease 2
```

The following example specifies a lease of **1 hour**:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#lease 0 1
```

The following example specifies a lease of **30 minutes**:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#lease 0 0 30
```

1.14 netbios-name-server

Use the **netbios-name-server** command to specify the primary and secondary network basic input/output system (NetBIOS) Windows Internet Naming Service (WINS) name servers available for use by the Dynamic Host Configuration Protocol version 4 (DHCPv4) clients. Use the **no** form of this command to remove a configured NetBIOS name server. Variations of this command include:

```
netbios-name-server <ipv4 address>
netbios-name-server <ipv4 address> <secondary>
```

1.14.1 Syntax Description

<ipv4 address>	Specifies the IPv4 address of the preferred NetBIOS WINS name server on the network. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<secondary>	Optional. Specifies the IPv4 address of the second preferred NetBIOS WINS name server on the network.

1.14.2 Default Values

By default, there are no configured NetBIOS WINS name servers.

1.14.3 Privilege Level

By default, this command has a privilege level of **13**.

1.14.4 Command History

ASE Release 4.4-41	Command was introduced.

1.14.5 Usage Examples

The following example specifies a primary NetBIOS WINS name server with an IPv4 address of **172.45.6.99** and a secondary with an IPv4 address of **172.45.8.15**:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#netbios-name-server 172.45.6.99 172.45.8.15
```

1.15 netbios-node-type

Use the **netbios-node-type** command to specify the type of network basic input/output system (NetBIOS) node used with Dynamic Host Configuration Protocol version 4 (DHCPv4) clients. Use the **no** form of this command to remove a configured NetBIOS node type. Variations of this command include:

```
netbios-node-type b-node
netbios-node-type h-node
netbios-node-type m-node
netbios-node-type p-node
```

1.15.1 Syntax Description

b-node	Specifies the broadcast node.
h-node	Specifies the hybrid node (recommended).
m-node	Specifies the mixed node.
p-node	Specifies the peer-to-peer node.

1.15.2 Default Values

By default, the **netbios-node-type** is set to **h-node** (hybrid node).

1.15.3 Privilege Level

By default, this command has a privilege level of **13**.

1.15.4 Command History

ASE Release 4.4-41	Command was introduced.

1.15.5 Usage Examples

The following example specifies a client's NetBIOS node type as **h-node**:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#netbios-node-type h-node
```

1.16 netbios-scope <*identifier*>

Use the **netbios-scope** <*identifier*> command to specify the type of network basic input/output system (NetBIOS) scope used with Dynamic Host Configuration Protocol version 4 (DHCPv4) clients. Use the **no** form of this command to remove a configured NetBIOS scope.

1.16.1 Syntax Description

<identifier>	Specifies the NetBIOS scope identifier for DHCPv4 clients. Identifiers are specified in an alphanumeric string of no more than 128 characters.

1.16.2 Default Values

By default, no NetBIOS scope identifier is specified.

1.16.3 Privilege Level

By default, this command has a privilege level of **13**.

1.16.4 Command History

ASE Release 4.4-41	Command was introduced.

1.16.5 Usage Examples

The following example specifies a NetBIOS scope identifier for DHCPv4 clients:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#netbios-scope SCOPEDEFINED1
```

1.17 network *<ipv4 address> <subnet mask>*

Use the **network** *<ipv4 address> <subnet mask>* command to specify the subnet number and mask for a Dynamic Host Configuration Protocol version 4 (DHCPv4) server address pool. Use the **no** form of this command to remove a configured subnet.

1.17.1 Syntax Description

<ipv4 address>	Specifies a valid IPv4 address for the DHCP server pool. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<subnet mask>	Specifies the subnet mask that corresponds to a range of IPv4 addresses (network) or a specific host. Subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**).

1.17.2 Default Values

By default, there are no configured DHCPv4 server address pools.

1.17.3 Privilege Level

By default, this command has a privilege level of **13**.

1.17.4 Command History

ASE Release 4.4-41	Command was introduced.

1.17.5 Usage Examples

The following example configures an address pool subnet of **192.34.0.0** with a 21-bit subnet mask:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#network 192.34.0.0 255.255.248.0
```

1.18 nis-domain-name <*name*>

Use the **nis-domain-name** <*name*> command to configure the network information system (NIS) available for use by the Dynamic Host Configuration Protocol version 4 (DHCPv4) clients. Use the **no** form of this command to remove a configured NIS server.

1.18.1 Syntax Description

<*name*>	Specifies the NIS server name for use by DHCPv4 clients using an alphanumeric string (up to 128 characters in length).

1.18.2 Default Values

By default, there are no NIS servers configured.

1.18.3 Privilege Level

By default, this command has a privilege level of **13**.

1.18.4 Command History

ASE Release 4.4-41	Command was introduced.

1.18.5 Usage Examples

The following example configures an NIS server for DHCPv4 clients:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#nis-domain-name NAMESERVER3
```

1.19 nis-server

Use the **nis-server** command to specify the default Internet Protocol version 4 (IPv4) network information system (NIS) servers (up to four servers) to use for the Dynamic Host Configuration Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove the configured IPv4 NIS server. Variations of this command include:

```
nis-server <ipv4 address>
nis-server <ipv4 address> <second>
nis-server <ipv4 address> <second> <third>
nis-server <ipv4 address> <second> <third> <fourth>
```

1.19.1 Syntax Description

<ipv4 address>	Specifies the IPv4 address of the preferred NIS server on the network. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<second>	Optional. Specifies the IPv4 address of the second preferred NIS server on the network.
<third>	Optional. Specifies the IPv4 address of the third preferred NIS server on the network.
<fourth>	Optional. Specifies the IPv4 address of the fourth preferred NIS server on the network.

1.19.2 Default Values

By default, there are no specified default NIS servers.

1.19.3 Privilege Level

By default, this command has a privilege level of **13**.

1.19.4 Command History

ASE Release 4.4-41	Command was introduced.

1.19.5 Usage Examples

The following example specifies a default IPv4 NIS server with address **192.72.3.254**:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#nis-server 192.72.3.254
```

1.20 ntp-server <*ipv4 address*>

Use the **ntp-server** command to specify the name of the Network Time Protocol (NTP) server published to the Dynamic Host Control Protocol version 4 (DHCPv4) client. Use the **no** form of this command to remove a defined NTP server.

1.20.1 Syntax Description

<ipv4 address>	Specifies the IPv4 address of the NTP server. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

1.20.2 Default Values

By default, no NTP server is defined.

1.20.3 Privilege Level

By default, this command has a privilege level of **13**.

1.20.4 Command History

Release 9.1	Command was introduced.

1.20.5 Usage Examples

The following example specifies the IPv4 address of the NTP server:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#ntp-server 192.168.1.1
```

1.21 option <*number*>

Use the **option** command to specify Dynamic Host Control Protocol (DHCP) generic options in the DHCP server pool configuration. DHCP options can be used to send additional information to clients connecting to the DHCP server, such as vendor class, host name, authentication credentials, or other standard or vendor-specific information. Use the **no** form of this command to remove a specified DHCP option from the DHCP server pool configuration. Variations of this command include:

option *<number>* **ascii** *<string>*
option *<number>* **hex** *<string>*
option *<number>* **ip** *<ipv4 address>*

1.21.1 Syntax Description

option *<number>*	Specifies the DHCP option to add to the DHCP server pool configuration. Valid range is **1** to **254**.
ascii *<string>*	Specifies DHCP option information as a text string. DHCP option text strings have a maximum length of **128** characters. Enter text strings in the following format: **stringxxx**.
hex *<string>*	Specifies DHCP option information in hexadecimal format. DHCP options specified in hexadecimal format have a maximum length of **128** characters. Enter hexadecimal information in the following format: **A0B2C3**.
ip *<ipv4 address>*	Specifies an Internet Protocol version 4 (IPv4) address associated with the DHCP option. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

1.21.2 Default Values

By default, no DHCP options are specified in the DHCP server pool.

1.21.3 Privilege Level

By default, this command has a privilege level of **13**.

1.21.4 Command History

ASE Release 4.4-42	Command was introduced.

1.21.5 Usage Examples

The following example specifies DHCP option **12**, with a text string, is sent to clients connecting to DHCP pool **MYPOOL1**:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#option 12 ascii stringxxx
```

The following example specifies DHCP option **60**, with a hexadecimal string, is sent to clients connecting to DHCP pool **MYPOOL1**:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#option 12 hex A0B2C3
```

The following example specifies DHCP option **121**, with IP address **10.22.232.200**, is sent to clients connecting to DHCP pool **MYPOOL1**:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#option 121 ip 10.22.232.200
```

The following example removes DHCP option **60** from the DHCP pool **MYPOOL1**:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#no option 60
```

1.22 vendor class-identifier <*string*> specific-info <*value*>

Use the **vendor-class-identifier** <*string*> command to define a vendor class identifier for use with Dynamic Host Control Protocol version 4 (DHCPv4) clients. Use the **no** form of this command to remove the DHCPv4 vendor class identifier.

1.22.1 Syntax Description

<string>	Specifies the DHCPv4 vendor class identifier in simple text (ASCII) with a string of up to **64** characters. The string must be included in double quotations.
specific-info *<value>*	Specifies the specific information for the particular vendor. Specify the *<value>* parameter as a hexadecimal value in **64** octets (**0x...**).

1.22.2 Default Values

By default, vendor class identifiers are not specified.

1.22.3 Privilege Level

By default, this command has a privilege level of **13**.

1.22.4 Command History

ASE Release 4.4-41	Command was introduced.

1.22.5 Usage Examples

The following example configures a vendor class identifier for DHCPv4 clients:

```
(config)#ip dhcp pool MYPOOL1
(config-dhcp-pool)#vendor class-identifier “MYSTERIOUSVENDOR” specific-info 0xAABB
```

2 IPMC Profile Command Set

2.1 Scope of this Section

This section outlines the commands available to configure the Internet Protocol Multicast Configuration (IPMC) Profile on the ADTRAN Switch Engine (ASE). The IPMC profile allows permission for certain multicast registrations by providing access authorization using certain configured matching criteria from the profile. Each profile creates a named range, which then is then configured with the rules used for matching multicast addresses for registration. The named ranges are then applied to specific multicast IPv4 and IPv6 addresses to maintain access control for multicast registrations.

2.2 Accessing the IPMC Profile Configuration Mode

The IPMC Profile configuration mode is accessed using the **ipmc profile** command from the Global Configuration mode prompt. This command enters the profile's configuration mode. To enter the IPMC Profile configuration mode, enter the command as follows:

```
#configure terminal
(config)#ipmc profile MYIPMCPROFILE
(config-ipmc-profile)#
```

2.3 Common Commands

The commands listed in Table 2-1 are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the section listed below:

Table 2-1. Common Commands

Sub-Section	Command	See Page …
1.4	do	19
1.5	end	20
1.6	exit	21
1.7	help	22

2.4 IPMC Profile Configuration Commands

Table 2-2 lists the commands available from the IPMC Profile configuration mode.

Table 2-2. IPMC Profile Configuration Commands

Sub-Section	Command	See Page …
2.5	default range <name>	656
2.6	description <description>	657
2.7	range <name>	658

2.5 default range <*name*>

Use the **default range** <*name*> command to return a specified Internet Protocol Multicast Configuration (IPMC) profile range entry to its default values.

2.5.1 Syntax Description

<name>	Specifies the name of the IPMC profile range entry to return to the default settings. Valid names do not exceed 16 characters in length.

2.5.2 Default Values

No default values are necessary for this command.

2.5.3 Command History

ASE Release 4.4-41	Command was introduced.

2.5.4 Functional Notes

The named IPMC profile range entry used in this command is the range entry created with the command “ipmc range <name>” on page 340. Each range entry includes a range of Internet Protocol version 4 (IPv4) and IP version 6 (IPv6) multicast addresses.

2.5.5 Usage Examples

The following example returns the range entry **RANGEENTRY1** to its default values:

```
(config)#ipmc profile MYIPMCPROFILE
(config-ipmc-profile)#default range RANGEENTRY1
```

2.6 description <*description*>

Use the **description** <*description*> command to specify a description for the designated Internet Protocol Multicast Configuration (IPMC) profile. Use the **no** form of this command to remove the description. Variations of this command include:

```
<description>
<description> <description>
<description> <description> <description>
```

2.6.1 Syntax Description

<description>	Specifies a description of the IPMC profile using an alphanumeric string (up to **32** characters in length). You can optionally specify up to **3** descriptions for a single profile.

2.6.2 Default Values

By default, no profile description is specified.

2.6.3 Command History

ASE Release 4.4-41	Command was introduced.

2.6.4 Usage Examples

The following example specifies a profile description for the IPMC profile **MYIPMCPROFILE**:

```
(config)#ipmc profile MYIPMCPROFILE
(config-ipmc-profile)#description REMOTEOFFICE PROFILE3
```

2.7 range <*name*>

Use the **range** <*name*> command to specify the actions taken by the Internet Protocol Multicast Configuration (IPMC) profile for IP version 4 (IPv4) and IP version 6 (IPv6) multicast addresses that match the defined rage (refer to the command "ipmc range <name>" on page 340 to define an IPMC range). Use the **no** form of this command to remove the range from the IPMC profile. Variations of this command include:

```
range <name> deny
range <name> deny log
range <name> deny log next <name>
range <name> deny next <name>
range <name> permit
range <name> permit log
range <name> permit log next <name>
range <name> permit next <name>
```

2.7.1 Syntax Description

<name>	Specifies the name of the IPMC range. Valid range names do not exceed 16 characters in length, and are configured using the command "ipmc range <name>" on page 340
deny	Specifies that the addresses matching the specified range are denied.
permit	Specifies that the addresses matching the specified range are permitted.
log	Optional. Specifies that logs are generated when matching traffic is intercepted.
next *<name>*	Optional. Specifies the next range entry used in the profile. If this parameter is not specified, the entry is added to the profile last.

2.7.2 Default Values

By default, the IPMC actions are not configured.

2.7.3 Command History

ASE Release 4.4-41	Command was introduced.

2.7.4 Usage Examples

The following example specifies that the IPMC profile **MYIPMCPROFILE** denies the IPv4 and IPv6 multicast addresses specified in the IPMC range **MYRANGE1**:

```
(config)#ipmc profile MYIPMCPROFILE
(config-ipmc-profile)#range MYRANGE1 deny
```

3 JSON Host Command Set

3.1 Scope of this Section

This section outlines the commands available to configure the JavaScript Object Notation (JSON) Host on the ADTRAN Switch Engine (ASE). The JSON Host, configured with a user name, password, and uniform resource locator (URL), receives JSON notifications from remote procedure calls (RPCs). You can access the host to review the JSON notifications received after RPCs have been initiated.

3.2 Accessing the JSON Host Configuration Mode

The JSON Host configuration mode is accessed using the **json notification host** command from the Global Configuration mode prompt. This command enters the host's configuration mode. To enter the JSON Host configuration mode, enter the command as follows:

```
#configure terminal
(config)#json notification host MYJSONHOST
(config-json-noti-host)#
```

3.3 Common Commands

The commands listed in Table 3-1 are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the section listed below:

Table 3-1. Common Commands

Sub-Section	Command	See Page …
1.4	do	19
1.5	end	20
1.6	exit	21
1.7	help	22

3.4 JSON Host Configuration Commands

Table 3-2 lists the commands available from the JSON Host configuration mode.

Table 3-2. JSON Host Configuration Commands

Sub-Section	Command	See Page …
3.5	authentication basic username <username> password <password>	660
3.6	url <url>	661

3.5 authentication basic username <*username*> password <*password*>

Use the **authentication basic** command to configure a user name and password for authenticated access to the JavaScript Object Notation (JSON) host. Use the no form of this command to disable authentication for the specified user name.

3.5.1 Syntax Description

<username>	Specifies the user name for authentication to the JSON host. User names cannot exceed 32 characters in length.
<password>	Specifies the password for authentication to the JSON host.

3.5.2 Default Values

No default values are necessary for this command.

3.5.3 Command History

ASE Release 4.4-41	Command was introduced.

3.5.4 Usage Examples

The following example configures authentication for the user **FIRSTUSER1** to the JSON host **MYJSONHOST**:

```
(config)#json notification host MYJSONHOST
(config-json-noti-host)#authentication basic username FIRSTUSER1 password SECRETWORD
```

3.6 url <*url*>

Use the **url** <*url*> command to specify the uniform resource locator (URL) address of the JavaScript Object Notation (JSON) host. This address is where JSON notifications are sent. Use the no form of this command to remove the URL from the JSON host configuration.

3.6.1 Syntax Description

<url>	Specifies the URL address of the JSON host. Specify the URL using either Hypertext Transfer Protocol (HTTP) or HTTP Secure (HTTPS), for example, **https://example.com**. URLs are limited to 256 characters.

3.6.2 Default Values

By default, no URL is specified.

3.6.3 Command History

ASE Release 4.4-41	Command was introduced.

3.6.4 Usage Examples

The following example specifies a URL of **http://myjsonhost.com** for the JSON host **MYJSONHOST**:

```
(config)#json notification host MYJSONHOST
(config-json-noti-host)#url http://myjsonhost.com
```

4 SNMP Server Host Command Set

4.1 Scope of this Section

This section outlines the commands available to configure the Simple Network Management Protocol (SNMP) server host on the ADTRAN Switch Engine (ASE).

4.2 Accessing the SNMP Server Host Configuration Mode

To access the SNMP server host configuration mode, enter the **snmp-server host** command at the Global Configuration mode prompt. For example:

```
(config)#snmp-server host MYHOST
(config-snmps-host)#
```

4.3 Common Commands

The commands listed in Table 4-1 are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the section listed below:

Table 4-1. Common Commands

Sub-Section	Command	See Page …
1.4	do	19
1.5	end	20
1.6	exit	21
1.7	help	22

4.4 SNMP Server Host Configuration Commands

This section contains the commands listed in Table 4-2.

Table 4-2. Privilege Configuration Mode Commands

Sub-Section	Command	See Page …
4.5	host	663
4.6	informs retries <number> timeout <interval>	665
4.7	shutdown	666
4.8	version	667

4.5 host

Use the **host** command to configure the Simple Network Management Protocol (SNMP) server host parameters. Use the **no** form of this command to remove the configured parameter. Variations of this command include:

```
host <domain name>
host <domain name> <port>
host <domain name> <port> informs
host <domain name> <port> informs traps
host <domain name> <port> traps
host <domain name> informs
host <domain name> informs traps
host <domain name> traps
host <ipv4 address>
host <ipv4 address> <port>
host <ipv4 address> <port> informs
host <ipv4 address> <port> informs traps
host <ipv4 address> <port> traps
host <ipv4 address> informs
host <ipv4 address> informs traps
host <ipv4 address> traps
host <ipv6 address>
host <ipv6 address> <port>
host <ipv6 address> <port> informs
host <ipv6 address> <port> informs traps
host <ipv6 address> <port> traps
host <ipv6 address> informs
host <ipv6 address> informs traps
host <ipv6 address> traps
```

4.5.1 Syntax Description

<domain name>	Specifies the SNMP trap host domain name.
<ipv4 address>	Specifies the unicast IPv4 address of the SNMP trap host. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).
<ipv6 address>	Specifies the unicast IPv6 address of the SNMP trap host. IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**.
<port>	Optional. Specifies the User Datagram Protocol (UDP) port for SNMP trap messages. Valid range is **1** to **65535**.
informs	Optional. Enables the sending of SNMP INFORM messages to this host.
traps	Optional. Enables the sending of SNMP trap messages to this host.

4.5.2 Default Values

By default, the SNMP server host is not configured.

4.5.3 Privilege Level

By default, this command has a privilege level of **15**.

4.5.4 Command History

ASE Release 4.4-41	Command was introduced.

4.5.5 Usage Examples

The following example specifies an IPv6 address for the SNMP server MYHOST, and enables the host to receive INFORM messages:

```
(config)#snmp-server MYHOST
(config-snmps-host)#host 2001:DB8:1::1 informs
```

4.6 informs retries <*number*> timeout <*interval*>

Use the **informs retries** <*number*> **timeout** <*interval*> command to set the number of retry attempts for a response to Simple Network Management Protocol (SNMP) INFORM messages and set the amount of time to wait for a response before allowing a new request. Use the **no** form of this command to return to the default setting.

4.6.1 Syntax Description

retries *<number>*	Specifies number of retries for a response. Valid range is **0** to **255**.
timeout *<interval>*	Specifies time (in seconds) to wait for a response. Valid range is **0** to **2147** seconds.

4.6.2 Default Values

By default, the number of retries for INFORM messages is **3** and the timeout is **5** seconds.

4.6.3 Privilege Level

By default, this command has a privilege level of **15**.

4.6.4 Command History

ASE Release 4.4-41	Command was introduced.

4.6.5 Usage Examples

The following example configures the INFORM message parameters for the SNMP server host **MYHOST**:

```
(config)#snmp-server host MYHOST
(config-snmps-host)#informs retries 10 timeout 30
```

4.7 shutdown

Use the **shutdown** command to disable traps on the Simple Network Management Protocol (SNMP) sever host.

4.7.1 Syntax Description

ASE Release 4.4-41	Command was introduced.

4.7.2 Default Values

No default values are necessary for this command.

4.7.3 Privilege Level

By default, this command has a privilege level of **15**.

4.7.4 Command History

ASE Release 4.4-41	Command was introduced.

4.7.5 Usage Examples

The following example disables traps on the SNMP server host **MYHOST**:

```
(config)#snmp-server host MYHOST
(config-snmps-host)#shutdown
```

4.8 version

Use the **version** command to specify the Simple Network Management Protocol (SNMP) trap version supported on the SNMP server host. Use the **no** form of this command to disable the setting. Variations of this command include:

```
version v1
version v1 <community>
version v1 encrypted <secret>
version v2
version v2 <community>
version v2 encrypted <secret>
version v3
version v3 <community>
version v3 encrypted <secret>
```

4.8.1 Syntax Description

v1	Specifies using SNMP version 1 security model.
v2	Specifies using SNMP version 2 security model.
v3	Specifies using SNMP version 3 user-based security model (USM).
<community>	Optional. Specifies the community string (used as a password) (63 characters maximum) for authorized agents to obtain access to SNMP information.
encrypted *<secret>*	Optional. Specifies an encrypted community secret. Valid secrets have between **96** and **244** characters.

4.8.2 Default Values

No default values are necessary for this command.

4.8.3 Privilege Level

By default, this command has a privilege level of **15**.

4.8.4 Command History

ASE Release 4.4-41	Command was introduced.

4.8.5 Usage Examples

The following example specifies that the SNMP server host **MYHOST** uses SNMP **v3** security:

```
(config)#snmp-server host MYHOST
(config-snmps-host)#version v3
```

5 QoS Egress Map Command Set

5.1 Scope of this Section

This section outlines the commands available to configure a Quality of Service (QoS) egress map on the ADTRAN Switch Engine (ASE) device. Egress maps are used to control the rewriting of packets at egress, where Priority Code Point (PCP), drop eligibility indicator (DEI), and Differentiated Service Code Points (DSCP) values can be updated based on their classified key values. Egress maps are configured by specifying which part of the packet is used for matching (Class of Service (CoS) ID, CoS ID-drop precedence level (DPL), DSCP, or DSCP-DPL), enabling the rewriting actions taken once the packet information is processed, and specifying which new values are mapped to the packet information.

The QoS egress map is a named list with sequenced entries. An entry contains a single match reference and one or more actions. To activate the QoS Egress Map command set (which allows you to create and/or edit a map), enter a valid version of the **qos map egress** command at the Global Configuration mode prompt. Multiple map entries for the same QoS map are differentiated by a sequence number. The sequence number is used to assign match order.

5.2 Accessing the QoS Egress Map Configuration Mode

To create a QoS egress map, and enter the QoS Egress Map configuration mode, enter the **qos map egress** command at the Global Configuration mode prompt. For example:

```
#configure terminal
(config)#qos map egress 75
(config-qos-map-egress)#
```

5.3 Common Commands

The commands listed in Table 5-1 are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the section listed below:

Table 5-1. Common Commands

Sub-Section	Command	See Page …
1.4	do	19
1.5	end	20
1.6	exit	21
1.7	help	22

5.4 QoS Egress Map Configuration Commands

Table 5-2 lists the commands available from the QoS Egress Map configuration mode.

Table 5-2. QoS Egress Map Configuration Mode Commands

Sub-Section	Command	See Page …
5.5	key	670
5.6	action	671
5.7	map class	672
5.8	map dscp	674
5.9	preset classes <number>	676

5.5 key

Use the **key** command to specify the keys used for packet matching in the Quality of Service (QoS) egress map. Use the **no** form of this command to remove the key from the map's configuration and return to the default classification behavior. Variations of this command include:

```
key class
key class-dpl
key dscp
key dscp-dpl
```

5.5.1 Syntax Description

class	Specifies that the classified Class of Service (CoS) ID value is used as a key for all traffic.
class-dpl	Specifies that the classified CoS ID and drop precedence level (DPL) value are used as keys for all traffic.
dscp	Specifies that the frame's Differentiated Service Code Points (DSCP) value is used as a key, and that no mapping is performed for non-IP frames.
dscp-dpl	Specifies that the classified DSCP and DPL values are used as keys for all traffic.

5.5.2 Default Values

By default, QoS egress maps are not configured. When configured, by default, classified COS ID values are used as keys for all traffic.

5.5.3 Command History

ASE Release 4.4-41	Command was introduced.

5.5.4 Functional Notes

Specifying matching criteria (keys) for egress traffic, consists of naming the part of the packet header used for matching purposes. Available packet information used for matching egress traffic includes CoS, DSCP, and DPL values. Once a key is defined, actions and traffic mapping can be associated to traffic that matches the key criteria.

5.5.5 Usage Examples

To configure an egress map to match traffic based on DSCP values, enter the command from the egress map's configuration mode prompt as follows:

```
(config)#qos map egress 75
(config-qos-map-egress)#key dscp
```

5.6 action

Use the **action** command to enable rewriting actions for traffic that matches the defined key in the Quality of Service (QoS) egress map. Each parameter specifies the type of rewriting you are enabling for matched traffic. Use the **no** form of this command to disable rewriting for the specified action. Variations of this command include:

```
action dei
action dscp
action path
action pcp
```

5.6.1 Syntax Description

dei	Enables rewriting of the packet's drop eligibility indicator (DEI) value.
dscp	Enables rewriting of the packet's Differentiated Service Code Points (DSCP) value.
path	Enables rewriting of the packet's path CoS ID value.
pcp	Enables rewriting of the packet's Priority Code Point (PCP) value.

5.6.2 Default Values

By default, QoS egress maps are not configured and no rewriting of packet values takes place.

5.6.3 Command History

ASE Release 4.4-41	Command was introduced.

5.6.4 Functional Notes

The action parameters for this command can be entered in any order and multiple parameters can be specified in a single command entry.

5.6.5 Usage Examples

To enable rewriting of DEI and PCP values for egress traffic that matches the **dscp** key specified in egress map **75**, enter the command as follows:

```
(config)#qos map egress 75
(config-qos-map-egress)#key dscp
(config-qos-map-egress)#action dei pcp
```

5.7 map class

Use the **map class** command to specify new values that are applied to traffic, based on the traffic's current Class of Service (CoS) class, when it matches the egress map key and a specific rewriting action has been enabled. Traffic with specific CoS ID values can be assigned new drop eligibility indicator (DEI), Differentiated Service Code Points (DSCP), path CoS ID or Priority Code Points (PCP) values using this command. Use the **no** form of this command to remove the mapping configuration from the Quality of Service (QoS) egress map configuration. Variations of this command include:

map class *<id>* **to dei** *<value>*
map class *<id>* **dpl** *<value>* **to dei** *<value>*
map class *<id>* **to dscp** *<value>*
map class *<id>* **dpl** *<value>* **to dscp** *<value>*
map class *<id>* **to path-cosid** *<id>*
map class *<id>* **dpl** *<value>* **to path-cosid** *<id>*
map class *<id>* **to pcp** *<value>*
map class *<id>* **dpl** *<value>* **to pcp** *<value>*

5.7.1 Syntax Description

map class *<id>*	Specifies the CoS ID value (or range) used for traffic matching, and enters the mapping configuration to specify the new values assigned to traffic that matches the specified CoS ID value. Valid range is **0** to **7**.
dpl *<value>*	Optional. Specifies the DPL value to which mapping also occurs. Valid range is **0** to **3**.
to	Specifies the values that are written to the frame when the key is matched and the action is enabled.
dei *<value>*	Specifies the DEI value to be written to matching traffic. Valid range is **0** to **1**.
dscp *<value>*	Specifies the DSCP value to be written to matching traffic. Valid range is **0** to **63**.
path-cosid *<id>*	Specifies the path CoS ID value to be written to matching traffic. Valid range is **0** to **7**.
pcp *<value>*	Specifies the PCP value to be written to matching traffic. Valid range is **0** to **7**.

5.7.2 Default Values

By default, class mapping is not configured for the QoS egress map. When the egress map is configured, if the optional DPL value is not specified, a DPL value of **0** is used for traffic matching.

5.7.3 Command History

ASE Release 4.4-41	Command was introduced.

5.7.4 Functional Notes

The new values specified with this command can be entered in any order and multiple value types can be specified in a single command entry.

5.7.5 Usage Examples

To map the DEI value of **1** and the PCP value of **5** to the CoS ID of **3** and a DPL value of **2**, for traffic that matches the **dscp** key specified in egress map **75**, which is also configured with DEI and PCP rewrite actions enabled, enter the command as follows:

```
(config)#qos map egress 75
(config-qos-map-egress)#key dscp
(config-qos-map-egress)#action dei pcp
(config-qos-map-egress)#map class 3 dpl 2 to dei 1 pcp 5
```

5.8 map dscp

Use the **map dscp** command to assign traffic with specific Differentiated Service Code Points (DSCP) values a new drop eligibility indicator (DEI), DSCP, path CoS ID or Priority Code Point (PCP) value. Use the **no** form of this command to remove the mapping configuration from the Quality of Service (QoS) egress map configuration. Variations of this command include:

```
map dscp <value> to dei <value>
map dscp <value> dpl <value> to dei <value>
map dscp <value> to dscp <value>
map dscp <value> dpl <value> to dscp <value>
map dscp <value> to path-cosid <id>
map dscp <value> dpl <value> to path-cosid <id>
map dscp <value> to pcp <value>
map dscp <value> dpl <value> to pcp <value>
```

5.8.1 Syntax Description

map dscp *<value>*	Specifies the DSCP value used for traffic matching, and enters the mapping configuration to specify the new values assigned to traffic that matches the specified DSCP value. Valid range is **0** to **63**.
dpl *<value>*	Optional. Specifies the drop precedence level (DPL) value to which mapping also occurs. Valid range is **0** to **3**.
to	Specifies the values that are written to the frame when the key is matched and the action is enabled.
dei *<value>*	Specifies the DEI value to be written to matching traffic. Valid range is **0** to **1**.
dpl *<value>*	Specifies the DPL value to be written to matching traffic. Valid range is **0** to **3**.
dscp *<value>*	Specifies the DSCP value to be written to matching traffic. Valid range is **0** to **63**.
path-cosid *<id>*	Specifies the path CoS ID value to be written to matching traffic. Valid range is **0** to **7**.
pcp *<value>*	Specifies the PCP value to be written to matching traffic. Valid range is **0** to **7**.

5.8.2 Default Values

By default, class mapping is not configured for the QoS egress map. When the egress map is configured, if the optional DPL value is not specified, a DPL value of **0** is used for traffic matching.

5.8.3 Command History

ASE Release 4.4-41	Command was introduced.

5.8.4 Functional Notes

The new values specified with this command can be entered in any order and multiple value types can be specified in a single command entry.

5.8.5 Usage Examples

To map the DSCP value of best effort (**be**) and a DPL value of **2** to a DEI value of **1** and a PCP value of **5** for traffic that matches the **dscp** key specified in egress map **75**, which is also configured with DEI and PCP value classification enabled, enter the command as follows:

```
(config)#qos map egress 75
(config-qos-map-egress)#key dscp
(config-qos-map-egress)#action dei pcp
(config-qos-map-egress)#map dscp be dpl 2 to dei 1 pcp 5
```

5.9 preset classes <*number*>

Use the **preset classes** <*number*> command to configure the Quality of Service (QoS) egress map to automatically apply to a specific number of traffic classes. Use the **no** form of this command to remove the traffic class preset configuration from the egress map. Variations of this command include:

```
preset classes <number>
preset classes <number> color-aware
```

5.9.1 Syntax Description

<*number*>	Specifies the number of traffic classes to which to apply the egress map. Valid range is **1** to **8**.
color-aware	Optional. Enables color awareness for traffic intercepted by the egress map.

5.9.2 Default Values

By default, traffic classes are not applied to QoS egress map traffic.

5.9.3 Command History

ASE Release 4.4-41	Command was introduced.

5.9.4 Usage Examples

To add this egress map to a number of traffic classes, enter the command as follows:

```
(config)#qos map egress 75
(config-qos-map-egress)#preset classes 5
```

6 QoS Ingress Map Command Set

6.1 Scope of this Section

This section outlines the commands available to configure a Quality of Service (QoS) ingress map on the ADTRAN Switch Engine (ASE) device. Ingress maps are used by QoS as a method for classifying incoming traffic based on key values in the packet or frame header.

The QoS ingress map is a named list with sequenced entries. An entry contains a single match reference and one or more actions. To activate the QoS Ingress Map command set (which allows you to create and/or edit a map), enter a valid version of the **qos map ingress** command at the Global Configuration mode prompt. Multiple map entries for the same QoS map are differentiated by a sequence number. The sequence number is used to assign match order.

6.2 Accessing the QoS Ingress Map Configuration Mode

To create a QoS ingress map, and enter the QoS Ingress Map configuration mode, enter the **qos map ingress** command at the Global Configuration mode prompt. For example:

```
#configure terminal
(config)#qos map ingress 20
(config-qos-map-ingress)#
```

6.3 Common Commands

The commands listed in Table 6-1 are common to multiple command sets and are covered in a centralized section of this guide. For more information, refer to the section listed below:

Table 6-1. Common Commands

Sub-Section	Command	See Page …
1.4	do	19
1.5	end	20
1.6	exit	21
1.7	help	22

6.4 QoS Ingress Map Configuration Commands

Table 6-2 lists the commands available from the QoS Ingress Map configuration mode.

Table 6-2. QoS Ingress Map Configuration Mode Commands

Sub-Section	Command	See Page …
6.5	key	679
6.6	action	680

Table 6-2. QoS Ingress Map Configuration Mode Commands (Continued)

Sub-Section	Command	See Page …
6.7	map dscp	681
6.8	map pcp	683
6.9	preset classes <number>	685

6.5 key

Use the **key** command to specify the keys used for packet matching in the Quality of Service (QoS) ingress map. Use the **no** form of this command to remove the key from the map's configuration and return to the default classification behavior. Variations of this command include:

```
key dscp
key dscp-pcp-dei
key pcp
key pcp-dei
```

6.5.1 Syntax Description

dscp	Specifies that the frame's Differentiated Service Code Points (DSCP) value is used as a key, and that no mapping is performed for non-IP frames.
dscp-pcp-dei	Specifies that the frame's DSCP value is used as a key, and that non-IP frames use the classified Priority Code Point (PCP) and drop eligibility indicator (DEI) values as keys.
pcp	Specifies that the classified PCP value is used as a key for all traffic.
pcp-dei	Specifies that the classified PCP and DEI values are used as keys for all traffic.

6.5.2 Default Values

By default, QoS ingress maps are not configured. When configured, by default, classified PCP values are used as keys for all traffic.

6.5.3 Command History

ASE Release 4.4-41	Command was introduced.

6.5.4 Functional Notes

Specifying matching criteria for incoming traffic, or "keys" as they are called in the ASE device, consists of naming the part of the packet header used for matching purposes. Available packet information used for matching includes DSCP, PCP, and DEI values. Once a key is defined, actions and traffic matching can be associated to traffic that matches the key criteria.

6.5.5 Usage Examples

To configure an ingress map to match traffic based on DSCP values for IP traffic, and PCP and DEI values for non-IP traffic, enter the command from the ingress map's configuration mode prompt as follows:

```
(config)#qos map ingress 20
(config-qos-map-ingress)#key dscp-pcp-dei
```

6.6 action

Use the **action** command to enable classification actions for traffic that matches the defined key in the Quality of Service (QoS) ingress map. Each parameter specifies the type of classification you are enabling for matched traffic. Use the **no** form of this command to disable classification for the specified action. Variations of this command include:

```
action class
action cos
action dei
action dpl
action dscp
action path
action pcp
```

6.6.1 Syntax Description

class	Enables traffic classification based on the packet's Class fo Service (CoS) ID.
cos	Enables traffic classification based on the packet's CoS value.
dei	Enables traffic classification based on the packet's drop eligibility indicator (DEI) value.
dpl	Enables traffic classification based on the packet's drop precedence level (DPL) value.
dscp	Enables traffic classification based on the packet's Differentiated Service Code Points (DSCP) value.
path	Enables traffic classification based on the packet's path CoS ID.
pcp	Enables traffic classification based on the packet's Priority Code Point (PCP) value.

6.6.2 Default Values

By default, QoS ingress maps are not configured and no traffic classification takes place.

6.6.3 Command History

ASE Release 4.4-41	Command was introduced.

6.6.4 Functional Notes

The action parameters for this command can be entered in any order and multiple parameters can be specified in a single command entry.

6.6.5 Usage Examples

To enable classification of DEI and PCP values for incoming traffic that matches the **dscp-pcp-dei** key specified in ingress map **20**, enter the command as follows:

```
(config)#qos map ingress 20
(config-qos-map-ingress)#key dscp-pcp-dei
(config-qos-map-ingress)#action dei pcp
```

6.7 map dscp

Use the **map dscp** command to assign traffic with specific Differentiated Service Code Points (DSCP) values a new Class of Service (CoS) ID, CoS, drop eligibility indicator (DEI), drop precedence level (DPL), DSCP, path CoS ID or Priority Code Point (PCP) value. Use the **no** form of this command to remove the mapping configuration from the Quality of Service (QoS) ingress map configuration. Variations of this command include:

map dscp *<value>* **to class** *<id>*
map dscp *<value>* **to cos** *<value>*
map dscp *<value>* **to dei** *<value>*
map dscp *<value>* **to dpl** *<value>*
map dscp *<value>* **to dscp** *<value>*
map dscp *<value>* **to path-cosid** *<id>*
map dscp *<value>* **to pcp** *<value>*

6.7.1 Syntax Description

map dscp *<value>*	Specifies the DSCP value used for traffic matching, and enters the mapping configuration to specify the new values assigned to traffic that matches the specified DSCP value. Valid range is **0** to **63**.
to	Specifies the classified values that are assigned when the key is matched and the action is enabled.
class *<id>*	Specifies the CoS ID value to be used by matching traffic. Valid range is **0** to **7**.
cos *<value>*	Specifies the CoS value to be used by matching traffic. Valid range is **0** to **7**.
dei *<value>*	Specifies the DEI value to be used by matching traffic. Valid range is **0** to **1**.
dpl *<value>*	Specifies the DPL value to be used by matching traffic. Valid range is **0** to **3**.
dscp *<value>*	Specifies the DSCP value to be used by matching traffic. Valid range is **0** to **63**.
path-cosid *<id>*	Specifies the path CoS ID value to be used by matching traffic. Valid range is **0** to **7**.
pcp *<value>*	Specifies the PCP value to be used by matching traffic. Valid range is **0** to **7**.

6.7.2 Default Values

By default, DSCP mapping is not configured for the QoS ingress map.

6.7.3 Command History

ASE Release 4.4-41	Command was introduced.

6.7.4 Functional Notes

The new values specified with this command can be entered in any order and multiple value types can be specified in a single command entry.

6.7.5 Usage Examples

To map the DSCP value of best effort (**be**) to a CoS ID value of **3** and a PCP value of **5** for traffic that matches the **dscp-pcp-dei** key specified in ingress map **20**, which is also configured with DEI and PCP value classification enabled, enter the command as follows:

```
(config)#qos map ingress 20
(config-qos-map-ingress)#key dscp-pcp-dei
(config-qos-map-ingress)#action dei pcp
(config-qos-map-ingress)#map dscp be to class 3 pcp 5
```

6.8 map pcp

Use the **map pcp** command to assign traffic with specific Priority Code Point (PCP) values a new Class of Service (CoS) ID, CoS, drop eligibility indicator (DEI), drop precedence level (DPL), Differentiated Service Code Points (DSCP), path CoS ID or PCP value. Use the **no** form of this command to remove the mapping configuration from the Quality of Service (QoS) ingress map configuration. Variations of this command include:

```
map pcp <value> to class <id>
map pcp <value> dei <value> to class <id>
map pcp <value> to cos <value>
map pcp <value> dei <value> to cos <value>
map pcp <value> to dei <value>
map pcp <value> dei <value> to dei <value>
map pcp <value> to dpl <value>
map pcp <value> dei <value> to dpl <value>
map pcp <value> to dscp <value>
map pcp <value> dei <value> to dscp <value>
map pcp <value> to path-cosid <id>
map pcp <value> dei <value> to path-cosid <id>
map pcp <value> to pcp <value>
map pcp <value> dei <value> to pcp <value>
```

6.8.1 Syntax Description

map pcp *<value>*	Specifies the PCP value used for traffic matching, and enters the mapping configuration to specify the new values assigned to traffic that matches the specified PCP value. Valid range is **0** to **7**.
dei *<value>*	Optional. Specifies a DEI value to which mapping also occurs. Valid range is **0** to **1**. If this parameter is not configured, then by default only mapping for DEI **0** is configured.
to	Specifies the classified values that are assigned when the key is matched and the action is enabled.
class *<id>*	Specifies the CoS ID value to be used by matching traffic. Valid range is **0** to **7**.
cos *<value>*	Specifies the CoS value to be used by matching traffic. Valid range is **0** to **7**.
dei *<value>*	Specifies the DEI value to be used by matching traffic. Valid range is **0** to **1**.
dpl *<value>*	Specifies the DPL value to be used by matching traffic. Valid range is **0** to **3**.
dscp *<value>*	Specifies the DSCP value to be used by matching traffic. Valid range is **0** to **63**.
path-cosid *<id>*	Specifies the path CoS ID value to be used by matching traffic. Valid range is **0** to **7**.
pcp *<value>*	Specifies the PCP value to be used by matching traffic. Valid range is **0** to **7**.

6.8.2 Default Values

By default, PCP mapping is not configured for the QoS ingress map.

6.8.3 Command History

ASE Release 4.4-41	Command was introduced.

6.8.4 Functional Notes

The new values specified with this command can be entered in any order and multiple value types can be specified in a single command entry.

6.8.5 Usage Examples

To map the PCP value of **4** and DEI value of **1** to a CoS ID value of **3** and a PCP value of **5** for traffic that matches the **dscp-pcp-dei** key specified in ingress map **20**, which is also configured with DEI and PCP value classification enabled, enter the command as follows:

```
(config)#qos map ingress 20
(config-qos-map-ingress)#key dscp-pcp-dei
(config-qos-map-ingress)#action dei pcp
(config-qos-map-ingress)#map pcp 4 dei 1 to cos 3 pcp 5
```

6.9 preset classes <*number*>

Use the **preset classes** <*number*> command to configure the Quality of Service (QoS) ingress map to automatically apply to a specific number of traffic classes. Use the **no** form of this command to remove the traffic class preset configuration from the ingress map. Variations of this command include:

```
preset classes <number>
preset classes <number> color-aware
```

6.9.1 Syntax Description

<*number*>	Specifies the number of traffic classes to which to apply the ingress map. Valid range is **1** to **8**.
color-aware	Optional. Enables color awareness for traffic intercepted by the ingress map.

6.9.2 Default Values

By default, traffic classes are not applied to QoS ingress map traffic.

6.9.3 Command History

ASE Release 4.4-41	Command was introduced.

6.9.4 Usage Examples

To add an ingress map to a number of traffic classes, enter the command as follows:

```
(config)#qos map ingress 20
(config-qos-map-ingress)#preset classes 5
```

Warranty

Warranty information can be found at:

www.adtran.com/warranty.

Contact Information

For all customer support inquiries, please contact ADTRAN Customer Care:

Department	Contact Information	
Customer Care	From within the U.S.: From outside the U.S.:	(888) 4ADTRAN ((888)-423-8726)+ +1 (256) 963-8716
Technical Support	Support Community Product Support:	www.supportcommu-nity.adtran.com www.adtran.com/support
Training	Email: ADTRAN University:	training@adtran.com www.adtran.com/training