6AOSCG0068-29B
April 2016

ADTRAN

Configuration Guide

Carrier Ethernet Services QoS Guide

This configuration guide will aid in the configuration of quality of service (QoS) for ADTRAN Operating System (AOS) products that support carrier Ethernet services. An overview of QoS terminology and general concepts are combined with detailed command descriptions and network examples to 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).

This guide contains the following sections:

Carrier Ethernet Services QoS Overview

The different types of traffic present on your network have specific needs for bandwidth, delay, and reliability. AOS must be able to recognize traffic types through classification and service the traffic according to specific requirements. QoS is used to appropriately allocate bandwidth, reduce packet delay, and ensure reliability for each data packet on your network.

ADTRAN provides a line of converged access router products that provide communication between customer networks (private local area networks (LAN)) and the service provider's Metro Ethernet network (MEN). This line of products is called Carrier Ethernet Customer Edge Solutions. Functioning as the demarcation point between the service provider's network and customer's network, these products are capable of providing QoS assurance. The traffic flow is controlled by using QoS maps, Ethernet virtual connection (EVC) maps, hardware queues, policers, and shapers.

The QoS explanations presented in this guide, only apply to ADTRAN Carrier Ethernet Customer Edge Solutions products capable of carrier Ethernet services. This configuration guide discusses advanced concepts and assumes prior knowledge of configuring these products. For more detailed information, refer to the *Carrier Ethernet Services in AOS* guide before attempting these advanced concepts.

For detailed information regarding specific command syntax, refer to the *AOS Command Reference Guide* available online at https://supportforums.adtran.com.

Policer

A policer is a bandwidth-limiting profile that limits the amount of inbound traffic into the AOS product from the user-network interface (UNI). This component is commonly used to limit Layer 2 traffic in the UNI-to-MEN direction. The amount of traffic can be limited per EVC, policer, UNI, subinterface, or EVC map based on traffic committed burst size (CBS), committed information rate (CIR), excess burst size (EBS), and excess information rate (EIR). These thresholds are used to determine when the bandwidth usage is too great, and how to mark or drop traffic based on the configured thresholds.

Policers can be applied in one of the following ways:

- Ingress bandwidth policer per UNI
- Ingress bandwidth policer per EVC
- Ingress bandwidth policer per EVC map
- Ingress bandwidth policer per Ethernet subinterface
- Ingress bandwidth policer from another policer

In typical applications, the bandwidth available on the EVC is less than the bandwidth available at the UNI port. Bandwidth bottleneck is typically in the UNI-to-MEN direction; therefore, all policers are applied only for traffic flowing in the UNI-to-MEN direction. Policers are not applied to the traffic flowing in the MEN-to-UNI direction.

The configurable attributes of the EVC policer include the profile name, the CBS, CIR, EBS, and EIR thresholds, whether the profile is enabled, and the components to which the policer profile is applied (EVCs, UNIs, EVC maps, etc.).

 Copyright © 2016 ADTRAN, Inc.

Policing

Policing is a rate-based admission control function using a leaky/token bucket algorithm. The purpose of a policer is to keep non-conforming traffic from entering the network and degrading other customers and/or services. The carrier Ethernet Services AOS products supports one rate two color (1R2C) and two rate three color (2R3C) policing using the policer.

One Rate Two Color

The 1R2C algorithm uses a leaky bucket algorithm to mark packets either green or red, where red packets are immediately dropped (see *Figure 1 on page 3*). At the output of the 1R2C policer, the average rate and burst size is no greater than CIR and CBS respectively. The leak rate of the bucket is set to the CIR in kbps. The depth of the bucket is set to CBS in bytes. If the traffic rate entering the policer exceeds both CIR and CBS, the packet will be marked red and discarded.

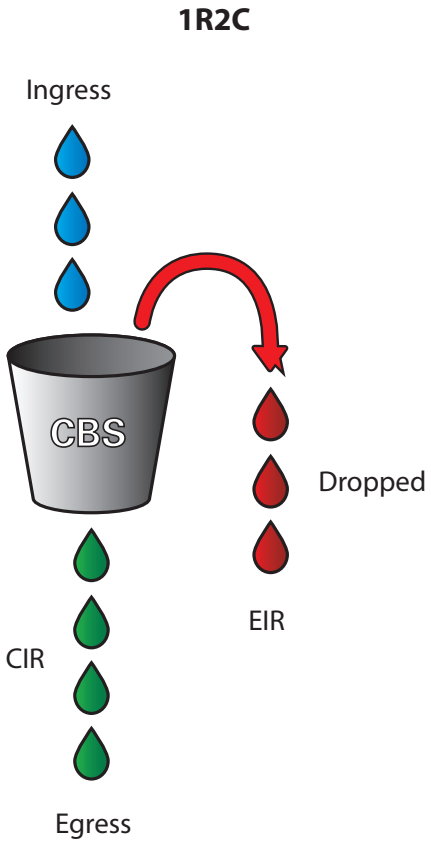


Figure 1. One Rate Two Color Leaky Bucket Algorithm

Two Rate Three Color (2R3C)

The 2R3C algorithm uses a dual leaky bucket algorithm to mark packets green, yellow, or red, where red packets are immediately dropped see *Figure 2 on page 4*). The leak rate of the first bucket is the CIR in kbps and the leak rate of the second bucket is the EIR in kbps. Packets meeting the CIR and CBS are marked green. Packets arriving in excess of CIR and CBS are treated as EIR and EBS packets and marked

 Copyright © 2016 ADTRAN, Inc.

yellow. Packets arriving in excess of CIR + CBS + EIR + EBS are marked red and discarded. At the output of the 2R3C policer, the average rate and burst size of green packets is no greater than CIR and CBS, respectively. The average rate and burst size of all packets is no greater then CIR + EIR and CBS + EBS, respectively.

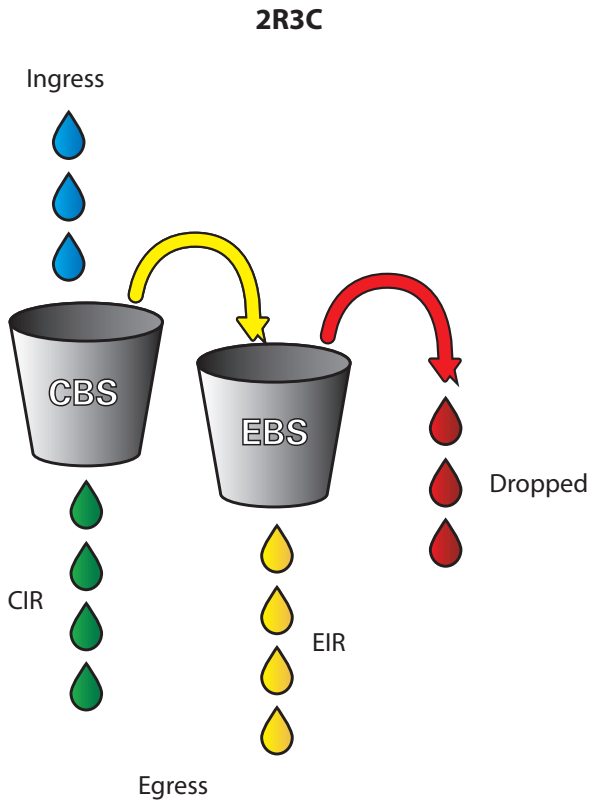


Figure 2. Two Rate Three Color Leaky Bucket Algorithm

Egress Rate Shaping

A shaper is used to limit the rate and smooth bursts of traffic traveling between the AOS product and the MEN. Unlike a policer, which discards large bursts of traffic, a shaper is able to *delay* bursts. Much like a policer, the port shaper uses a token bucket. However, when large bursts are received, the packets are backed up into the queue rather than being discarded immediately. When a packet arrives at the shaper, if there are sufficient tokens available, the packet is transmitted without delay. If there are insufficient tokens in the bucket, the packet is delayed until there are enough tokens in the bucket to allow transmission. Shapers can be used for both Layer 2 and Layer 3 transmissions.

The benefit of a shaper is that it will not drop frames with a small burst of traffic, but it does add latency. The benefit of a policer is that it does not add latency while protecting the network, but does drop any traffic that exceeds the burst capacity. Selecting one over the other is dependent on the latency and loss tolerance of the data. Rate shapers are much friendlier to Transmission Control Protocol (TCP) traffic flows than policers. A small increase in latency leads to better TCP throughput than large losses of packets that can force TCP to revert to slow start. Traffic may still be discarded due to the queue congestion management strategy employed.

Copyright © 2016 ADTRAN, Inc.

The configurable attributes of the shaper include specifying to which interface or queue(s) the shaper is applied and the traffic rate.

Queue Management

Queuing and queue management forms the basis of most congestion management strategies currently deployed in networks. The purpose of a queue is to absorb packets when the ingress rate exceeds the egress rate. This allows bursts of packets to be transmitted through the system without incurring loss. However, while queues can keep packet loss to a managed level, it is at the expense of packet delay and packet delay variation.

Interface Queues

Each interface, whether an Ethernet in the first mile (EFM) group or Gigabit Ethernet interface, provides eight hardware queues for traffic management and congestion avoidance. Queues are used for both Layer 2 and Layer 3 traffic. These queues absorb packets when the ingress rate of traffic exceeds the egress rate, allowing bursts of packets to be transmitted through the system without incurring loss. The individual queues can be used in strict priority or weighted fair queuing (WFQ) configurations to allow the desired traffic prioritization.

Queues must be managed to prevent packet loss and delay along the network. Configurable attributes of the queue include specifying the queue congestion management algorithm, class of service (CoS) settings, drop probabilities, queue depth, thresholds, and the weight of the queue (when using WFQ) for traffic traversing the MEN port interface.

Queue Depth

The queue depth should be carefully considered. Queues that are too deep can have an adverse affect on TCP throughput, by increasing the round trip time. Queues that are too shallow can result in queue overflows (packet loss) and decreased TCP window size, which also adversely affects TCP throughput.

The effect of network delay (caused by queue depth, congestion, link speed, and other factors) can lead to surprisingly low TCP throughput even when the links are high speed. Maximum theoretical TCP throughput can be calculated as follows:

TCP Window Size (in bits) / Round Trip Time (in seconds)

For example, a computer with a 65,535 bit window size connecting to an FTP server with a round trip time of 30 ms will have the following theoretical maximum throughput level:

65535*8 / 0.030 = 17.476 Mbps

Queue Congestion Management

A method for controlling the admission of packets to the queue is necessary during times of traffic congestion. AOS supports the following four queue congestion management disciplines for this task:

- *Tail Drop on page 6*
- *Weighted Tail Drop on page 7*
- *Random Early Detection on page 8*
- *Weighted Random Early Detection on page 9*

 Copyright © 2016 ADTRAN, Inc.

Tail Drop

Tail drop is a first-in first-out (FIFO) queue congestion management discipline. When a queue fills up, no additional packets are admitted to the queue. They are simply discarded. The packets that arrive first in the queue are the first out of the queue. Packet color is not a criteria used in the drop probability. This is the default queue congestion management discipline for AOS.

Figure 3 illustrates how tail drop behaves when the queue is filled and emptied, and the queue is not completely full. The packets arriving at the ingress port at a higher rate than can be emptied out of the egress port will fill the queue.

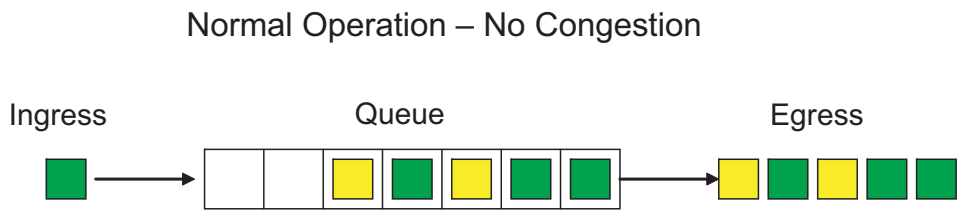


Figure 3. Tail Drop Queue, No Congestion

In *Figure 4*, packets that arrive while the queue is full (in a congested state) are discarded. Once the congestion is alleviated and space becomes available in the queue, new arriving packets are admitted.

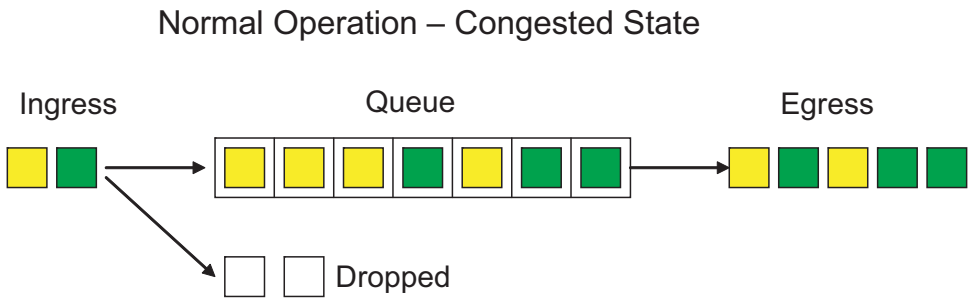


Figure 4. Tail Drop Queue, Congested

Figure 5 on page 7 illustrates the drop probability for tail drop with a maximum queue depth of 125 packets. Maximum queue depth is user configurable. Packet color is not a criteria used for drop probability.

Copyright © 2016 ADTRAN, Inc.

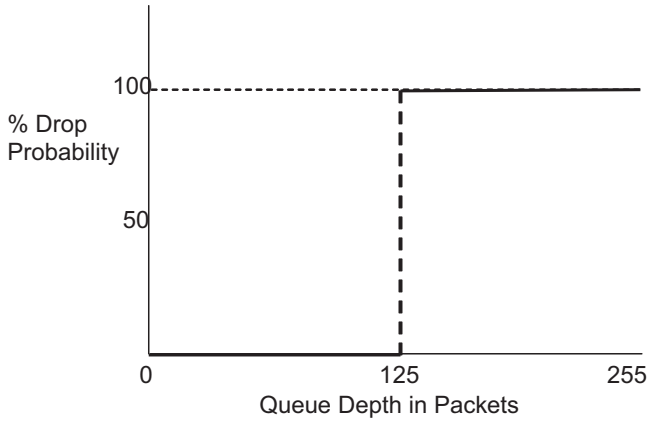


Figure 5. Drop Probability for Tail Drop

Weighted Tail Drop

Weighted tail drop is a color-aware FIFO queue congestion management discipline. When a queue fills up, no additional packets are admitted to the queue. They are simply discarded. The packets that arrive first in the queue are the first out of the queue. Packet color is used as a criteria in the drop probability.

This is the default queue congestion management discipline for the AOS products when using policers with EIR settings.

Figure 6 and *Figure 7* illustrate how tail drop behaves when the queue is filled and emptied, and the queue is not completely full. Packets arriving at the ingress port at a higher rate than can be emptied out of the egress port will fill the queue.

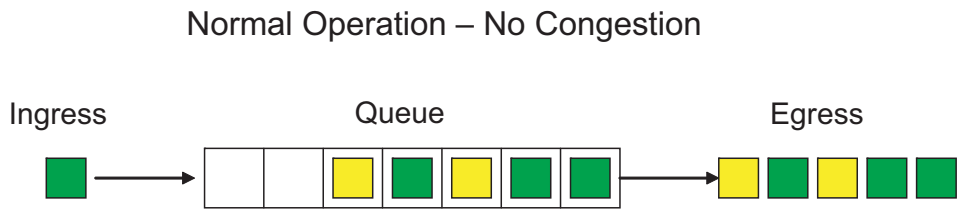


Figure 6. Tail Drop Queue, No Congestion

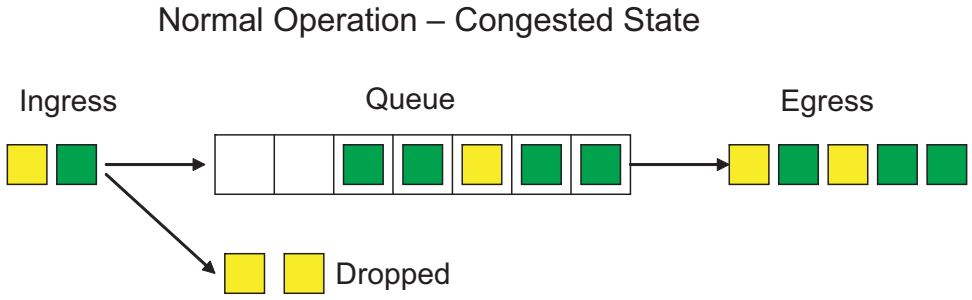


Figure 7. Tail Drop Queue, Congested

Copyright © 2016 ADTRAN, Inc.

Random Early Detection

Random early detection (RED) is an active queue management discipline designed for TCP traffic flows. When multiple TCP flows are congested, packets can be discarded. If enough packets are lost, TCP will revert back to TCP slow start. If several flows return to TCP slow start, they will quickly ramp up and cause congestion, resulting in packet loss and the return to TCP slow start. This see-saw affect on TCP throughput is called global TCP synchronization. RED was designed to alleviate the global TCP synchronization issue by randomly discarding packets entering the queue after the average queue depth reaches a configured threshold.

When the average queue depth reaches the configured threshold, a drop probability is assigned to the next incoming packet. Each incoming packet may be dropped based on the configured drop probability. When the maximum threshold of the average queue depth is reached, all packets will be discarded (100 percent drop probability), making the queue management discipline similar to tail drop.

Figure 8 illustrates how packets are treated when the configured minimum threshold is reached. A newly arriving packet will be assigned a drop probability according to the average queue depth and the RED slope. Packets will be admitted to the queue or discarded, depending on the probability.

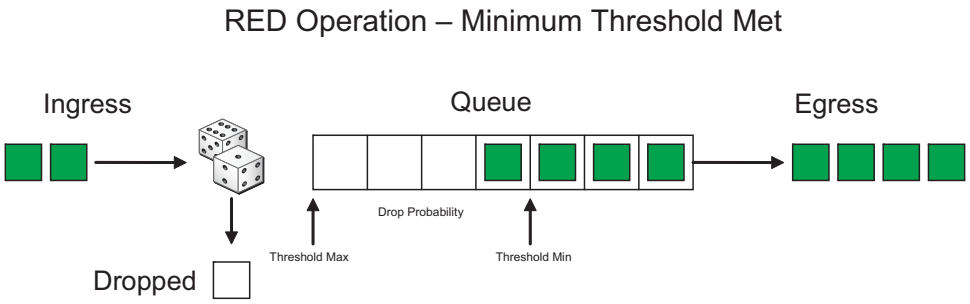


Figure 8. Random Early Detection Queue Minimum Threshold

In *Figure 9*, once the maximum configured threshold is reached, all packets are discarded until congestion is relieved.

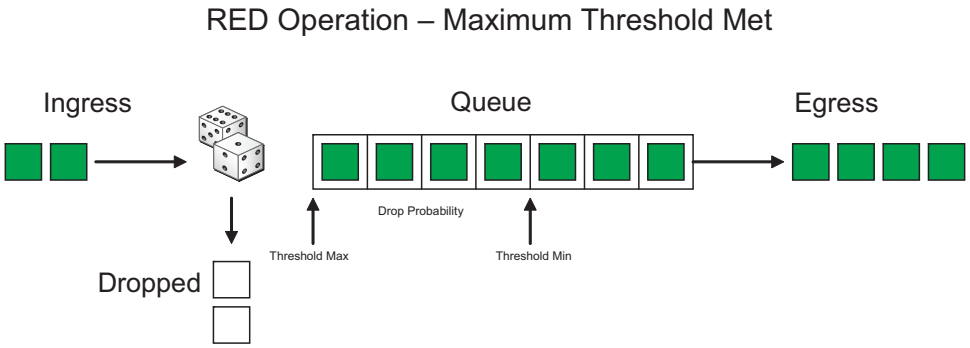


Figure 9. RED Queue Maximum Threshold

Copyright © 2016 ADTRAN, Inc.

Figure 10 illustrates the drop probability for RED with a minimum threshold of 125 packets, a maximum threshold of 185 packets, and a drop probability of 40 percent. Packet color is not a criteria used for drop probability.

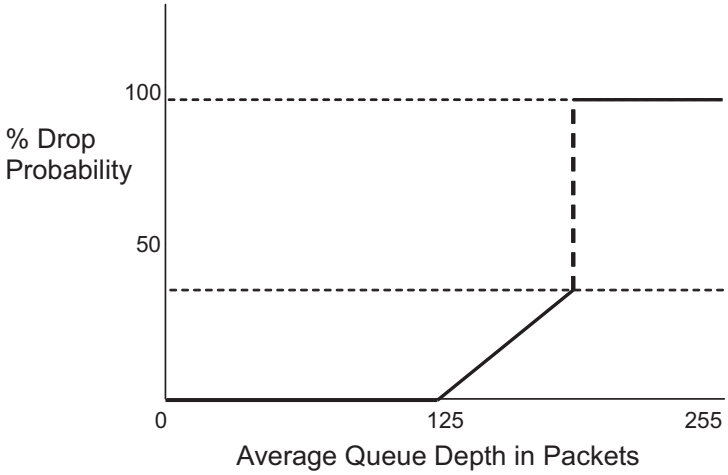


Figure 10. Drop Probability for RED

NOTE *The maximum queue depth should be set to the max threshold.*

Weighted Random Early Detection

Weighted random early detection (WRED) is an active queue congestion management discipline that adds packet color to the thresholds of the drop probability slopes. Different slopes can be set up to treat conforming (green) and non-conforming (yellow) packets differently. As the average queue depth increases, AOS will begin randomly discarding yellow packets before randomly discarding green packets. Once the maximum threshold of the average queue depth is reached, all packets will be discarded (100 percent drop probability) making WRED perform similar to tail drop. Color and average queue depth are the criteria used to determine drop probability.

NOTE *The yellow maximum threshold should be less than or equal to the green minimum threshold to avoid dropping green packets before all yellow packets are dropped.*

WRED is NOT a suitable queue congestion management discipline for User Datagram Protocol (UDP) traffic flows or any protocol that is packet loss sensitive.

Figure 11 illustrates queue management when no congestion is present. Ingress packets are queued and transmitted in a FIFO manner.

 Copyright © 2016 ADTRAN, Inc.

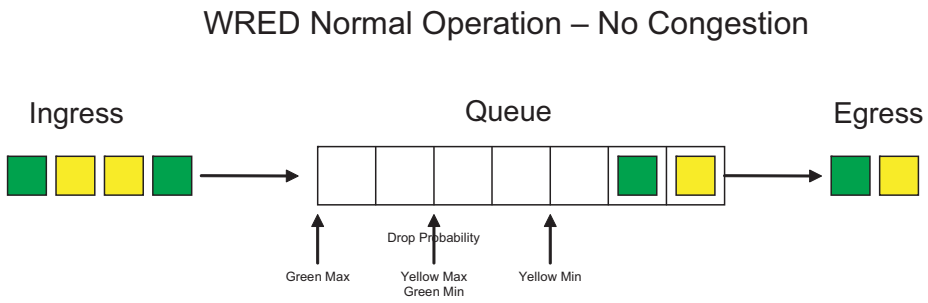


Figure 11. WRED Queue, No Congestion

Figure 12 illustrates the behavior for WRED yellow packets when the minimum threshold is met. Yellow packets are dropped with probability determined by the average queue depth and the Yellow WRED slope, while Green packets are admitted to the queue.

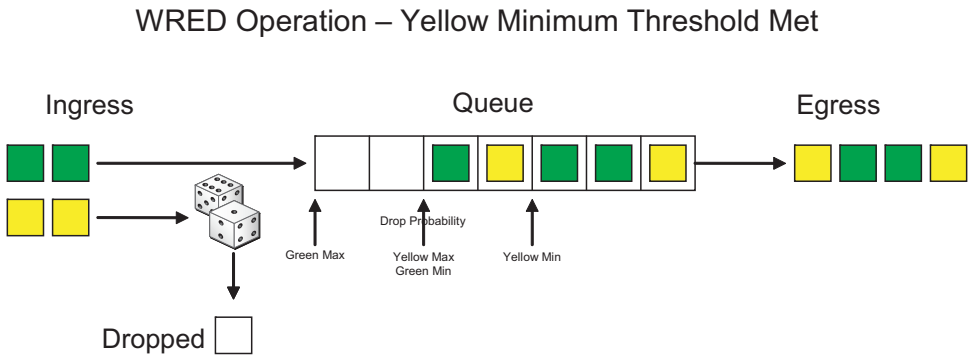


Figure 12. WRED Queue Yellow Minimum Threshold

Figure 13 illustrates queue admittance for yellow and green packets when the yellow maximum and green minimum thresholds have been met. Yellow packets are discarded while green packets are run against the drop probability of the WRED slope to determine queue admittance.

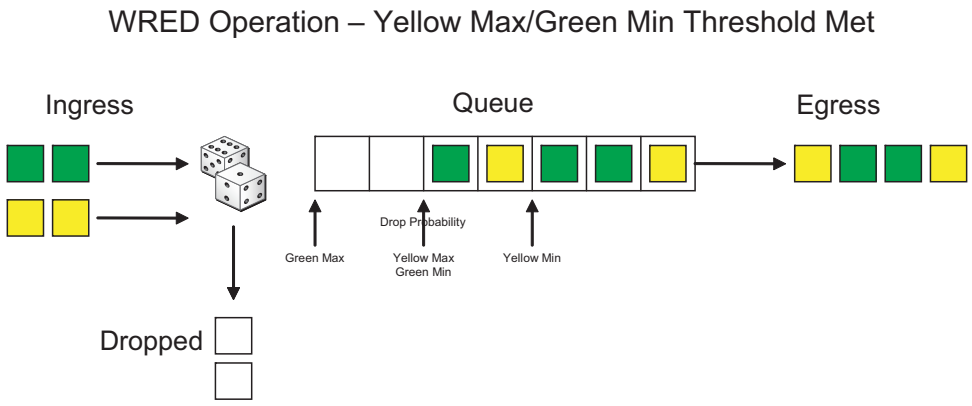


Figure 13. WRED Queue Yellow Maximum and Green Minimum Threshold

Copyright © 2016 ADTRAN, Inc.

In *Figure 14*, once the maximum configured green threshold is reached, all packets are discarded until congestion is relieved.

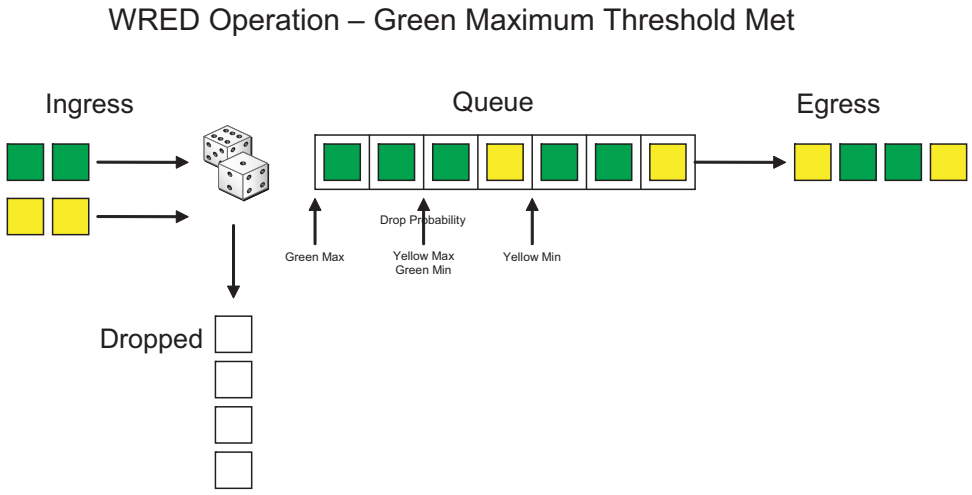


Figure 14. WRED Queue Green Maximum Threshold

The maximum queue depth should be set to the maximum threshold.

Figure 15 illustrates the drop probabilities of green and yellow packets based on the configurable slopes with the following settings: yellow minimum threshold 75, yellow maximum threshold 125, yellow drop probability of 40 percent, green minimum threshold 125, green maximum threshold 180 and green drop probability of 40 percent.

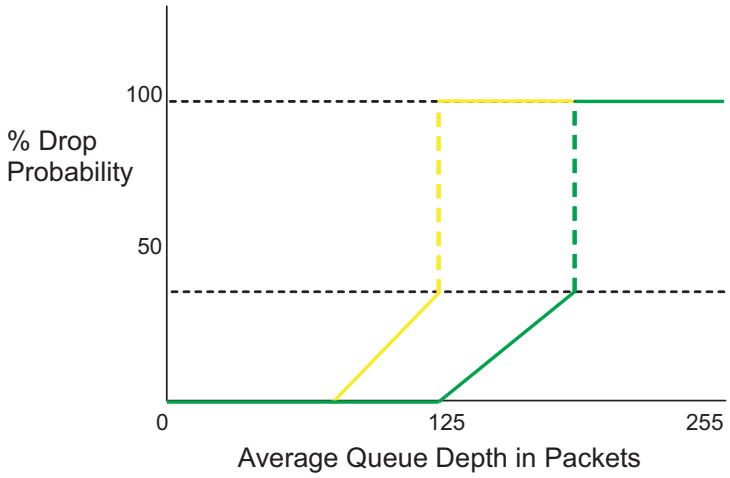


Figure 15. Drop Probability for WRED Slopes

Copyright © 2016 ADTRAN, Inc.

> *The yellow maximum threshold should be less than or equal to the green minimum threshold to avoid dropping green packets before all yellow packets are dropped.*

Packet Scheduling

The final step in the packet flow through the device is scheduling to the egress port. The following scheduling disciplines are currently used by ADTRAN:

- Strict Priority Scheduling (SPS)
- WFQ

Strict Priority Scheduler

The AOS carrier Ethernet products use a SPS (see *Figure 16*). Queue 7 will be serviced first before all other queues. Once Queue 7 is empty, Queue 6 will be serviced, then Queues 5, 4, 3, 2, 1, and 0 respectively. A lower priority queue will not be serviced until all of the higher priority queues are empty. If a packet enters a higher priority queue than the one currently being serviced, the switch continues with the current packet before returning to schedule the higher priority queue. For example, if the switch is currently emptying Queue 1, and a packet enters Queue 3, the switch will complete servicing the current Queue 1 packet, then return to Queue 3 and empty it before resuming packet scheduling on Queue 1.

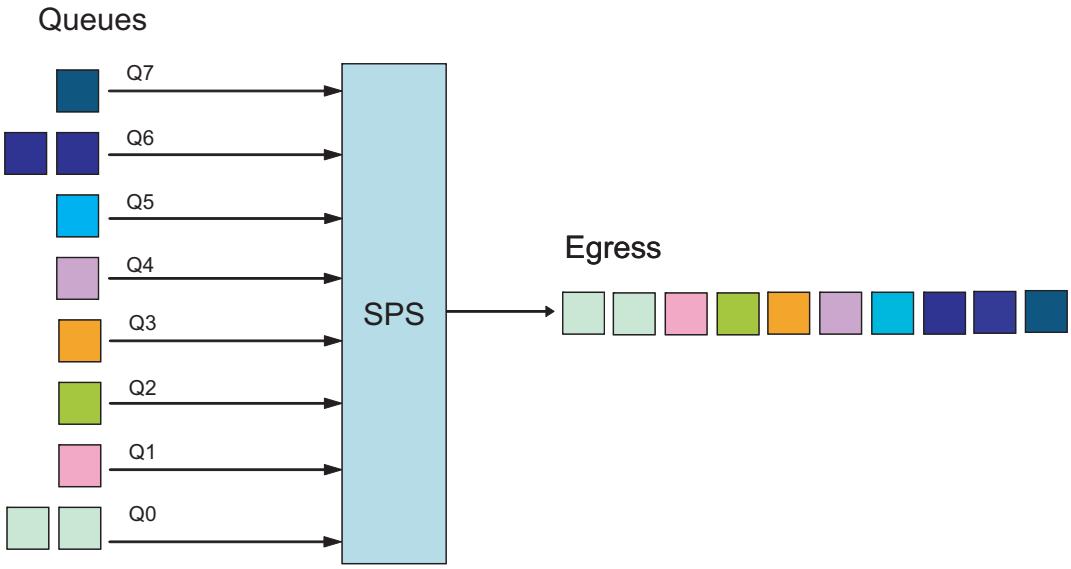


Figure 16. Strict Priority Scheduling

SPS is an excellent choice for latency sensitive traffic, such as (VoIP) and video. However, it has one potential drawback. If the higher priority queues are oversubscribed or not policed, they can potentially starve the lower priority queues.

Copyright © 2016 ADTRAN, Inc.

Weighted Fair Queuing

The AOS carrier Ethernet products support WFQ using the deficit weighted round robin (DWRR) scheduling algorithm. DWRR is a packet-based version of the generalized process sharing (GPS) scheduling ideal and ensures that bandwidth is shared fairly regardless of packet size distribution in the data stream.

When two or more queues are set to the same CoS value, a DWRR scheduler is nested below the SPS of the switch. When a weight is assigned using the queue interface command set, the queues will be weighed against each other using the weights assigned, 0 to 100 percent. DWRR will ensure that each queue is scheduled with a minimum level of bandwidth available and in the percentage stated compared to the other queues in the same CoS. If no weight is assigned, the queues will be weighed against each other evenly. For instance, if two queues share the same CoS value, each queue will be given 50 percent of the bandwidth available. If four queues share the same CoS value, each queue will be given 25 percent of the bandwidth available.

In the architecture shown in *Figure 17*, the expedited forwarding (EF) queue will be serviced first, before the assured forwarding (AF) queues will be serviced. The packets coming from the DWRR nested scheduler will be weighed against each other and sent to the SPS scheduler before egressing the interface. Only after the EF and AF queues are emptied will the best effort (BE) queue be serviced.

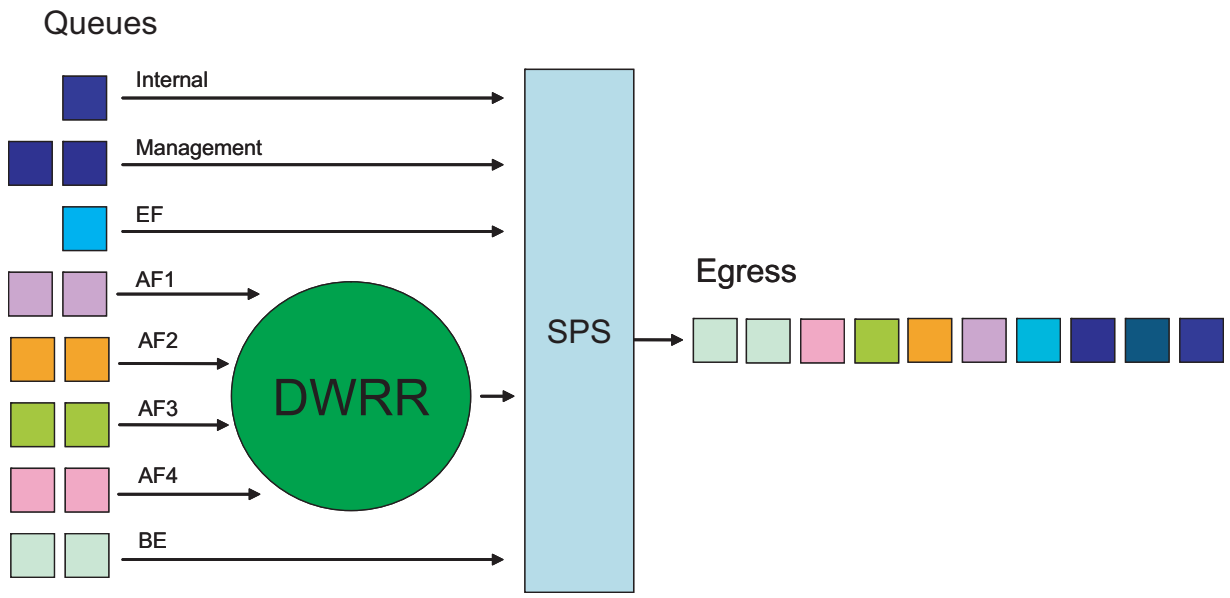


Figure 17. DWRR Scheduling

 Copyright © 2016 ADTRAN, Inc.

NOTE *It is still possible to starve the lower priority BE queue if the EF and AF traffic classes are not policed.*

DSCP 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 (type of service (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:

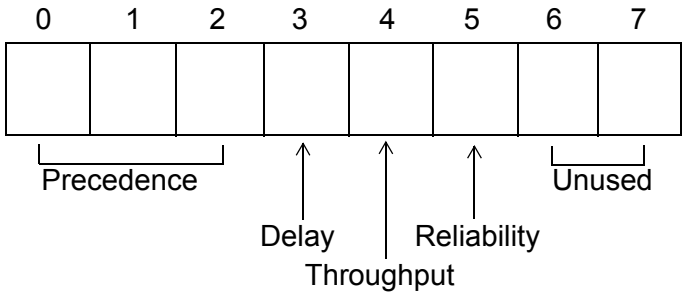


Figure 18. Type of Service Field Bits

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. See *Table 1* for the 3-bit IP precedence field and an explanation of the traffic type it represents.

Table 1. 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

 Copyright © 2016 ADTRAN, Inc.

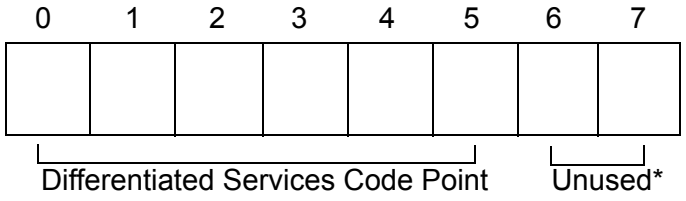
Table 1. IP Precedence Values

3-bit IP Precedence Value	Traffic
001	Priority Traffic
000	Routine Data

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 DiffServ (DS) 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 19. Differentiated Services Field Bits

Equipment following the DiffServ model (DS-compliant nodes) must use the entire 6-bit differentiated services code point (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

 Copyright © 2016 ADTRAN, Inc.

to 0. This compatibility requires DiffServ nodes to provide the same data services as are provided by nodes implementing IP precedence. *Table 2* provides a comparison of IP precedence values to their corresponding DSCP values.

Table 2. 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 AF PHB creates four main classes of service (see *Table 3*.)

Table 3. 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 as shown in *Table 4*.

Table 4. Assured Forwarding PHB Subclasses

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

Copyright © 2016 ADTRAN, Inc.

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

Table 5. 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).

For reference purposes, *Table 6* provides the command line interface (CLI) entries to use when entering AF values and their corresponding DSCP value.

Table 6. 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

Copyright © 2016 ADTRAN, Inc.

Table 6. Assured Forwarding DSCP Values *(Continued)*

CLI Entry	DSCP Value
41	100010
42	100100
43	100110

Hardware and Software Requirements and Limitations

QoS for carrier Ethernet services is only available on AOS platforms running AOS firmware R10.10.0 or later as outlined in the *AOS Product Feature Matrix*, available online at http://supportforums.adtran.com.

Rules for Provisioning EVCs, EVC Maps, Policers, Shapers, and Queues

To ensure valid provisioning, the rules below are enforced for EVCs, EVC maps, queues, policers, and shapers. In most cases, the value of the status attribute for an entity provides a brief description of the condition.

1. An EVC, EVC map, policer, or shaper is applied only if the respective EVC or interface is running.
2. Two EVC maps are considered to be duplicate if they both have the same UNI port, customer-edge (CE) virtual local area network (VLAN) ID, and overlapping ranges for CE VLAN priority, DSCP value, or untagged/priority tagged frames.
3. Two EVCs are considered to be duplicate if they both have the same value for the s-tag attribute.
4. Two policers are considered to be duplicate if they both have the same mode, UNI, and EVC attributes.
5. No two EVCs can have the same name.
6. No two EVC maps can have the same name.
7. No two policers can have the same name.
8. No two shapers can have the same name.
9. If the network element is managed through a VLAN on a designated EFM group or Ethernet port to which the system management EVC is connected as a MEN port, the following applies:
   - Any EVC connected to the same MEN port with an s-tag VLAN ID (VID) value equal to the management VID value is invalid.
   - If there are no EVCs connected to the MEN port, then any EVC map connected to the same port as a UNI is invalid.
   - If a port is connected to the system management EVC as a UNI, it cannot be used by any EVCs or EVC maps.
10. If the CE VLAN ID preservation attribute of an EVC is disabled, all of the associated EVC maps must have the same CE VLAN ID attribute value.
11. When multiple EVC maps are applied to a common EVC, each EVC map must have the same UNI. Multiple UNIs cannot be mapped to a common EVC.
12. If two EVC maps have the same UNI, only one of the EVC maps can be provisioned to allow untagged and priority tagged frames.

 Copyright © 2016 ADTRAN, Inc.

13. No one Ethernet frame can be governed by more than one policer.
14. When two or more EVC maps have overlapping criteria, and an incoming packet matches two or more of the criteria for the EVC maps, the EVC map that has provisioning options of higher precedence is used to forward traffic. EVC map order of precedence is outlined in *Table 7 on page 19*.

Table 7. EVC Map Traffic Forwarding Order of Precedence

Precedence	Provisioning Options
1	Traffic type + Untagged + DSCP + UNI port
2	Traffic type + Untagged + UNI port
3	Traffic type + P-bit + CE VLAN ID + UNI port
4	Traffic type + P-bit + UNI port
5	Traffic type + DSCP + CE VLAN ID + UNI port
6	Traffic type + DSCP + UNI port
7	Traffic type + CE VLAN ID + UNI port
8	Traffic type + UNI port
9	CE VLAN ID + Ethertype + DSCP + UNI port
10	Untagged + Ethertype + DSCP + UNI port
11	Untagged + Ethertype + UNI port
12	Untagged + DSCP + UNI port
13	Untagged + UNI port
14	CE VLAN ID + DSCP + UNI port
15	CE VLAN ID + P-bit + UNI port
16	Ethertype + DSCP + UNI port
17	CE VLAN ID + Ethertype + UNI port
18	CE VLAN ID + UNI port
19	DSCP + UNI port
20	P-bit + UNI port
21	Ethertype + UNI port
22	UNI port

 Copyright © 2016 ADTRAN, Inc.

Configuring Carrier Ethernet QoS

To configure QoS for carrier Ethernet services on an AOS product, you will need to complete several tasks, depending on your specific network requirements. The following sections are provided to assist you with configuration steps. Read each section carefully and complete the steps necessary for your deployment.

Accessing the AOS CLI

To begin configuring the carrier Ethernet services on the AOS product, access the CLI following 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.

> NOTE *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. Enter the Enable mode on your unit by entering **enable** at the prompt as follows:

   >enable

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

   #configure terminal
   (config)#

You can now begin configuring the carrier Ethernet features.

Configuring QoS for Layer 2 Carrier Ethernet Services

This section provides configuration options for only Layer 2 carrier Ethernet services. If your specific needs do not require Layer 2 services, you can skip this section.

For Layer 2 carrier Ethernet services, configure an EVC map that will match traffic destined for a specified EVC. Each EVC map is associated with a single EVC, and can match traffic based on various criteria. Optionally, you can specify 802.1p values for the s-tag and c-tag of the traffic and the queue used when the traffic is sent to the MEN.

 Copyright © 2016 ADTRAN, Inc.

Configuring QoS for Layer 2 services consists of the following steps:

Step 1: Create an EVC Map

Specify a name for the EVC map and enter the map's configuration mode using the **evc-map** <*name*> command from the Global Configuration mode prompt. The <*name*> parameter is the name of the EVC map. Using the **no** form of this command removes the EVC map from the AOS product's configuration. For example, to create an EVC map called **MAP1** and enter the EVC map's configuration mode, enter the command as follows:

```
(config)#evc-map MAP1
(config-evc-map MAP1)#
```

Step 2: Configure Traffic Match Criteria

Each EVC map can match traffic to an EVC based on the traffic's category of destination MAC address (for example, broadcast, multicast, unicast, or L2CP), CE VLAN ID, the CE VLAN priority (PRI) bit value, the DSCP value, Ethertype value, or if the traffic has no CE VLAN ID (untagged). When determining traffic match criteria, keep in mind you can specify multiple criteria for a single map. Multiple match statements function as a logical AND. If multiple criteria are entered in the map, the traffic must match all criteria to be mapped to the EVC.

Specify the traffic matching criteria for the map to send traffic to the associated EVC using the command **match [broadcast | ce-vlan-id** <*vlan id*> **| ce-vlan-pri** <*value*> **| destination mac address** <*mac address*>**| dscp** <*value*> **| ethertype** <*value*> **| l2cp | multicast | unicast | untagged]** from the EVC map's configuration mode. Use the **match** commands shown in *Table 8* to select traffic for the map entry.

By default, no matching criteria is specified. Using the **no** form of this command removes the matching criteria from the EVC map.

Table 8. EVC Map Match Commands

Command	Explanation
match broadcast	Matches traffic with a broadcast destination MAC address.
match ce-vlan-id <*vlan id*>	Matches traffic with the specified customer equipment (CE) virtual local area network (VLAN) ID. Valid range for <*vlan id*> is 1 to 4095.
match ce-vlan-pri <*value*>	Matches traffic with the specified CE VLAN priority value. The priority value is also the CE VLAN 802.1p value. Valid range for <*value*> is 0 to 7.
match destination mac address <*mac address*>	Matches traffic with the specified destination MAC address. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, 00:A0:C8:00:00:01).

 Copyright © 2016 ADTRAN, Inc.

Table 8. EVC Map Match Commands *(Continued)*

Command	Explanation
match dscp <*value*>	Matches IPv4 and IPv6 traffic based on DSCP value. Valid range is 0 to 63. For more information about DSCP values, refer to *DSCP Values Explained on page 14*.
match ethertype <*value***>**	Matches traffic with an Ethertype filter. The <*value*> parameter is expressed in hexadecimal format.
match l2cp	Matches traffic with an L2CP destination MAC address.
match multicast	Matches traffic with a multicast destination MAC address.
match unicast	Matches traffic with a unicast destination MAC address.
match untagged	Matches all untagged traffic.
All of these commands are entered from the EVC Map Configuration mode.	

For example, to configure an EVC map to send all traffic with a CE VLAN ID of **5** *and* a DSCP value of **10** to a specific EVC, enter the **match** command as follows:

```
(config-evc-map MAP1)#match ce-vlan-id 5
(config-evc-map MAP1)#match dscp 10
(config-evc-map MAP1)#
```

A common configuration mistake is to forget that Address Resolution Protocol (ARP) is not IPv4 traffic and thus create an EVC map to match IPv4 traffic with a certain DSCP value to send over an EVC without also adding a map that sends ARP over the same EVC. Without ARP to resolve the initial MAC address to IPv4 address binding, no IPv4 traffic can be sent.

You can also specify an Ethertype filter to use as matching criteria on the EVC map. Ethertype filters allow you to specify a certain Ethertype (such as ARP or Internet Protocol version 6 (IPv6)) as EVC map matching criteria for allowed traffic into the UNI interface. This feature can also be configured to drop certain Ethertypes by associating an EVC map with a discard type, rather than a valid EVC. To specify Ethertype matching on the EVC map, enter the **match ethertype** <*value*> command from the EVC map's configuration mode. The <*value*> parameter is the hexadecimal value to use as an additional match criteria for the EVC map. Enter the command as follows:

```
(config-evc-map MAP1)#match ethertype 0x0806
(config-evc-map MAP1)#
```

Step 3: Associate the EVC Map to an EVC and UNI

Once you have specified the match criteria for the EVC map, you must associate the EVC map with both an EVC and a UNI. EVC maps are associated with both an EVC and a UNI (Gigabit Ethernet interface or EFM group) to specify the traffic source from which it is evaluated (UNI) and where it is to be mapped if it matches the criteria (EVC). The UNI in this case is the interface from which you want to map the traffic. EVC maps will always have two connection statements: one to an EVC and one to a UNI, unless the traffic matching the EVC map is to be discarded, in which case you need a connection to a UNI and a connection to the discard target.

 Copyright © 2016 ADTRAN, Inc.

EVC maps are associated with a UNI and an EVC using the **connect [evc** <*name*> **| uni gigabit-ethernet** <*slot/port*> **| uni efm-group** <*slot/group*>**]** command. Both an EVC and a UNI must be entered as separate commands for the EVC map to function properly. The **evc** <*name*> parameter specifies the EVC to which the matching traffic is mapped, and the **uni gigabit-ethernet** <*slot/port*> and **uni efm-group** <*slot/group*> parameters specify the UNI from which the traffic is evaluated. Using the **no** form of this command removes the association between the EVC map and the EVC or the UNI. For example, to specify that EVC map **MAP1** is associated with UNI Gigabit Ethernet interface **0/2** and with EVC **DATA**, enter the command from the EVC map's configuration mode as follows:

```
(config-evc-map MAP1)#connect uni gigabit-ethernet 0/2
(config-evc-map MAP1)#connect evc DATA
(config-evc-map MAP1)#
```

Alternatively, you can use the **connect discard** command instead of the **connect evc** command to specify that traffic matching the EVC map criteria is discarded. Using the **no** form of this command disables traffic discard. For example, to specify that traffic matching the criteria outlined in EVC map **MAP1** is discarded, enter the command from the EVC map's configuration mode as follows:

```
(config-evc-map MAP1)#connect discard
(config-evc-map MAP1)#
```

Step 4: Enable the EVC Map

To enable the EVC map, enter the **no shutdown** command from the EVC map's configuration mode as follows:

```
(config-evc-map MAP1)#no shutdown
(config-evc-map MAP1)#
```

Step 5: Specify the MEN Values to be set (Optional)

After you have configured the matching criteria used by the EVC map and associated the EVC map with both a UNI and an EVC, you can optionally define the MEN values applied to the traffic matching the EVC map. The configurable MEN values for traffic matching the EVC map include the s-tag priority bit (802.1p value), specifying the queue to which the traffic is sent, specifying a c-tag, and specifying the c-tag priority. The following section details how to configure the MEN values for the matched traffic.

S-tag Priority Bits

You can optionally specify the s-tag priority bits (802.1p value) that the EVC will use for traffic matching the specific EVC map by entering the **men-pri [inherit |** <*value*>**]** command from the EVC map's configuration mode prompt. The **inherit** parameter specifies that the priority value for the matched traffic is inherited from the 802.1p value of the CE VLAN. By default, matched traffic has an inherited priority. The <*value*> parameter specifies the priority value given to the matched traffic in the EVC. Valid range is **0** to **7**. Using the **no** form of this command returns the MEN priority to the default value.

For example, to specify that traffic matching EVC map **MAP1** is given an s-tag priority of **5** in the associated EVC, enter the command as follows:

```
(config-evc-map MAP1)#men-pri 5
(config-evc-map MAP1)#
```

 Copyright © 2016 ADTRAN, Inc.

Output Queue

You can optionally specify the output queue used by the EVC for traffic that matches the particular EVC map using the **men-queue [inherit |** <*value*>**]** command from the EVC map's configuration mode. The **inherit** parameter specifies that the queue used by the EVC for the matched traffic is based on the default global p-bit-to-queue mapping (based on the priority bits (802.1p) of the s-tag). By default, matched traffic inherits the queue information. The <*value*> parameter specifies a queue to which the matched traffic is mapped by the EVC. Valid queue range is **0** to **7**. Using the **no** form of this command returns the MEN queue to the default. For example, to specify that traffic matching EVC map **MAP1** is queued in output queue **4**, enter the command as follows:

```
(config-evc-map MAP1)#men-queue 4
(config-evc-map MAP1)#
```

Insert C-tag

You can optionally specify the c-tag to be inserted and that will be used to identify a specific customer's traffic on the EVC using the **men-c-tag** <*value*> command from the EVC map's configuration mode. When traffic matches the EVC map, it will be tagged with this c-tag <*value*>. Valid range is **2** to **4094**. By default, the c-tag is not specified. Using the **no** form of this command removes the c-tag value. For example, to specify that traffic matching EVC map **MAP1** is tagged with a c-tag value of **20**, enter the command as follows:

```
(config-evc-map MAP1)#men-c-tag 20
(config-evc-map MAP1)#
```

C-tag Priority Bits

You can optionally specify the c-tag priority bits that the EVC will use on the c-tag using the **men-c-tag-pri [inherit |** <*value*>**]** command from the EVC map's configuration mode. The **inherit** parameter specifies that the c-tag 802.1p value for the matched traffic is inherited from the 802.1p value of the s-tag. By default, matched traffic has an inherited priority. The <*value*> parameter specifies the priority value given to the matched traffic in the EVC. Valid range is **0** to **7**. Using the **no** form of this command returns the MEN c-tag priority to the default value. For example, to specify the c-tag priority as **6** for traffic matching EVC map **MAP1**, enter the command as follows:

```
(config-evc-map MAP1)#men-c-tag-pri 6
(config-evc-map MAP1)#
```

Configuring QoS for Layer 3 Carrier Ethernet Services

This section provides configuration options for only Layer 3 carrier Ethernet services. If your specific needs do not require Layer 3 services, you can skip this section.

When providing Layer 3 services, additional QoS granularity can be provided by using QoS settings on the Layer 3 interface. Configuring QoS for Layer 3 services consists of the following steps:

- *Step 1: Create QoS Map on page 25*
- *Step 2: Configure Traffic Match Criteria on page 25*
- *Step 3: Apply Actions on page 29*
- *Step 4: Associate the QoS Map to a Subinterface on page 30*
- *Step 5: Configure Additional Subinterface Settings (Optional) on page 30*

 Copyright © 2016 ADTRAN, Inc.

Step 1: Create 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 specify actions to take on that traffic. In addition, QoS maps can be used to set 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 can 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 **WAN**:

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

Step 2: Configure Traffic Match Criteria

Specify the match criteria 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 9 on page 26* 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 26*
- *Match by CE VLAN Identifier on page 26*
- *Match by Access Control List on page 27*
- *Match by Traffic Priority (DSCP or IP Precedence Value) on page 27*
- *Match by IP RTP on page 28*
- *Match by Protocol on page 28*

 Copyright © 2016 ADTRAN, Inc.

Table 9. QoS Map Match Commands

Command	Explanation
match any	Matches packets not matched in a previous map entry.
match ce-vlan-id <*vlan id*>	Matches traffic associated with a particular CE VLAN ID. Valid range for <*vlan id*> is 1 to 4095.
match [ip | ipv6] list <*list name*>	Matches IP traffic based on a standard or extended access control lists (ACL). Use the **ip** keyword to match only IPv4 packets. Use the **ipv6** keyword to match only IPv6 packets.
match [ip | ipv6] dscp [af*xx* | **cs***x* | **default** | **ef |** <*value*>**]**	Matches traffic based on DiffServ AF, Class selector (CS), default, 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 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 [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.
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 WAN 10**

(config-qos-map)**#match any**

Match by CE VLAN Identifier

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

(config)**#qos map WAN 10**

(config-qos-map)**#match ce-vlan-id 3**

 Copyright © 2016 ADTRAN, Inc.

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 permitted 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** <*ipv6 acl name*> command. For example, the following command matches the QoS map **WAN** to traffic using the IPv4 ACL **MATCHALL**:

(config)**#qos map WAN 10**

(config-qos-map)**#match ip list MATCHALL**

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 Values Explained on page 14*.

> 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*> | **afxx | csx | 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 **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). 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 matches the QoS map **WAN** to IPv4 and IPv6 traffic with the DSCP value **46**:

 Copyright © 2016 ADTRAN, Inc.

(config)**#qos map WAN 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 Values Explained on page 14*.

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 **WAN** to IPv4 and IPv6 traffic with the IP precedence value **5**:

(config)**#qos map WAN 10**

(config-qos-map)**#match precedence 5**

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. The **all** keyword is used to match even (RTP) and odd (Realtime Transport Control Protocol (RTCP)) UDP port numbers in the specified range and can only be used with IPv4 addresses. This command can be used to define a class-based weighted fair queuing (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 **WAN** to IP RTP traffic destined for ports from **16384** to **32764**:

(config)**#qos map WAN 10**

(config-qos-map)**#match ip rtp 16384 32764**

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 **WAN** to IPv4 traffic:

(config)**#qos map WAN 10 match-all**

(config-qos-map)**#match protocol ip**

 Copyright © 2016 ADTRAN, Inc.

Step 3: Apply Actions

Actions can be applied to change various field values for outgoing traffic serviced by the QoS policy. The **set** command is used to apply override actions to change several values. Refer to the following descriptions for more details for altering each field value.

Ethernet CE VLAN priority field value

Use the **set ce-vlan-pri** <*value*> to override an Ethernet CE VLAN priority field value. Valid range is **0** to **7**. By default, the packet's priority value field is not set. Using the **no** form of this command returns the priority field value to the default setting. To specify a CE VLAN priority field value, enter the command from the QoS map's configuration mode as follows:

```
(config)#qos map MAP1
(config-qos-map)#set ce-vlan-pri 3
```

Egress queue

Use the **set egress-queue** <*value*> command to override the QoS map's egress queue. Valid range is **0** to **7**. By default, no egress queue is specified. Using the **no** form of this command returns the egress queue setting to the default value. To specify an egress queue, enter the command from the QoS map's configuration mode as follows:

```
(config)#qos map MAP1
(config-qos-map)#set egress-queue 2
```

Ethernet s-tag priority value

Use the **set men-pri** <*value*> command to override the Ethernet s-tag priority value for traffic matching the QoS map. Valid range is **0** to **7**. By default, the s-tag priority is not set. Using the **no** form of this command returns the s-tag priority to the default value. To specify the s-tag priority for the QoS map, enter the command from the QoS map's configuration mode as follows:

```
(config)#qos map MAP1
(config-qos-map)#set men-pri 5
```

Ethernet c-tag priority value

Use the **set men-c-tag-pri** <*value*> command to override the Ethernet c-tag priority value for traffic matched by the QoS map. Valid range is **0** to **7**. By default, the c-tag priority is not set. Using the **no** form of this command returns the c-tag priority to the default value. To specify the c-tag priority for the QoS map, enter the command from the QoS map's configuration mode as follows:

```
(config)#qos map MAP1
(config-qos-map)#set men-c-tag-pri 3
```

DSCP value

Use the **set dscp [**<*value*> **| af***xx* **| cs***xx* **| default | ef]** command to modify the DSCP field on packets matching the QoS map policy. The valid range for <*value*> is **0** to **63**. 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). 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). Setting A DSCP value of EF is accomplished by using the **ef** keyword. Use the **no** form of this command to remove the specified DSCP value from the QoS map policy. To specify the DSCP value **46** for matching traffic, enter the command from the QoS map's configuration mode as follows:

 Copyright © 2016 ADTRAN, Inc.

```
(config)#qos map MAP1
(config-qos-map)#set dscp 46
```

Precedence value

Use the **set precedence** <*value*> command to modify the precedence value on packets matching the QoS map policy. The valid range for <*value*> is **0** to **7**. Using the **no** form of this command discontinues the action from the QoS map policy. To specify the IP precedence value for packets matching the QoS map policy, enter the command from the QoS map's configuration mode as follows:

```
(config)#qos map MAP1
(config-qos-map)#set precedence 1
```

Step 4: Associate the QoS Map to a Subinterface

Once created, a QoS map must be associated with 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, requires a QoS map to be assigned to the ingress interface using the **qos-policy in** command. Outbound traffic that needs to be given priority over other traffic leaving the router, requires a QoS map assigned to the egress 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.

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. Use the **no** form of this command to remove the map from the interface.

The following command applies the QoS map **WAN** to the output of EFM group **1/1.201**:

```
(config)#interface efm-group 1/1.201
(config-efm-group 1/1)#qos-policy out WAN
```

All queuing and QoS packet reorganization takes place on the egress wide area network (WAN) interface.

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.

Step 5: Configure Additional Subinterface Settings (Optional)

The following commands can be used to configure additional settings on the Layer 3 subinterface:

Specify a Queue for Egress Traffic

Use the **egress-queue [inherit |** <*value*>**]** command to specify the queue for traffic egressing the subinterface. If the QoS map also sets a queue for egress traffic matching the QoS map, priority is given to the settings at the QoS map level. The **inherit** parameter specifies packet's outer tag value is used to automatically map traffic to the egress queue on a per-packet basis using the QoS CoS map settings. The <*value*> parameter specifies an egress queue for the subinterface. Valid range is **0** to **7**. By default, egress queue mapping is set to **inherit**. Using the **no** form of this command returns the egress queue to the default value.

 Copyright © 2016 ADTRAN, Inc.

To change the egress queue for the subinterface, enter the command from the subinterface's configuration mode as follows:

(config)**#interface gigabit-ethernet 0/1.123**
(config-giga-eth 0/1.123)**#egress-queue 5**

Specify S-tag Priority Bits for Egress Traffic

Use the **men-pri [inherit |** <*value*>] command to specify the s-tag priority bits (802.1p value) for traffic egressing the subinterface. If the QoS map also specifies a value for this setting for egress traffic matching the QoS map, priority is given to the settings at the QoS map level. The **inherit** parameter specifies that the priority value for the matched traffic is inherited from the 802.1p value of the CE VLAN. The <*value*> parameter specifies an s-tag priority value. Valid range is **0** to **7**. By default, the s-tag priority value is set to **inherit**. Using the **no** form of this command returns the s-tag priority value to the default setting.

To change the s-tag priority on the subinterface, enter the command from the subinterface's configuration mode as follows:

(config-giga-eth 0/1.123)**#men-pri 5**

Insert C-tag into Subinterface Traffic

Use the **men-c-tag** <*value*> parameter to specify the c-tag to be inserted into subinterface traffic. If the QoS map also specifies a value for this setting for egress traffic matching the QoS map, priority is given to the settings at the QoS map level. Valid c-tag <*value*> range is **2** to **4094**. By default, c-tags are not inserted into subinterface traffic. Using the **no** form of this command returns to the default setting.

To specify a c-tag for the subinterface, enter the command from the subinterface's configuration mode as follows:

(config-giga-eth 0/1.123)**#men-c-tag 20**

Specify C-tag Priority Bits for Matching Traffic

Use the **men-c-tag-pri [inherit |** <*value*>**]** command to specify the c-tag priority bits (802.1p value) for matching traffic on the subinterface. If the QoS map also specifies a value for this setting for egress traffic matching the QoS map, priority is given to the settings at the QoS map level. The **inherit** parameter specifies that the c-tag priority is inherited from the 802.1p value of the s-tag. The <*value*> parameter specifies a c-tag priority value. Valid range is **0** to **7**. By default, the c-tag priority value is set to **inherit**. Using the **no** form of this command returns the c-tag priority value to the default setting.

To change the c-tag priority on the subinterface, enter the command from the subinterface's configuration mode as follows:

(config-giga-eth 0/1.123)**#men-c-tag-pri 6**

Configuring Additional QoS Components

Additional QoS components can be configured depending on your particular networking requirements. This section explains in detail the following configuration options:

- *Configure the Class of Service (CoS) Map on page 32*
- *Configure the Interface Queues on page 32*

 Copyright © 2016 ADTRAN, Inc.

Configure the Class of Service (CoS) Map

The CoS map specifies the default mapping of p-bit markings to specific queues. Configure the CoS map with the command **qos cos-map** <*queue*> <*cos value*> command from the Global Configuration mode. The <*queue*> parameter is the queue to which the map is assigned; valid range is **0** to **7**. The <*cos value*> is the CoS value assigned to the queue; valid range is **0** to **7**. The default CoS values for each queue are outlined in *Table 10*.

To map a p-bit marking to a queue, enter the command as follows:

```
(config)#qos cos-map 0 0
(config)#
```

Table 10. Default CoS Map Queue and Value Settings

Queue	CoS Value
0	1
1	0
2	2
3	3
4	4
5	5
6	6
7	7

Configure the Interface Queues

Eight hardware queues are provided per MEN port, whether an EFM group or Gigabit Ethernet interface, that facilitate traffic management and congestion avoidance. These queues absorb packets when the ingress rate of traffic exceeds the egress rate, allowing bursts of packets to be transmitted through the system without incurring loss. Queues must be managed to prevent packet loss and delay in the network. From the queue's configuration mode you can specify the congestion avoidance algorithm, WFQ, CoS settings, drop probabilities, queue depth, and thresholds. To configure the queues, follow these steps:

1. Enter the **queue interface [efm-group** <*slot/group*> | **gigabit-ethernet** <*slot/port*>**]** <*queue*> command from the Global Configuration mode prompt. The <*queue* > parameter specifies the queue number. Valid range is **0** to **7**. To enter the queue configuration mode for queue **1** of EFM group **1/1**, enter the command as follows:

   ```
   (config)#queue interface efm-group 1/1 1
   (config-queue 1 efm-group 1/1)#
   ```

 Copyright © 2016 ADTRAN, Inc.

2. Configure the maximum number of packets that can be held by the queue using the **max-depth** <*number*> command. The <*number*> parameter is the maximum number of packets. Valid range is **1** to **16383** packets. By default, the maximum queue depth is **255** packets. Use the **no** form of this command to return the queue depth to the default value. To specify a new queue depth, enter the command from the queue's configuration mode as follows:

   (config-queue 1 efm-group 1/1)**#max-depth 150**
   (config-queue 1 efm-group 1/1)**#**

Configure the Queue for WRED

You can configure a queue to use WRED for traffic management. WRED is an active queue congestion management discipline that adds thresholds and drop probability slopes for queued traffic. Different slopes can be configured to treat conforming (green) and nonconforming (yellow) packets differently. As the average queue depth increases, the AOS product begins to randomly discard packets based on the configured drop probability and thresholds. Only if the drop probability is configured to be 100 percent when the maximum threshold is reached will all packets be discarded. Packet color and average queue depth are used to determine drop probability. When using WRED, make sure to configure the yellow maximum threshold to be less than or equal to the green minimum threshold (using the **thresholds wred** command) to avoid dropping green packets before all yellow packets are dropped. To configure WRED for the queue, follow these steps:

1. Use the **algorithm wred** command from the queue's configuration mode to enable WRED in the queue. Use the **no** form of this command to disable this feature. By default, WRED is disabled. To enable WRED in the queue, enter the command as follows:

   (config-queue 1 efm-group 1/1)**#algorithm wred**
   (config-queue 1 efm-group 1/1)**#**

2. Configure the WRED average queue depth thresholds using the **thresholds wred green [maximum** <*value*> **| minimum** <*value*>**]** and the **thresholds wred yellow [maximum** <*value*> **| minimum** <*value*>**]** commands. Specifying the green minimum and maximum thresholds configures the maximum and minimum threshold for dropping conforming (green) traffic. Specifying the yellow minimum and maximum thresholds configures the maximum and minimum thresholds for dropping nonconforming (yellow) traffic. Valid threshold ranges are **1** to **16382** for minimum and **2** to **16383** for maximum. By default, the WRED thresholds are set as follows: green maximum **25**, green minimum **15**, yellow maximum **15**, and yellow minimum **5**. When setting the maximum value for WRED thresholds, if the minimum value is not less than the new maximum value, the minimum is adjusted to be one less than the maximum value. When setting the minimum value, if the maximum value does not exceed the minimum, the maximum value is adjusted to be one more than the minimum. A warning is displayed if either the minimum or maximum value is automatically adjusted. In addition, when using WRED, make sure to configure the yellow maximum threshold to be less than or equal to the green minimum threshold to avoid dropping green packets before all yellow packets are dropped. WRED minimum thresholds should be configured before WRED maximum thresholds. To configure the WRED thresholds, enter the commands from the queue's configuration mode as follows:

   (config-queue 1 efm-group 1/1)**#thresholds wred green minimum 50**
   (config-queue 1 efm-group 1/1)**#thresholds wred yellow minimum 3**
   (config-queue 1 efm-group 1/1)**#thresholds wred green maximum 100**
   (config-queue 1 efm-group 1/1)**#thresholds wred yellow maximum 30**

 Copyright © 2016 ADTRAN, Inc.

3. Configure the drop probability of WRED traffic entering the queue using the **drop-probability [yellow** <*value*> **| green** <*value*>**]** command. The **yellow** and **green** parameters specify that the drop probability percentage for yellow and green traffic, respectively, when the maximum threshold is reached. Valid value range is **0** to **100** percent. By default, the drop probability for all traffic is set to **10** percent. Using the **no** form of this command returns the drop probability to the default value. To configure the drop probability for green traffic, enter the command as follows:

   ```
   (config-queue 1 efm-group 1/1)#drop-probability green 50
   (config-queue 1 efm-group 1/1)#
   ```

Configure Weighted Fair Queueing

You can also configure the CoS settings and enable WFQ for the queue, which is the relative priority of a queue when the queue scheduler runs in order to dequeue a packet. Queues with the same CoS value enable the scheduling of packets between the same CoS queues using the WFQ algorithm. Queues with different CoS values are serviced with a strict priority algorithm where the queues with higher CoS values are serviced before queues with lower CoS values. Valid CoS value range is **0** to **7**. By default, the CoS value matches the queue number (for example, queue **0** has a default CoS value of **0**). To configure the queue's CoS settings, follow these steps:

1. Use the **cos group lower-adjacent** command to lower the CoS of the queue to the lower adjacent numbered queue's CoS value to enable WFQ. By default, the CoS value of a queue exactly matches the queue number. Use the **no** form of this command to set the CoS of a queue back to its default value. To enable this feature, enter the command as follows:

   ```
   (config-queue 1 efm-group 1/1)#cos group lower-adjacent
   (config-queue 1 efm-group 1/1)#
   ```

2. Specify the weight given to the queue using the **weight [dynamic |** <*number*>**]** command. You can specify that weight is determined dynamically using the **dynamic** keyword, or you can specify a percentage weight by entering the value. Valid range is **1** to **100** percent. By default, traffic weight is determined dynamically. Use the **no** form of this command to return to the default setting. To configure the percentage of weight given to the queue, enter the command as follows:

   ```
   (config-queue 1 efm-group 1/1)#weight 25
   (config-queue 1 efm-group 1/1)#
   ```

The queue is now configured.

Configuring the Policer (Optional)

The policer limits the amount of traffic inbound to the AOS product. Traffic can be limited based on CBS, CIR, EBS, and EIR thresholds. The CBS and CIR thresholds specify the committed burst sizes and transmission rates of traffic. When these thresholds are exceeded, traffic will be colored as yellow (non-conforming) traffic. The EBS and EIR thresholds specify the excess burst sizes and transmission rates (over and above the committed sizes or rates), thereby specifying the maximum burst size or rate allowed before the traffic is dropped. In this way, the policer functions similarly to Frame Relay policing. Properly configuring the policer relies on specifying the name and the thresholds for the policer, and applying the policer to a component (UNI, E VC, or EVC map) or first tier policer. The policer is applied to the specified traffic as it ingresses on a UNI. To configure the policer, follow these steps:

1. Create and name the policer by entering the **policer** <*name*> **[**<*slot*>**]** command from the Global Configuration mode prompt. The <*name*> parameter is the name given to this policer. The optional

 Copyright © 2016 ADTRAN, Inc.

<*slot*> parameter specifies the policer's slot. For example, to create the policer **POLICER1** and enter the policer's configuration mode, enter the command as follows:

```
(config)#policer POLICER1
(config-policer POLICER1)#
```

2. Once you have entered the policer's configuration mode, you can specify the CBS, CIR, EBS, and EIR thresholds. To set the CIR threshold, enter the **cir** <*number*> command from the policer's configuration mode. The <*number*> parameter is the average maximum transmission rate of traffic in kilobits per second (kbps) allowed before the traffic is dropped. Valid range is **0** to **1000000** kbps. By default, the CIR threshold is **0** kbps. Using the **no** form of this command returns the CIR threshold to the default value. For example, to change the CIR threshold for the policer, enter the command as follows:

   ```
   (config-policer POLICER1)#cir 5000
   ```

   To set the committed burst size (CBS) threshold, enter the **cbs** <*number*> command. The CBS threshold, or the maximum number of bytes transmitted as a burst before the policer begins to drop traffic. Valid range is **0** to **999999** bytes. By default, the CBS threshold is **3125** bytes. Using the **no** form of this command returns the CBS threshold to the default value. To change the CBS threshold for the policer, enter the command as follows:

   ```
   (config-policer POLICER1)#cbs 6500
   ```

   To set the EIR threshold, enter the **eir** <*number*> command from the policer's configuration mode. The <*number*> parameter is the allowed maximum rate in kbps, at which traffic will be transmitted before the policer drops the traffic. This is the maximum above the CIR value. Valid range is **0** to **1000000** kbps. By default, the EIR threshold is **600000** kbps. Using the **no** form of this command returns the EIR threshold to the default value. To change the EIR threshold for the policer, enter the command as follows:

   ```
   (config-policer POLICER1)#eir 6000
   ```

   To set the EBS threshold, enter the **ebs** <*number*> command from the policer's configuration mode. The <*number*> parameter is the allowed maximum number of bytes transmitted as a burst of data, over and above the CBS threshold, before the policer drops the traffic. Valid range is **0** to **999999** bytes, with a default value of **12500** bytes. Using the **no** form of this command returns the threshold to the default value. To change the EBS threshold for the policer, enter the command as follows:

   ```
   (config-policer POLICER1)#ebs 1000
   ```

3. Additional features can be enabled for this policer, including color-awareness and coupling flag. A color-aware policer takes the color marking of a packet into consideration when determining the new color marking. Incoming green packets can be declared green, yellow, or red (dropped) by a color-aware policer. Incoming yellow packets can only be declared yellow or red. Use the **color-aware** command to enable this feature. To enable color-awareness enter the commands as follows:

   ```
   (config-policer POLICER1)#color-aware
   ```

   A color-aware policer can use coupling to couple internal operation for token refills from the CIR to EIR buckets. Tokens that cannot fill the green bucket when it is full (i.e., when no green traffic is currently running) will overflow into the yellow bucket so that yellow traffic is processed at a rate of CIR + EIR. The coupling flag is enabled by using the **coupling** command. To enable coupling, enter the commands as follows:

   ```
   (config-policer POLICER1)#coupling
   ```

 Copyright © 2016 ADTRAN, Inc.

4. After configuring the thresholds for queuing or dropping traffic, you must apply the policer to a component. Policers are applied to components using the **per** command from the policer's configuration mode. There are several parameters to include with this command depending on the component to which you are applying the policer. These parameters are explained in further detail below.

   Using the **per custom [evc-map** <*name*> **| interface gigabit-ethernet** <*slot/port.subinterface*>**]** command allows you to apply the policer to all ingress traffic that matches one or more EVC maps or to an Ethernet subinterface. The **evc-map** <*name*> **parameter** specifies the EVC map. The **interface gigabit-ethernet** <*slot/port.subinterface*> command specifies a Gigabit Ethernet interface. You must specify the slot and port of the interface to apply the policer. Using the **no** form of this command removes the policer from the component. For example, to apply policer **POLICER1** to all ingress traffic on interface Gigabit-Ethernet 0/2.1, enter the command as follows:

   (config)**#policer POLICER1**

   (config-policer POLICER1)**#per custom interface gigabit-ethernet 0/2.1**

   The **per evc** <*name*> command allows you to apply the policer to every EVC map that is connected to the specified EVC. For example, to apply policer **POLICER1** to all EVC maps associated with EVC **DATA**, enter the command as follows:

   (config)**#policer POLICER1**

   (config-policer POLICER1)**#per evc DATA**

   Second tier policers can be used in addition to a first tier policer. This allows limiting the overall rate or burst size of traffic. To set a specific policer to per policer mode, use the **per policer <***name*> command from within the policer command set which will be the second tier policer. The **<***name*> parameter specifies the first tier policer name. To set the policer **POLICER1** as the second tier policer and enable the **POLICER2** as the first tier policer, enter the commands as follows:

   (config)**#policer POLICER1**

   (config-policer POLICER1)**#per policer POLICER2**

   Policers can be applied to ingress traffic on the specified interface (the UNI) for all connected EVC maps using the **per uni [efm-group** <*slot/group*> **| gigabit-ethernet** <*slot/port*>**]** command from the policer's configuration mode. You must specify the slot and port (or group ID and port) of the interface to apply the policer. For example, to apply policer **POLICER1** to all EVC maps associated with the Gigabit Ethernet interface 0/2, enter the command as follows:

   (config)**#policer POLICER1**

   (config-policer POLICER1)**#per uni gigabit-ethernet 0/2**

5. Enable the policer by entering the **no shutdown** command from the policer's configuration mode as follows:

   (config-policer POLICER1)**#no shutdown**

The policer configuration is now complete.

 Copyright © 2016 ADTRAN, Inc.

Configure the Shaper (Optional)

A traffic shaper can be used to enforce a maximum transmission rate into the MEN and to smooth bursts of traffic traveling between the AOS product and the MEN. When a packet arrives at the shaper, if there are sufficient tokens available, the packet is transmitted without delay. If there are insufficient tokens, the packet is delayed until there are enough tokens to allow transmission. Shapers do not drop frames with a small burst of traffic, but they can add latency. You can configure the shaper by specifying to which interface, or queue(s), it is applied and the rate that will be applied on egress traffic from that interface or queue. To configure the shaper, follow these steps:

You can apply a shaper to an interface, or apply a shaper to interface queues, but you cannot do both with a single shaper. These actions are mutually exclusive.

1. Create and name the shaper by entering the **shaper** <*name*> **[**<*slot*>**]** command from the Global Configuration mode prompt. The <*name*> parameter is the name given to this policy. The optional <*slot*> parameter specifies the shaper's slot. For example, to create the shaper **SHAPER1** and enter the shaper's configuration mode, enter the command as follows:

   (config)**#shaper SHAPER1**
   (config-shaper SHAPER1)#

2. To specify the interface to which the shaper is applied, enter the **per interface [efm-group** <*slot/group*> | **gigabit-ethernet** <*slot/port*>**]** command from the shaper's configuration mode. The **gigabit-ethernet** <*slot/port*> and **efm-group** <*slot/group*> parameters specify the interface on which the egress traffic is evaluated. Using the **no** form of this command removes the shaper from the interface. By default, no interfaces are assigned. To specify that shaper **SHAPER1** is associated with Gigabit Ethernet interface **0/1**, enter the command from the shaper's configuration mode as follows:

   (config-shaper SHAPER1)**#per interface gigabit-ethernet 0/1**
   (config-shaper SHAPER1)#

3. To specify the interface queue to which the shaper is applied, enter the **per interface [efm-group** <*slot/group*> | **gigabit-ethernet** <*slot/port*>**]** <*queue*> command from the shaper's configuration mode. An interface can have up to seven unique per-queue shapers and one per-interface shaper applied to it. If more than seven unique per-queue shapers are applied to an interface, they will appear as disabled in the output of the **show shaper** command. The **gigabit-ethernet** <*slot/port*> and **efm-group** <*slot/group*> parameters specify the interface on which the egress traffic is evaluated, and the <*queue*> parameter specifies to which queues on the interface the shaper is applied. Valid range is **0** to **7**. Separate queues in a list using commas (for example, **1, 3**) or use a hyphen to define a range (for example, **1-3**). Using the **no** form of this command removes the shaper from the queue(s). By default, no shapers are assigned to a queue. To specify that shaper **SHAPER1** is associated with queues **1**, **3**, **4**, and **5** on Gigabit Ethernet interface **0/1**, enter the command from the shaper's configuration mode as follows:

   (config-shaper SHAPER1)**#per interface gigabit-ethernet 0/1 1,3-5**
   (config-shaper SHAPER1)#

4. Specify the traffic rate limit that will be applied by the shaper to the egress traffic using the **rate** <*value*> command from the shaper's configuration mode. The <*value*> parameter is the rate in kilobits per second (kbps) that is applied to the traffic. Valid rate range is **0** to **1000000** kbps. Using the **no** form of this command returns the rate to the default value of **1000000** kbps. To specify the traffic rate as **3500** kbps for the shaper, enter the command from the shaper's configuration mode as follows:

 Copyright © 2016 ADTRAN, Inc.

```
(config-shaper SHAPER1)#rate 3500
(config-shaper SHAPER1)#
```

5. Enable the shaper using the **no shutdown** command from the shaper's configuration mode. Enter the command as follows:

```
(config-shaper SHAPER1)#no shutdown
(config-shaper SHAPER1)#
```

The shaper configuration is now complete.

Configuration Example

The following example is a configuration for both Layer 2 and Layer 3 carrier Ethernet QoS services. The configuration parameters entered in this example are sample configurations only. You should configure these applications in a manner consistent with the needs of your particular network. CLI prompts have been removed from the configuration examples to provide you with a method of copying and pasting directly from this guide into the CLI. You should make the necessary adjustments to these configurations before adding them to your configuration to ensure they will function properly in your network.

```
!
qos map Management 10
 match any
 set precedence 7
!
qos map LAN 10
 match dscp ef
 match dscp af31
 match dscp cs1
qos map LAN 20
 match any
 set dscp 0
!
qos map WAN 10
 match dscp ef
 set men-pri 5
 set egress-queue 5
qos map WAN 20
 match dscp af31
 set men-pri 3
 set egress-queue 3
qos map WAN 30
 match dscp cs1
 set men-pri 1
 set egress-queue 1
!
!
interface gigabit-eth 0/1
 description NNI
 no shutdown
```

 Copyright © 2016 ADTRAN, Inc.

```
!
interface gigabit-eth 0/1.300
 ce-vlan-id untagged
 connect evc L3_Data
 men-pri 0
 egress-queue 0
 ip address  198.51.100.2  255.255.255.252
 qos-policy out WAN
 no shutdown
!
!
interface gigabit-eth 0/2
 description Layer 2 UNI
 no shutdown
!
!
interface gigabit-eth 0/3
 description Layer 3 UNI
 no shutdown
!
interface gigabit-eth 0/3.1
 ce-vlan-id untagged
 ip address  192.0.2.1  255.255.255.248
 qos-policy in LAN
 no shutdown
!
!
evc EPL
 s-tag 200
 connect men-port gigabit-ethernet 0/1
 no shutdown
!
!
evc L3_Data
 s-tag 300
 connect men-port gigabit-ethernet 0/1
 no shutdown
!
!
evc-map EPL
 connect uni gigabit-ethernet 0/2
 connect evc EPL
 men-queue 2
 no shutdown
!
!
```

 Copyright © 2016 ADTRAN, Inc.

```
policer EPL
 per custom evc-map EPL
 cir 150000
 cbs 2000
 eir 0
 ebs 0
 no shutdown
!
!
shaper NNI
 rate 500000
 per interface gigabit-ethernet 0/1
!
!
shaper RTP
 rate 20000
 per interface gigabit-ethernet 0/1 5
!
!
shaper SIP
 rate 1000
 per interface gigabit-ethernet 0/1 3
!
!
queue interface gigabit-ethernet 0/1 0
 algorithm wred
 drop-probability green 1
 thresholds wred green maximum 255
 thresholds wred green minimum 120
 weight 10
!
!
queue interface gigabit-ethernet 0/1 1
 algorithm wred
 cos group lower-adjacent
 drop-probability green 1
 thresholds wred green maximum 255
 thresholds wred green minimum 120
 weight 90
!
!
queue interface gigabit-ethernet 0/1 3
 max-depth 42
!
!
queue interface gigabit-ethernet 0/1 5
 max-depth 24
```

 Copyright © 2016 ADTRAN, Inc.

```
!
!
qos cos-map 0  0
qos cos-map 1  1
qos cos-map 2  2
qos cos-map 3  3
qos cos-map 4  4
qos cos-map 5  5
qos cos-map 6  6
qos cos-map 7  7
!
!
system-management-evc
  connect men-port gigabit-ethernet 0/1
  vrf forwarding system-management
  ip address 10.255.1.2  255.255.255.0
  s-tag 1000
  qos-policy out Management
  no shutdown
```

 Copyright © 2016 ADTRAN, Inc.

Command Summary

The following tables summarize the commands associated with configuring QoS carrier Ethernet services AOS products.

Layer 2 Carrier Ethernet Services QoS Configuration Commands

The following table summarizes commands specific to Layer 2 carrier Ethernet QoS configurations.

Table 11. Layer 2 Carrier Ethernet Services QoS Commands

Step	Command and Description
Step 1	Create an EVC map.
	(config)**#evc-map** <*name*> Creates an EVC map and enters the EVC map's configuration mode. The <*name*> parameter is the name of the EVC map. Using the **no** form of this command removes the EVC map from the unit's configuration.
Step 2	Configure traffic match criteria.
	(config-evc-map MAP1)**#match [broadcast | ce-vlan-id** <*vlan id*> **| ce-vlan-pri** <*value*> **| destination mac address** <*mac address*> **| dscp** <*value*> **| ethertype** <*value*> **| l2cp | multicast | unicast | untagged]** Specifies the traffic matching criteria used by the EVC map to identify which traffic to send to the associated EVC. The **L2CP**, **broadcast**, **multicast**, and **unicast** parameters specify that traffic matching the respective type is mapped to the EVC. The **ce-vlan-id** <*vlan id*> parameter specifies that traffic with a CE VLAN ID that matches the specified ID is mapped to the EVC. Valid VLAN ID range is **1** to **4094**. The **ce-vlan-pri** <*value*> parameter specifies that traffic with a CE VLAN PRI value that matches the specified value is mapped to the EVC. The <*value*> parameter is the priority bit value associated with the CE VLAN, or the CE VLAN 802.1p value. Valid range is **0** to **7**. The **destination mac address** <*mac address*> parameter specifies that traffic matching the specified destination MAC address is mapped to the EVC. MAC addresses should be expressed in the following format: xx:xx:xx:xx:xx:xx (for example, 00:A0:C8:00:00:01). The **dscp** <*value*> parameter specifies that IPv4 and IPv6 traffic matching the specified DSCP value is mapped to the EVC. Valid DSCP value range is **0** to **63**. The **ethertype** <*value*> parameter specifies that traffic with the specified Ethertype filter is mapped to the EVC. The <*value*> parameter is expressed in hexadecimal format. The **untagged** parameter specifies that untagged traffic is mapped to the EVC. By default, all traffic on the connected UNI port is matched. Using the **no** form of this command removes the matching criteria from the EVC map. Multiple matches form a logical AND.

 Copyright © 2016 ADTRAN, Inc.

Table 11. Layer 2 Carrier Ethernet Services QoS Commands *(Continued)*

Step	Command and Description
Step 3	Associate the EVC map to an EVC and UNI.
	(config-evc-map MAP1)**#connect [evc** <*name*> **| discard]** Associates the EVC map with an EVC. EVC maps must be associated with both an EVC (or **discard** target) and a UNI for the map to function properly. The **evc** <*name*> parameter specifies the EVC to which the matching traffic is mapped. The **discard** parameter specifies that traffic matching the EVC map criteria is discarded. Using the **no** form of this command removes the association between the EVC map and the EVC or discard target.
	(config-evc-map MAP1)**#connect uni [efm-group** <*slot/group*> **| gigabit-ethernet** <*slot/port*>**]** Associates the EVC map with a UNI component. EVC maps must be associated with both an EVC (or **discard** target) and a UNI for the map to function properly. The **uni efm-group** <*slot/group*> and **uni gigabit-ethernet** <*slot/port*> parameters specify the UNI from which the traffic is evaluated. Using the **no** form of this command removes the association between the EVC map and the UNI.
Step 4	Enable the EVC map.
	(config-evc-map MAP1)**#no shutdown** Enables the EVC map.
Step 5 (Optional)	Specify the MEN values to be set.
	(config-evc-map MAP1)**#men-pri [inherit |** <*value*>**]** Specifies the 802.1p value to the service VLAN tag (s-tag) that the EVC will use for traffic that matches the specified EVC map. The **inherit** parameter specifies that the s-tag priority value for the matched traffic is inherited from the 802.1p value of the CE VLAN. By default, matched traffic inherits the priority. The <*value*> parameter specifies the priority value. Valid range is **0** to **7**. Using the **no** form of this command returns the MEN priority to the default value.
	(config-evc-map MAP1)**#men-queue [inherit |** <*value*>**]** Specifies the output queue used by the EVC for traffic that matches the EVC map. The **inherit** parameter specifies that the queue used is based on the MEN priority-to-queue mapping (QoS CoS map). By default, matched traffic inherits the queue information. The <*value*> parameter specifies a queue to which the matched traffic is mapped by the EVC. Valid queue range is **0** to **7**. Using the **no** form of this command returns the MEN queue to the default.
	(config-evc-map MAP1)**#men-c-tag** <*value*> Specifies the c-tag that is inserted on the matching packets as they leave the MEN port and is used to further identify traffic on the EVC. Valid <*value*> range is **2** to **4094**. By default, a c-tag is not added. Using the **no** form of this command removes the C-tag value.

 Copyright © 2016 ADTRAN, Inc.

Table 11. Layer 2 Carrier Ethernet Services QoS Commands *(Continued)*

Step	Command and Description
Step 5 ***Cont'd***	(config-evc-map MAP1)**#men-c-tag-pri [inherit |** <*value*>**]** Specifies the 802.1p value in the c-tag. The **inherit** parameter specifies that the c-tag 802.1p value for the matched traffic is inherited from the 802.1p value of the s-tag. The <*value*> parameter assigns a specific priority value to the c-tag. Valid range is **0** to **7**. By default, the c-tag priority is set to **inherit**. This setting has no effect if the **men-c-tag** is not specified. Using the **no** form of this command returns to the default value.

Layer 3 Ethernet Services QoS Configuration Commands

The following tables summarize the commands used in Layer 3 configurations of QoS for carrier Ethernet services.

Table 12. Layer 3 QoS Configuration Commands

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. Use the **no** form of this command to delete a map entry.
Step 2	Configure traffic 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. Use the **no** form of this command to discontinue matching.
	(config-qos-map)**#match ce-vlan-id** <*vlan id*> Matches traffic associated with a particular CE VLAN ID. Valid range for <*vlan id*> is **1** to **4095**. Use the **no** form of this command to discontinue matching.
	(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. Use the **no** form of this command to discontinue matching.

 Copyright © 2016 ADTRAN, Inc.

Table 12. Layer 3 QoS Configuration Commands *(Continued)*

Step	Command and Description
Step 2 ***Cont'd***	(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. 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). 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 EF is indicated by the **ef** keyword. Valid range for <*value*> is **0** to **63**. Use the **no** form of this command to discontinue matching.
	(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. Use the **no** form of this command to discontinue matching.
	(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. The **all** keyword is used to match even (RTP) and odd (RTCP) 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. Use the **no** form of this command to discontinue matching.
	(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. Use the **no** form of this command to discontinue matching.

 Copyright © 2016 ADTRAN, Inc.

Table 12. Layer 3 QoS Configuration Commands *(Continued)*

Step	Command and Description
Step 3	Apply actions.
	(config-qos-map)**#set ce-vlan-pri** <*value*> Overrides an Ethernet CE VLAN priority field value for the QoS map. Valid <*value*> range is **0** to **7**. By default, the packet's priority value field is not set. Using the **no** form of this command returns the priority field value to the default setting.
	(config-qos-map)**#set egress-queue** <*value*> Overrides the QoS map's egress queue. Valid range is **0** to **7**. By default, no egress queue is specified. Using the **no** form of this command returns the egress queue setting to the default value.
	(config-qos-map)**#set men-pri** <*value*> Overrides an Ethernet s-tag priority value for the QoS map. Valid range is **0** to **7**. By default, the s-tag priority is not set. Using the **no** form of this command returns the s-tag priority to the default value.
	(config-qos-map)**#set men-c-tag-pri** <*value*> Overrides an Ethernet c-tag priority value for the QoS map. Valid range is **0** to **7**. By default, the c-tag priority is not set. Using the **no** form of this command returns the c-tag priority to the default value.
	(config-qos-map)**#set dscp [af***xx* | **cs***x* | **default** | **ef** | <*value*>**]** Modifies DSCP fields on packets matching the QoS map policy. 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). 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**. Use the **no** form of this command to remove the specified DSCP value from the QoS map policy.
	(config-qos-map)**#set precedence** <*value*> Modifies the precedence value on packets matching the QoS map policy. The valid range for <*value*> is **0** to **7**. Using the **no** form of this command discontinues the action from the QoS map policy.
Step 4	Associate the QoS map to the a subinterface.
	(config)**#interface** <*interface*> (config-interface)**#qos-policy [in** | **out]** <*name*> Associates the QoS map to the interface. Using the **in** parameter assigns the map to the ingress traffic, and using the **out** parameter assigns the map to the egress traffic. Using the **no** form of this command removes the map from the interface.

 Copyright © 2016 ADTRAN, Inc.

Table 12. Layer 3 QoS Configuration Commands *(Continued)*

Step	Command and Description
Step 5 (Optional)	Configure additional subinterface settings.
	(config-interface)**#egress-queue [inherit |** <*value*>**]** Specifies the queue used for traffic egressing the subinterface. The **inherit** parameter specifies that the value of the traffic's outer tag is used to automatically map traffic to the egress queue on a per-packet basis using the QoS CoS map settings. The <*value*> parameter specifies an egress queue for the subinterface. Valid range is **0** to **7**. Using the **no** form of this command returns to the default setting.
	(config-interface)**#men-pri [inherit |** <*value*>**]** Specifies the s-tag priority bits (802.1p value) for traffic egressing the subinterface. The **inherit** parameter specifies that the priority value for the matched traffic is inherited from the 802.1p value of the CE VLAN. The <*value*> parameter specifies an s-tag priority value. Valid range is **0** to **7**. Using the **no** form of this command returns to the default setting.
	(config-interface)**#men-c-tag** <*value*> Specifies the c-tag to be inserted into subinterface traffic. Valid <*value*> range is **2** to **4094**. Using the **no** form of this command removes the C-tag value.
	(config-interface)**#men-c-tag-pri [inherit | <*value*>]** Specifies the c-tag priority bits (802.1p value) for matching traffic on the subinterface. The **inherit** parameter specifies that the c-tag priority is inherited from the 802.1p value of the s-tag. The <*value*> parameter specifies a c-tag priority value. Valid range is **0** to **7**. Using the **no** form of this command returns to the default value.

Additional QoS Configuration Components

The following tables summarize the commands used in additional QoS configurations for carrier Ethernet services.

Table 13. CoS Configuration Commands

Command	Description
(config)**#qos cos-map** <*queue*> <*cos value*>	Specifies the default mapping of p-bit markings to specific queues. The <*queue*> parameter is the queue to which the map is assigned; valid range is **0** to **7**. The <*cos value*> parameter is the CoS value assigned to the queue; valid range is **0** to **7**. The default CoS values for each queue are outlined in *Table 10 on page 32*. Using the **no** form of this command returns the CoS map settings to the default value.

 Copyright © 2016 ADTRAN, Inc.

Table 14. Interface Queue Commands

Step	Command and Description
Step 1	Enter the queue configuration mode.
	(config)**#queue interface [efm-group** <*slot/group*> **| gigabit-ethernet** <*slot/port*>**]** <*queue*> Enters the queue's configuration mode. The <*queue*> parameter specifies the queue number. Valid range is **0** to **7**. Use the **no** form of this command to remove the queue configuration on the interface.
Step 2	Configure the maximum queue depth.
	(config-queue 1 gigabit-ethernet 0/1)**#max-depth** <*number*> Specifies the maximum number of packets held by the queue. By default, queues hold **255** packets. Use the **no** form of this command to return to the default setting.

Table 15. WRED Queue Commands

Step	Command and Description
Step 1	Enable WRED in the queue.
	(config-queue 1 efm-group 1/1)**#algorithm wred** Enables WRED in the queue. Use the **no** form of this command to disable WRED. By default, WRED is disabled.
Step 2	Specify minimum and maximum thresholds for green and yellow traffic.
	(config-queue 1 efm-group 1/1)**#thresholds green [minimum** <*value*> **| maximum** <*value*>**]** Specifies the minimum and maximum WRED thresholds for green (conforming) traffic in the queue. Valid threshold ranges are **1** to **16382** for minimum and **2** to **16383** for maximum. By default, the green WRED maximum threshold is set to **25** and the green WRED minimum threshold is set to **15**. Configure all WRED minimum values before configuring the maximum values. Use the **no** form of this command to return the thresholds to the default value.
	(config-queue 1 efm-group 1/1)**#thresholds yellow [minimum** <*value*> **| maximum** <*value*>**]** Specifies the minimum and maximum WRED thresholds for yellow (nonconforming) traffic in the queue. Valid threshold ranges are **1** to **16382** for minimum and **2** to **16383** for maximum. By default, the yellow WRED maximum threshold is set to **15** and the minimum threshold is set to **5**. The yellow maximum threshold should be set to less than or equal to the green minimum threshold for proper function. Configure all WRED minimum values before configuring the maximum values. Use the **no** form of this command to return the thresholds to the default value.

 Copyright © 2016 ADTRAN, Inc.

Table 15. WRED Queue Commands *(Continued)*

Step	Command and Description
Step 3	Configure the drop probability.
	(config-queue 1 efm-group 1/1)**#drop-probability [green** <*value*> **| yellow** <*value*>**]**
	Specifies the drop probability for both green (conforming) and yellow (nonconforming) traffic in the queue when WRED is enabled and the average queue depth has reached the maximum WRED threshold. Valid probability values are **0** to **100** percent. By default, drop probability for all traffic is **10** percent. Use the **no** form of this command to return the drop probability to the default value.

Table 16. WFQ Configuration Commands

Step	Command and Description
Step 1	Set the CoS value to match the CoS value of the next lower queue.
	(config-queue 1 gigabit-ethernet 0/1)**#cos group lower-adjacent** Lowers the CoS of the queue to match the CoS of the queue with the next lowest queue number to enable WFQ. By default, the CoS value matches the queue number. Use the **no** form of this command to set the CoS value of the queue back to the default value.
Step 2	Specify the queue weight.
	(config-queue 1 gigabit-ethernet 0/1)**#weight [dynamic |** <*number*>**]** Specifies the weight given to a specific queue when using WFQ. The **dynamic** parameter specifies that weight is set dynamically, and the <*number*> parameter assigns a percentage weight. Valid range is **1** to **100** percent. By default, weight is assigned dynamically. Using the **no** form of this command returns the weight to the default value.

Table 17. Policer Configuration Commands

Step	Command and Description
Step 1	Create a policer.
	(config)**#policer** <*name*> **[**<*slot*>**]** Creates and names the policer, and enters the policer's configuration mode. The <*name*> parameter is the name given to this policer. The optional <*slot*> parameter identifies the slot associated with this policer. Using the **no** form of this command removes the policer from the unit's configuration.

 Copyright © 2016 ADTRAN, Inc.

Table 17. Policer Configuration Commands *(Continued)*

Step	Command and Description
Step 2	Specify transmission thresholds.
	(config-policer POLICER1)**#cir** <*number*> Specifies the average maximum transmission rate of traffic in kbps allowed before the traffic is dropped. Valid range is **0** to **1000000** kbps. By default, the CIR threshold is **0** kbps. Using the **no** form of this command returns the CIR threshold to the default value.
	(config-policer POLICER1)**#cbs** <*number*> Specifies the maximum allowable number of bytes transmitted as a burst before the policer drops the traffic. Valid range is **0** to **999999** bytes. By default, the CBS threshold is **3125** bytes. Using the **no** form of this command returns the CBS threshold to the default value.
	(config-policer POLICER1)**#eir** <*number*> Specifies the allowed maximum transmission rate of traffic, over and above the CIR threshold, before the policer drops the traffic. Valid range is **0** to **1000000** kbps. By default, the EIR threshold is **600000** kbps. The EIR is the rate above and beyond the CIR value. If the CIR is set to 10 Mbps and the EIR is set to 1 Mbps, then the policer will not drop traffic until it exceeds 11 Mbps. Any traffic above the CIR is colored yellow and any traffic below the CIR is colored green. Any traffic that exceeds the CIR + EIR rate is considered red, which means that it is dropped. Using the **no** form of this command returns the EIR threshold to the default value.
	(config-policer POLICER1)**#ebs** <*number*> Specifies the allowed maximum number of bytes transmitted as a burst of data, over and above the CBS threshold, before the policer drops the traffic. Valid <*number*> range is **0** to **999999** bytes. By default, the EBS threshold is **12500** bytes. Using the **no** form of this command returns the EBS threshold to the default value.
Step 3	Configure additional features for policer.
	(config-policer POLICER1)**#color-aware** Enables **color-aware** for the policer to allow examining incoming packets for color markings and consider those color markings when determining the new color marking. By default, color-aware is disabled. Use the **no** form of this command to return to the default setting.
	(config-policer POLICER1)**#coupling** Enables **coupling** to couple internal operation for token refills from the CIR to EIR buckets. Coupling is disabled by default. Use the **no** form of this command to return to the default setting.
Step 4	Apply policer to a component.
	(config-policer POLICER1)**#per custom [evc-map** <*name*> **| interface gigabit-ethernet** <*slot/port.subinterface*>**]**

 Copyright © 2016 ADTRAN, Inc.

Table 17. Policer Configuration Commands *(Continued)*

Step	Command and Description
Step 4 ***Cont'd***	Applies the policer to all ingress traffic that matches one or more EVC maps or to an Ethernet subinterface. The **evc-map** <*name*> parameter specifies the name of the EVC map. The **interface gigabit-ethernet** <*slot/port.subinterface*> parameter specifies the Ethernet interface. By default, no policers are applied to any components. Using the **no** form of this command removes the policer from the component.
	(config-policer POLICER1)**#per evc** <*name*> Applies the current policer to every EVC map that is connected to the specified EVC. Using the **no** form of this command removes the policer from the component.
	(config-policer POLICER1)**#per policer** <*policer-name*> Sets the current policer to per policer mode by assigning the policer specified in <*policer-name*> parameter as the first tier policer. The current policer from which the command is issued, becomes the second tier policer.
	(config-policer POLICER1)**#per uni [efm-group** <*slot/group*> **| gigabit-ethernet** <*slot/port*>**]** Applies the policer to all EVC maps that are connected to the specified UNI interface. The **uni efm-group** <*slot/group*> and **uni gigabit-ethernet** <*slot/port*> parameters to specify the UNI interface. By default, no policers are applied to any components. Using the **no** form of this command removes the policer from the component.
Step 5	Enable policer.
	(config-policer POLICER1)**#no shutdown** Enables the policer.

Table 18. Shaper Configuration Commands

Step	Command and Description
Step 1	Create the shaper.
	(config)**#shaper** <*name*> **[**<*slot*>**]** Creates a shaper and enters the shaper's configuration mode. The <*name*> parameter names the shaper, and the optional <*slot*> parameter specifies the slot to which the shaper is assigned. Using the **no** form of this command removes the shaper from the unit's configuration. By default, no shapers are configured.
Step 2	Apply the shaper to an interface.
	(config-shaper SHAPER1)**#per interface [efm-group** <*slot/group*> **| gigabit-ethernet** <*slot/port*>**]** Specifies the interface to which the shaper is applied. The shaper can be applied to an EFM group or Gigabit Ethernet interface. Using the **no** form of this command removes the shaper from the interface.

 Copyright © 2016 ADTRAN, Inc.

Table 18. Shaper Configuration Commands *(Continued)*

Step	Command and Description
Step 3	Apply the shaper to an interface queue.
	(config-shaper SHAPER1)**#per interface [efm-group** <*slot/group*> **| gigabit-ethernet** <*slot/port*>**]** <*queue*> Specifies the interface queue(s) to which the shaper is applied. Up to seven per-queue shapers can be active at any one time. Valid range is **0** to **7**. Using the **no** form of this command removes the shaper from the interface queue.
Step 4	Specify the traffic rate limit.
	(config-shaper SHAPER1)**#rate** <*value*> Specifies the egress traffic rate for the shaper. Valid value range is **0** to **1000000** kbps. Use the **no** form of this command to return to the default rate (**1000000** kbps).
Step 5	Enable the shaper.
	(config-shaper SHAPER1)**#no shutdown** Enables the shaper.

 Copyright © 2016 ADTRAN, Inc.

Troubleshooting

Troubleshooting the QoS configuration for carrier Ethernet services can be done by using various **show** commands from the CLI.

The **show** commands are used to display current configurations and states of the various components, including any configured EVCs, EVC maps, shapers, policers, and queues. Reviewing the configuration of these items allows you to verify item configurations as a first step in troubleshooting functionality issues. The **show** commands are entered from the Enable mode prompt.

For example, to display information about EVC configurations, you can enter the **show evc** command as follows:

```
#show evc
All EVC Tags Available in MEN
EVC evc1
    S-TAG                    :123
    Admin State              : Enabled
    EVC Status               : Running
    MEN-Port                 : gigabit-ethernet 0/1
    CE-VLAN Preservation     : Enabled
```

Table 19 describes the **show** commands available for Layer 2/Layer 3 carrier Ethernet components in AOS.

Table 19. Show Commands for Layer 2/Layer 3 Carrier Ethernet Components

Command	Description
show evc [<*name*>**] [counters [**<*queue*>**] [performance-statistics [15-minute [**<*value*>**] | 24-hour [**<*value*>**]]**	Displays configuration and state information for all configured EVCs. You can optionally display information for a single EVC by entering the EVC name. The **counters** parameter can be used to display MEF counters for the specified EVC. Specifying the <*queue*> displays MEF counters for the specified queue number on the MEN port associated with the EVC. Valid entry for <*queue*> is **0** through **7**. You can optionally display the performance statistics for the interface by entering the **performance-statistics** parameter. These statistics can be displayed for 15-minute or 24-hour intervals, and can optionally be limited to a specific range of historic intervals using the <*value*> parameter. Valid interval range is **1** to **96** for 15-minute intervals and **0** to **7** for 24-hour intervals.
show evc-map [<*name*>**]**	Displays configuration and state information for all configured EVC maps. You can optionally display information for a single EVC map by entering the EVC map name.

 Copyright © 2016 ADTRAN, Inc.

Table 19. Show Commands for Layer 2/Layer 3 Carrier Ethernet Components *(Continued)*

Command	Description
show policer [<*name*>**]**	Displays configuration and state information for all configured policers. You can optionally display information for a single policer by entering the policer name.
show shaper [<*name*>**]**	Displays configuration and state information for all configured shapers. You can optionally display information for a single shaper by entering the shaper name. Displayed information includes the interface and queue(s) to which the shaper is applied, the configured and actual shaper rates, and the shaper mode (per-queue or per-interface).
show queue interface [efm-group <*slot/group*> **| gigabit-ethernet** <*slot/port*>**] [counters] [**<*queue*>**] [performance-statistics [15-minute [**<*value*>**] | 24-hour [**<*value*>**]]**	Displays the configuration information for the specified queues. You can optionally specify the queue number associated with the interface. Valid queue range is **0** to **7**. The **counters** parameter can be used to display MEF counters for the specified interface. You can optionally display the performance statistics for the interface by entering the **performance-statistics** parameter. These statistics can be displayed for 15-minute or 24-hour intervals, and can optionally be limited to a specific range of historic intervals using the <*value*> parameter. Valid interval range is **1** to **96** for 15-minute intervals and **0** to **7** for 24-hour intervals.
show interface [efm-group <*slot/group*> **| efm-group** <*slot/group.subinterface*> **| gigabit-ethernet** <*slot/port*> **| gigabit-ethernet** <*slot/port.subinterface*>**] [performance-statistics [15-minute [**<*value*>**] | 24-hour [**<*value*>**]]**	Displays the configuration information for the specified interface or subinterface. You can optionally display the performance statistics for the interface by entering the **performance-statistics** parameter. These statistics can be displayed for 15-minute or 24-hour intervals, and can optionally be limited to a specific range of historic intervals using the <*value*> parameter. Valid interval range is **1** to **96** for 15-minute intervals and **0** to **7** for 24-hour intervals.
show system-control-evc [performance-statistics [15-minute [<*value*>**] | 24-hour [**<*value*>**]]**	Displays the configuration information for the system control EVC. You can optionally the display the performance statistics for the EVC by entering the **performance-statistics** parameter. These statistics can be displayed for 15-minute or 24-hour intervals, and can optionally be limited to a specific range of historical intervals using the <*value*> parameter. Valid interval range is **1** to **96** for 15-minute intervals and **0** to **7** for 24-hour intervals.

 Copyright © 2016 ADTRAN, Inc.

Table 19. Show Commands for Layer 2/Layer 3 Carrier Ethernet Components *(Continued)*

Command	Description
show system-management-evc [performance-statistics [15-minute [<*value*>**] | 24-hour [**<*value*>**]]**	Displays the configuration information for the system management EVC. You can optionally the display the performance statistics for the EVC by entering the **performance-statistics** parameter. These statistics can be displayed for 15-minute or 24-hour intervals, and can optionally be limited to a specific range of historical intervals using the <*value*> parameter. Valid interval range is **1** to **96** for 15-minute intervals and **0** to **7** for 24-hour intervals.

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*
- *Carrier Ethernet Services Guide*
- *Configuring IP Access Control Lists (ACLs) in AOS*

Copyright © 2016 ADTRAN, Inc.