61200860L1-29.3M
October 2015

Configuration Guide

Configuring Quality of Service in AOS

This configuration guide will aid in the setup of quality of service (QoS) for ADTRAN Operating System (AOS) products. An overview of QoS general concepts combined with detailed command descriptions and network examples provide step-by-step assistance for configuration. The troubleshooting section outlines proper use of **show** commands to verify that QoS has been configured properly on the AOS product(s). For detailed information regarding specific command syntax, refer to the *AOS Command Reference Guide* available online at https://supportforums.adtran.com.

This guide consists of the following sections:

QoS Overview

Today’s network traffic can be quite complex. Different types of traffic (routine data, real-time, and system-critical traffic, etc.) have specific needs for bandwidth, delay, and reliability. Routers must be able to recognize traffic types and service the traffic appropriately. QoS is used to appropriately allocate bandwidth, reduce packet delay, and ensure reliability for each data packet on the network. Each network must be analyzed to identify the specific types of traffic, and each traffic type must be handled according to its requirements. The following provides a quick glimpse at a few traffic types and the requirements necessary for each type of traffic.

> NOTE *Analyzing network traffic is a complex process and is beyond the scope of this document. The traffic discussion included here is generalized and may not include a comprehensive list of all traffic present on your network.*

Basic Traffic Types

The integration of data, voice, and video services onto a single packet-based IP infrastructure increases the complexity of traffic flowing on any given network. Each type of traffic has specific needs for optimum performance.

- **Traditional Data Traffic**
  Traditional data traffic can be greedy and bursty, requiring large amounts of bandwidth at any given time. However, data traffic is also less sensitive to dropped packets, as well as delay, making it a possible candidate for fragmentation on lower bandwidth links. Data packets can be fragmented into smaller pieces, transmitted, and reconstructed on the other side without damaging the integrity of the data. Breaking large data packets into smaller pieces allows them to be queued and gives other data on the network higher priority.
- **Real-Time Traffic**
  Real-time traffic requires smooth delivery through the network; it is very sensitive to dropped packets, as well as delay. Real-time traffic is generally low to medium bandwidth, but requires high priority to avoid degradation of the transmitted information. This type of traffic is classified as low-latency traffic (indicating that it requires low delay). For example, Voice over Internet Protocol (VoIP) traffic is real-time traffic that is sensitive to transmission delay and dropped packets. This traffic should be given priority to ensure that the quality of the voice is maintained through the network.
- **Critical Traffic**
  Critical traffic is information that must be sent to maintain proper operation of the network. Critical traffic is generally low bandwidth, but requires high priority. Routing updates, status messages, and alarm information are all good examples of critical traffic. By default, AOS reserves 25 percent of the allocated bandwidth for critical traffic. (You can change the reserve default on each interface using the **max-reserved-bandwidth** command.)

QoS mapping is used to give specific traffic classes higher (or possibly lesser) priority when transmitting on the router’s interface.

Types of Service

There are several types of service used to move traffic through a network. Each type provides a different level of priority for the packets being processed. They range from very simple theories, to more complex.

- **First In, First Out (FIFO)**
  The FIFO method is the most basic type of service. All packets are given the same best-effort service, where the first packet that arrives on an interface (first in) is the first packet forwarded (first out). During times of heavy traffic, this method must queue the excess packets and process them when bandwidth permits or drop them. This is not the best method to use if you want to consider a packet's level of importance when determining how to proceed.

  Fast caching can be used to speed up processing packets that travel often used routes. When a packet arrives on a fast-cache interface, the router interrupts its other processes to look up a route for the packet in the fast-cache table. This table contains the forwarding interfaces for the destinations of the most recently served packets. If a match is found, the packet is forwarded immediately. If a match is not found, the packet is queued.
- **Weighted Fair Queuing (WFQ)**
  WFQ is one method for granting differentiated service to packets with various IP type of service (ToS) bit values. When an interface uses WFQ, it classifies traffic flows into several subqueues according to source and destination IP addresses and protocol ports. The router then assigns each subqueue a weight according to its IP precedence value and a bandwidth relative to its weight. WFQ is the default queuing method on AOS router interfaces with a rate equal to or less than T1/E1.
- **Class-Based Weighted Fair Queuing (CBWFQ)**
  CBWFQ is an extension of WFQ that allows definition of classes according to user-defined criteria. The bandwidth can also be allocated to these classes manually. Each class is assigned an absolute or a relative amount of bandwidth instead of the router automatically assigning bandwidth to each subqueue based on relative IP precedence.
- **Low Latency Queuing (LLQ)**
  LLQ guarantees a set amount or a set percentage of bandwidth to certain types of traffic. LLQ also ensures that a router serves traffic in the low-latency queue first. This is a better solution than WFQ for real-time traffic, such as VoIP, that cannot tolerate jitter or delays.

Hardware and Software Requirements and Limitations

QoS is available on AOS products as outlined in the *AOS Product Feature Matrix*, located in the ADTRAN support community at https://supportforums.adtran.com. Some commands are interface specific and may not be available on all platforms listed. Use the context-sensitive help (type **?**) from the command line interface (CLI) to determine if a command is supported by your hardware platform.

IPv4 and IPv6 Address Support in AOS

The next generation Internet protocol require an increased number of available addresses to replace the current standard of Internet Protocol version 4 (IPv4). Due to its limiting 32-bit addressing, the available IPv4 address space is diminishing. Internet Protocol version 6 (IPv6) is emerging and can provide enough IP addresses for the foreseeable future, as well as many other benefits.

In the interest of supporting both IPv4 and IPv6 addresses in multiple networks, changes have been made to the AOS CLI. These changes affect QoS with the release of firmware R10.1.0 and, where applicable, are noted in this configuration guide. Some commands can be executed in multiple syntax structures to accommodate IPv4 addresses only, IPv6 addresses only, or both.

For more information, refer to *Configuring IPv6 in AOS* available online from ADTRAN's support community at https://supportforums.adtran.com.

Configuring QoS

There are two ways to configure QoS: (1) the CLI and (2) the web-based graphical user interface (GUI). Both configuration modes will be covered in this guide, beginning with *CLI Configuration on page 4* and followed by *GUI Configuration on page 25*.

The basis of configuring QoS requires defining a QoS policy with QoS map entries and applying the policy to an interface. A QoS map consists of multiple sequenced numbers using a common QoS map name. Each map entry has a unique sequence number. The sequence number has two functions:

- It identifies different entries in the same QoS map. For example, a single QoS map can establish several low-latency queues. It can also define multiple classes for traffic sharing the remaining bandwidth using CBWFQ. Each entry defines one low-latency queue or one class.
- It designates the order in which to match traffic. The QoS entries with the lowest number are searched first. Sequence numbers are only significant within the named map.

Each QoS map entry has at least one match statement (using the **match** command) and one or more action items (using the **priority**, **bandwidth**, **shape**, or **set** commands). Optionally, a separate, more specific child QoS map can be referenced from within the base or parent QoS map to further define actions on the traffic (as explained in *Subdividing Policy Classes on page 37*). The final step of configuring QoS is to apply the QoS map to the applicable interface.

The following is the minimum configuration required for QoS on an AOS product:

1. Create a QoS map.
2. Classify traffic using match criteria.
3. Apply an action to the matched traffic.
4. Assign the QoS map to the wide area network (WAN) interface.

CLI Configuration

To access the CLI on your AOS unit, follow these steps:

1. Boot up the unit.
2. Telnet to the unit (**telnet** <*ip address*>), for example:

   telnet 10.10.10.1.

> NOTE *If during the unit's setup process you have changed the default IP address (10.10.10.1), use the configured IP address.*

3. Enter your user name and password at the prompt.

> *The AOS default user name is* ***admin*** *and the default password is* ***password****. If your product no longer has the default user name and password, contact your system administrator for the appropriate user name and password.*

4. Enable your unit by entering **enable** at the prompt as follows:

```
>enable
```

5. If configured, enter your Enable mode password at the prompt.
6. Enter the unit's Global Configuration mode as follows:

```
#configure terminal
(config)#
```

Step 1: Create a QoS Map

A QoS map is a named list with sequenced entries each defined by a name and a number. QoS maps are used to define matched traffic and place the traffic in priority or class-based queues or other traffic groupings, such as shaped classes. In addition, QoS maps can be used to set differentiated services code point (DSCP) and IP precedence values. Each map entry contains one or more match statements and one or more actions. The actions are performed on traffic matching the QoS policy criteria.

You can create a single QoS map with multiple entries, but a unique sequence number is required to differentiate each entry. Using sequence numbers, for example, a single QoS map could establish a priority queue (also known as a low-latency queue) and multiple traffic classes for CBWFQ.

To create a QoS map and enter the QoS map configuration mode, enter the **qos map** <*name*> <*number*> **[match-all | match-any]** command from the Global Configuration mode. The <*name*> parameter specifies the QoS map name. The <*number*> parameter assigns a sequence number to differentiate this QoS map and provide a match order. Valid range is **0** to **65535**. The **match-all** keyword is optional and is used when defining QoS maps with multiple match conditions. Using match-all indicates the traffic must match all conditions before the set action is issued. (This modifier is rarely used or required.) The **match-any** modifier is optional and used when defining QoS maps with multiple match conditions. Using **match-any** indicates the traffic can match any of the conditions to be processed. This is the default behavior.

The following example creates a QoS map named **MY_VOICE**:

```
(config)#qos map MY_VOICE 10
(config-qos-map)#
```

Step 2: Classify Traffic Using Match Criteria

The **match** commands specify a parameter to which traffic on an interface with the active QoS policy is compared. QoS maps have a matching selector and an action (how the traffic should be handled) which make up the QoS policy. The special handling instructions contained in the QoS map action are applied to all packets that contain the specified match parameter.

Depending on your configuration, it could be necessary to configure multiple traffic matches from within one QoS map entry (map name and sequence number). Multiple match statements can exist within the same QoS map, allowing a single QoS map to service various types of traffic. The commands in this step specify which traffic should be processed by a particular QoS map.

Use the **match** commands shown in *Table 1 on page 6* to select traffic for the map entry. Read the following sections for explanations of the types of policies you can establish with the various **match** commands.

- *Match Any Packets on page 7*
- *Match by Access Control List on page 7*
- *Match by Frame Relay DLCI Value on page 7*
- *Match by Traffic Priority (DSCP or IP Precedence Value) on page 7*
- *Match by IP RTP on page 12*
- *Match by Protocol Bridge on page 13*
- *Match by Protocol on page 13*
- *Match by VLAN Identifier on page 13*

Table 1. QoS Map Match Commands

Command	Explanation
match any	Matches packets not matched in a previous map entry.
match [ip | ipv6] list *<list name>*	Matches IP traffic based on an extended access control lists (ACL). Use the **ip** keyword to match only IPv4 packets. Use the **ipv6** keyword to match only IPv6 packets.
match fr-dlci *<number>*	Matches traffic based on a Frame Relay data link connection identifier (DLCI) number.
match [ip | ipv6] dscp [af*xx* | **cs***x* | **default** | **ef |** *<value>***]**	Matches traffic based on DiffServ assured forwarding (AF), class selector (CS), default, expedited forwarding (EF), or numerical value (0 to 63). Use the **ip** keyword to match only IPv4 packets. Use the **ipv6** keyword to match only IPv6 packets. Omitting the keywords **ip** and **ipv6** will match both IPv4 and IPv6 packets.
match [ip | ipv6] precedence *<value>*	Matches traffic based on an IP precedence numerical value (0 to 7). Use the **ip** keyword to match only IPv4 packets. Use the **ipv6** keyword to match only IPv6 packets. Omitting the keywords **ip** and **ipv6** will match both IPv4 and IPv6 packets.
match ip rtp [*<port>* **|** *<begin port> <end port range>***] [all]**	Matches IPv4 traffic according to User Datagram Protocol (UDP) port destination. The optional **all** keyword is used to match even and odd UDP port numbers in the specified range and can only be used with IPv4 addresses.
match ipv6 rtp [*<port>* **|** *<begin port> <end port range>***]**	Matches IPv6 traffic according to UDP port destination.
match protocol bridge [netbeui]	Matches traffic being bridged by the router.
match protocol [ip | ipv6]	Matches traffic based on the specified protocol, either IPv4 or IPv6 packets. Use **ip** keyword to match only IPv4 packets. Use the **ipv6** keyword to match only IPv6 packets.
match vlan *<id>*	Matches traffic associated with a particular virtual local area network (VLAN). Indicate VLAN ID number 1 to 4095.
All of these commands are entered from the QoS Map Configuration mode.	

Match Any Packets

Packets not matched in a previous map entry can be matched using the **match any** command. This variation of the **match** command can also serve as a default case if it is specified as the last QoS map entry.

For example, the following command matches this QoS map to any traffic not matched previously:

```
(config)#qos map MY_VOICE 10
(config-qos-map)#match any
```

Match by Access Control List

Traffic can be matched based on a configured ACL. ACLs are traffic selectors that include a matching parameter (to select the traffic) and an action statement (to either permit or deny the matched traffic). The special handling instructions defined in the QoS map are applied to all packets allowed by the specified ACL. The ACL must be configured prior to creating and using QoS maps. Create an ACL to permit or deny specified traffic by using the **ip access-list extended** or **ipv6 access-list extended** commands as indicated in the *AOS Command Reference Guide*.

> NOTE
>
> *Only extended ACLs can be used with QoS.*

To match traffic based on an IPv4 ACL, use the **match ip list** <*ipv4 acl name*> command. To match traffic based on an IPv6 ACL, use the **match ipv6 list** <*ipv4 acl name*> command. For example, the following command matches the QoS map **MY_VOICE** to traffic using the IPv4 ACL **MATCHALL**:

```
(config)#qos map MY_VOICE 10
(config-qos-map)#match ip list MATCHALL
```

Match by Frame Relay DLCI Value

Traffic can be matched based on a Frame Relay DLCI number. The DLCI numbers can range from 16 to 1007. To match traffic based on the DLCI number, use the **match fr-dlci** <*number*> command. For example, the following command matches the QoS map **MY_VOICE** to traffic with the DLCI number **20**:

```
(config)#qos map MY_VOICE 10
(config-qos-map)#match fr-dlci 20
```

Match by Traffic Priority (DSCP or IP Precedence Value)

Every IPv4 header includes a ToS field that can be marked with various values to request a certain QoS for that packet. The ToS field can include either an IP precedence value or a DSCP value. IPv6 headers have an 8-bit traffic-class field serving the same purpose.

DSCP values (as specified by RFC 2474) are contained in six bits of the IPv4 or IPv6 header. A QoS map entry can specify up to eight DSCP values as matching criteria. If any one of the DSCP values match, the packet will be processed. DSCP values are explained in greater detail in *DSCP and IP Precedence Values Explained on page 9*.

> NOTE
>
> *Beginning with AOS firmware release R10.1.0, the **match dscp** command can be used to match both IPv6 and IPv4 packets simultaneously. To limit matching only IPv4 packets, use the **match ip dscp** command. To limit matching only IPv6 packets, use the **match ipv6 dscp** command.*

To match traffic based on the DSCP value in the IP header of both IPv4 and IPv6 packets, use the **match dscp [<*value*> | af*xx* | cs*x* | default | ef]** command. To match traffic based on the DSCP value in the IP header of only IPv4 packets, use the **match ip dscp [**<*value*> | **af***xx* | **cs***x* | **default** | **ef]** command. To match traffic based on the DSCP value in the IP header of only IPv6 packets, use the **match ipv6 dscp [**<*value*> | **af***xx* | **cs***x* | **default** | **ef]** command.

The valid range for <*value*> is **0** to **63**. AF class and subclass can be specified using the **af***xx* keyword. Select from the options shown in *Table 2*. CS value can be specified using the **cs***x* keyword. The valid range for CS is **1** to **7**. The **default** keyword indicates using the default IP DSCP value (000000). Matching the packets marked for EF is accomplished by using the **ef** keyword.

Table 2. Assured Forwarding DSCP Values

CLI Entry	DSCP Value
11	001010
12	001100
13	001110
21	010010
22	010100
23	010110
31	011010
32	011100
33	011110
41	100010
42	100100
43	100110

For example, the following command matches the QoS map **MY_VOICE** to IPv4 and IPv6 traffic with the DSCP value **46**:

```
(config)#qos map MY_VOICE 10
(config-qos-map)#match dscp 46
```

To remove a match DSCP statement, enter the command string with the **no** keyword, for example:

```
(config-qos-map)#no match dscp 46
```

Traffic can be matched by a specified IP precedence value in the IP header of IPv4 or IPv6 packets. IP precedence values (as specified by RFC 791) are contained in three bits of the IP header. IP precedence values are explained in greater detail in *DSCP and IP Precedence Values Explained on page 9*.

NOTE

*Beginning with AOS firmware release R10.1.0, the **match precedence** command can be used to match both IPv6 and IPv4 packets simultaneously. To limit matching only IPv4 packets, use the **match ip precedence** command. To limit matching only IPv6 packets, use the **match ipv6 precedence** command.*

To match traffic based on precedence value for IPv4 and IPv6 packets, use the **match precedence** <*value*> command. To match traffic based on precedence value for only IPv4 packets, use the **match ip precedence** <*value*> command. To match traffic based on precedence value for only IPv6 packets, use the **match ipv6 precedence** <*value*> command. The valid range for <*value*> is **0** to **7**, in ascending order of importance.

For example, the following command matches the QoS map **MY_VOICE** to IPv4 and IPv6 traffic with the IP precedence value **5**:

```
(config)#qos map MY_VOICE 10
(config-qos-map)#match precedence 5
```

DSCP and IP Precedence Values Explained

Private IP networks provide the best environment for controlling all QoS handling. The bandwidth and all the equipment that make up the network are under the customer’s control. Each piece can be programmed according to the needs of the network. Public IP networks, however, are less than ideal environments for proper QoS handling. RFC 791 created a single octet (labeled ToS in IPv4 packets and traffic-class in IPv6 packets) to help with the difficulty of trying to provide QoS handling in IP networks.

According to RFC 791, the ToS field contains the following bits:

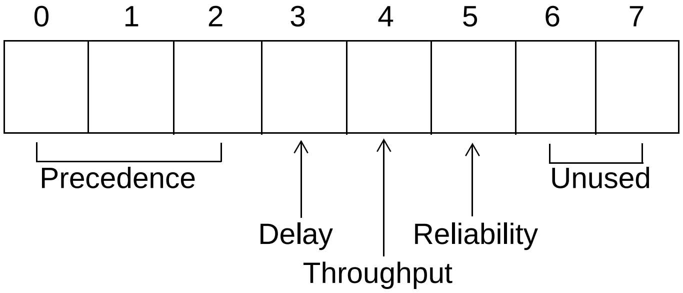


Figure 1. Type of Service Field Bits

The 3-bit IP precedence field is further defined in *Table 3 on page 9* from the highest value (7) to the lowest (0).

Table 3. IP Precedence Values

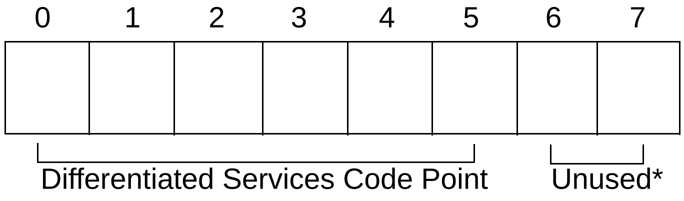
3-bit IP Precedence Value	Traffic
111	Network Control Packets
110	Internetwork Control Packets
101	Critical Traffic
100	Flash Override
011	Flash
010	Immediate Servicing
001	Priority Traffic
000	Routine Data

IP precedence values provide network routers with information about what kind of traffic is contained in the IP packet. Based on the IP precedence values, some networks (when supported) can offer special handling to certain packets. In addition, providing IP precedence values to critical traffic (such as route information) ensures that critical packets will always be delivered regardless of network congestion. This traffic is often critical to network and internetwork operation. In general, the higher the IP precedence value, the more important the traffic and the better handling it should receive in the network. It is important to remember that not all equipment in the public IP network will be configured to recognize and handle IP precedence values. Therefore, configuring an IP precedence value does not guarantee special handling.

In addition to IP precedence values, RFC 791 specifies bits for delay, throughput, and reliability to help balance the needs of particular traffic types when traveling on the IP network infrastructure. When these bits are set to 0, they are handled with normal operation. When set to 1, each bit specifies premium handling for that parameter. For example, a 1 in the delay position indicates that the traffic is delay sensitive and care should be taken to minimize delay. A 1 in the throughput position indicates that the traffic has higher bandwidth requirements that should be met. A 1 in the reliability position indicates that the traffic is sensitive to delivery issues and care should be taken to ensure proper delivery with all packets of this type. These extra bits are rarely used because it is quite difficult to balance the cost and benefits of each parameter (especially when more than one bit is set to 1).

The DS or DiffServ model was created in RFC 2474 and 2475 to build on the original ToS field by creating a 6-bit sequence (combining the IP precedence value with the delay, throughput, and reliability bits). This 6-bit sequence increased the number of available values from 8 to 64. The DiffServ model introduced a new concept to QoS in the IP network environment: per-hop behaviors (PHBs). The PHB premise is that equipment using the DiffServ model have an agreed upon set of rules (PHB types) for handling certain network traffic. Though the RFC explicitly defines what each PHB should be capable of, it does not restrict vendor-specific implementation of the PHBs. Each vendor is free to decide how their network product implements the various defined PHBs.

According to RFC 2474, the DS field contains the following bits:



* The previously unused bits in the DS field are now used for congestion control and are not discussed in this document.

Figure 2. Differentiated Services Field Bits

Equipment following the DiffServ model (DS-compliant nodes) must use the entire 6-bit DSCP value to determine the appropriate PHB. The PHBs are defined as default PHB, class selector PHB, assured forwarding PHB (RFC 2597), and expedited forwarding PHB (RFC 2598).

- **Default PHB**
  All DiffServ nodes must provide a default PHB to offer best-effort forwarding service. For default PHBs, the DSCP value is 0. Any packet that does not contain a standardized DSCP should be mapped to the default PHB and handled accordingly.
- **Class Selector PHB**
  In the class selector PHB, the first three bits in the DSCP value are used for backwards compatibility to systems implementing IP precedence. In this scenario, all but the first three bits of the DS field are set

to 0. This compatibility requires DiffServ nodes to provide the same data services as are provided by nodes implementing IP precedence. *Table 4* is a comparison of IP precedence values to their corresponding DSCP values.

Table 4. IP Precedence Values and Their Corresponding DSCP Values

IP Precedence Value (bits)	DSCP Value (bits)
0 (000)	0 (000000)
1 (001)	8 (001000)
2 (010)	16 (010000)
3 (011)	24 (011000)
4 (100)	32 (100000)
5 (101)	40 (101000)
6 (110)	48 (110000)
7 (111)	56 (111000)

- **Assured Forwarding PHB**
  The flexibility of DiffServ allows more developed subclasses of service within each main class using the last three bits of the DSCP. As defined in RFC 2597, the assured forwarding PHB creates four main classes of service (see *Table 5*.)

Table 5. Assured Forwarding PHB Classes of Service

Class	DSCP Bits
AF1	001XX0
AF2	010XX0
AF3	011XX0
AF4	100XX0
X indicates a do not care value	

The first three bits of the DSCP specify the class and the last bit is always zero. Each class is separated into subclasses using the two remaining bits in the DSCP (bits 3 and 4). The subclasses are divided based on the likelihood that packets in the class will be dropped in the event of network congestion. The higher the value for bits 3 and 4, the greater the likelihood that the packets will be dropped. (The bits are counted beginning with 0.)

Table 6. Assured Forwarding PHB Subclasses

Bit 3	Bit 4	Drop Precedence
0	1	Low
1	0	Medium
1	1	High

The following table lists the assured forwarding PHB subclasses and their corresponding DSCP bits and values.

Table 7. Assured Forwarding PHB Subclasses and Corresponding DSCP Values

Class	Subclass	DSCP Bits	DSCP Value
AF1	1	001010	10
	2	001100	12
	3	001110	14
AF2	1	010010	18
	2	010100	20
	3	010110	22
AF3	1	011010	26
	2	011100	28
	3	011110	30
AF4	1	100010	34
	2	100100	36
	3	100110	38

- **Expedited Forwarding PHB**
  RFC 2598 created a new DiffServ PHB intended to provide the best service possible on an IP network. Packets using the expedited forwarding PHB markings should be provided service to reduce latency, jitter, dropped packets, and be guaranteed bandwidth during the entire end-to-end transmission journey through the network. The DSCP value for the expedited forwarding PHB is 46 (DSCP bits are 101110).

Match by IP RTP

Realtime Transport Protocol (RTP) packets can be matched according to the specified UDP destination port number. This can be clarified further to include only even port numbers from a specific range by including the beginning port number and an ending port number. (Typically servers listen for RTP user traffic on even ports.) The **all** keyword is used to match even and odd UDP port numbers in the specified range and can only be used with IPv4 addresses. This command could be used to define a CBWFQ class, however, it selects real-time traffic which generally should use a low-latency queue.

To match traffic based on the UDP port destination of the IPv4 packet, use the **match ip rtp [***<port>* **|** *<begin port> <end port range>***] [all]** command. To match traffic based on the UDP port destination of the IPv6 packet, use the **match ipv6 rtp [***<port>* **|** *<begin port> <end port range>***]** command. Valid entries for *<port>*, *<begin port>*, and *<end port range>* are **0** through **65535**.

For example, the following command matches the QoS map **MY_VOICE** to IP RTP traffic destined for all ports from **16384** to **32764**:

```
(config)#qos map MY_VOICE 10
(config-qos-map)#match ip rtp 16384 32764 all
```

Match by Protocol Bridge

Traffic being bridged by the router can be included in a class for the purpose of setting maximum bandwidth for that class. This traffic is classified by using the **match protocol bridge** command. To match traffic based on protocol bridge, use the **match protocol bridge [netbeui]** command.

For example, the following command matches the QoS map **MY_VOICE** to bridged traffic:

```
(config)#qos map MY_VOICE 10
(config-qos-map)#match protocol bridge
```

Instead of including all bridged traffic, you can specify to include only NetBIOS Extended User Interface (NetBEUI) traffic. NetBEUI is an uncommon protocol that allows hosts to communicate within a local area network (LAN).

Match by Protocol

Matching IPv4 or IPv6 packets based on a specified protocol using the **match protocol** command is most useful when used in conjunction with another match case to further specify filtering in a general case. When configuring this option, specify **match-all** for the QoS map entry to require all matches to be true, since **match-any** is the default. To match IPv4 traffic based on protocol, use the **match protocol ip** command. To match IPv6 traffic based on protocol, use the **match protocol ipv6** command.

For example, the following command matches the QoS map **MY_VOICE** to IPv4 traffic:

```
(config)#qos map MY_VOICE 10 match-all
(config-qos-map)#match protocol ip
```

Match by VLAN Identifier

Packets associated with a particular VLAN can be matched using the **match vlan** <*id*> command. The valid entry for <*id*> is an identifier from **1** to **4095**. For example, the following command matches the QoS map **MY_VOICE** to traffic associated with VLAN 3:

```
(config)#qos map MY_VOICE 10
(config-qos-map)#match vlan 3
```

Step 3: Apply an Action to the Matched Traffic

Once traffic is matched, its handling method must be determined. This step involves applying an action to the traffic matching the criteria in Step 2. Multiple actions can be applied to the packets. These actions include allocating class-based queues, priority or low-latency queues, using the **set** command to mark packets, and applying traffic shaping. Each one serves a different purpose and is described in greater detail in the following sections.

- *Bandwidth Commands on page 14*
- *Priority Commands on page 19*
- *Packet Marking (Optional) on page 21*
- *Configure Traffic Shaping (Optional) on page 22*

Even though limits are defined regarding bandwidth consumption of traffic in a QoS map, traffic can burst up to the maximum interface rate when the output queue is not in a congested state. QoS maps are classifying traffic constantly when they are active on an interface, but some of their actions depend on the state of the output queue. When congestion is present, policies defined with the **bandwidth** command will be limited to the minimum value specified while excess traffic is queued. During a congested state, policies defined with the **priority** command will be limited to the maximum value specified while excess traffic is dropped. Policies defined with the **shape** or **set** commands are always enforced regardless of congestion.

Bandwidth Commands

The **bandwidth** commands are used to specify the bandwidth allocation for individual traffic classes. This is referred to as CBWFQ. Bandwidth for CBWFQ is allocated from the available interface bandwidth minus any bandwidth allocated to a priority queue (using the **priority** command).

When configuring **bandwidth** allocations for CBWFQ, there are a few rules that must be obeyed.

1. The units of the bandwidth (**Kbps**, **Mbps**, **percent**, or **remaining percent**) must be consistent for all class-based entries (using the **bandwidth** command) in a QoS map set.
2. The total bandwidth between all priority entries (**priority** command) and class-based entries (**bandwidth** command) in a QoS map set should not exceed the specified **max-reserved-bandwidth** (default **75** percent) on the interface to which the QoS policy is applied (using the **qos-policy** command), or the map will be disabled. When the configured QoS map is applied to a physical interface, AOS displays bandwidth information for the map and the physical interface. For example, if the Frame Relay interface (**fr 1**) has been connected to the E1 subinterface (**e1 1/1**) using the **cross-connect** command, applying the QoS map (**MY_MAPA**) to the Frame Relay interface (**fr 1**) produces the following status message:

   ```
   2005.08.09 07:28:22 QOS.INTERFACE QOS policy “MY_MAPA” requires 1288 Kbps of bandwidth and 1488 Kbps is now available for interface fr 1 -> the QOS policy for this port has been forced ACTIVE.
   ```

   This status message displays the total of the bandwidths specified in the QoS map (1288 Kbps) and the available interface bandwidth using the total line rate configured on the interface multiplied by the value of the **max-reserved-bandwidth** (1488 Kbps).
3. Up to eight class-based entries (**bandwidth** commands) can be configured in a particular QoS map set.
4. Within a QoS map entry, CBWFQ bandwidth and low-latency priority actions are mutually exclusive. However, **bandwidth** and **priority** actions can be applied to different entries in the same QoS map.

To set an absolute amount of bandwidth, use the **bandwidth** *<rate>* **[Kbps | Mbps]** command. The valid range for **bandwidth** *<rate>* is **8** to **2000000** Kbps. The bandwidth rate is assumed to be provided in Kbps unless **Mbps** is specified. The **Kbps** parameter for this command is optional.

For example, to specify a total of 512 Kbps of available bandwidth, enter the following command:

```
(config-qos-map)#bandwidth 512
```

Determining Bandwidth Entries

> NOTE
>
> *When possible, use the **bandwidth** <rate> command to specify an absolute amount of bandwidth for a traffic class.*

When determining the **percent** <*value*> entry, use the following formula:

$$\frac{\text{Bandwidth}}{\text{Line Rate}} \quad \text{x } 100$$

where

Bandwidth Specifies the minimum amount of bandwidth needed for the traffic (in Kbps).

Line Rate Specifies the total data rate configured on the interface (for example, 8 DS0s (64 Kbps per DS0) on a T1 equals a line rate of 512 Kbps).

> NOTE
>
> *The **max-reserved-bandwidth** command is set from the interface configuration mode. By default, it is set to **75** percent, which reserves 25 percent of the interface bandwidth for system-critical and best-effort traffic. Refer to the AOS Command Reference Guide for more information on this command.*

> NOTE
>
> *The **traffic-shape rate** <rate> command is required for VLAN and Ethernet WAN IP interfaces to set the upload speed of the connection, which enables QoS to be enforced. When this value is specified, it will replace the Line Rate in the previous formula.*

> NOTE
>
> *In the previous formula, if the **bandwidth** <rate> command has been applied to the IP interface, the Line Rate would be replaced with the bandwidth rate configured on the interface. If the **bandwidth** <rate> command is applied to a VLAN or Ethernet WAN IP interface, it will override the value set in the **traffic-shape rate** command for QoS calculations. Applying the **bandwidth** <rate> to an IP interface reduces the amount of bandwidth available for QoS and therefore, is not recommended. Instead, use the **max-reserved-bandwidth** command to adjust the bandwidth appropriately.*

To set the bandwidth percentage, use the **bandwidth percent** <*value*> command. For example, to specify 76.8 Kbps of data on an interface with a total of 512 Kbps of available bandwidth, and reserving 5 percent of the bandwidth for best effort, routing, and Layer 2 protocol traffic (**max-reserved-bandwidth** = 95) enter the following commands:

```
(config-qos-map)#bandwidth percent 15
(config)#interface ethernet 0/1
(config-eth 0/1)#max-reserved-bandwidth 95
```

Guidelines may be necessary for using the remaining bandwidth available on an interface after priority traffic and CBWFQ traffic (specified using the **bandwidth percent** command). Since all bandwidth statements in the QoS map must use the same units, when using remaining percent, all bandwidth statements share unallocated bandwidth on the interface at a level proportional to their specified values. Using the **bandwidth remaining percent** command to specify bandwidth for a class does not guarantee absolute bandwidth.

When determining the **remaining percent** <*value*> entry, use the following formula:

$$\frac{\text{Bandwidth}}{\text{Line Rate}} \quad \text{x } 100$$

where

Bandwidth Specifies the minimum amount of bandwidth needed for the traffic (in Kbps).

Line Rate Specifies the total data rate configured on the interface (for example, 8 DS0s (64 Kbps per DS0) on a T1 equals a line rate of 512 Kbps).

To set the remaining bandwidth percentage, use the **bandwidth remaining percent** <*value*> command. For example, to specify 76.8 Kbps of data on an interface with a total of 512 Kbps of available bandwidth, 256 Kbps reserved (using the **priority** command), and reserving 15 percent of the bandwidth for best effort, routing, and Layer 2 protocol traffic (**max-reserved-bandwidth** = 85) enter the following commands:

```
(config-qos-map)#bandwidth remaining percent 15
(config)#interface ethernet 0/1
(config-eth 0/1)#max-reserved-bandwidth 85
```

Setting the Bandwidth for a Queue on a Multilink Interface

Multilink protocols, such as Multilink PPP (MLPPP) and Multilink Frame Relay (MLFR), increase the total bandwidth of a connection by bundling multiple carrier access lines into a single logical connection. Because carrier lines may go down and change the current available bandwidth, allocating bandwidth on a multilink interface requires special consideration.

For example, an MLPPP connection with two T1 lines provides 3.072 Mbps of bandwidth. If you use the default **max-reserved-bandwidth** of 75 percent, you can allocate 2.304 Mbps of the interface bandwidth to QoS queues. Consider the following CBWFQ scenario (shown in *Table 8*) using the **bandwidth** command to allocate a specified amount of bandwidth (in Kbps) for each class:

Table 8. Multilink Interface Bandwidth Allocation Example

Class	Bandwidth (in Kbps)
Class 1	307 Kbps
Class 2	614 Kbps
Class 3	614 Kbps
Class 4	768 Kbps

In this scenario, if one of the T1 lines fails, the connection only has 1.536 Mbps of available bandwidth of the original guaranteed 2.304 Mbps. Interfaces are evaluated every 30 seconds to verify that there is sufficient available bandwidth for the QoS configuration. In this case, the QoS map would be disabled due to insufficient available bandwidth on the interface.

To help avoid this situation, consider allocating bandwidth to the multilink connection as if it had one carrier line less than the total. This is particularly true when the multilink is designed more to provide redundancy than to increase a connection’s bandwidth.

Using the **bandwidth percent** or **bandwidth remaining percent** commands can also safeguard against a QoS map on a multilink being disabled due to insufficient available bandwidth. The **bandwidth percent** and **bandwidth remaining percent** commands provide guidelines on how to allocate available bandwidth, but do not provide guaranteed bandwidth to a class. Consider the CBWFQ scenario using the **bandwidth percent** command as outlined in *Table 9 on page 17*.

Table 9. Multilink Interface Bandwidth Percent Allocation Example

Class	Percent	Bandwidth (in Kbps)
Class 1	10	307 Kbps
Class 2	20	614 Kbps
Class 3	20	614 Kbps
Class 4	25	768 Kbps

In this scenario (shown in *Table 10*), if one of the T1 lines fails, the connection only has 1.536 Mbps of available bandwidth of the original guaranteed 2.304 Mbps. When this occurs, the following adjustment to the QoS bandwidth allocation is made:

Table 10. QoS Bandwidth Adjustment with Single T1

Class	Percent	Bandwidth in Kbps (during normal operation)	Bandwidth in Kbps (with a single T1)
Class 1	10	307 Kbps	154 Kbps
Class 2	20	614 Kbps	307 Kbps
Class 3	20	614 Kbps	307 Kbps
Class 4	25	768 Kbps	384 Kbps

Though the bandwidth available for each class is smaller than originally requested, the QoS map is still active and the relative priority among the classes is maintained.

Now, consider the following CBWFQ scenario (shown in *Table 11*) using the **bandwidth remaining percent** command:

Table 11. Multilink Interface Bandwidth Remaining Percent Allocation Example

Class	Remaining Percent	Bandwidth in Kbps (during normal operation)
Class 1	13	292.5 Kbps
Class 2	27	607.5 Kbps
Class 3	27	607.5 Kbps
Class 4	33	742.5 Kbps

In this scenario (shown in *Table 12*), if one of the T1 lines fails, the connection only has 1.536 Mbps of available bandwidth of the original guaranteed 2.304 Mbps. When this occurs, the following adjustment to the QoS bandwidth allocation is made:

Table 12. QoS Bandwidth Adjustment with Single T1

Class	Remaining Percent	Bandwidth in Kbps (during normal operation)	Bandwidth in Kbps (with a single T1)
Class 1	13	292.5 Kbps	195 Kbps
Class 2	27	607.5 Kbps	405 Kbps
Class 3	27	607.5 Kbps	405 Kbps
Class 4	33	742.5 Kbps	495 Kbps

Though the bandwidth available for each class is smaller than originally configured, the QoS map is still active and the relative priority among the classes is maintained.

Special Consideration for Layer 1 Available Bandwidth

It is important to note that there is an order of precedence in determining the interface bandwidth reported by the router for QoS. Under normal circumstances, the Layer 1 bandwidth is reported based on the interface type. For example, a T1 interface will report the available bandwidth as 1.536 Mbps. This could be misleading if the bandwidth command has been applied to the IP interface for routing purposes. The Layer 1 bandwidth can be reduced by using the **bandwidth** command issued in the interface configuration mode. This overrides the reported available bandwidth that can be utilized for QoS. It is not a common occurrence in network configurations and is strongly discouraged if you plan to use QoS on the same interface. It can severely disrupt the configuration of QoS bandwidth mentioned in this section.

Shaping Traffic at the Interface Level

One configuration that could alter your available interface bandwidth is shaping applied to an Ethernet or VLAN interface. If only interface-level shaping is required, then the interface **traffic-shape rate** command can be used to set up shaping without applying a QoS map. If it is applied to the same interface that will also have a QoS map applied to it, the amount of bandwidth available for the QoS policy is reduced to the value set with the **traffic-shape rate** command. This value should be set to match the upload speed of the circuit. For example, under normal circumstances, an Ethernet interface can negotiate to 100 Mbps. However, the throughput of the upstream equipment is usually significantly less than the negotiated rate. The **traffic-shape rate** command is used to define the limit of when QoS policies containing the **bandwidth** or **priority** commands should be enforced according to the upload speed of the circuit.

If the **bandwidth** <*rate*> command (discussed in *Special Consideration for Layer 1 Available Bandwidth on page 18*) is also entered on the same IP interface as the **traffic-shape rate** command, it will overwrite the value of the **traffic-shape rate** command for QoS purposes. As described in the previous section, it is not recommended to use the **bandwidth** <*rate*> command for QoS. However, the **traffic-shape rate** command is required for QoS to function properly on VLAN and Ethernet WAN IP interfaces.

For more information about the **traffic-shape rate** command, refer to the *AOS Command Reference Guide* available online at https://supportforums.adtran.com.

Priority Commands

The **priority** command provides a low-latency queue that prioritizes the selected traffic above all other user traffic. If no other traffic is present in any other queue on the interface, priority traffic is allowed to burst up to the interface rate. Otherwise, priority traffic above the specified bandwidth will be dropped. Priority queues are intended for constant bit rate (CBR) traffic, such as voice (due to the rate limiting). Non-CBR traffic typically does not respond well to packet dropping when it is rate limited, so the transfer rate can be much less efficient.

> NOTE *The **priority** command cannot be specified in conjunction with the **shape average** command in a QoS map entry.*

The sum of the bandwidths reserved by **priority** and **bandwidth** commands for all entries in parent and child QoS maps cannot exceed the available bandwidth on the interface (calculated by the total interface bandwidth multiplied by the **max-reserved-bandwidth** specified for the interfaces to which the QoS map is applied). Priority bandwidth is guaranteed bandwidth (in Kbps).

> NOTE *WFQ must be enabled on an interface to use priority queuing. By default, WFQ is enabled for all interfaces with maximum bandwidth speeds equivalent to T1/E1 and below.*

Bandwidth in a priority queue can be specified as an absolute value (using the **priority** command) or as a percentage of the total interface bandwidth (using the **priority percent** command). When possible, use the **priority** command to specify an absolute amount of bandwidth (in **Kbps** or **Mbps**) for the priority queue. The bandwidth rate is assumed to be provided in Kbps unless **Mbps** is specified. The **Kbps** parameter for this command is optional.

To specify an absolute value (in Kbps or Mbps) allocated to the priority queue on the interface, use the **priority** *<rate>* **[Kbps** | **Mbps] [***<burst size>***] [Bytes | KB | MB] [strict-rate-limiting]** command. The valid range for *<rate>* is **8** to **1000000** Kbps and for *<burst size>* from **32** to **1000000** bytes. The **strict-rate-limiting** keyword (when used with **priority** command) limits priority traffic to a maximum rate as specified by the *<rate>* variable.

For example, the following command provides 64 Kbps of bandwidth in a priority queue for traffic matching the defined pattern:

```
(config-qos-map)#priority 64
```

Additionally, the **priority unlimited** command specifies that no rate limiting is performed on traffic contained in the priority queue.

> CAUTION *Use the **priority unlimited** command with extreme caution because it could prevent vital Layer 2 traffic from being processed. A network outage could occur when excessive priority traffic is present and consumes all of the available bandwidth on the interface.*

For example, the following command configures an unlimited bandwidth for the applicably matched traffic:

```
(config-qos-map)#priority unlimited
```

The **priority percent** command can be used in applications with multilink interfaces to avoid having the QoS map disabled (due to inadequate interface bandwidth) in the event that one link in the multilink bundle fails. The optional <*burst size*> parameter specifies the maximum burst size (in **Bytes**, **KB**, or **MB**) for traffic in the priority queue. The burst size is assumed to be provided in bytes unless **KB** or **MB** is specified. The <*burst size*> parameter should be left unconfigured in most situations for optimal performance.

> NOTE
>
> *The **priority percent** command cannot specify a value greater than the value set for the **max-reserved-bandwidth** on the interface on which the QoS map will be used. The **priority percent** is calculated from the total interface bandwidth instead of the total amount of bandwidth allocated for use with QoS.*

To set the bandwidth to a percentage of the total interface, use the **priority percent** <*value*> **[**<*burst size*>**] [Bytes | KB | MB] [strict-rate-limiting]** command. The valid range for <*value*> is **1** to **100** percent and the valid range for <*burst size*> is **32** to **1000000** bytes. The **strict-rate-limiting** keyword (when used with **priority percent** command) specifies a limit on priority traffic to a maximum percentage of the interface bandwidth as specified by the <*value*> variable.

For example, to specify 80 Kbps of data on an interface with a total of 512 Kbps of available bandwidth, enter the following command:

```
(config-qos-map)#priority percent 16
```

Determining Bandwidth Entries

> NOTE
>
> *When possible, use the **priority** <rate> command to specify an absolute amount of bandwidth (in Kbps) for the priority queue.*

When determining the **priority percent** <*value*> entry, use the following formula:

$$\frac{\text{Bandwidth}}{\text{Line Rate}} \times 100$$

where

Bandwidth Specifies the minimum amount of bandwidth needed for the traffic (in Kbps).

Line Rate Specifies the total data rate configured on the interface (for example, 8 DS0s (64 Kbps per DS0) on a T1 equals a line rate of 512 Kbps).

> NOTE
>
> *The **max-reserved-bandwidth** command is set from the interface configuration mode. By default, it is set to **75** percent, which reserves 25 percent of the interface bandwidth for system-critical traffic. Refer to the AOS Command Reference Guide for more information on this command.*

NOTE *The **traffic-shape rate** <rate> command is required for VLAN and Ethernet WAN IP interfaces to set the upload speed of the connection, which enables QoS to be enforced. When this value is specified, it will replace the Line Rate in the previous formula.*

NOTE *In the previous formula, if the **bandwidth** <rate> command has been applied to the IP interface, the Line Rate would be replaced with the bandwidth rate configured on the interface. If the **bandwidth** <rate> command is applied to a VLAN or Ethernet WAN IP interface, it will override the value set in the **traffic-shape rate** command for QoS calculations. Applying the **bandwidth** <rate> to an IP interface reduces the amount of bandwidth available for QoS and therefore, is not recommended. Instead, use the **max-reserved-bandwidth** command to adjust the bandwidth appropriately.*

For example, to specify 76.8 Kbps of data on an interface with a total of 512 Kbps of available bandwidth, enter the following command:

```
(config-qos-map 1)#priority percent 15
```

Packet Marking (Optional)

The **set** commands are used for packet marking, allowing changes to be made to the class of service (CoS) value, DSCP field, or IP precedence value for outgoing traffic serviced by the QoS policy. Every IPv4 header contains an 8-bit ToS field used for marking packets requiring special handling instructions for the next-hop router. IPv6 headers have an 8-bit traffic-class field serving the same purpose. Originally, this ToS field was used for IP precedence markings (using only the first three bits of the 8-bit field), but was later revised in RFC 2474 to create the 6-bit DSCP field (reserving the last two bits of the field for future use). The DSCP field can be manipulated to indicate higher or lower traffic priority using a value between 0 and 63. DSCP and precedence remarking can be applied to both IPv4 and IPv6 packets. For more details on determining DSCP values, refer to *DSCP and IP Precedence Values Explained on page 9*.

To change the CoS value on matching packets, use the **set cos** *<value>* **command.** The valid range for *<value>* is **0** to **7**. For example, the following command sets the CoS value for all matching traffic to **5**:

```
(config-qos-map)#set cos 5
```

To change the DSCP field on matching packets, use the **set dscp [***<value>* **| af***xx* **| cs***xx* **| default | ef]** command. The valid range for *<value>* is **0** to **63**. AF class and subclass can be specified using the **af***xx* keyword. Select from the options shown in *Table 2 on page 8*. CS value can be specified using the **cs***x* keyword. The valid range for CS is **1** to **7**. The **default** keyword indicates using the default IP DSCP value (000000). Matching the packets marked for EF is accomplished by using the **ef** keyword.

For example, the following command sets the DSCP value for all matching traffic to **46**:

```
(config-qos-map)#set dscp 46
```

To change the IP precedence value on matching packets, use the **set precedence** *<value>* command. The valid range for *<value>* is **0** to **7**. For example, the following sets the IP precedence value for all matching traffic to **1**:

```
(config-qos-map)#set precedence 1
```

NOTE *Beginning with AOS firmware release R10.1.0, the **set dscp** and **set precedence** commands apply remark packet DSCP and precedence values to all IPv4 and IPv6 packets that match the QoS map entry. In order to mark a particular version of traffic, it is necessary to create a QoS map match for that particular version.*

Configure Traffic Shaping (Optional)

Once traffic is matched in a QoS map, traffic shaping can be applied. Traffic shaping allows the traffic to be smoothed in order to maintain a uniform rate to take advantage of the provided bandwidth. Short bursts of traffic above the configured rate are allowed when there is sufficient budget. Traffic outside the current budget is put into a shaping queue and transmitted once the budget is available.

To specify the traffic shaping for a QoS map, use the **shape average** <*rate*> [**bps** | **Kbps** | **Mbps**] [**burst** <*size*>] [**Bytes** | **KB** | **MB**] [**count-eth-overhead**] command. The average bandwidth is specified as bits per second (bps), Kbps, or Mbps and the valid range for <*rate*> is **8192** to **1000000000**. The maximum burst size is specified in bytes, KB, or MB and the **burst** <*size*> valid range is **1600** to **6250000**. This parameter should be left unconfigured for optimal performance. The **count-eth-overhead** keyword is optional and specifies to include the Ethernet header overhead bytes when determining packet size.

For example, the following command specifies an average bandwidth of 768000 bps:

```
(config-qos-map)#shape average 768000
```

NOTE *A maximum of five different traffic shapers per QoS map can be defined using the **shape average** command.*

Configure Traffic Policing (Optional)

Once traffic is matched in a QoS map, traffic policing can be applied. Traffic policing allows traffic exceeding a specified committed information rate (CIR) or committed burst size (CBS) threshold to be dropped. This type of QoS map is used on ingress and egress traffic on a tunnel interface.

To specify the policing for a QoS map, use the **police cir** <*rate*> [**bps** | **Kbps** | **Mbps**] [**cbs** <*size*>] [**Bytes** | **KB** | **MB**] [**count-eth-overhead**] command. The maximum CIR is specified as bits per second (bps), Kbps, or Mbps and the valid range for **cir** <*rate*> is **8192** to **1000000000**. The maximum CBS size is specified in bytes, KB, or MB and the **cbs** <*size*> valid range is **1600** to **6250000**. The **count-eth-overhead** keyword is optional and specifies to include the Ethernet header overhead bytes when determining packet size.

For example, the following command specifies a CIR of 768000 bps:

```
(config-qos-map)#police cir 768000
```

NOTE *If traffic policing is configured in the QoS map, other QoS map configurations (aside from **match any**), are not allowed in the QoS map. If other QoS configurations are included in the map, when it is associated with the tunnel interface, it will be rejected.*

Step 4: Assign the QoS Map to the Interface

Once created, a QoS map must be applied to an interface in order to actively process traffic. QoS maps can be applied independently to inbound and outbound traffic traversing the interface. Inbound traffic that needs to be matched to set a DSCP value, as shown in *Example 4: Multi Tenant on page 42*, requires a QoS map to be assigned to the interface using the **qos-policy in** command. Outbound traffic that needs to be given priority over other traffic leaving the router, as shown in *Example 2: CBWFQ Ethernet WAN on page 39*, requires a QoS map assigned to the interface using the **qos-policy out** command. There are many different configurations where QoS maps are necessary on only inbound or outbound traffic. These are just a couple of examples for your understanding of the command usage.

> NOTE
>
> *QoS maps applied to inbound traffic only function with Ethernet interfaces.*

> CAUTION
>
> *Applying a QoS Map to a PPP or demand interface will cause the interface to drop briefly. This causes a temporary service interruption and the interface should come back up momentarily.*

To apply the QoS map to an interface for incoming packets, enter the **qos-policy in** <*name*> command or to apply the QoS map to outgoing packets, enter the **qos-policy out** <*name*> command. The <*name*> parameter specifies the QoS map name and should already be configured.

The following command applies the QoS map **MY_VOICE** to the output of the Frame Relay interface:

```
(config)#interface fr 1
(config-fr 1)#qos-policy out MY_VOICE
```

> NOTE
>
> *QoS maps containing **bandwidth**, **priority**, or **shape** commands cannot be applied to Ethernet subinterfaces. Instead, a QoS map should be applied to the main Ethernet interface that matches based on the VLAN ID or an ACL applicable to the desired Ethernet subinterface.*

If more than one QoS map is used in the configuration, such as with additional subclasses, the **qos-policy out** command is only used to apply the parent or base map to the interface. Refer to *Subdividing QoS Classes on page 24* for more information on subclasses.

Traffic leaving the WAN interface that is not specified in the QoS map is sent using WFQ. All queuing and QoS packet reorganization takes place on the egress WAN interface.

> NOTE
>
> *Apply a QoS map name (not a sequence number) to the WAN interface. All QoS maps with the same name are searched by the interface in order, based on the sequence number (from lowest to highest). The same QoS map can be applied to multiple interfaces.*

Additional Settings Using the CLI

The following section provides information about additional settings not covered in the previous steps. These settings may pertain to your particular configuration.

Subdividing QoS Classes

The **qos-policy** command can also be used within a QoS map to further subdivide a class into more specific subclasses. The most specific QoS map (or child map) is created first and then the map is referenced using the **qos-policy** command within the QoS map entry of the base (or parent) map that is being subdivided. The base (or parent) map is applied to the QoS capable interface using the **qos-policy out** command (shown in *Step 4: Assign the QoS Map to the Interface on page 23*).

Only two levels of maps are allowed, which means child maps (or subclasses) cannot be further subdivided. A child map cannot reference another child map. If the child map is deleted, then the parent map is also deleted.

For example, the following configuration uses the **SHAPEPVCS** QoS map to constrain each PVC's traffic to specific rates. The PVC DLCI 16 traffic that is put into the shaping queue is then broken up into class-based queuing (CBQ) or LLQ subclasses using the **CLASSQUEUES** QoS map. Traffic not matching a QoS map entry is treated as best effort, and is dynamically assigned to a best-effort WFQ.

```
(config)#qos map CLASSQUEUES 10
(config-qos-map)#match dscp ef
(config-qos-map)#priority 200

(config-qos-map)#qos map CLASSQUEUES 20
(config-qos-map)#match dscp af31 af32 af33
(config-qos-map)#bandwidth 300            ! class based rate in Kbps

(config-qos-map)#qos map SHAPEPVCS 10
(config-qos-map)#match fr-dlci 16
(config-qos-map)#shape average 768000    ! dlci 16 shape rate in bps
(config-qos-map)#qos-policy CLASSQUEUES

(config-qos-map)#qos map SHAPEPVCS 20
(config-qos-map)#match fr-dlci 17
(config-qos-map)#shape average 768000    ! dlci 17 shape rate in bps

(config-qos-map)#interface frame-relay 1
(config-fr 1)#qos-policy out SHAPEPVCS
(config-fr 1)#exit

(config)#interface frame-relay 1.16
(config-fr 1.16)#frame-relay interface-dlci 16
(config-fr 1.16)#exit

(config)#interface frame-relay 1.17
(config-fr 1.17)#frame-relay interface-dlci 17
```

GUI Configuration

The GUI is an especially useful tool for those who are less familiar with CLI configuration. AOS products ship with a user-friendly GUI that can be used to perform many basic management and configuration functions on the AOS product. Some advanced options can be configured using the GUI as well. A QoS Wizard is provided to initially set up and begin using QoS. This section will explain how to access the GUI, how to use the QoS Wizard, and the necessary steps to manually configure QoS using the GUI.

Accessing the GUI

To begin configuring QoS through the GUI, follow these steps to access the GUI:

1. Open a new web page in your browser.
2. Enter your AOS product's IP address in the browser's address field, **http://**<*ip address*>, for example:

   http://65.162.109.200
3. At the prompt, enter your user name and password and select **OK**.

> NOTE *The default user name is **admin** and the default password is **password**.*

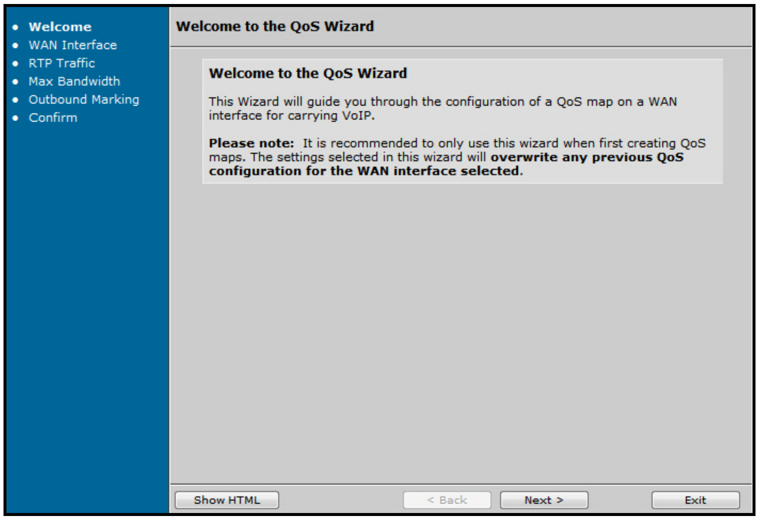
Using the QoS Wizard

The QoS Wizard will guide you through creation of a QoS map on a WAN interface for the purpose of carrying VoIP. If you are configuring QoS for another purpose, it is best to use the steps described in *Manually Configuring QoS Using the GUI on page 29*.

> NOTE *ADTRAN recommends using the QoS Wizard when first setting up QoS maps before any other QoS configuration is undertaken. The settings selected in the QoS Wizard will overwrite any previous QoS configuration for the WAN interfaces.*

Step 1: Welcome to the QoS Wizard

Navigate to **Data** > **Router/Bridge** > **QoS Wizard**. The QoS Wizard welcome menu will appear. At any time while using the QoS Wizard, you can return to a previous screen by selecting the links in the upper left corner. Select **Next** to begin configuration.



Welcome to the QoS Wizard

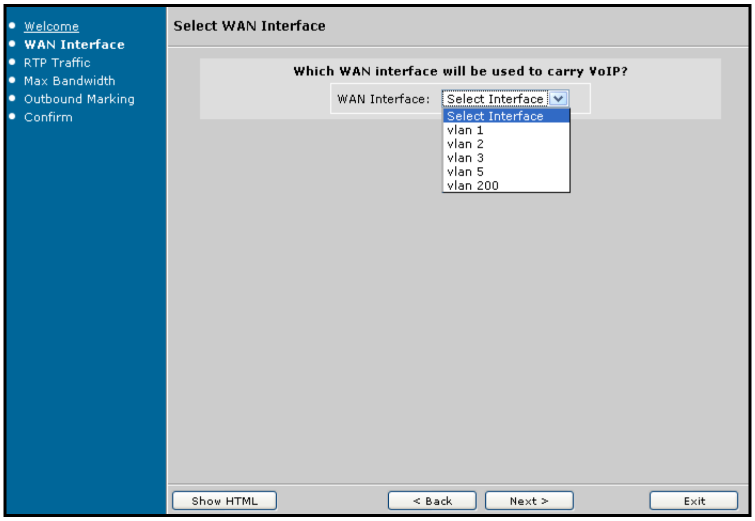
This Wizard will guide you through the configuration of a QoS map on a WAN interface for carrying VoIP.

Please note: It is recommended to only use this wizard when first creating QoS maps. The settings selected in this wizard will **overwrite any previous QoS configuration for the WAN interface selected.**

Figure 3. Welcome to the QoS Wizard Menu

Step 2: Select a WAN Interface

Select a WAN interface from the drop-down menu. Select **Next** to continue.



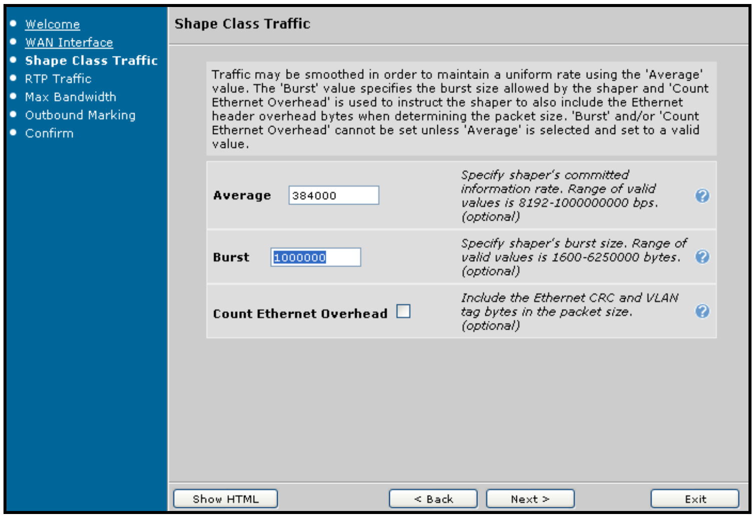
Which WAN interface will be used to carry VoIP?

WAN Interface: Select Interface

Figure 4. WAN Interface

Step 3: Apply Traffic Shaping

If traffic shaping is required for this interface, select the parameters for **Average** and **Burst** size. These settings only apply to Ethernet or VLAN interfaces and are explained in greater detail in *Traffic Shaping (Optional) on page 34*. Choose whether to include the Ethernet cyclic redundancy check (CRC) and VLAN tag bytes in the packet size by selecting **Count Ethernet Overhead**. Select **Next** to continue.



Shape Class Traffic

Traffic may be smoothed in order to maintain a uniform rate using the 'Average' value. The 'Burst' value specifies the burst size allowed by the shaper and 'Count Ethernet Overhead' is used to instruct the shaper to also include the Ethernet header overhead bytes when determining the packet size. 'Burst' and/or 'Count Ethernet Overhead' cannot be set unless 'Average' is selected and set to a valid value.

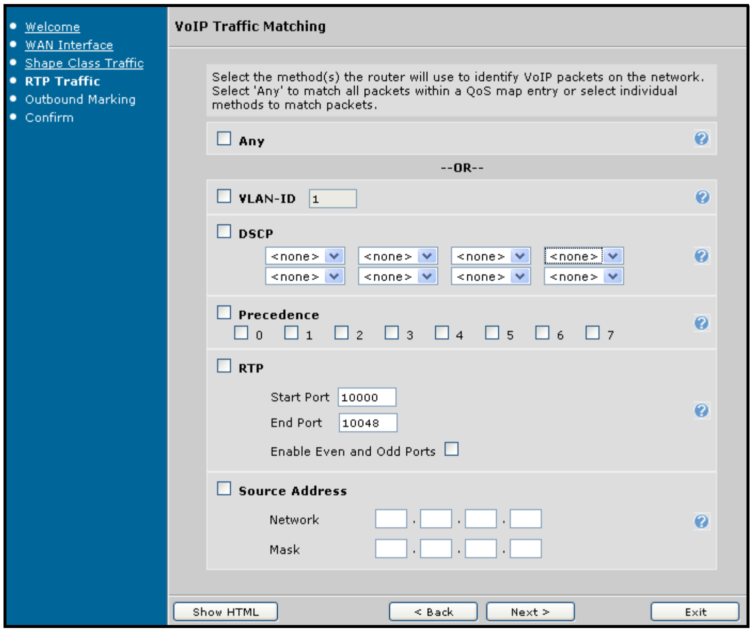
Average	384000	*Specify shaper's committed information rate. Range of valid values is 8192-1000000000 bps. (optional)*
Burst	1000000	*Specify shaper's burst size. Range of valid values is 1600-6250000 bytes. (optional)*
Count Ethernet Overhead	□	*Include the Ethernet CRC and VLAN tag bytes in the packet size. (optional)*

Figure 5. Shape Class Traffic Menu

Step 4: Identify Traffic Matching Criteria

Select the method or methods to use when identifying packets on the network. Each of these settings are explained in more detail in *Step 2: Classify Traffic Using Match Criteria on page 30*. Once the matching methods have been selected. Select **Next** to continue.

NOTE *The GUI does not currently support configuration of IPv4- and IPv6-specific matching. Any packet match cases added in the GUI will apply to both IPv4 and IPv6 packets.*



VoIP Traffic Matching

Select the method(s) the router will use to identify VoIP packets on the network. Select 'Any' to match all packets within a QoS map entry or select individual methods to match packets.

□ Any

--OR--

□ VLAN-ID 1

□ DSCP
<none> <none> <none> <none>
<none> <none> <none> <none>

□ Precedence
□ 0 □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7

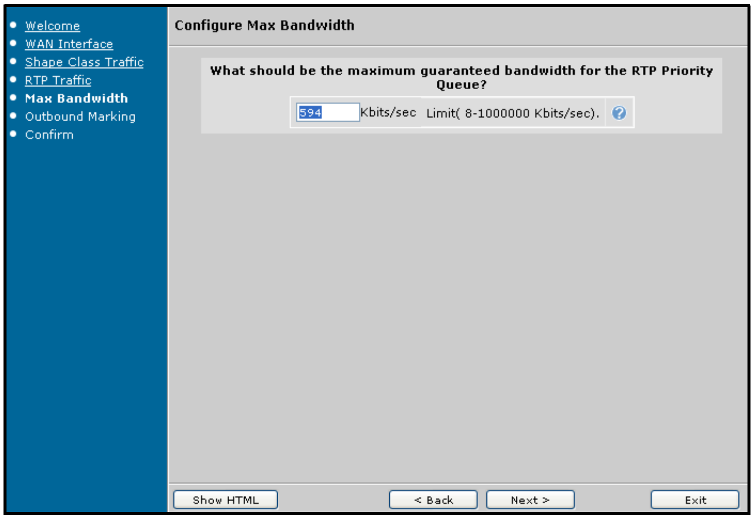
□ RTP
Start Port 10000
End Port 10048
Enable Even and Odd Ports □

□ Source Address
Network . . .
Mask . . .

Figure 6. VoIP Traffic Matching Menu

Step 5: Configure the Maximum Bandwidth

Enter the maximum guaranteed bandwidth for the priority queue. It is recommended that voice traffic be limited to a maximum value so the AOS unit will reserve some of the bandwidth for other traffic. The unit will limit the rate and drop traffic that exceeds the specified bandwidth. Select **Next** to continue.



Configure Max Bandwidth

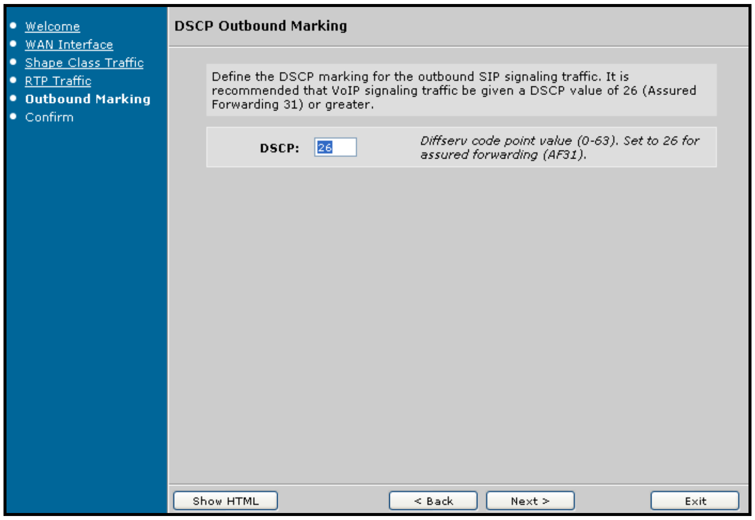
What should be the maximum guaranteed bandwidth for the RTP Priority Queue?

594 Kbits/sec Limit(8-1000000 Kbits/sec).

Figure 7. Configure Max Bandwidth Menu

Step 6: Assign Packet Marking

If it is necessary to mark outbound packets, enter the DSCP value. The field will automatically populate with the default (**26**). Select **Next** to continue.



DSCP Outbound Marking

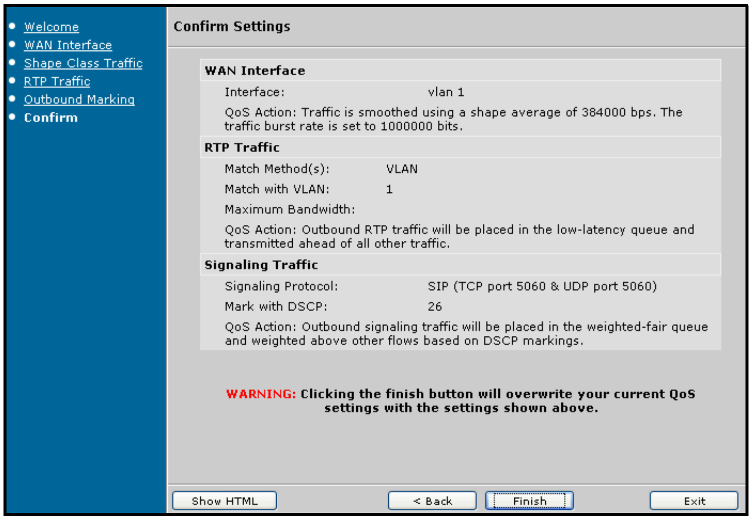
Define the DSCP marking for the outbound SIP signaling traffic. It is recommended that VoIP signaling traffic be given a DSCP value of 26 (Assured Forwarding 31) or greater.

DSCP: 26 *Diffserv code point value (0-63). Set to 26 for assured forwarding (AF31).*

Figure 8. DSCP Outbound Marking Menu

Step 7: Confirm Settings

Select **Finish** once you have checked your configuration settings and are ready to apply them to the WAN interface. Remember that these settings will override any previously configured settings for this interface.



Confirm Settings

WAN Interface

Interface: vlan 1

QoS Action: Traffic is smoothed using a shape average of 384000 bps. The traffic burst rate is set to 1000000 bits.

RTP Traffic

Match Method(s): VLAN

Match with VLAN: 1

Maximum Bandwidth:

QoS Action: Outbound RTP traffic will be placed in the low-latency queue and transmitted ahead of all other traffic.

Signaling Traffic

Signaling Protocol: SIP (TCP port 5060 & UDP port 5060)

Mark with DSCP: 26

QoS Action: Outbound signaling traffic will be placed in the weighted-fair queue and weighted above other flows based on DSCP markings.

WARNING: Clicking the finish button will overwrite your current QoS settings with the settings shown above.

Figure 9. Confirm Settings Menu

Manually Configuring QoS Using the GUI

Use the following steps to manually configure QoS for purposes that can not be accomplished through the QoS Wizard. These instructions are also useful if you need to make adjustments to any settings already configured in your unit.

Step 1: Create a QoS Map

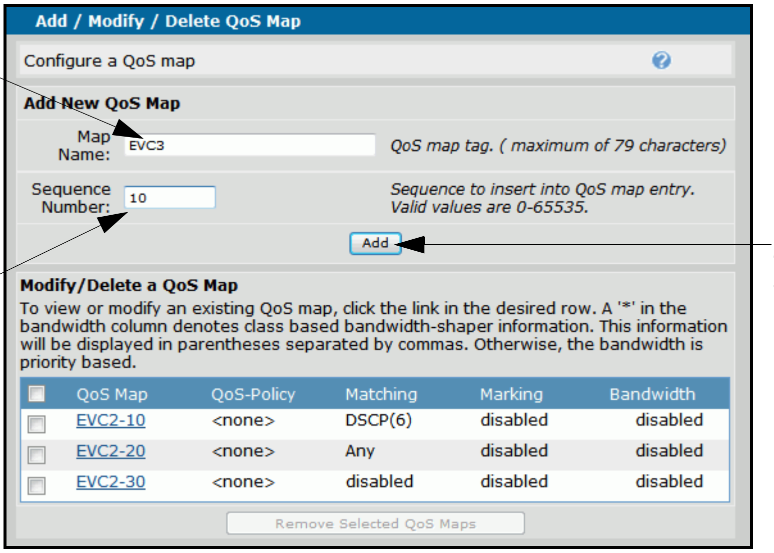
As described in *CLI Configuration on page 4*, the first step is to create a QoS map. To access the QoS configuration menu, navigate to **Data** > **Router/Bridge** > **QoS Maps** from the left side of the menu. The **Add/Modify/Delete QoS Map** menu appears.

Multiple map entries for the same QoS map are differentiated by a sequence number. The sequence number is used to assign match order. For example, when creating multiple entries in the QoS map named **EVC2**, the sequence numbers are provided in increments as follows: **EVC2-10**, **EVC2- 20**, and **EVC2-30**.

To create the QoS map, enter a name for the map and a sequence number. Select **Add** to create the map entry. The **QoS Map Setup** menu appears, displaying the **Packet Matching** menu (shown in *Figure 11 on page 31*) for further configuration.

Enter a name for the QoS map.

Enter a sequence number for the map entry.



Select **Add** to create the map entry.

Add / Modify / Delete QoS Map

Configure a QoS map

Add New QoS Map

Map Name: EVC3 — *QoS map tag. (maximum of 79 characters)*

Sequence Number: 10 — *Sequence to insert into QoS map entry. Valid values are 0-65535.*

Add

Modify/Delete a QoS Map

To view or modify an existing QoS map, click the link in the desired row. A '*' in the bandwidth column denotes class based bandwidth-shaper information. This information will be displayed in parentheses separated by commas. Otherwise, the bandwidth is priority based.

□	QoS Map	QoS-Policy	Matching	Marking	Bandwidth
□	EVC2-10	<none>	DSCP(6)	disabled	disabled
□	EVC2-20	<none>	Any	disabled	disabled
□	EVC2-30	<none>	disabled	disabled	disabled

Remove Selected QoS Maps

Figure 10. Add/Modify/Delete QoS Map Menu

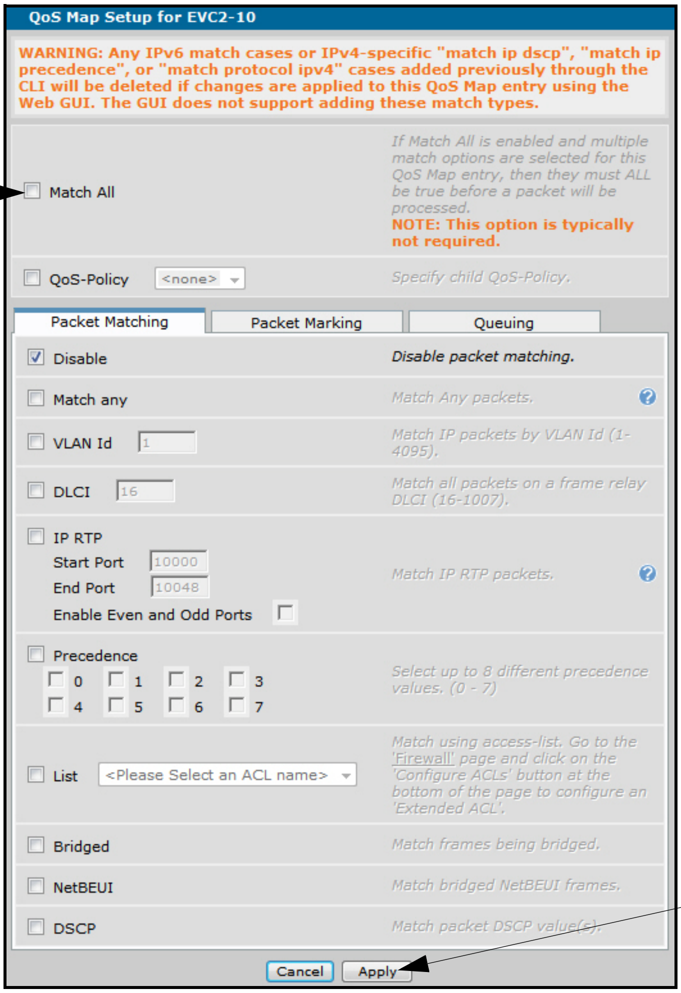
Step 2: Classify Traffic Using Match Criteria

Multiple match criteria can exist within the same QoS map, allowing a single QoS policy to service various types of traffic. Traffic is matched based on VLAN ID, IP RTP, IP precedence value, ACL, bridge frames, and DSCP values. If the **Packet Matching** menu does not initially display from the **QoS Map Setup** menu, select the **Packet Matching** tab. Enable the match criteria as described in *Table 13 on page 32* and select **Apply** to accept the new settings.

The **Match All** check box is normally left unchecked, indicating that a packet may match any of the packet matching cases specified. If it is checked, it requires that all specified packet matching cases must be true before a packet will be processed as part of this class.

> NOTE
>
> *The GUI does not currently support configuration of IPv4- or IPv6-specific matching. Any packet match cases added in the GUI will apply to both IPv4 and IPv6 packets.*

Do not select **Match All** unless you want to require matching all packet matching criteria.



QoS Map Setup for EVC2-10

WARNING: Any IPv6 match cases or IPv4-specific "match ip dscp", "match ip precedence", or "match protocol ipv4" cases added previously through the CLI will be deleted if changes are applied to this QoS Map entry using the Web GUI. The GUI does not support adding these match types.

□ Match All	If Match All is enabled and multiple match options are selected for this QoS Map entry, then they must ALL be true before a packet will be processed. NOTE: This option is typically not required.
□ QoS-Policy <none>	Specify child QoS-Policy.

Packet Matching | Packet Marking | Queuing

☑ Disable	Disable packet matching.
□ Match any	Match Any packets.
□ VLAN Id 1	Match IP packets by VLAN Id (1-4095).
□ DLCI 16	Match all packets on a frame relay DLCI (16-1007).
□ IP RTP Start Port 10000 End Port 10048 Enable Even and Odd Ports □	Match IP RTP packets.
□ Precedence □ 0 □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7	Select up to 8 different precedence values. (0 - 7)
□ List <Please Select an ACL name>	Match using access-list. Go to the 'Firewall' page and click on the 'Configure ACLs' button at the bottom of the page to configure an 'Extended ACL'.
□ Bridged	Match frames being bridged.
□ NetBEUI	Match bridged NetBEUI frames.
□ DSCP	Match packet DSCP value(s).

Select **Apply**.

Figure 11. Packet Matching Tab Menu

Table 13. Packet Matching Options

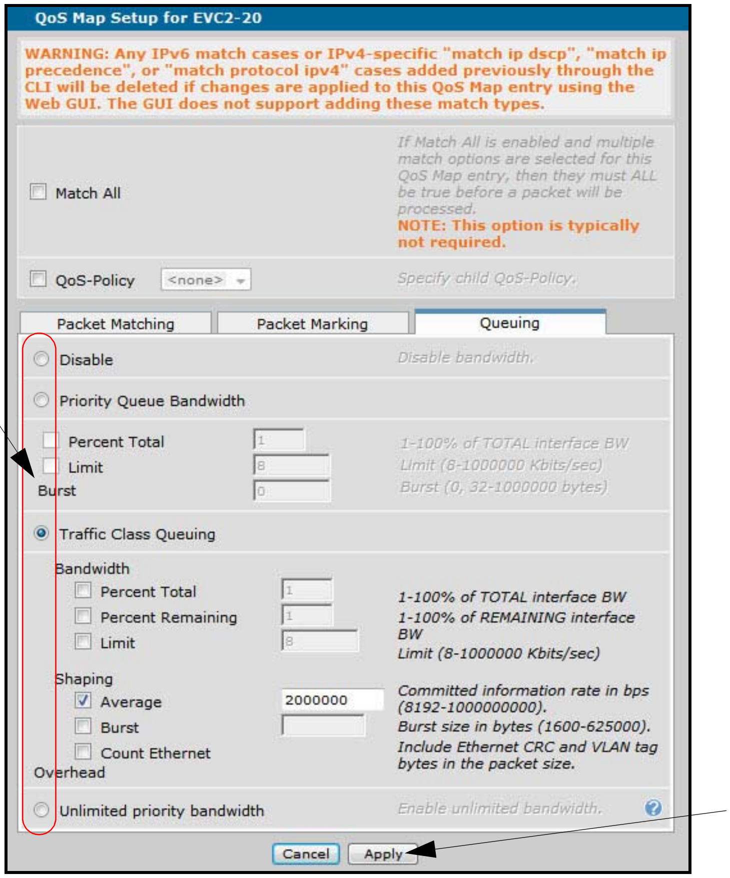
Menu Option	Description
Disable	Select to disable packet matching for this traffic class.
Match any	Select to match any packets within the QoS map entry. Since map entries are processed in the order of their sequence numbers, the **match any** class can be used to process all packets not previously matched by a map entry.
VLAN Id	Select to match packets associated with a particular VLAN. Indicate VLAN ID number (**1** to **4095**).
DLCI	Select to match packets based on the Frame Relay DLCI number associated with a packet. Enter a value of **16** to **1007**.
IP RTP	Select to match IPv4 RTP packets with the specified UDP destination port. **Start Port** - Specify a port number **0** to **65535**. **End Port** - Specify a port number **0** to **65535**. The value must be greater than or equal to the start port number. **Enable Even and Odd Ports** - Select to enable all ports in the start to end range. Otherwise, only even ports are enabled.
Precedence	Select to match packets on IP precedence value in IP header. Indicate a value **0** to **7**, in ascending order of importance.
List	Select an IPv4 ACL from the drop-down list to match packets.
Bridged	Select to match frames being bridged.
NetBEUI	Select to match bridged NetBEUI frames.
DSCP	Select to match packets based on DSCP values in the IP header. Select **Add a new DSCP Line** to create a new entry. Up to eight DSCP values can be indicated per QoS map. If any one of the values match, the packet will be processed. Select from the following: **Default** (000000) **AF11** (001010) **AF12** (001100) **AF13** (001110) **AF21** (010010) **AF22** (010100) **AF23** (010110) **AF31** (011010) **AF32** (011100) **AF33** (011110) **AF41** (100010) **AF42** (100100) **AF43** (100110) **CS1** (001000) **CS2** (010000) **CS3** (011000) **CS4** (100000) **CS5** (101000) **CS6** (110000) **CS7** (111000) **EF** (101110) **1** to **63** To remove a DSCP value, select **Delete** from the corresponding line.

Step 3: Apply an Action to the Matched Traffic

Once traffic is matched, its handling method must be determined. This step involves applying an action to the traffic which matched the criteria in Step 2. Multiple actions can be applied to the packets. These actions include allocating class-based queues, priority or low-latency queues, packet marking, and traffic shaping.

Configure the policy action by selecting the **Queuing** tab. Enable an action (described in *Table 14 on page 34*), and select **Apply** to accept the new settings.

Select one of the four available policy actions to apply to the traffic class.



QoS Map Setup for EVC2-20

WARNING: Any IPv6 match cases or IPv4-specific "match ip dscp", "match ip precedence", or "match protocol ipv4" cases added previously through the CLI will be deleted if changes are applied to this QoS Map entry using the Web GUI. The GUI does not support adding these match types.

□ Match All — *If Match All is enabled and multiple match options are selected for this QoS Map entry, then they must ALL be true before a packet will be processed.* **NOTE: This option is typically not required.**

□ QoS-Policy <none> — *Specify child QoS-Policy.*

○ Disable — *Disable bandwidth.*

○ Priority Queue Bandwidth

□ Percent Total 1 — *1-100% of TOTAL interface BW*
□ Limit 8 — *Limit (8-1000000 Kbits/sec)*
Burst 0 — *Burst (0, 32-1000000 bytes)*

● Traffic Class Queuing

Bandwidth
□ Percent Total 1 — *1-100% of TOTAL interface BW*
□ Percent Remaining 1 — *1-100% of REMAINING interface BW*
□ Limit 8 — *Limit (8-1000000 Kbits/sec)*

Shaping
☑ Average 2000000 — *Committed information rate in bps (8192-1000000000).*
□ Burst — *Burst size in bytes (1600-625000).*
□ Count Ethernet Overhead — *Include Ethernet CRC and VLAN tag bytes in the packet size.*

○ Unlimited priority bandwidth — *Enable unlimited bandwidth.*

Select **Apply**.

Figure 12. Queuing Tab Menu

Only one of the four options listed on this menu can be configured per traffic class. After selecting **Disable**, **Priority Queue Bandwidth**, **Traffic Class Queuing**, or **Unlimited priority bandwidth**, the other options will not be available.

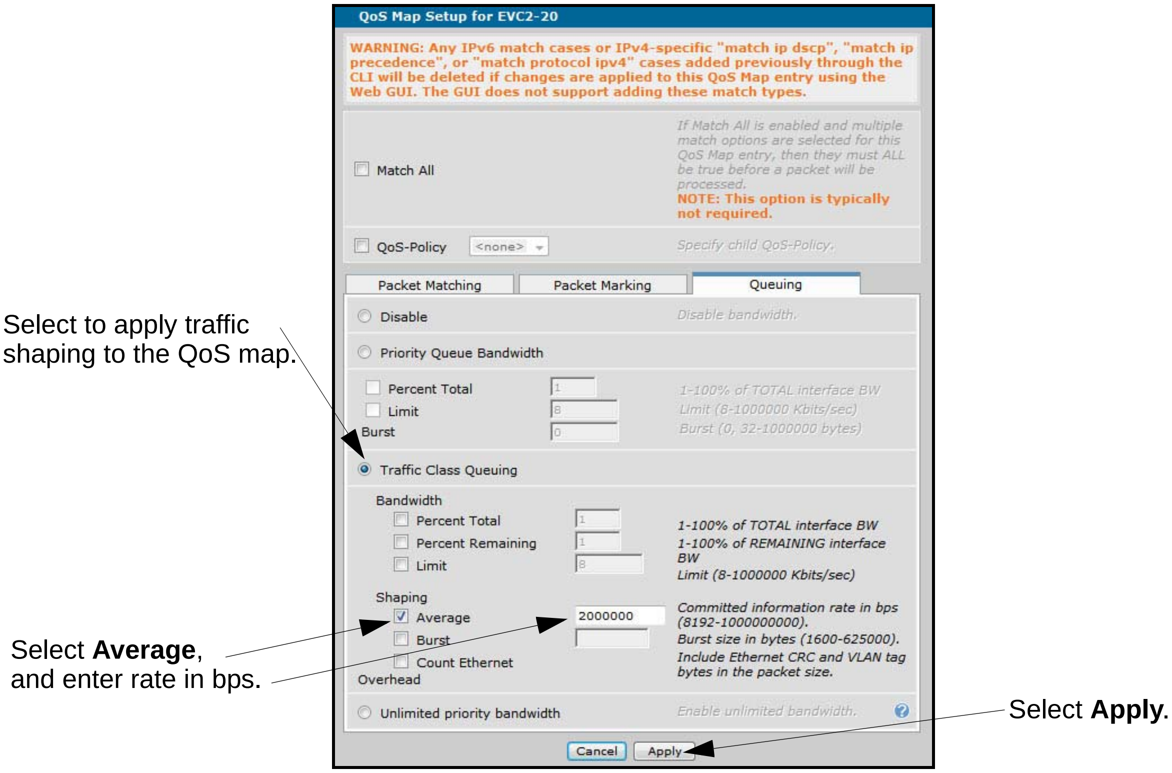
Table 14. Traffic Queuing Options

Menu Option	Description
Disable	Select to remove any specific queuing requirement for the class on interfaces using this policy.
Priority Queue Bandwidth	**Percent Total** - Specify **1** to **100** percent of the total interface bandwidth. **Limit** - Specify **8** to **1000000** Kbps. **Burst -** Specify **0** to let the router determine the optimum burst size, or **32** to **1000000** bytes to set the value manually.
Traffic Class Queuing	**Bandwidth** **Percent Total** - Specify **1** to **100** percent of total interface bandwidth. **Percent Remaining** - Specify **1** to **100** percent of remaining interface bandwidth. **Limit** - Specify **8** to **1000000** Kbps. **Shaping** **Average** - Specify **8192** to **1000000000** bps. **Burst** - Specify **1600** to **625000** bytes. If the **Burst** check box is not selected, the router will choose the default automatically. **Count Ethernet Overhead** - Select to include Ethernet CRC and VLAN/MAC header bytes in the packet size.
Unlimited Priority Bandwidth	Select to allow unlimited priority traffic. No rate limiting will be performed on this traffic class. Use with caution as excessive traffic matching the QoS map can potentially use all of the available bandwidth on the WAN port, blocking out other important traffic.

Traffic Shaping (Optional)

Once traffic is matched in a QoS map, traffic shaping can be applied. Traffic shaping allows the traffic to be smoothed in order to maintain a uniform rate to take advantage of the provided bandwidth. Short bursts of traffic above the configured rate are allowed when there is sufficient budget. Traffic outside of the current budget is put into a shaping queue and transmitted once the budget is available. There are many options available for shaping traffic and these are explained in *Table 14*. Traffic shaping is applied through the **Queuing** tab menu from the **QoS Map Setup** menu.

Select **Traffic Class Queuing** to shape the traffic to an average rate. Select **Average**, and enter a rate in bps. This example will smooth the traffic through the interface using the **EVC2-20** policy to **2000000** bps. Bursts of traffic above this rate will be placed in a queue for transmission when enough bandwidth is available.



WARNING: Any IPv6 match cases or IPv4-specific "match ip dscp", "match ip precedence", or "match protocol ipv4" cases added previously through the CLI will be deleted if changes are applied to this QoS Map entry using the Web GUI. The GUI does not support adding these match types.

☐ Match All — If Match All is enabled and multiple match options are selected for this QoS Map entry, then they must ALL be true before a packet will be processed. NOTE: This option is typically not required.

☐ QoS-Policy <none> — Specify child QoS-Policy.

○ Disable — Disable bandwidth.

○ Priority Queue Bandwidth

☐ Percent Total 1 — 1-100% of TOTAL interface BW
☐ Limit 8 — Limit (8-1000000 Kbits/sec)
Burst 0 — Burst (0, 32-1000000 bytes)

● Traffic Class Queuing

Bandwidth
☐ Percent Total 1 — 1-100% of TOTAL interface BW
☐ Percent Remaining 1 — 1-100% of REMAINING interface BW
☐ Limit 8 — Limit (8-1000000 Kbits/sec)

Shaping
☑ Average 2000000 — Committed information rate in bps (8192-1000000000).
☐ Burst — Burst size in bytes (1600-625000).
☐ Count Ethernet Overhead — Include Ethernet CRC and VLAN tag bytes in the packet size.

○ Unlimited priority bandwidth — Enable unlimited bandwidth.

Select to apply traffic shaping to the QoS map.

Select **Average**, and enter rate in bps.

Select **Apply**.

Figure 13. Applying Traffic Shaping in the GUI

Packet Marking

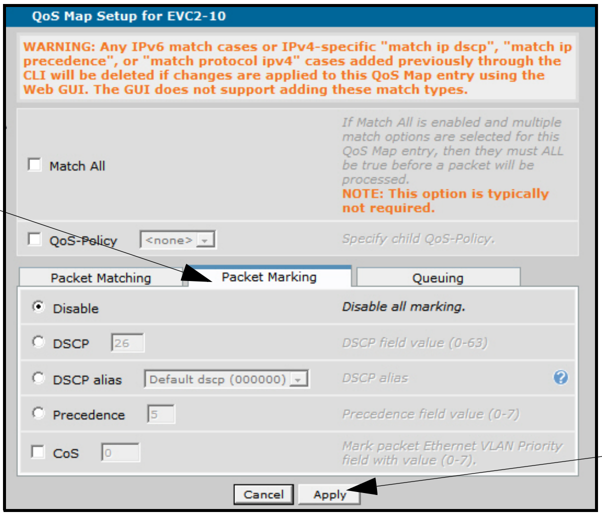
The options provided for packet marking allow you to change the DSCP field, IP precedence value, or CoS value for outgoing traffic serviced by the QoS policy. Every IPv4 header contains an 8-bit ToS field used for marking packets requiring special handling when traveling through the network. IPv6 headers have an 8-bit traffic-class field serving the same purpose. Originally, this ToS field was used for IP precedence markings (using only the first three bits of the 8-bit field), and was later revised in RFC 2474 to create the 6-bit DSCP field (reserving the last two bits of the field for future use). The DSCP field can be manipulated to indicate higher or lower traffic priority using a value between **0** and **63**. DSCP and precedence remarking can be applied to both IPv4 and IPv6 packets.

To change the DSCP field on matching packets, enable the **DSCP** or **DSCP alias** options from the **Packet Marking** tab menu (see *Figure 14 on page 36*). Similarly, to change the IP precedence value on matching packets, enable the **Precedence** option and enter a value between **0** and **7**. Be sure to select **Apply** to save the settings.

NOTE

The GUI does not currently support configuration of IPv4- or IPv6-specific matching. Any packet match cases added in the GUI will apply to both IPv4 and IPv6 packets.

Select **Packet Marking** to mark the DSCP field, IP precedence value, or CoS value for outgoing traffic.



QoS Map Setup for EVC2-10

WARNING: Any IPv6 match cases or IPv4-specific "match ip dscp", "match ip precedence", or "match protocol ipv4" cases added previously through the CLI will be deleted if changes are applied to this QoS Map entry using the Web GUI. The GUI does not support adding these match types.

□ Match All — If Match All is enabled and multiple match options are selected for this QoS Map entry, then they must ALL be true before a packet will be processed. NOTE: This option is typically not required.

□ QoS-Policy <none> Specify child QoS-Policy.

● Disable — Disable all marking.

○ DSCP 26 — DSCP field value (0-63)

○ DSCP alias Default dscp (000000) — DSCP alias

○ Precedence 5 — Precedence field value (0-7)

□ CoS 0 — Mark packet Ethernet VLAN Priority field with value (0-7).

Select **Apply**.

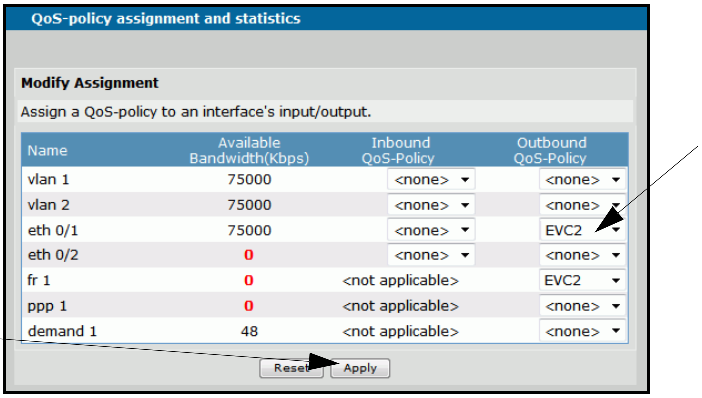
Figure 14. Packet Marking Tab Menu

Table 15. Packet Marking Options

Menu Options	Description
Disable	Select to discontinue marking of packets. By default, packet marking is disabled.
DSCP	Changes the DSCP field value for outgoing traffic serviced by the QoS map. Indicate a value of **0** to **63**.
DSCP alias	Changes the DSCP field value for outgoing traffic serviced by the QoS map. Select an alias from the drop-down list: **Default** (000000) **AF11** (001010) **AF12** (001100) **AF13** (001110) **AF21** (010010) **AF22** (010100) **AF23** (010110) **AF31** (011010) **AF32** (011100) **AF33** (011110) **AF41** (100010) **AF42** (100100) **AF43** (100110) **CS1** (001000) **CS2** (010000) **CS3** (011000) **CS4** (100000) **CS5** (101000) **CS6** (110000) **CS7** (111000) **EF** (101110)
Precedence	Changes the IP precedence field value for incoming traffic serviced by the QoS map. Indicate a value of **0** to **7**.
CoS	Assigns the CoS value for outgoing traffic serviced by the QoS map. Indicate a value of **0** to **7**. This is only applied to Ethernet or VLAN interfaces.

Step 4: Assign the QoS Map to the Interface

After the QoS map is created, you will be returned to the **Add/Modify/Delete QoS Map** menu. It is easiest to apply the QoS map to the interface now and then continue on with the rest of the interface configuration. From the QoS configuration menu located at **Data** > **Router/Bridge** > **QoS Maps**, scroll down to the **QoS-policy assignment and statistics** section. Under **Modify Assignment**, select an **Outbound QoS-Policy** for the appropriate interface. For example, in *Figure 15*, the QoS policy **EVC2** has been selected for **eth 0/1**.



QoS-policy assignment and statistics

Modify Assignment

Assign a QoS-policy to an interface's input/output.

Name	Available Bandwidth(Kbps)	Inbound QoS-Policy	Outbound QoS-Policy
vlan 1	75000	<none>	<none>
vlan 2	75000	<none>	<none>
eth 0/1	75000	<none>	EVC2
eth 0/2	0	<none>	<none>
fr 1	0	<not applicable>	EVC2
ppp 1	0	<not applicable>	<none>
demand 1	48	<not applicable>	<none>

Select a policy from the drop-down list to apply to the interface.

Select **Apply**.

Figure 15. Apply QoS Policy to the Interface

WARNING *Applying a QoS Map to a PPP or demand interface will cause the interface to drop briefly. This causes a temporary service interruption and the interface should come back up momentarily.*

Additional Settings Using the GUI

The following section provides information about additional settings not covered in the previous steps. These settings may pertain to your particular configuration. You can also refer to *Additional Settings Using the CLI on page 24* for more information.

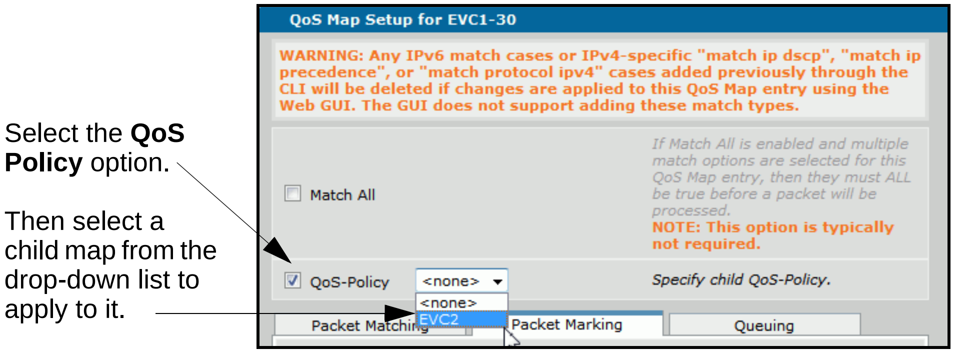
Subdividing Policy Classes

The QoS policy action can be used within a QoS map to further subdivide a class into more specific subclasses. The most specific QoS map (or child map) is created first. The base (or parent) map is created next and then the QoS map is referenced by selecting the QoS parent map from within the QoS map configuration menu. The base (or parent) map is applied to the interface.

Only two levels of maps are allowed, which means child maps (or subclasses) cannot be further subdivided. A child map cannot reference another child map. If the child map is deleted, then the parent map is also deleted.

To apply a child map to a parent QoS map, navigate to **Data** > **Router/Bridge** > **QoS Maps**. Select the parent QoS map to configure. The QoS policy option is available at the top of the menu as shown in *Figure 16 on page 38*.

Select the **QoS-Policy** option and choose the child map to apply to it from the drop-down list. Select **Apply** to accept the changes.



Select the **QoS Policy** option.

Then select a child map from the drop-down list to apply to it.

QoS Map Setup for EVC1-30

WARNING: Any IPv6 match cases or IPv4-specific "match ip dscp", "match ip precedence", or "match protocol ipv4" cases added previously through the CLI will be deleted if changes are applied to this QoS Map entry using the Web GUI. The GUI does not support adding these match types.

□ Match All

If Match All is enabled and multiple match options are selected for this QoS Map entry, then they must ALL be true before a packet will be processed.

NOTE: This option is typically not required.

☑ QoS-Policy <none>

Specify child QoS-Policy.

Figure 16. Adding a QoS Policy within a QoS Map

Example Configurations

The following examples are designed to enhance your understanding of QoS configuration on AOS products. Adjust the commands appropriately to fit your specific network requirements.

Example 1: Low-Latency Queue VoIP DSCP

In this example, a customer has an IP phone on their network using VoIP. The IP phone tags RTP VoIP packets with a DSCP value of 46 and uses the G.711 coder-decoder (CODEC). The phone also uses Session Initiation Protocol (SIP) and tags the call control packets with a DSCP of 26. A low-latency queue is created to allocate 100 Kbps for the VoIP traffic to ensure quality is preserved during a congested state on the WAN. This scenario is accomplished by creating a QoS map named **VOIP** that matches IPv4 and IPv6 packets tagged with a DSCP of 26 or 46. The **priority 100** command is issued to allocate a low-latency queue of 100 Kbps for that traffic. The QoS map is applied to the **PPP 1** WAN interface with the **qos-policy out VOIP** command.

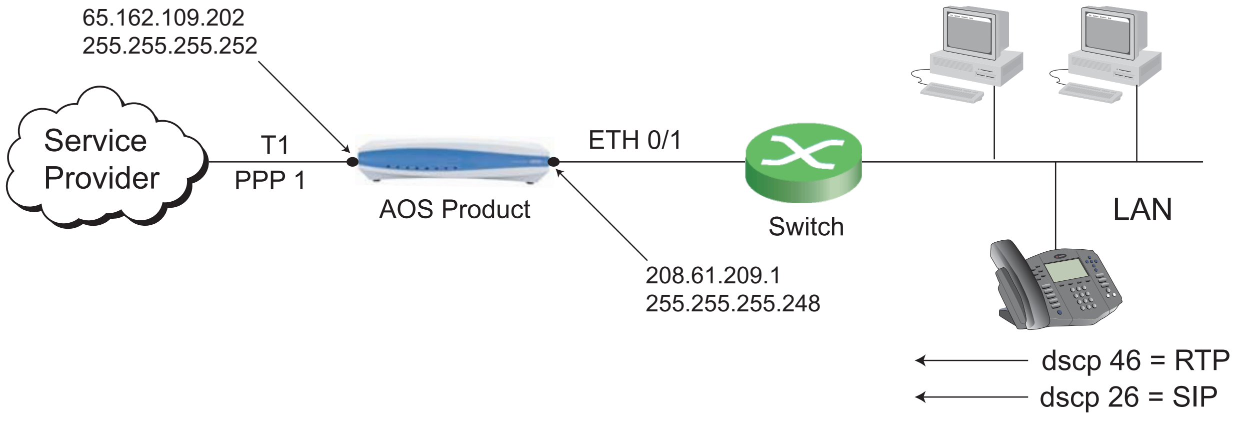


Figure 17. Example of VoIP Using Low-Latency Queue

```
!
qos map VOIP 10
  match dscp 46 26
  priority 100
!
interface eth 0/1
  ip address 208.61.209.1 255.255.255.248
  no shutdown
!
interface t1 1/1
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface ppp 1
  ip address 65.162.109.202 255.255.255.252
  qos-policy out VOIP
  no shutdown
  cross-connect 1 t1 1/1 1 ppp 1
!
ip route 0.0.0.0 0.0.0.0 ppp 1
```

Example 2: CBWFQ Ethernet WAN

In this example, a customer has an Ethernet WAN connection with an upload speed of 384 Kbps and wants to allocate bandwidth to certain data applications. A custom application that uses TCP destination port 285 requires 72 Kbps of bandwidth and the administrator wants to reserve 100 Kbps for web traffic. This is accomplished by creating a QoS map named **DATA** containing two separate sequence numbers (**DATA 10** and **DATA 20**). Each sequence number selects IPv4 traffic based on the specified ACL using the **match ip list** command and allocates the appropriate bandwidth (with the **bandwidth** command). The QoS map is applied to the **ETH 0/1** WAN interface (with the **qos-policy out DATA** command). The maximum upload speed for the connection is defined by applying traffic shaping (using the **traffic-shape rate 384000** command) to the **ETH 0/1** WAN interface so QoS can be enforced.

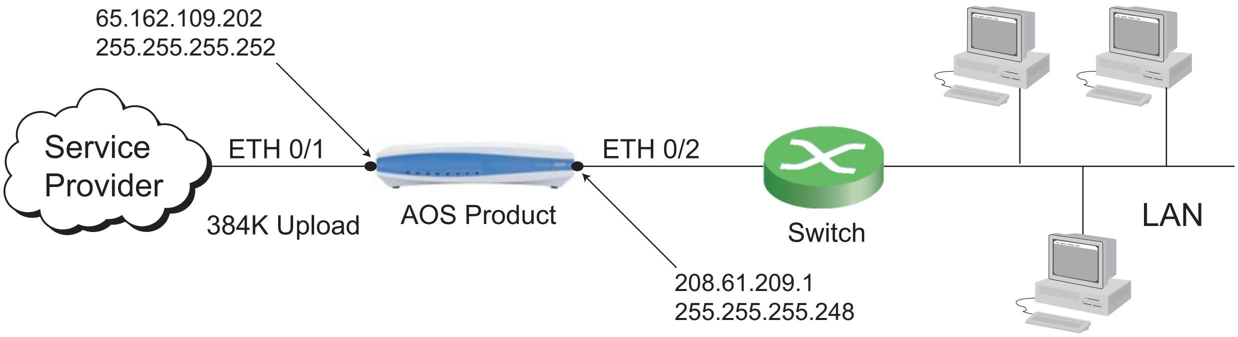


Figure 18. CBWFQ Example with Ethernet WAN

```
!
qos map DATA 10
  match ip list CUSTOM-APP
  bandwidth 72
qos map DATA 20
  match ip list WEB-TRAFFIC
  bandwidth 100
!
interface eth 0/1
  ip address 65.162.109.202 255.255.255.252
  traffic-shape rate 384000
  qos-policy out DATA
  no shutdown
!
interface eth 0/2
  ip address 208.61.209.1 255.255.255.248
  no shutdown
!
!
ip route 0.0.0.0 0.0.0.0 65.162.109.201
!
!
ip access-list extended CUSTOM-APP
  permit tcp any any eq 285
!
ip access-list extended WEB-TRAFFIC
  permit tcp any any eq www
!
```

Example 3: Low-Latency Queue VoIP Subnet

In this example, a customer has a T1 PPP connection to a host site. Both VoIP and data traffic are carried across this T1 connection to access resources on the host network. The VoIP equipment at the remote site does not tag packets with a DSCP value, so that cannot be used as the match criteria. Instead, the voice and data are segregated into different subnets. All data traffic at the remote site is contained in the 192.168.1.0 /24 subnet, and all voice traffic is contained in the 192.168.2.0 /24 subnet. The customer has determined that no more than eight calls using the G.711 CODEC will be active at one time, and that 800 Kbps of bandwidth should be reserved for this purpose. This is accomplished by using a QoS map named **VOIP** that matches IPv4 traffic based on the ACL named **VOICE**. The **VOICE** ACL permits any traffic on the 192.168.2.0 /24 voice subnet. The QoS map **VOIP** allocates 800 Kbps to a low-latency queue for the specified traffic giving it priority during times of congestion. The QoS map is applied to the **PPP 1** WAN interface with the **qos-policy out VOIP** command.

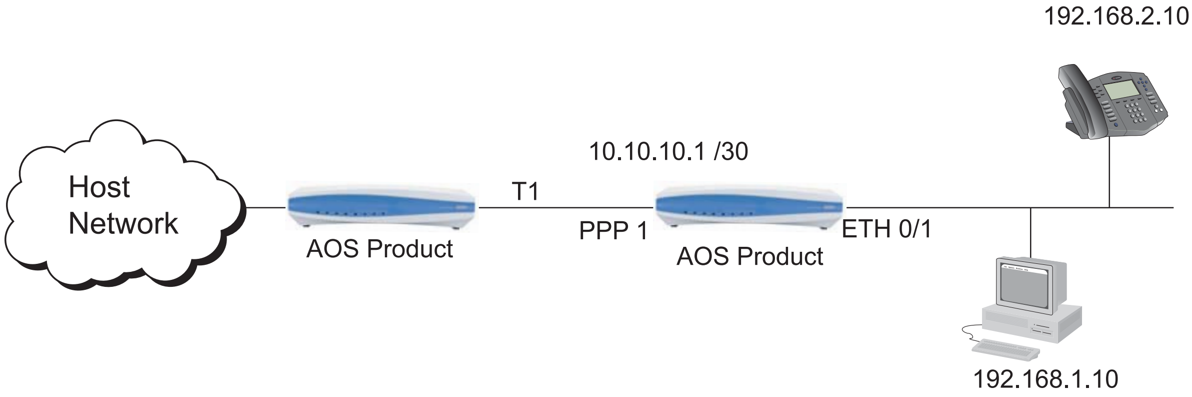


Figure 19. Low-Latency Queue with VoIP Subnet

```
!
qos map VOIP 10
  match ip list VOICE
  priority 800
!
!
interface eth 0/1
  ip address 192.168.1.1 255.255.255.0
  ip address 192.168.2.1 255.255.255.0 secondary
  no shutdown
!
interface t1 1/1
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface ppp 1
  ip address 10.10.10.1 255.255.255.252
  qos-policy out VOIP
  no shutdown
  cross-connect 1 t1 1/1 1 ppp 1
!
!
ip route 0.0.0.0 0.0.0.0 ppp 1
!
!
ip access-list extended VOICE
  permit ip 192.168.2.0 0.0.0.255 any
!
```

Example 4: Multi Tenant

In the following example, a single AOS router provides Internet access for three separate customers. The WAN is a T1 PPP connection to a service provider. The configuration limits each customer's outbound traffic to the service provider to 400 Kbps. Due to the fact that outbound QoS is one of the last actions taken by the router before a IPv4 packet is sent, network address translation (NAT) will have already taken place. This prevents using the customer’s original private IPv4 address as the match criteria for traffic shaping. Instead, an inbound QoS map named **SET-DSCP** is applied to the private interface of the router to match each customer’s subnet and assign a different DSCP value for each. After NAT takes place, the DSCP values are preserved and can be used to match on an outbound QoS map named **SHAPE-OUT** that limits each customer to 400 Kbps for outbound traffic.

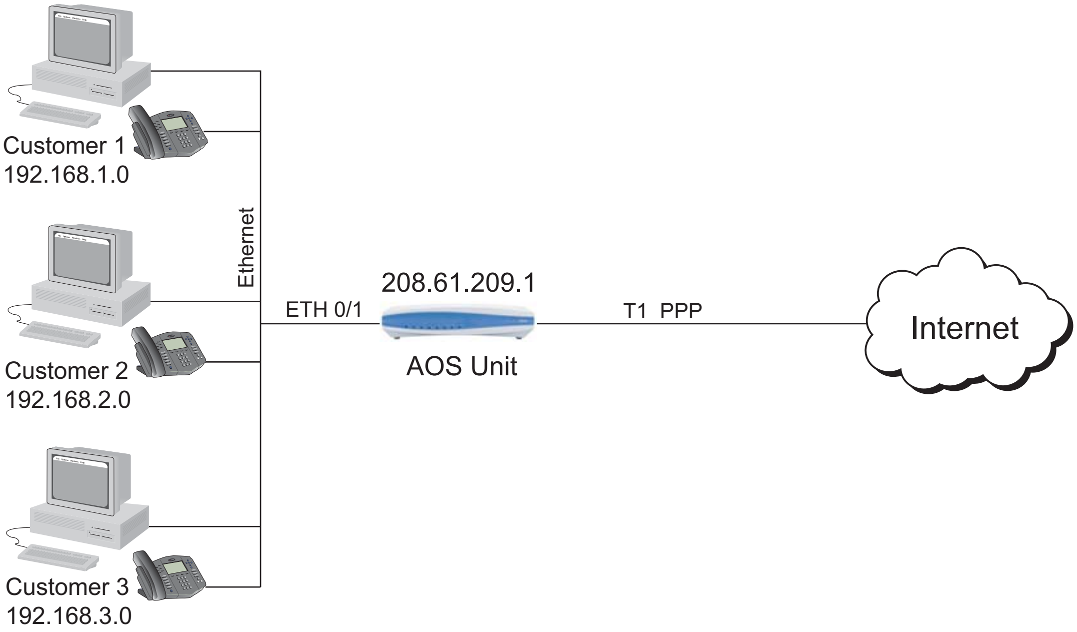


Figure 20. Multi Tenant QoS Application

The following commands are entered to configure QoS for this example:

```
!
ip firewall
!
qos map SET-DSCP 10
    match ip list CUSTOMER1
    set dscp af11
qos map SET-DSCP 20
    match ip list CUSTOMER2
    set dscp af21
qos map SET-DSCP 30
    match ip list CUSTOMER3
    set dscp af31
!
```

```
qos map SHAPE-OUT 10
    match ip dscp af11
    shape average 400000
qos map SHAPE-OUT 20
    match ip dscp af21
    shape average 400000
qos map SHAPE-OUT 30
    match ip dscp af31
    shape average 400000
!
interface eth 0/1
    ip address 192.168.1.1 255.255.255.0
    ip address 192.168.2.1 255.255.255.0 secondary
    ip address 192.168.3.1 255.255.255.0 secondary
    ip access-policy Private
    qos-policy in SET-DSCP
    no shutdown
!
interface t1 1/1
    tdm-group 1 timeslots 1-24 speed 64
    no shutdown
!
interface ppp 1
    ip address 208.61.209.1 255.255.255.252
    ip access-policy Public
    qos-policy out SHAPE-OUT
    no shutdown
    cross-connect 1 t1 1/1 1 ppp 1
!
ip access-list standard wizard-ics
    remark Internet Connection Sharing
    permit any
!
ip access-list extended CUSTOMER1
    permit ip 192.168.1.0 0.0.0.255 any
!
ip access-list extended CUSTOMER2
    permit ip 192.168.2.0 0.0.0.255 any
!
ip access-list extended CUSTOMER3
    permit ip 192.168.3.0 0.0.0.255 any
!
ip access-list extended NO-INTERNAL-TRAFFIC
    permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
!
ip policy-class Private
    allow list self self
    discard list NO-INTERNAL-TRAFFIC
    nat source list wizard-ics interface ppp 1 overload
```

```
!
ip policy-class Public
!
ip route 0.0.0.0 0.0.0.0 208.61.209.2
!
```

Command Summary

The following tables summarize the minimum steps and additional settings required to configure QoS on an AOS product.

Table 16. QoS Configuration Steps

Step	Command and Description
Step 1	Create a QoS Map.
	(config)#**qos map** <*name*> <*number*> **[match-all | match-any]** Creates a QoS map and assigns a name and sequence number. Both **match-all** and **match-any** statements can be used when defining QoS maps with multiple match conditions. When the **match-all** keyword is specified, the traffic must match all conditions before the actions are performed. When the **match-any** keyword is specified, the behavior is set back to the default which is to match any of the conditions.
Step 2	Classify traffic using match criteria.
	(config-qos-map)#**match any** Matches all traffic not matched in a previous map entry. This variation of the **match** command can also serve as a default case if specified as the last QoS map entry.
	(config-qos-map)#**match [ip | ipv6] list** <*list name*> Specifies which traffic should be processed by this QoS map based on a configured extended ACL. The special handling instructions defined in the QoS map are applied to all packets allowed by the specified ACL list. Use **ip** keyword to match only IPv4 packets. Use the **ipv6** keyword to match only IPv6 packets.
	(config-qos-map)#**match fr-dlci** <*number*> Specifies which traffic should be processed by this QoS map based on the Frame Relay DLCI number. The DLCI numbers can range from **16** to **1007**.
	(config-qos-map)#**match [ip | ipv6] dscp [af***xx* **| cs***x* **| default | ef |** <*value*>**]** Specifies which traffic should be processed by this QoS map based on the DSCP value in the IPv4 or IPv6 header of the packet. Use the **no** form of this command to discontinue matching. Use **ip** keyword to match only IPv4 packets. Use the **ipv6** keyword to match only IPv6 packets. Omitting the keywords **ip** and **ipv6** will match both IPv4 and IPv6 packets. Assured forwarding (AF) class and subclass can be specified using the **af***xx* keyword. Select from **11** (001010), **12** (001100), **13** (001110), **21** (010010), **22** (010100), **23** (010110), **31** (011010), **32** (011100), **33** (011110), **41** (100010), **42** (100100), or **43** (100110). Class selector (CS) value can be specified using the **cs***x* keyword. Valid range for CS is **1** to **7**. The **default** keyword indicates using the default IP DCSP value (0). Marking for expedited forwarding (EF) is indicated by the **ef** keyword. Valid range for <*value*> is **0** to **63**.

Table 16. QoS Configuration Steps *(Continued)*

Step	Command and Description
Step 2 cont'd	(config-qos-map)#**match [ip | ipv6] precedence** <*value*> Specifies which traffic should be processed by this QoS map based on the IP precedence value in the IP header of the packet. Use the **no** form of this command to discontinue matching. Use **ip** keyword to match only IPv4 packets. Use the **ipv6** keyword to match only IPv6 packets. Omitting the keywords **ip** and **ipv6** will match both IPv4 and IPv6 packets. Valid range is **0** to **7** in ascending order of importance.
	(config-qos-map)#**match ip rtp [**<*port*> **|** <*begin port*> <*end port range*>**] [all]** or (config-qos-map)#**match ipv6 rtp [**<*port*> **|** <*begin port*> <*end port range*>**]** Specifies which traffic should be processed by this QoS map according to UDP port destination. Including the beginning port number and an ending port number specifies including only even port numbers from the specified range. (Typically, servers listen for user traffic on even ports.) The **all** keyword is used to match even and odd port numbers in the specified range for IPv4 traffic only. Use **ip** keyword to match only IPv4 packets. Use the **ipv6** keyword to match only IPv6 packets.
	(config-qos-map)#**match protocol bridge [netbeui]** Specifies all traffic being bridged by the router should be processed by this QoS map for the purpose of setting maximum bandwidth for that class. Instead of including all bridged traffic, you can specify to include only NetBEUI traffic by using the **netbeui** keyword.
	(config-qos-map)#**match protocol [ip | ipv6]** Specifies all traffic match the specified protocol, either IPv4 or IPv6 packets. Use **ip** keyword to match only IPv4 packets. Use the **ipv6** keyword to match only IPv6 packets.
	(config-qos-map)#**match vlan** <*id*> Specifies which traffic should be processed by this QoS map according to VLAN association. Valid range is **1** to **4095**.
Step 3	Apply an action to the matched traffic.
	(config-qos-map)#**bandwidth** <*rate*> **[Kbps** | **Mbps]** or (config-qos-map)#**bandwidth [percent** <*value*> **| remaining percent** <*value*>**]** Specifies the bandwidth allocation for individual traffic classes for CBWFQ configurations. The **bandwidth** <*rate*> command allocates the minimum bandwidth for an absolute bandwidth in Kbps. The valid range is **8** to **2000000** Kbps. The **bandwidth percent** <*value*> command allocates the minimum bandwidth as a percentage of the total interface bandwidth. The **bandwidth remaining percent** <*value*> command allocates the minimum bandwidth as a percentage of the total interface bandwidth not allocated to priority classes in the QoS map.

Table 16. QoS Configuration Steps *(Continued)*

Step	Command and Description
	(config-qos-map)#**priority** <*rate*> **[Kbps | Mbps] [**<*burst size*>**] [Bytes | KB | MB] [strict-rate-limiting]** or (config-qos-map)#**priority percent** <*value*> **[**<*burst size*>**] [Bytes | KB | MB] [strict-rate-limiting]** or (config-qos-map)#**priority unlimited** Specifies a high-priority queue, prioritizing the traffic above all others. The **priority percent** <*value*> command allocates a maximum bandwidth for the queue as a percentage of the total interface bandwidth. The **priority unlimited** command indicates there is no limit on the queue bandwidth. Entering a <*burst size*> value specifies a maximum burst size (in bytes) for traffic in this queue. Range for <*burst size*> is **32** to **1000000** bytes. The **strict-rate-limiting** keyword, when used with the **priority** command, limits priority traffic to a maximum rate as specified by the <*rate*> variable. When used with **priority percent** command, it limits priority traffic to a maximum percentage of the interface bandwidth as specified by the <*value*> variable.
(Optional)	Mark packets using **set** commands.
	(config-qos-map)#**set cos** <*value*> Assigns the CoS value within a QoS map. Valid range is **0** to **7**.
	(config-qos-map)#**set dscp [**<*value*> **| af***xx* **| cs***x* **| default | ef]** Modifies the DSCP field of packets for outgoing traffic serviced by the QoS policy. Use the **no** form of this command to remove a specified DSCP value. Valid range for <*value*> is **0** to **63**. Assured forwarding (AF) class and subclass can be specified using the **af***xx* keyword. Select from **11** (001010), **12** (001100), **13** (001110), **21** (010010), **22** (010100), **23** (010110), **31** (011010), **32** (011100), **33** (011110), **41** (100010), **42** (100100), or **43** (100110). Class selector (CS) value can be specified using the **cs***x* keyword. Valid range for CS is **1** to **7**. The **default** keyword indicates using the default IP DCSP value (000000). Marking for expedited forwarding (EF) is indicated by the **ef** keyword.
	(config-qos-map)#**set precedence** <*value*> Modifies the IP precedence field of packets for outgoing traffic serviced by the QoS policy. The valid range is **0** to **7**.
(Optional)	Configure traffic shaping.
	(config-qos-map)#**shape average** <*rate*> **[bps | Kbps | Mbps] [burst** <*size*>**] [Bytes | KB | MB] [count-eth-overhead]** Shapes the traffic in this class to an average rate. Valid range is **8192** to **1000000000** bps. An optional burst rate can be configured in bytes using the **burst** keyword followed by the number of bytes. Valid range for burst size is **1600** to **6250000** bytes. Including the keyword **count-eth-overhead** includes the Ethernet header overhead bytes when determining packet size. The **shape average** command cannot be specified in conjunction with the **priority** command in a QoS entry.

Table 16. QoS Configuration Steps *(Continued)*

Step	Command and Description
(Optional)	Configure traffic policing.
	(config-qos-map)#**police cir** <*rate*> **[bps | Kbps | Mbps] [cbs** <*size*>**] [Bytes | KB | MB] [count-eth-overhead]** Polices the traffic in this class based on CBS and CIR values. Valid CBS range is **8192** to **1000000000** bps. An optional CBS rate can be configured in bytes using the **cbs** keyword followed by the number of bytes. Valid range for CBS size is **1600** to **6250000** bytes. Including the keyword **count-eth-overhead** includes the Ethernet header overhead bytes when determining packet size.
(Optional)	Configure traffic shaping.
Step 4	Assign the QoS map to the WAN interface.
	(config)#**interface** <*interface*> (config-interface)#**qos-policy [in | out]** <*name*> Assigns the QoS map to the interface.

Table 17. Additional QoS Configuration Settings

Command	Description
(config-qos-map)#**qos-policy** <*name*>	Subdividing QoS Classes
	Divides a class into more specific subclasses within a QoS map. Child maps cannot be further subdivided. A child map cannot reference another child map.

Troubleshooting

After configuring QoS, several **show** commands can be issued from Enable mode in the CLI to assist in troubleshooting and verifying your configuration. The following table contains these commands and descriptions.

Table 18. Enable Mode Troubleshooting Commands

Command	Description
show ip access-lists <*ipv4 acl name*> or **show ipv6 access-lists** <*ipv6 acl name*>	Displays all configured IPv4 or IPv6 ACLs in the system (or a specific list).

Table 18. Enable Mode Troubleshooting Commands

Command	Description
show interfaces <*interface*>	Displays configuration parameters and current statistics for all interfaces (or a specified interface). Specify an interface in the format <*interface type [slot/port* | *slot/port.subinterface id* | *interface id* | *interface id.subinterface id]*>. For example, for a Frame Relay subinterface, use **fr 1.17**. Type **show qos map interface ?** command for a complete list of interfaces.
show qos map [<*name*> **|** <*name*> <*number*>**]**	Displays configuration information, entries, and interfaces using the map. Use the <*name*> option to show only the entries of a specific map. Use the <*name*> and <*number*> options together to show only the specified entry of the specified map.
show qos map interface <*interface*>	Displays priority queue discards per class information for the QoS map applied to the specific interface including the number of packet matches.
show queue <*interface*> **[child]**	Displays summary and per-conversation information associated with an interface queue. Per-conversation details are only displayed if the interface has sufficient traffic to be congested and packets are being held in the interface queue. Use the **child** keyword to display subqueue statistics.
show queuing [fair]	Displays information associated with configured queuing methods. Use the optional keyword **fair** to display only information on the WFQ configuration.
show running-config qos-map [verbose]	Displays the QoS maps configured in the unit. The optional **verbose** keyword displays detailed information.

Show Commands Sample Output

The following examples provide sample output from each of the show commands mentioned in *Table 18 on page 47*.

```
#show ip access-lists
* - Indicates access list entry disabled by track.
Standard IP access list wizard-ics
   remark Internet Connection Sharing
  permit any (5 matches)
Extended IP access list CUSTOMER1
  permit ip 192.168.1.0 0.0.0.255 any (4151312 matches)
Extended IP access list CUSTOMER2
  permit ip 192.168.2.0 0.0.0.255 any (0 matches)
Extended IP access list CUSTOMER3
  permit ip 192.168.3.0 0.0.0.255 any (0 matches)
Extended IP access list internet
  permit tcp any  any eq www (0 matches)
Extended IP access list self
```

```
    remark Traffic to NetVanta
   permit ip any any log (0 matches)
Extended IP access list udp
   permit udp any any (0 matches)

#show interfaces t1 1/1
t1 1/1 is UP
      Receiver has no alarms
      T1 coding is B8ZS, framing is ESF
      Clock source is internal, FDL type is ANSI
      Line build-out is 0dB
      No remote loopbacks, No network loopbacks
      Acceptance of remote loopback requests enabled
      Tx Alarm Enable: rai
      Last clearing of counters 00:21:45
            loss of frame  : 0
            loss of signal : 0
            AIS alarm      : 0
            Remote alarm   : 0

DS0 Status: 123456789012345678901234
                  NNNNNNNNNNNNNNNNNNNNNNNN
Status Legend: '-' = DS0 is unallocated
                              'N' = DS0 is dedicated (nailed)

Line Status: -- No Alarms --

5 minute input rate 64 bits/sec, 0 packets/sec
5 minute output rate 401832 bits/sec, 440 packets/sec
Current Performance Statistics:
      0 Errored Seconds, 0 Bursty Errored Seconds
      0 Severely Errored Seconds, 0 Severely Errored Frame Seconds
      0 Unavailable Seconds, 0 Path Code Violations
      0 Line Code Violations, 0 Controlled Slip Seconds
      0 Line Errored Seconds, 0 Degraded Minutes

TDM group 1, line protocol is UP
Encapsulation PPP (ppp 1)
      306 packets input, 11724 bytes, 0 no buffer
      0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame
      0 abort, 0 discards, 0 overruns
      570907 packets output, 65060028 bytes, 0 underruns

#show qos map
qos map SET-DSCP
      map entry 10
            match ip list CUSTOMER1
            set DSCP value to af11 (10)
    map entry 20
        match ip list CUSTOMER2
        set DSCP value to af21 (18)

    map entry 30
        match ip list ACL CUSTOMER3
        set DSCP value to af31 (26)

    Interfaces using qos map SET-DSCP:
        eth 0/1:Input (enabled)

qos map SHAPE-IN
    map entry 10
        match ip list CUSTOMER1
        class shape rate: 400 (kilobits/sec), average

    map entry 20
        match ip list CUSTOMER2
        class shape rate: 400 (kilobits/sec), average

    map entry 30
        match ip list CUSTOMER3
        class shape rate: 400 (kilobits/sec), average

    Interfaces using qos map SHAPE-IN:
        eth 0/1:Output (enabled)

qos map SHAPE-OUT
    map entry 10
        match dscp af11
        class shape rate: 400 (kilobits/sec), average

    map entry 20
        match dscp af21
        class shape rate: 400 (kilobits/sec), average

    map entry 30
        match dscp af31
        class shape rate: 400 (kilobits/sec), average

    Interfaces using qos map SHAPE-OUT:
        ppp 1:Output (enabled)
```

#**show qos map interface ethernet 0/1**

```
eth 0/1

    qos-policy out: SHAPE-IN
    map entry 10
        match ip list CUSTOMER1
        class shape rate: 400 (kilobits/sec), average
        budget: 2500/2500 bytes (current/max)
        800 bytes added to budget every 16 ms
        packets sent: 0
        packets waiting: 0
        packets dropped: 0
        packets delayed: 0

    map entry 20
        match ip list CUSTOMER2
        class shape rate: 400 (kilobits/sec), average
        budget: 2500/2500 bytes (current/max)
        800 bytes added to budget every 16 ms
        packets sent: 0
        packets waiting: 0
        packets dropped: 0
        packets delayed: 0

    map entry 30
        match ip list CUSTOMER3
        class shape rate: 400 (kilobits/sec), average
        budget: 2500/2500 bytes (current/max)
        800 bytes added to budget every 16 ms
        packets sent: 0
        packets waiting: 0
        packets dropped: 0
        packets delayed: 0

    map entry default
        packets matched: 46, bytes matched: 11868
        packets dropped: 0, bytes dropped: 0
        5 minute offered rate 64 bits/sec, drop rate 0 bits/sec

#show qos map interface gig 0/2.1
 giga-eth 0/2.1
  qos-policy out: MAP_OUT
   map entry 11
     match ip dscp af11
     set egress-queue value to 0
     packets matched: 7, bytes matched: 1022
     5 minute offered rate 0 bits/sec
   map entry 12
     match ip dscp af12
     set egress-queue value to 0
     packets matched: 0, bytes matched: 0
     5 minute offered rate 0 bits/sec
   map entry 13
```

```
     match ip dscp af13
     set egress-queue value to 0
     packets matched: 5, bytes matched: 730
     5 minute offered rate 16 bits/sec
   map entry default
     packets matched: 26, bytes matched: 4812
     packets dropped: 0, bytes dropped: 0
     5 minute offered rate 0 bits/sec, drop rate 0 bits/sec

 giga-eth 0/2.1
  qos-policy in: MAP_IN (enabled)
   map entry 11
     match ip dscp af11
     set DSCP value to 0
     packets matched: 7, bytes matched: 896
     5 minute offered rate 0 bits/sec, drop rate 0 bits/sec
   map entry 12
     match ip dscp af12
     set DSCP value to 0
     packets matched: 5, bytes matched: 640
     5 minute offered rate 16 bits/sec
   map entry 13
     match ip dscp af13
     set DSCP value to 0
     packets matched: 5, bytes matched: 640
     5 minute offered rate 16 bits/sec, drop rate 0 bits/sec
   map entry default
     packets matched: 0, bytes matched: 0
     5 minute offered rate 0 bits/sec
```

```
#show qos map interface ppp 1
ppp 1

      qos-policy out: SHAPE-OUT

      map entry 10
            match dscp af11
            class shape rate: 400 (kilobits/sec), average
            budget: 82/2500 bytes (current/max)
            100 bytes added to budget every 2 ms
            packets sent: 506739
            packets waiting: 64
            packets dropped: 596
            packets delayed: 491621

      map entry 20
            match dscp af21
            class shape rate: 400 (kilobits/sec), average
            budget: 2500/2500 bytes (current/max)
            100 bytes added to budget every 2 ms
            packets sent: 0
            packets waiting: 0
            packets dropped: 0
            packets delayed: 0

      map entry 30
            match dscp af31
            class shape rate: 400 (kilobits/sec), average
            budget: 2500/2500 bytes (current/max)
            100 bytes added to budget every 2 ms
            packets sent: 0
            packets waiting: 0
            packets dropped: 0
            packets delayed: 0

      map entry default
            packets matched: 38, bytes matched: 7220
            packets dropped: 0, bytes dropped: 0
            5 minute offered rate 48 bits/sec, drop rate 0 bits/sec
#show queue vlan 1
      Queueing method: weighted fair
      Output queue: 0/1/540/64/0 (size/highest/max total/threshold/drops)
      Conversations 0/1/256 (active/max active/max total)
      Available Bandwidth 75000 kilobits/sec

#show queuing
Weighted fair queue configuration:

      Interface       Discard         Conversation
                      threshold       subqueues
      eth 0/1         64              256
      ppp 1           64              256

#show running-config qos-map
Building configuration...
!
!
qos map SET-DSCP 10
  match list CUSTOMER1
  set dscp af11
qos map SET-DSCP 20
  match list CUSTOMER2
  set dscp af21
qos map SET-DSCP 30
  match list CUSTOMER3
  set dscp af31
!
qos map SHAPE-IN 10
```

```
 match list CUSTOMER1
 shape average 400000

qos map SHAPE-IN 20
 match list CUSTOMER2
 shape average 400000
qos map SHAPE-IN 30
 match list CUSTOMER3
 shape average 400000
!
qos map SHAPE-OUT 10
 match dscp af11
 bandwidth 1024
qos map SHAPE-OUT 20
 match dscp af21
 shape average 400000
qos map SHAPE-OUT 30
 match dscp af31
 shape average 400000
!
end
```

Additional Resources

There are additional resources available to aid in configuring your AOS unit. Many of the topics discussed in this guide are complex and require additional understanding. The documents listed below are available online at ADTRAN’s Support Forum at https://supportforums.adtran.com.

- *AOS Command Reference Guide*
- *Configuring IPv6 in AOS*
- *Configuring IP Access Control Lists (ACLs) in AOS*