ADTRAN Switch Engine (ASE)

Quality of Service (QoS)

Configuration Guide

6AMCCG0002-29B

May 2020

To the Holder of this Document

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

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

Trademark Information

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

Disclaimer of Liability

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

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

Revision History

Rev A	March 2019	Initial release
Rev B	May 2020	Updated format and supported hardware.

Table of Contents

Overview 6

QoS Overview. 6

Ingress Traffic and QoS 6
Ingress Traffic Classification on the Port. 6
Queues 6
Egress Traffic and QoS. 9
DSCP Use in QoS. 9
QoS Control Lists 9

Hardware and Software Requirements and Limitations 10

QoS Configuration Overview 10

QoS Configuration Considerations for ASE Devices 11

Configuring Ingress QoS Parameters Using the GUI. 11

Configuring Ingress Port Traffic Classification Via the GUI. 11
Configuring the Ingress Port Policer Via the GUI 15
Configuring the QoS Ingress Map Via the GUI 16

Configuring QoS Queue Parameters via the GUI 19

Configuring the Queue Policer via the GUI. 19
Configuring WRED via the GUI. 20
Configuring the Queue Shaper via the GUI 22

Configuring QoS Egress Parameters Using the GUI 24

Configuring Egress Port Scheduling via the GUI 24
Configuring Egress Port Shapers via the GUI. 25
Configuring Egress Port Tag Remarking Using the GUI. 27
Configuring the QoS Egress Map via the GUI 29

Configuring QoS DSCP via the GUI (Optional) 33

Configuring Port DSCP Values via the GUI 34
Configuring DSCP Translation via the GUI. 35
Configuring DSCP Classification via the GUI 36
Configuring DSCP-Based QoS via the GUI 37

Configuring the QoS Control List via the GUI (Optional). 38

Configuring Global Storm Policers via the GUI (Optional) 43

Configuring Ingress QoS Parameters Using the CLI 43

Configuring QoS on a Per-Port Basis Via the CLI. 44
Configuring the Ingress Port Policer via the CLI 47
Configuring the QoS Ingress Map via the CLI. 47

Configuring QoS Queue Parameters via the CLI 50

Configuring the Queue Policer via the CLI 51
Configuring the Queue Shaper via the CLI. 51
Configuring WRED via the CLI 51

Configuring QoS Egress Parameters Using the CLI 52

Configuring Egress Port Scheduling via the CLI 52
Configuring Egress Port Shapers via the CLI 52
Configuring Egress Port Tag Remarking via the CLI 53
Configuring the QoS Egress Map via the CLI 53

Configuring QoS DSCP via the CLI (Optional) 56

Enabling DSCP Features on the Port via the CLI 57
Configure the DSCP Classify Map (Global) via the CLI 57
Configure the DSCP Ingress Translation Map (Global) via the CLI 58
Configure the DSCP Egress Translation Map (Global) via the CLI. 58
Configuring DSCP-Based QoS via the CLI 59

Configuring the QoS Control List via the CLI (Optional) 60

QCE Configuration Command Overview 60
Configuring QCE Actions (`[<action>]` Parameter) 61
Configuring QCE Matching Criteria (`[<matching criteria>]` Parameter) 62
Configuring QCE Operations (`[<qce operations>]` Parameter) 66

Configuring Global Storm Policers via the CLI (Optional). 66

QoS Configuration Examples Using the CLI 67

Classifying Ingress Traffic by Class 67
Classifying Ingress Traffic by Frame Tags 67
QoS Traffic Mapping 67
Configuring DSCP to QoS Classification 67
Configuring DSCP Translation for Ingress Traffic 68
Configuring Queue Shaper to Measure Data Rate 68
Configuring WRED Maximum Threshold 68
Configuring the QoS Ingress Map. 68
Configuring the QoS Egress Map 69

QoS Configuration Command Summary 69

Troubleshooting. 76

Viewing QoS Statistics Using the GUI 77
Viewing QoS Statistics and Configurations Using the CLI 77

Additional QoS Information 80

DSCP Values Explained 80
WRED Queue Management 84

Warranty and Contact Information. 87

Warranty 87
Contact Information. 87

1. Overview

This document explains the technology, applications, and configuration involved with Quality of Service (QoS) for use with ADTRAN switch engines (ASEs). Included in this guide are a brief introduction to QoS concepts and their implementation in ASE products, specific ASE QoS configurations and instructions, QoS configuration examples, and a troubleshooting section.

2. QoS Overview

The different types of traffic present on your network have specific needs for bandwidth, delay, and reliability. ASE devices 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.

The following sections give an overview of the processes and components tied to QoS configuration and implementation on the ASE device.

Ingress Traffic and QoS

QoS begins in the ASE device whenever traffic enters the port on which QoS is configured. Ingress traffic is subject to traffic classification by class of service (CoS), Drop Precedence Level (DPL), Priority Code Points (PCP), Drop Eligible Indicator (DEI), and Differentiated Service Code Points (DSCP) values. Classification can occur through port classification configurations, QoS ingress maps, and QoS policers.

Ingress Traffic Classification on the Port

All incoming traffic can be classified on a per-port basis, according to CoS class or ID, DEI values, DPL values, PCP values, or DSCP values. In addition, ingress traffic can be mapped by these values or other tag values included in packet headers. Once traffic is classified, it can be directed to specific queues and marked for rewriting or remapping on egress.

QoS Ingress Maps

Ingress maps are used by QoS as a method for further classifying incoming traffic based on key values in the packet or frame header. Maps use specified key matching criteria, such as DSCP, PCP, or DEI values contained in the packet header, which is then compared to the values in the incoming traffic. If the values match, configured actions can be taken on the matching traffic, in which new values can be assigned to the traffic as it moves through the ASE switch.

Ingress maps are applied on a per-port basis, but can also be associated with QoS control lists.

QoS Policers

Policers are used as bandwidth limiters for incoming traffic, and can be applied on a per-port basis, to a specific queue, or as a storm policer for the entire ASE switch. Port and queue policers limit the bandwidth of received frames that exceed configured rates for the port. The global storm policer can be used to restrict the amount of flooded frames, those without previously-learned source media access control (MAC) addresses, from entering the device.

Queues

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.

Queues can be managed by policers, queue shapers, and scheduling algorithms.

Queue Shapers

Queue shapers are used to control bandwidth usage and traffic flow parameters for egress traffic on the ASE device. Shapers can be applied on a per-port or per-queue basis, and when applied to a queue, can be used to measure data or line rates of traffic from the queue associated with a port.

Schedulers

QoS scheduling is configured at the port level, and uses two types of scheduling algorithms to determine the pace at which traffic moves through the ASE device: strict priority scheduling, and deficit weighted round robin (DWRR).

Strict Priority Scheduling

The first type of scheduling algorithm used by QoS on the ASE device is strict priority scheduling. By default, all queues use this method.

In strict priority scheduling, as shown in *Figure 1* below, queues are serviced in a specific order. In this type of scheduling, Queue 7 (highest priority) 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.

Strict priority scheduling 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.

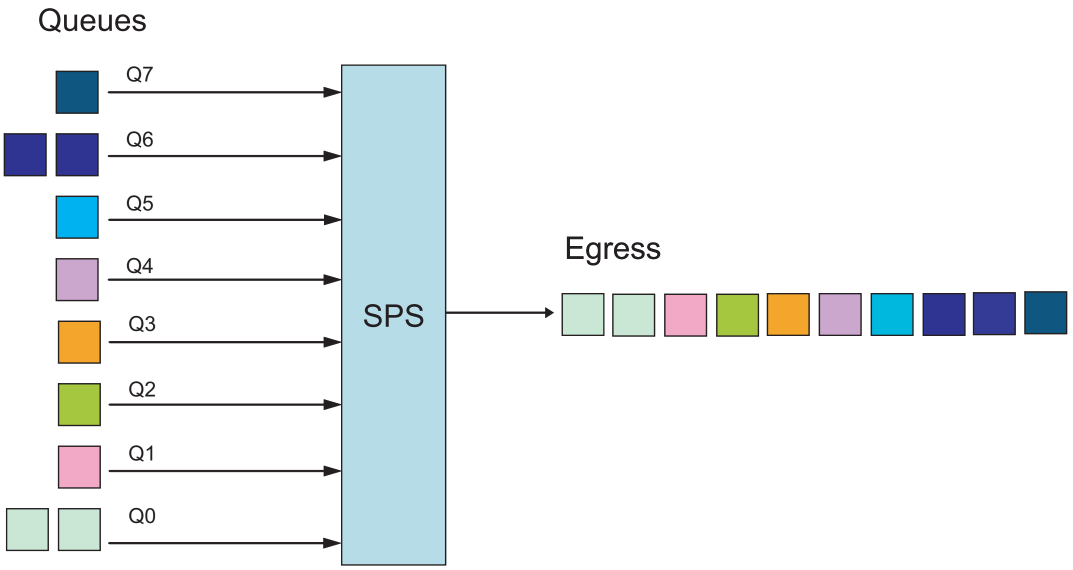


Figure 1. Strict Priority Scheduling

Weighted Fair Queuing (WFQ)

The ASE device supports 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 strict priority scheduling 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 2 on page 8*, 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 strict priority scheduler (SPS) before egressing the interface. Only after the EF and AF queues are emptied will the best effort (BE) queue be serviced.

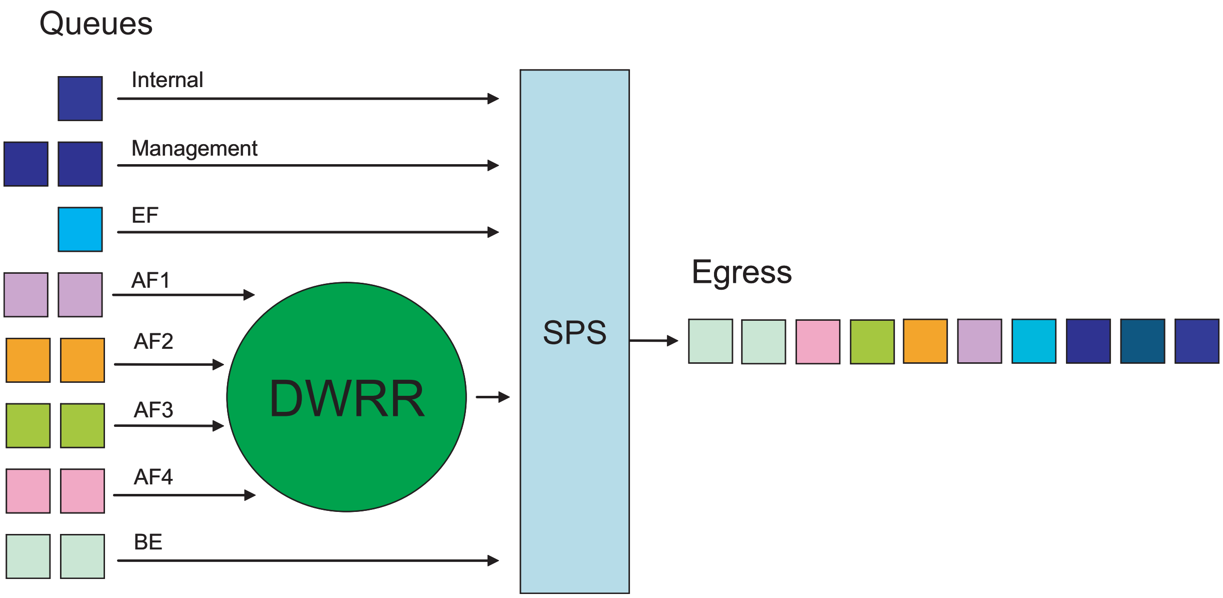


Figure 2. DWRR Scheduling

NOTE

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

When the number of queues selected for DWRR is less than eight, then the lowest priority queues are put in DWRR and higher priority queues are put in strict priority scheduling. For example, if DWRR is set for two queues, then queues zero and one are put in DWRR, and the remaining queues are placed in strict priority scheduling.

Weighted Random Early Detection (WRED)

Congestion can be avoided in the queue system by enabling and configuring the Weighted Random Early Detection (WRED) function. WRED is an active queue congestion management discipline that adds thresholds for queued traffic. As the average queue depth increases, the ASE device 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.

There are three separate WRED groups, and each port belongs to one of these groups.

For more specific information about WRED operation in QoS, refer to *WRED Queue Management on page 84*.

Egress Traffic and QoS

Egress traffic can also be manipulated and directed by QoS configurations. As traffic moves throughout the switch and prepares to exit, traffic can be directed by port schedulers and shapers, which operate similarly to queue shapers and schedulers, but on a per-port basis. Egress traffic can also be manipulated by a QoS egress map, which controls the rewriting of PCP, DEI, and DSCP packet values at egress, or packet remarking and remapping configurations.

Egress Traffic Manipulation on the Port

All egress traffic can be scheduled by a port scheduler, which can help to avoid or manage egress traffic congestion. Port shapers are also useful to control bandwidth allocation for egress traffic on the port. In addition, packet header values can be rewritten on egress using port tag remarking features, configured based on mappings between CoS and DPL values and their PCP and DEI counterparts.

QoS Egress Maps

Egress maps are used by QoS as a method for further controlling the rewriting of packets at egress, where PCP, DEI, and DSCP values can be updated based on their classified key values. Egress maps are configured by specifying which part of the packet is used for matching, enabling the rewriting actions taken once the packet information is processed, and specifying which new values are mapped to the packet information.

Egress maps are applied on a per-port basis, but can also be associated with QoS control lists.

DSCP Use in QoS

QoS on the ASE device can include DSCP configuration for packet classification, translation, rewriting, or remapping purposes, based on packet DSCP values and information. These features can be applied on a per-port basis for both ingress traffic classification and translation and egress traffic rewriting and remapping. Typical DSCP configurations include enabling DSCP features on the port, configuring the DSCP classification map, specifying the DSCP ingress translation map, and then configuring DSCP-based QoS.

More detailed information about DSCP values, and their use in QoS, is available in *DSCP Values Explained on page 80*.

QoS Control Lists

The ASE QoS feature includes the available use of QoS control lists (QCLs), which function as other traffic control lists, but can be used to configure flexible classification for Layer 2, 3, and 4 network traffic, as well as to perform reclassification of traffic based on CoS, DPL, PCP, DEI, DSCP, and access control list (ACL) values. The QCL is comprised of various QoS control entries (QCEs), which are applied on a per-port basis, and can specify source and destination MAC addresses, traffic types, virtual local area network (VLAN) IDs, PCP values, and frame types that receive certain classification is traffic matches the QCE criteria.

QCEs are applied on a per-port basis, but can also be associated with QoS ingress and egress maps, as well as ACLs.

3. Hardware and Software Requirements and Limitations

QoS features are supported on the ASE products outlined in *Table 1* that are running ASE firmware 4.4-41 or later.

Table 1. Supported Products

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

4. QoS Configuration Overview

QoS configuration begins with configuring ingress traffic classification, then specifying how that traffic is organized, directed, and managed as it moves through the switch. QoS configuration ends by determining how the traffic is labeled and organized to egress the switch. The following are the required and optional configuration tasks associated with QoS configuration on the ASE device. All configurations are available via the GUI or the CLI.

The following are the required QoS configurations and their associated tasks:

1. Configuration of the ingress QoS parameters. Instructions are available in *Configuring Ingress QoS Parameters Using the GUI on page 11* and *Configuring Ingress QoS Parameters Using the CLI on page 43*.
2. Configuration of the QoS queue parameters. Instructions are available in *Configuring QoS Queue Parameters via the GUI on page 19* and *Configuring QoS Queue Parameters via the CLI on page 50*.
3. Configuration of the QoS egress parameters. Instructions are available in *Configuring QoS Egress Parameters Using the GUI on page 24* and *Configuring QoS Egress Parameters Using the CLI on page 52*.

The following are the optional QoS configurations and their associated tasks:

1. Configuration of DSCP-based QoS. Instructions are available in *Configuring QoS DSCP via the GUI (Optional) on page 33* and *Configuring QoS DSCP via the CLI (Optional) on page 56*.
2. Configuration of QoS Control Lists. Instructions are available in *Configuring the QoS Control List via the GUI (Optional) on page 38* and *Configuring the QoS Control List via the CLI (Optional) on page 60*.
3. Configuration of global storm policers. Instructions are available in *Configuring Global Storm Policers via the GUI (Optional) on page 43* and *Configuring Global Storm Policers via the CLI (Optional) on page 66*.

QoS Configuration Considerations for ASE Devices

The following information includes parameters specific for QoS configurations in the ASE device, and should be considered when configuring QoS.

- In the ASE device, there is a one-to-one mapping between the terms CoS, QoS class, queue, and priority. A CoS value of zero has the lowest priority.
- CoS IDs, within the ASE QoS configuration, are used as values for selectors associated with egress maps and other Ethernet services. They do not relate to CoS in any way.
- WRED can be configured globally to avoid congestion and drop the yellow framed traffic when the queues are filled.
- Ingress maps, when applied, always take precedence over other kinds of port-based classification.

5. Configuring Ingress QoS Parameters Using the GUI

The first steps in configuring the QoS feature on the ASE device is to specify how traffic is handled on the incoming port. To configure the ingress QoS parameters, configure the traffic classification on the ingress port, the port policer, and an ingress traffic map. To configure these settings, connect to the ASE GUI and complete the following tasks:

- *Configuring Ingress Port Traffic Classification Via the GUI on page 11*
- *Configuring the Ingress Port Policer Via the GUI on page 15*
- *Configuring the QoS Ingress Map Via the GUI on page 16*

These actions serve to classify and police the incoming traffic on the ASE device.

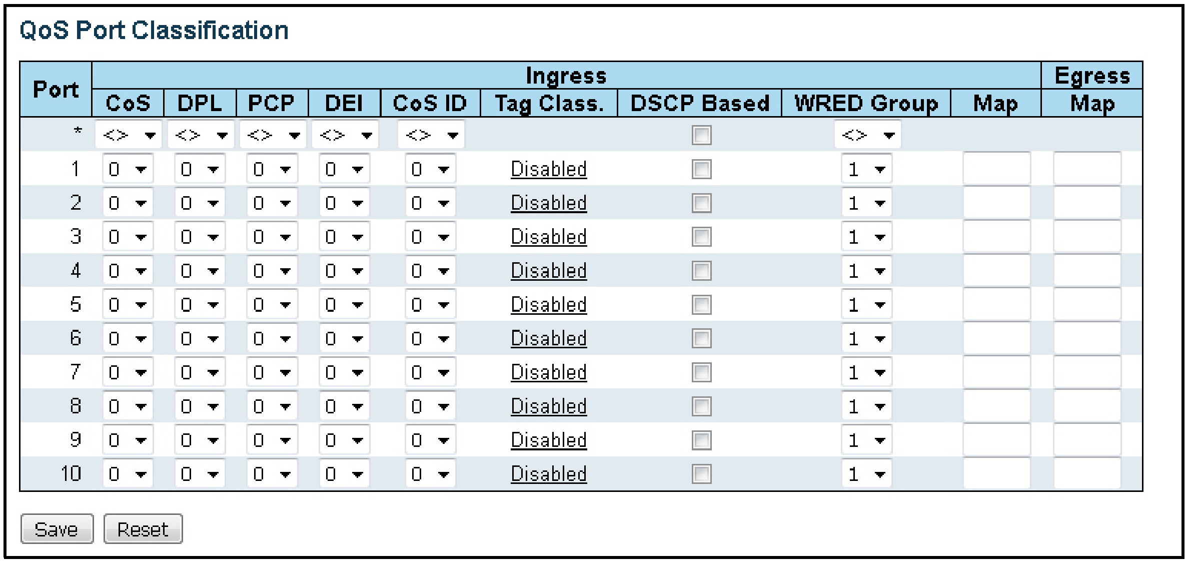
NOTE

*It is recommended to restore defaults on the ASE device before beginning any configuration. To restore the defaults on the device, connect to the GUI, navigate to the **Maintenance** tab, and select **Factory Defaults**. Be aware this will erase the IP address of the switch itself.*

Configuring Ingress Port Traffic Classification Via the GUI

The first step in configuring the QoS feature is to specify how the ingress traffic is classified when it first enters the switch. The menu shown below is used to configure QoS ingress classification for all ports on the switch.

To access the QoS ingress classification menu, connect to the GUI and navigate to the **Configuration** tab, then select **QoS** > **Port Classification**.



QoS Port Classification

Port	Ingress									Egress
	CoS	DPL	PCP	DEI	CoS ID	Tag Class.	DSCP Based	WRED Group	Map	Map
*	<>	<>	<>	<>	<>		□	<>		
1	0	0	0	0	0	Disabled	□	1		
2	0	0	0	0	0	Disabled	□	1		
3	0	0	0	0	0	Disabled	□	1		
4	0	0	0	0	0	Disabled	□	1		
5	0	0	0	0	0	Disabled	□	1		
6	0	0	0	0	0	Disabled	□	1		
7	0	0	0	0	0	Disabled	□	1		
8	0	0	0	0	0	Disabled	□	1		
9	0	0	0	0	0	Disabled	□	1		
10	0	0	0	0	0	Disabled	□	1		

From this menu, you can configure the following QoS settings for all the ports on the switch:

1. The **Port** column specifies on which port the QoS configuration is taking place. Configuring the * row in the **Port** column indicates that the configuration is applicable to all ports on the switch.
2. The **CoS** drop-down menu specifies the CoS value assigned to incoming traffic on the port. Every frame that enters the port is associated with a CoS value. Valid CoS range is **0** to **7**, with a value of **0** being the lowest priority. The CoS value can be mapped from the PCP and DEI values in the frame tag (if the port is VLAN-aware, the frame is tagged, and the **Tag Class** menu setting is enabled). If the port is not VLAN-aware, or the frame is not tagged, the default CoS value is used.

NOTE

The CoS value specified here applies to all ingress traffic on the port, and is only overwritten by a QoS Control List entry (refer to Configuring the QoS Control List via the GUI (Optional) on page 38 for more information about QCLs and QCEs).

3. The **DPL** drop-down menu specifies the drop precedence level (DPL) assigned to the incoming traffic on the port. Every frame that enters the port is associated with a DPL value. Valid DPL range is **0** to **3**, with a default value of **0**. Like with CoS values, the DPL value can be mapped from the PCP and DEI values of the frame tag (if the port is VLAN-aware, the frame is tagged, and the **Tag Class** menu setting is enabled). If the port is not VLAN-aware, or the frame is not tagged, the default DPL value is used.

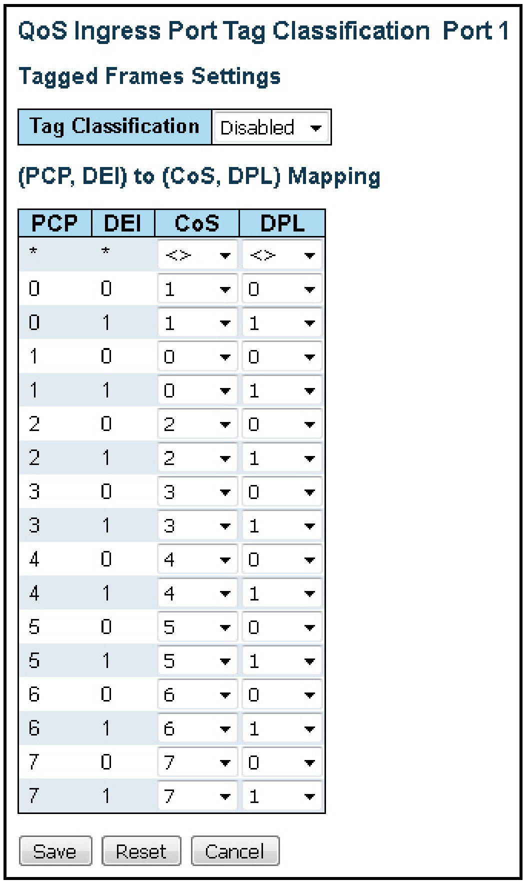
NOTE

Again, like the CoS value, The DPL value specified here applies to all ingress traffic on the port, and is only overwritten by a QCE (refer to Configuring the QoS Control List via the GUI (Optional) on page 38 for more information about QCLs and QCEs).

4. The **PCP** drop-down menu specifies the priority code point (PCP) value of the incoming traffic on the port. Every frame that enters the port is associated with a PCP value. Valid PCP range is **0** to **7**. By default, all

frames are classified using the default PCP value unless the port is VLAN-aware and the frame is tagged, in which case the PCP value given in the frame tag is used.

5. The **DEI** drop-down menu specifies the drop eligibility indicator (DEI) value for incoming traffic on the port. The valid DEI range is **0** to **1**. Each frame that enters the port is associated with a DEI bit, and uses the default DEI bit value unless the port is VLAN-aware and the frame is tagged, in which case the DEI value from the frame tag is used.
6. The **CoS ID** drop-down menu assigns a CoS ID to the incoming traffic on the port. Valid ID range is **0** to **7**, and is configured as **0** by default. This value is used in the creation of QoS ingress and egress maps to identify specific traffic flows or classes (refer to *Configuring the QoS Ingress Map Via the GUI on page 16* or *Configuring the QoS Egress Map via the GUI on page 29* for information regarding map configuration).
7. The **Tag Class** field specifies how incoming tagged frames on the VLAN-aware port are handled. By default, this feature is **Disabled**, which indicates the default CoS and DPL values are used for tagged frames. When enabled, this feature specifies that PCP and DEI values, mapped from the CoS and DPL values in the frame tags, are used instead. To enable this feature, select the **Disabled** link in the **Tag Class** field for the specific port and enter the tag classification parameters in the **QoS Ingress Port Tag Classification** menu that appears for the specific port. Here you can enable tag classification by selecting **Enabled** from the **Tag Classification** drop-down menu, and specify the **Cos** and **DPL** values that are mapped to the associated **PCP** and **DEI** values. The CoS and DPL values are selected using the appropriate drop-down menu, and have valid ranges of **0** to **7** and **0** to **3**, respectively. When the tag classification configuration is complete, select **Save** at the bottom of the menu to save the settings and return to the **QoS Port Classification Menu**.



QoS Ingress Port Tag Classification Port 1

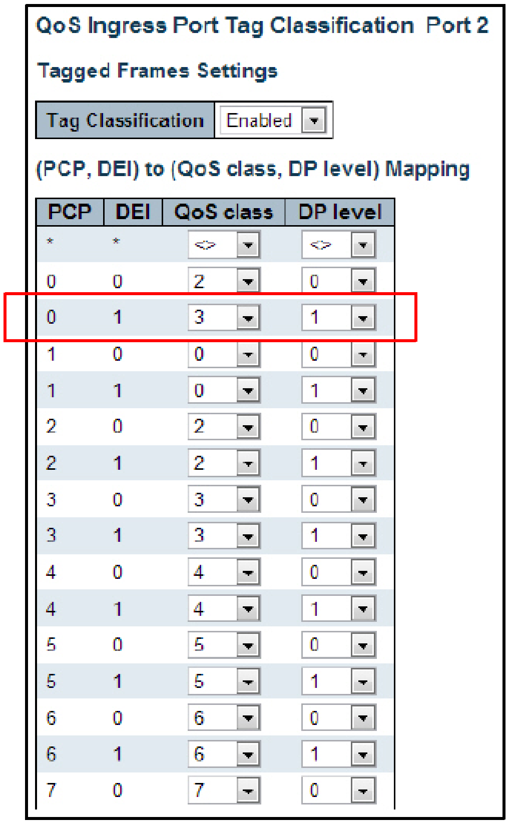
Tagged Frames Settings

Tag Classification: Disabled

(PCP, DEI) to (CoS, DPL) Mapping

PCP	DEI	CoS	DPL
*	*	<>	<>
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	2	0
2	1	2	1
3	0	3	0
3	1	3	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0
7	1	7	1

For example, as shown below, the **PCP 0** and **DEI 1** values on **Port 2** are mapped to the **CoS 3** and **DPL 1** values:



QoS Ingress Port Tag Classification Port 2

Tagged Frames Settings

Tag Classification: Enabled

(PCP, DEI) to (QoS class, DP level) Mapping

PCP	DEI	QoS class	DP level
*	*	<>	<>
0	0	2	0
0	1	3	1
1	0	0	0
1	1	0	1
2	0	2	0
2	1	2	1
3	0	3	0
3	1	3	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0

NOTE

The ***Tag Class*** *configuration is only necessary for VLAN-aware ports, and will have no affect on a port that is not VLAN-aware.*

8. Once you have returned to the **QoS Port Classification Menu**, the next field to configure is the **DSCP Based** field. This feature is disabled by default, and can be enabled by selecting the check box on the appropriate port. When enabled, the incoming traffic on the port is mapped to a specific CoS and DPL value, based on the DSCP value already inherent in the frame. These mappings are configured using the **DSCP-Based QoS Ingress Classification** menu, described in *Configuring DSCP-Based QoS via the GUI on page 37*. When this feature is disabled, the traffic uses the default CoS and DPL values.

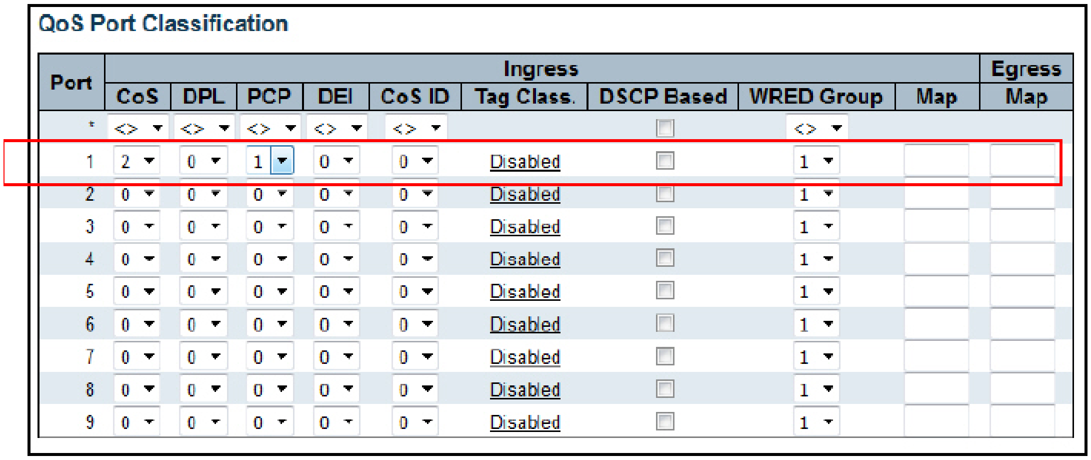
9. The **WRED Group** drop-down menu specifies the WRED group associated with incoming traffic on the port. Valid group range is **1** to **3**. The WRED group is part of the queue system used by the ASE switch to avoid traffic congestion, and is configured using the **Weighted Random Early Detection Configuration** menu, as described in *Configuring WRED via the GUI on page 20*.

10. The **Map** field specifies an ingress map to be used by the port for all incoming traffic. Specify the ingress map ID in the appropriate field. Ingress maps are configured as described in *Configuring the QoS Ingress Map Via the GUI on page 16*. Entering a map ID in this field indicates that the mapping rules and configurations in the configured map are applied to incoming traffic on the port.

11. The **Egress Map** field specifies an egress map to be used by the port for all egress traffic that matches the specified criteria. Specify the egress map ID in the appropriate field. Egress maps are configured as described in *Configuring the QoS Egress Map via the GUI on page 29*. Entering a map ID in this field

indicates that traffic matching the other port classification configurations will use the mapping rules configured in the egress map when it leaves the switch system.

For example, in the image below, **Port 1** is configured so that all incoming traffic on the port is mapped to a CoS value of **2**, and the PCP value is set to **1**:



QoS Port Classification

Port	Ingress									Egress
	CoS	DPL	PCP	DEI	CoS ID	Tag Class.	DSCP Based	WRED Group	Map	Map
*	<>	<>	<>	<>	<>		□	<>		
1	2	0	1	0	0	Disabled	□	1		
2	0	0	0	0	0	Disabled	□	1		
3	0	0	0	0	0	Disabled	□	1		
4	0	0	0	0	0	Disabled	□	1		
5	0	0	0	0	0	Disabled	□	1		
6	0	0	0	0	0	Disabled	□	1		
7	0	0	0	0	0	Disabled	□	1		
8	0	0	0	0	0	Disabled	□	1		
9	0	0	0	0	0	Disabled	□	1		

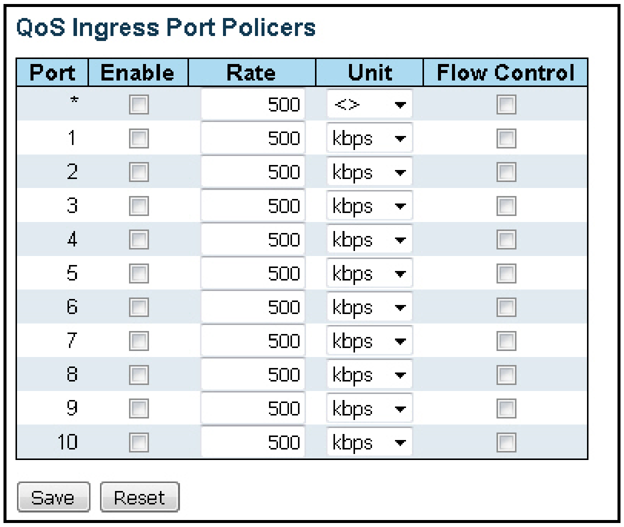
Once all port(s) have been configured, select **Save** at the bottom of the **QoS Port Classification** menu to apply the traffic classification parameters to all incoming traffic on the configured port(s). You can now proceed to configure the remaining QoS ingress parameters on the switch.

Configuring the Ingress Port Policer Via the GUI

After configuring the QoS ingress classification for traffic on the port, the next step in configuring QoS ingress parameters is to configure the port policer used by QoS for ingress traffic. This policer serves to classify even further the incoming traffic on the port. The policer is applied on a per-port basis, where it is either enabled or disabled, and traffic rates and flow control are configured.

To configure the QoS ingress port policer, complete these steps:

1. Navigate to the **Configuration** tab, and select **QoS** > **Port Policing** to display the **QoS Ingress Port Policers** menu.

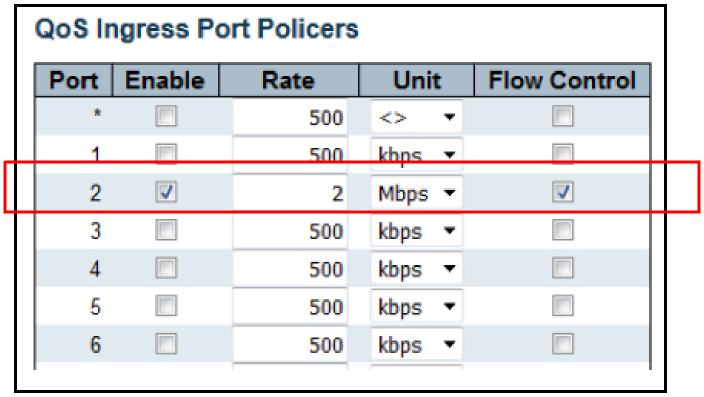


QoS Ingress Port Policers

Port	Enable	Rate	Unit	Flow Control
*	□	500	<>	□
1	□	500	kbps	□
2	□	500	kbps	□
3	□	500	kbps	□
4	□	500	kbps	□
5	□	500	kbps	□
6	□	500	kbps	□
7	□	500	kbps	□
8	□	500	kbps	□
9	□	500	kbps	□
10	□	500	kbps	□

2. Enable the QoS policer on the port by selecting the check box for the appropriate port in the **Enable** field. The ***** in the **Port** column indicates the configuration is for all ports on the switch, rather than a single specified port.
3. Specify the policer rate from the **Rate** drop-down menu and the unit of measurement from the **Unit** drop-down menu. Valid rate range is **100** to **1000000** if the unit is set to **kbps** or **fps**, and is **1** to **3300** if the unit is set to **Mbps** or **kfps**. By default, the policer is configured for a rate and unit of **500 kbps**.
4. Enable flow control for the policer by selecting the check box in the **Flow Control** field. By default, flow control is disabled. When enabled, and the port is configured in flow control mode, the policer will not discard TCP traffic paused frames, but rather will continue to send them.
5. When all the policer fields have been configured for the port(s), select **Save** at the bottom of the menu to save the settings and apply the policer to incoming traffic on the port.

In the example shown below, the policer on Port 2 is enabled, and configured with a policer rate of 2 Mbps and flow control enabled.



QoS Ingress Port Policers

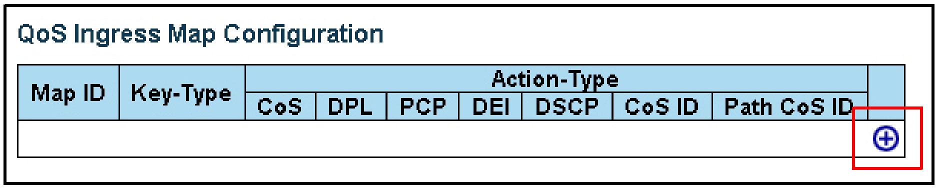
Port	Enable	Rate	Unit	Flow Control
*	□	500	<>	□
1	□	500	kbps	□
2	☑	2	Mbps	☑
3	□	500	kbps	□
4	□	500	kbps	□
5	□	500	kbps	□
6	□	500	kbps	□

Configuring the QoS Ingress Map Via the GUI

Once the port traffic classification and port policer have been configured for QoS, you can begin configuration of the QoS ingress map. Ingress maps are used by QoS as a method for further classifying incoming traffic based on key values in the packet or frame header. Maps are configured by specifying which part of the packet is used for matching (PCP, PCP/DEI, DSCP, or PCP/DEI/DSCP), specifying the actions taken once the packet information is processed, and the specifying which values are mapped to the packet information.

To being configuring a QoS ingress map, complete these steps:

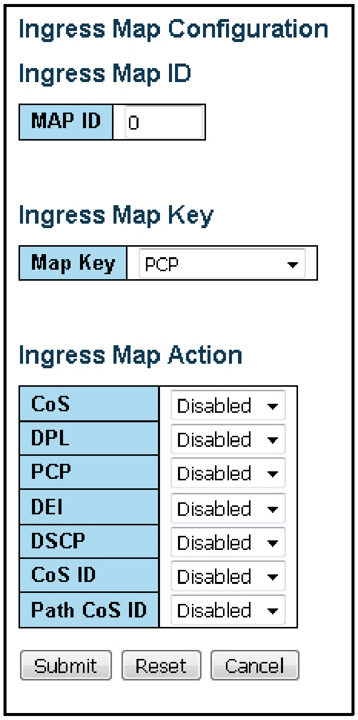
1. Navigate to the **Configuration** tab, and then select **QoS** > **Ingress Map**. The **QoS Ingress Map Configuration** menu is displayed, where all configured ingress maps are listed.



QoS Ingress Map Configuration

Map ID	Key-Type	Action-Type							
		CoS	DPL	PCP	DEI	DSCP	CoS ID	Path CoS ID	
									⊕

2. To configure a new QoS ingress map, select the **plus** sign at the bottom right of the **QoS Ingress Map Configuration** menu. This action will open the **Ingress Map Configuration** menu.



Ingress Map Configuration

Ingress Map ID

MAP ID	0

Ingress Map Key

Map Key	PCP

Ingress Map Action

CoS	Disabled
DPL	Disabled
PCP	Disabled
DEI	Disabled
DSCP	Disabled
CoS ID	Disabled
Path CoS ID	Disabled

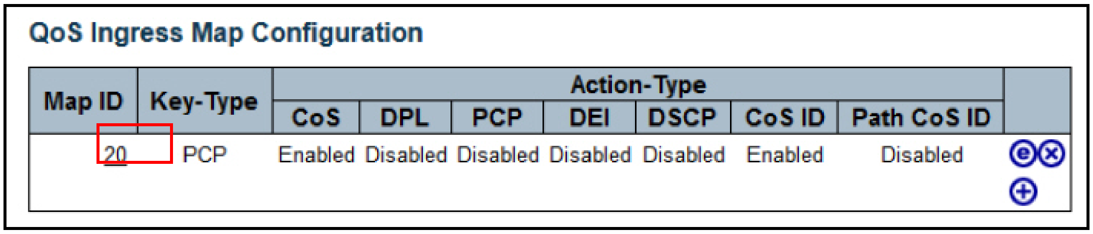
3. Specify the ID number for the ingress map in the **MAP ID** field.

4. Next, specify the **Map Key** from the drop-down menu. The map key is the part of the packet header used for matching purposes. The key type choices are **PCP** (default), **PCP-DEI**, **DSCP**, or **DSCP-PCP-DEI**. Selecting **PCP** indicates the map applies mapping actions to incoming traffic based on the PCP header, **PCP-DEI** indicates mapping actions take place based on both PCP and DEI information from the packet, **DSCP** indicates mapping actions take place based on the DSCP value in the packet, and **DSCP-PCP-DEI** indicates all values are used to determine mapping actions.

5. Lastly, specify the action to be taken by the map for the **CoS**, **DPL**, **PCP**, **DEI**, **DSCP**, **CoS ID**, and **Path CoS ID** parameters. Each parameter can be enabled or disabled from the appropriate drop-down menu. When enabled, these values are used to further classify the traffic and are assigned to packets and traffic flows matched by map key specified in the ingress map.

6. Select **Submit** to create the ingress map. Once created, the map will be displayed in the **QoS Ingress Map Configuration** menu.

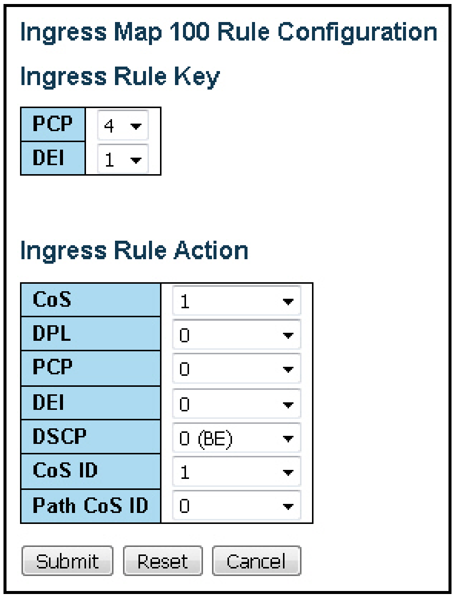
7. Add additional rules to each map by selecting the **Map ID** from the list in the **QoS Ingress Map Configuration** menu. These rules are used to define the mapping between the traffic matched based on the ingress map key (for example, **PCP**) and the new values specified by the map rules.



QoS Ingress Map Configuration

Map ID	Key-Type	Action-Type							
		CoS	DPL	PCP	DEI	DSCP	CoS ID	Path CoS ID	
20	PCP	Enabled	Disabled	Disabled	Disabled	Disabled	Enabled	Disabled	ⓔ ⊗
									⊕

8. In the **Ingress Rule Map Configuration** menu, specify the **Ingress Rule Key** for the keys you selected for the map (refer to Step 4 above) from the drop-down menu. Here you are defining the values for the keys, for example, PCP value **4** or DEI value **1**. These values are used for matching ingress traffic. In addition, specify the **Ingress Rule Action** by selecting the appropriate value from the action drop-down menu. For example, if PCP value is specified as **4**, you can map that to a CoS value of **1**, with a CoS ID value of **1** by selecting those values from the appropriate **CoS** or **CoS ID** drop-down menus and then selecting **Submit**.



Ingress Map 100 Rule Configuration

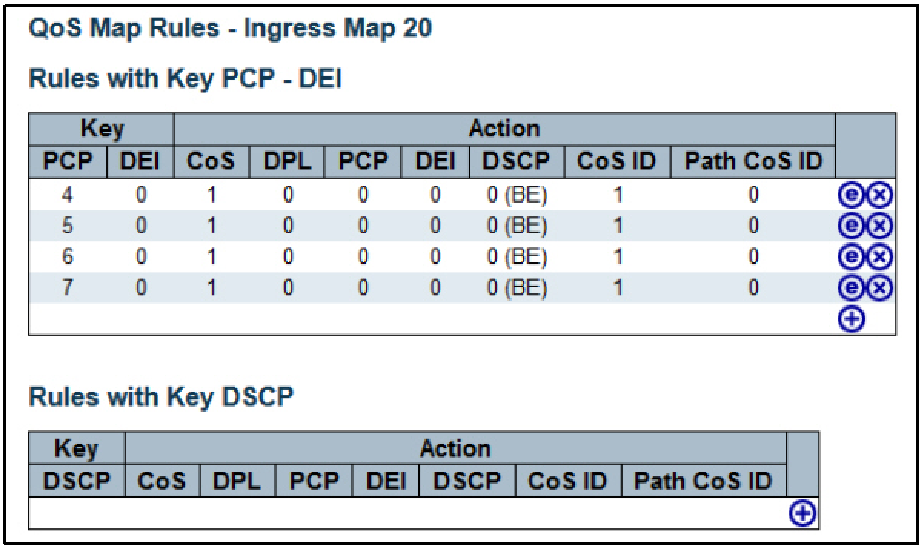
Ingress Rule Key

PCP	4
DEI	1

Ingress Rule Action

CoS	1
DPL	0
PCP	0
DEI	0
DSCP	0 (BE)
CoS ID	1
Path CoS ID	0

9. Once you select **Submit**, the map rules are shown in the **QoS Map Rules** configuration menu for the specific map. You can add as many rules as necessary to define the proper traffic matching and mapping properties for the QoS ingress map.



QoS Map Rules - Ingress Map 20

Rules with Key PCP - DEI

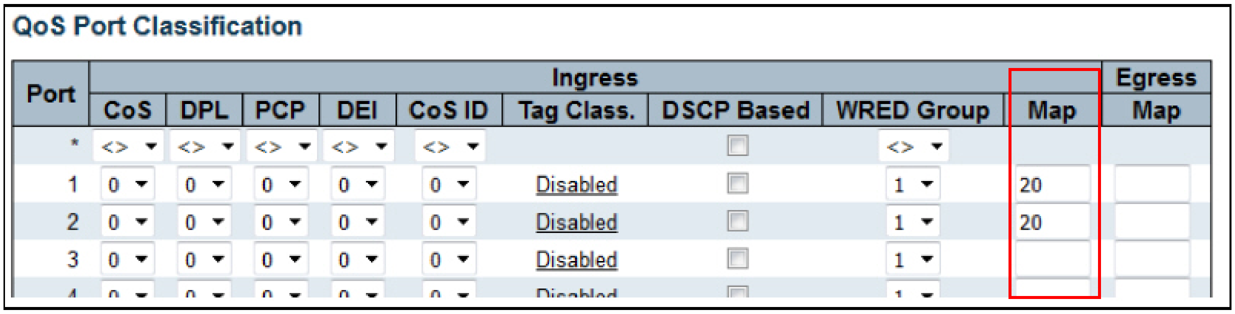
Key		Action						
PCP	DEI	CoS	DPL	PCP	DEI	DSCP	CoS ID	Path CoS ID
4	0	1	0	0	0	0 (BE)	1	0
5	0	1	0	0	0	0 (BE)	1	0
6	0	1	0	0	0	0 (BE)	1	0
7	0	1	0	0	0	0 (BE)	1	0

Rules with Key DSCP

Key	Action						
DSCP	CoS	DPL	PCP	DEI	DSCP	CoS ID	Path CoS ID

10. Once the map and its rules have been configured, the map must be applied for it to take effect. You can apply the ingress map to a specific port, using the **QoS Port Classification** menu (refer to *Configuring*

Ingress Port Traffic Classification Via the GUI on page 11), or you can apply the map to a QoS Control List, as described in *Configuring the QoS Control List via the GUI (Optional) on page 38*.



QoS Port Classification

Port	Ingress									Egress
	CoS	DPL	PCP	DEI	CoS ID	Tag Class.	DSCP Based	WRED Group	Map	Map
*	<>	<>	<>	<>	<>		□	<>		
1	0	0	0	0	0	Disabled	□	1	20	
2	0	0	0	0	0	Disabled	□	1	20	
3	0	0	0	0	0	Disabled	□	1		
4	0	0	0	0	0	Disabled	□	1		

After configuring the QoS ingress map, the ingress portion of QoS configuration is completed. The next steps include configuring the QoS queue parameters and the QoS egress behaviors.

6. Configuring QoS Queue Parameters via the GUI

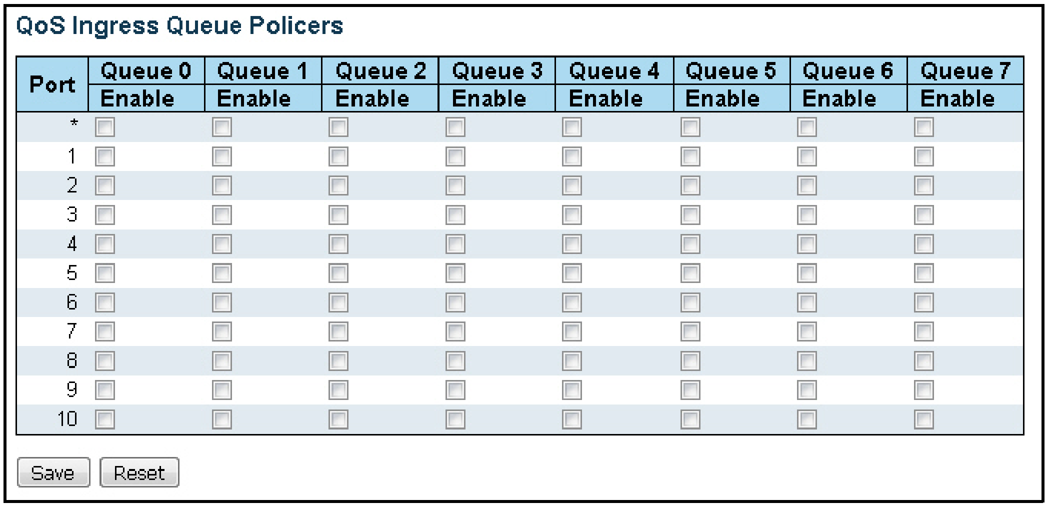
Configuring the QoS queue parameters on the ASE switch determines how traffic is handled to avoid or manage traffic congestions. Queues are managed by a queue policer, WRED algorithm, and a queue shaper. To configure the QoS queue parameters, connect to the ASE GUI and complete the following tasks:

- *Configuring the Queue Policer via the GUI on page 19*
- *Configuring WRED via the GUI on page 20*
- *Configuring the Queue Shaper via the GUI on page 22*

Configuring the Queue Policer via the GUI

Configuration of the queue policer occurs on a per-port basis, and consists of enabling the queue policer and specifying the traffic rate for the enabled policer. The queue policers limit the bandwidth of received frames that exceed configured rates for the port. To configure the queue policer, complete these steps:

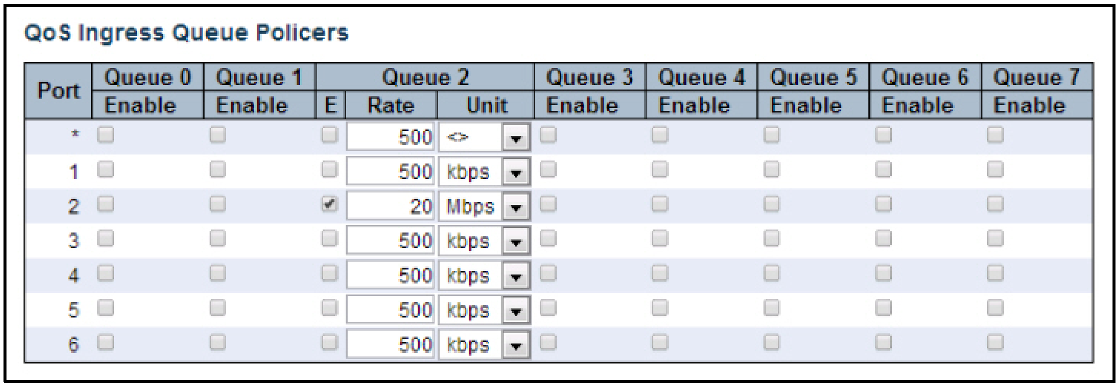
1. Navigate to the **Configuration** tab and select **Qos** > **Queue Policing**. The **QoS Ingress Queue Policers** configuration menu appears.



QoS Ingress Queue Policers

Port	Queue 0	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable
*	□	□	□	□	□	□	□	□
1	□	□	□	□	□	□	□	□
2	□	□	□	□	□	□	□	□
3	□	□	□	□	□	□	□	□
4	□	□	□	□	□	□	□	□
5	□	□	□	□	□	□	□	□
6	□	□	□	□	□	□	□	□
7	□	□	□	□	□	□	□	□
8	□	□	□	□	□	□	□	□
9	□	□	□	□	□	□	□	□
10	□	□	□	□	□	□	□	□

2. Enable the queue policer on a specific port by selecting the **Enable** check box for the queue (**0** to **7**) you want to enable on the port.
3. Once you have enabled the policer for the queue, you can specify the rate for the policer by entering the rate value and unit from the appropriate **Rate** and **Unit** drop-down menus. Valid **Rate** range is **100** to **1000000** for the **kbps** unit, and **1** to **3300** for the **Mbps** unit. By default, the policer rate is configured for **500 kbps**.



QoS Ingress Queue Policers

Port	Queue 0	Queue 1	Queue 2			Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	Enable	Enable	E	Rate	Unit	Enable	Enable	Enable	Enable	Enable
*	□	□	□	500	<>	□	□	□	□	□
1	□	□	□	500	kbps	□	□	□	□	□
2	□	□	☑	20	Mbps	□	□	□	□	□
3	□	□	□	500	kbps	□	□	□	□	□
4	□	□	□	500	kbps	□	□	□	□	□
5	□	□	□	500	kbps	□	□	□	□	□
6	□	□	□	500	kbps	□	□	□	□	□

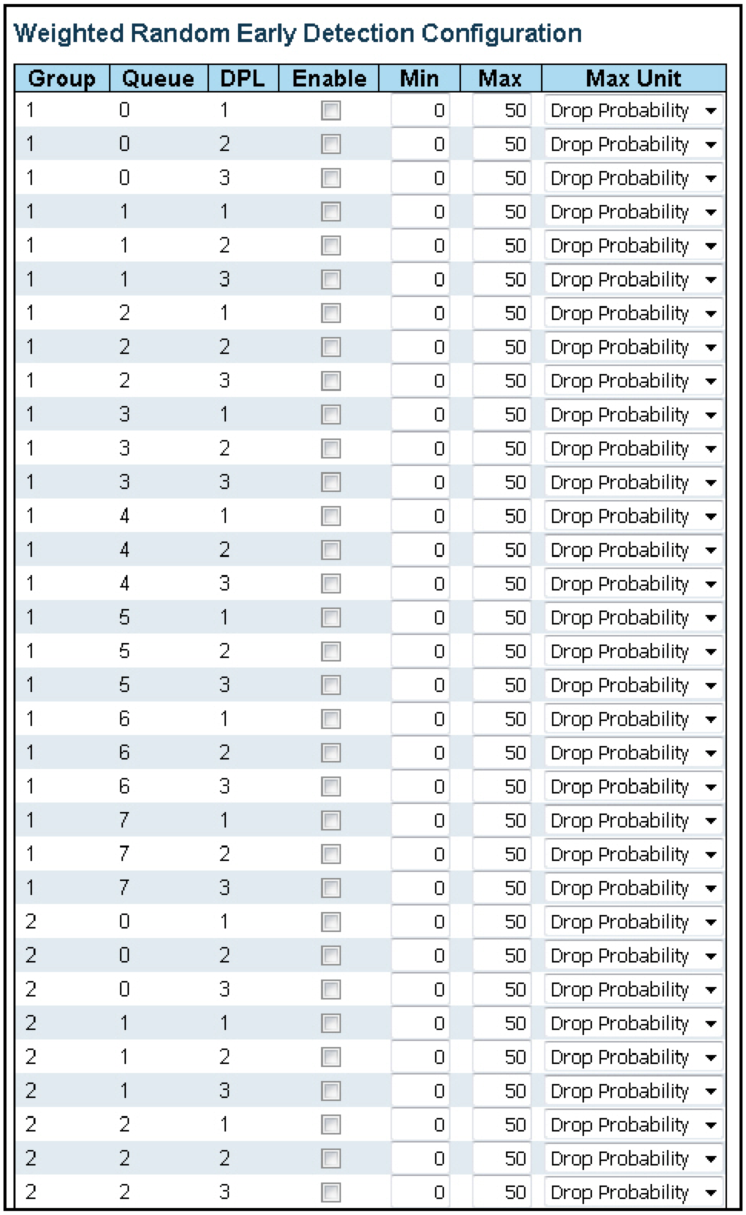
4. Once you have enabled the queue policer and specified its rate, select **Save** to apply the queue policer to the port.

Configuring WRED via the GUI

Congestion can be avoided in the QoS queue system by enabling and configuring the Weighted Random Early Detection (WRED) function on the ASE device. WRED configuration includes enabling the feature and specifying the minimum and maximum threshold for packets held within the queue. When the minimum threshold is reached, packets begin to be dropped from the queue. The maximum threshold, on the other hand, specifies that packets are dropped from the queue when the queue fill level reaches the threshold, or all packets are dropped when the queue is 100 percent full.

To configure the QoS WRED settings, complete these steps:

1. Navigate to the **Configuration** tab, and select **QoS** > **WRED** to display the **Weighted Random Early Detection Configuration** menu.



Weighted Random Early Detection Configuration

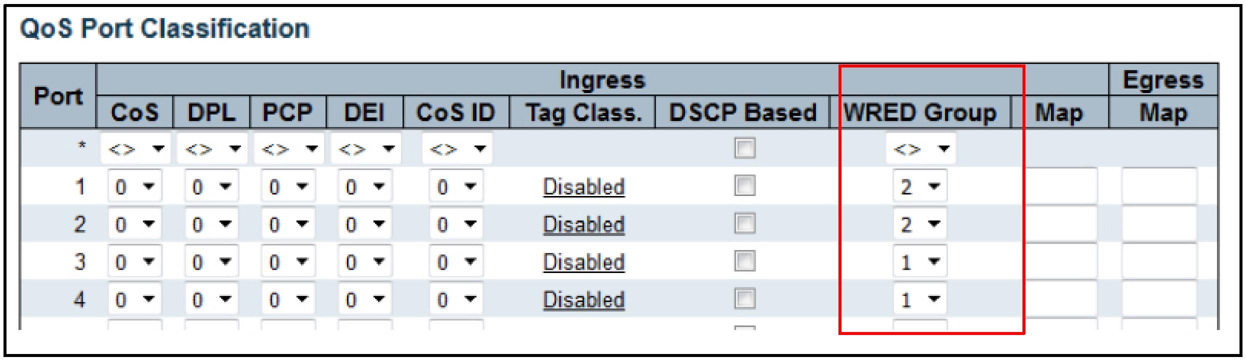
Group	Queue	DPL	Enable	Min	Max	Max Unit
1	0	1	□	0	50	Drop Probability ▾
1	0	2	□	0	50	Drop Probability ▾
1	0	3	□	0	50	Drop Probability ▾
1	1	1	□	0	50	Drop Probability ▾
1	1	2	□	0	50	Drop Probability ▾
1	1	3	□	0	50	Drop Probability ▾
1	2	1	□	0	50	Drop Probability ▾
1	2	2	□	0	50	Drop Probability ▾
1	2	3	□	0	50	Drop Probability ▾
1	3	1	□	0	50	Drop Probability ▾
1	3	2	□	0	50	Drop Probability ▾
1	3	3	□	0	50	Drop Probability ▾
1	4	1	□	0	50	Drop Probability ▾
1	4	2	□	0	50	Drop Probability ▾
1	4	3	□	0	50	Drop Probability ▾
1	5	1	□	0	50	Drop Probability ▾
1	5	2	□	0	50	Drop Probability ▾
1	5	3	□	0	50	Drop Probability ▾
1	6	1	□	0	50	Drop Probability ▾
1	6	2	□	0	50	Drop Probability ▾
1	6	3	□	0	50	Drop Probability ▾
1	7	1	□	0	50	Drop Probability ▾
1	7	2	□	0	50	Drop Probability ▾
1	7	3	□	0	50	Drop Probability ▾
2	0	1	□	0	50	Drop Probability ▾
2	0	2	□	0	50	Drop Probability ▾
2	0	3	□	0	50	Drop Probability ▾
2	1	1	□	0	50	Drop Probability ▾
2	1	2	□	0	50	Drop Probability ▾
2	1	3	□	0	50	Drop Probability ▾
2	2	1	□	0	50	Drop Probability ▾
2	2	2	□	0	50	Drop Probability ▾
2	2	3	□	0	50	Drop Probability ▾

2. The first two columns of the menu display the WRED group and its associated queue. There are three total WRED groups, and eight queues available for WRED configuration, and the first two columns contain each available combination of WRED group and queue number. The third column lists the DPL value associated with each combination of WRED group and queue.

NOTE

*The previous image only captures the first part of the **WRED Configuration** menu. The menu itself is long enough to cover all three WRED groups, all eight queues, and all possible combinations of both.*

3. To enable the WRED algorithm on the appropriate WRED group, queue, and DPL value combination, select the **Enable** check box. By default, WRED is disabled on all queues.
4. Once WRED is enabled, specify the minimum threshold for the queue by entering the appropriate value in the **Min** field. The **Min** threshold is the queue fill level at which WRED begins discarding traffic frames. By default this value is set to **0** frames.
5. Next, specify the maximum threshold for the queue by entering the appropriate value in the **Max** field. The **Max** threshold is a percentage that specifies the likelihood of traffic frames being dropped by WRED. By default, this value is set to **50** percent. In addition to specifying the **Max** threshold percentage, you must also specify the **Max Unit** from the **Max Unit** drop-down menu. There are two choices for the **Max Unit**: **Drop Probability** and **Fill Level**. When the maximum unit is set to **Drop Probability**, the **Max** threshold value indicates the probability that traffic frames will be dropped when the queue is filled nearly to 100 percent. By default, the maximum threshold is set to **50**, and the maximum unit is set to **Drop Probability**, indicating there is a 50 percent likelihood that traffic frames will be dropped when the queue is nearly full. When the **Max Unit** is set to **Fill Level**, the maximum threshold value indicates the fullness of the queue when traffic frames will certainly be dropped. For example, if the maximum threshold is set to **50** and the maximum unit is set to **Fill Level**, then WRED will begin dropping frames when the queue is 50 percent full.
6. Once WRED has been enabled for the queue, and the maximum and minimum thresholds have been configured, select **Save** at the bottom of the menu to save the WRED configuration.
7. Once the WRED configuration is complete, to enforce the WRED and queue configurations, you must apply the WRED group to incoming traffic on the switch. To accomplish this, navigate back to the **QoS Port Classification** menu (**Configuration** tab, **QoS** > **Port Classification**) and specify the WRED group associated with the port using the **WRED Group** drop-down menu.



QoS Port Classification

Port	Ingress									Egress
	CoS	DPL	PCP	DEI	CoS ID	Tag Class.	DSCP Based	WRED Group	Map	Map
*	<>	<>	<>	<>	<>		☐	<>		
1	0	0	0	0	0	Disabled	☐	2		
2	0	0	0	0	0	Disabled	☐	2		
3	0	0	0	0	0	Disabled	☐	1		
4	0	0	0	0	0	Disabled	☐	1		

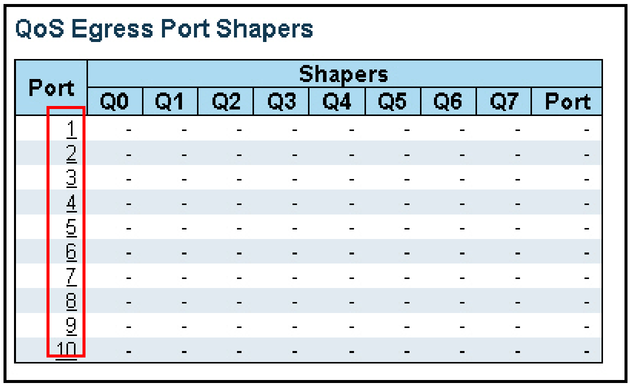
Once the WRED groups have been configured and associated with the necessary port(s), you can continue the QoS queue configuration by configuring the queue shaper.

Configuring the Queue Shaper via the GUI

The shaper available for the queues configures bandwidth usage and traffic flow parameters for egress traffic on the ASE device. Shapers can also be applied at port-level (refer to *Configuring Egress Port Scheduling via the GUI on page 24*), however, queue-level shapers can be used to measure data rates or line rates of traffic from the queue associated with a port. To configure the queue shaper, you must first access the port on which the queue is applied, and then configure the shaper for each queue associated with the port.

To configure queue shapers, complete these steps:

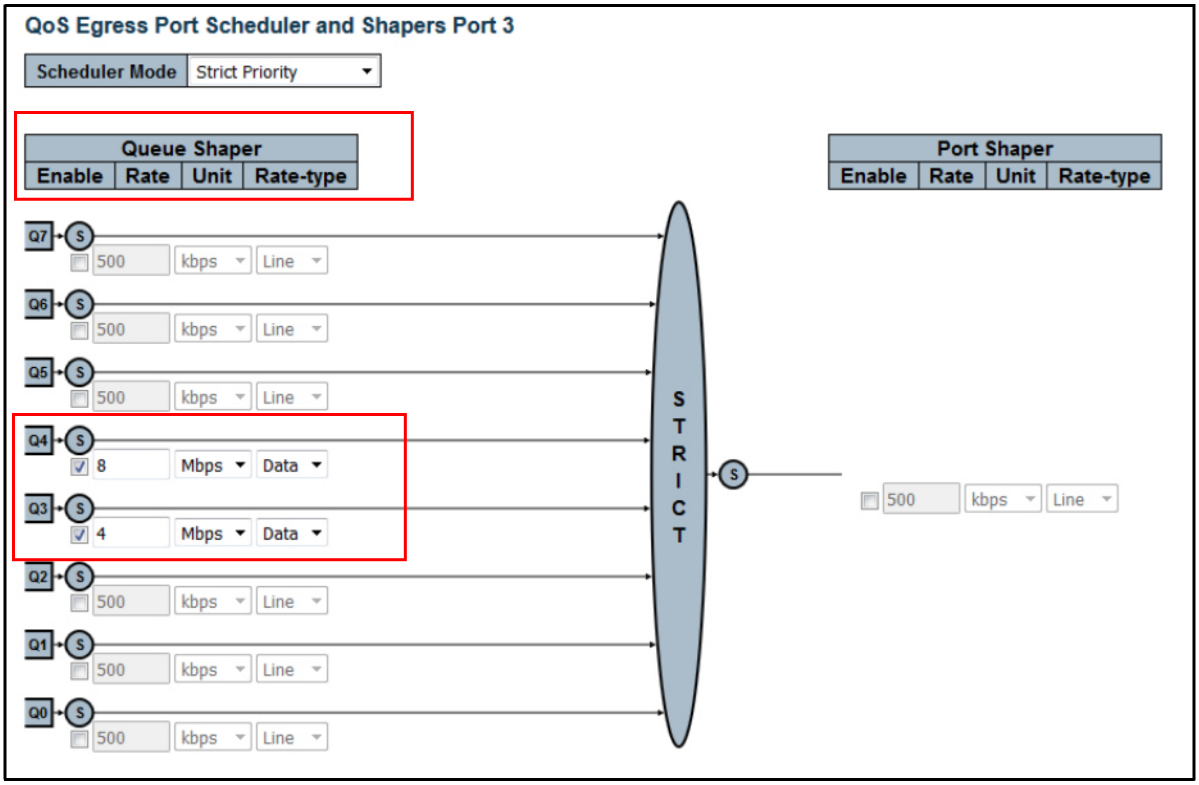
1. Navigate to the **Configuration** tab, and select **QoS** > **Port Shapers**. In the **QoS Egress Port Shapers** menu, select the port on which you want to configure the queue shaper.



QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-

2. In the **QoS Egress Port Shapers and Schedulers** menu, use the **Queue Shaper** menu to configure the queue shaper for the queues used on the port. You can configure all queues to measure bandwidth rates independently.



QoS Egress Port Scheduler and Shapers Port 3

Scheduler Mode: Strict Priority

Queue	Queue Shaper Enable	Rate	Unit	Rate-type
Q7	□	500	kbps	Line
Q6	□	500	kbps	Line
Q5	□	500	kbps	Line
Q4	☑	8	Mbps	Data
Q3	☑	4	Mbps	Data
Q2	□	500	kbps	Line
Q1	□	500	kbps	Line
Q0	□	500	kbps	Line

Port Shaper Enable	Rate	Unit	Rate-type
□	500	kbps	Line

3. Enable the queue shaper by selecting the check box next to the appropriate queue number.

4. Specify the bandwidth rate used by the shaper in the **Rate** field and select the bandwidth rate unit by choosing the appropriate measurement (**Mbps** or **kbps**) from the drop-down menu. By default, the bandwidth rate for the shaper is set to **500 kbps**.

5. Next specify the **Rate-type** from the drop-down menu. You can choose either **Line** or **Data** rate, which specifies that the queue shaper measures either line bandwidth rates or data bandwidth rates. By default, the shaper will measure **Line** bandwidth rates.

6. Once you have configured all queue shapers applicable to the port, select **Save** at the bottom of the menu to save the queue shaper settings on the port.

7. Configuring QoS Egress Parameters Using the GUI

The last steps in configuring the QoS feature on the ASE device is to specify how traffic is handled on the egress port. To configure the egress QoS parameters, configure the traffic schedulers and shapers on the port, any packet or frame tag remarking on the port, and an egress traffic map. To configure these settings, connect to the ASE GUI and complete the following tasks:

- *Configuring Egress Port Scheduling via the GUI on page 24*
- *Configuring Egress Port Shapers via the GUI on page 25*
- *Configuring Egress Port Tag Remarking Using the GUI on page 27*
- *Configuring the QoS Egress Map via the GUI on page 29*

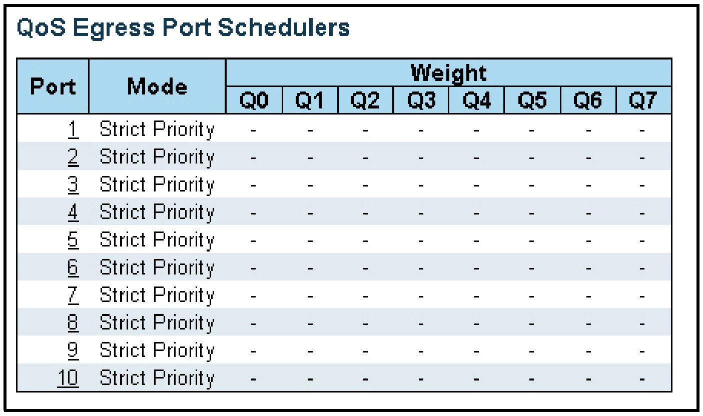
These actions serve to shape, schedule, and prepare the outgoing traffic on the ASE device.

Configuring Egress Port Scheduling via the GUI

As part of QoS configuration, you can configure port-level scheduling for egress traffic to help avoid or manage egress traffic congestion. Scheduling is performed by scheduling algorithms, which follow either strict priority scheduling or weighted round robin (WRR) scheduling. Strict priority scheduling specifies that all queues adhere to the priority values applied to the egress traffic when deciding which packets and frames to send first. WRR scheduling is based on the weights configured for each queue associated with the port.

To configure egress traffic scheduling for each port, complete these steps:

1. Navigate to the **Configuration** tab, and select **QoS** > **Port Scheduling**. In the **QoS Egress Port Schedulers** menu, each port, along with its configured scheduling mode and associated queue weight is displayed.

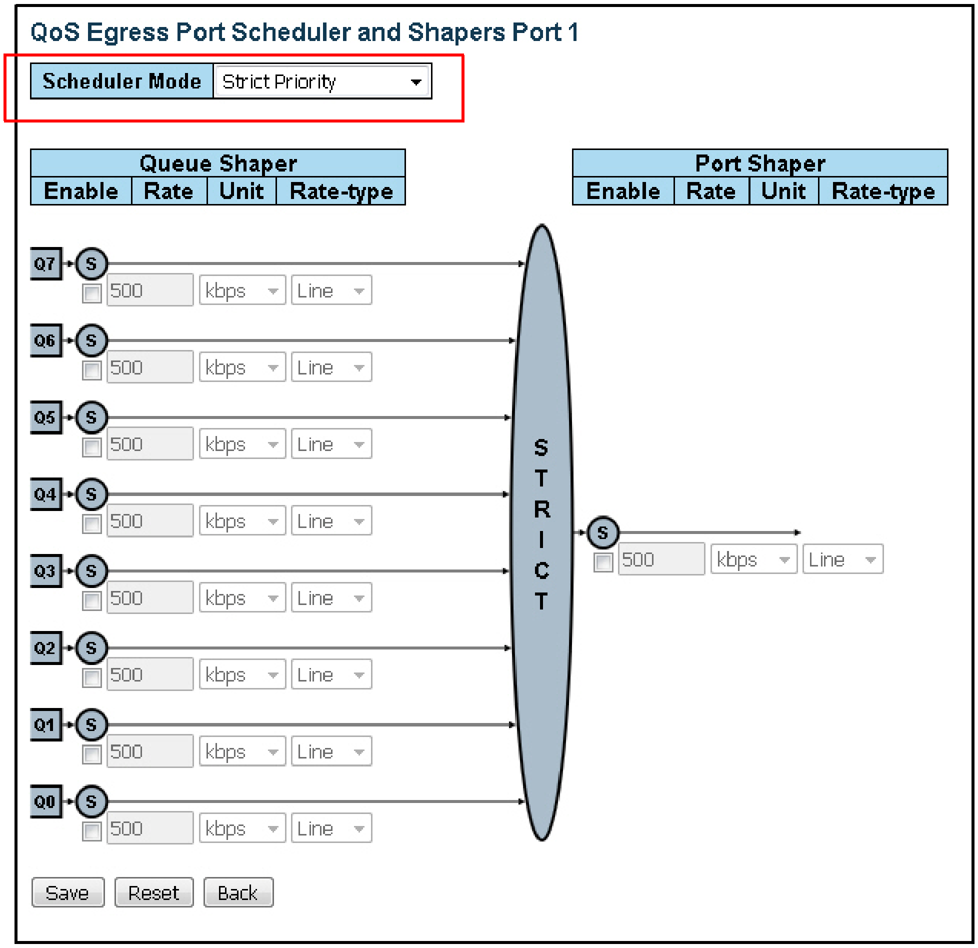


QoS Egress Port Schedulers

Port	Mode	Weight							
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	Strict Priority	-	-	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-	-	-

2. Select the port from the numbered list on which you want to configure the scheduler. By default, each port is configured with a scheduler set to **Strict Priority**.

3. In the **QoS Egress Port Scheduler and Shaper** menu for the port you selected, you can specify the port scheduler mode from the **Scheduler Mode** drop-down menu.



QoS Egress Port Scheduler and Shapers Port 1

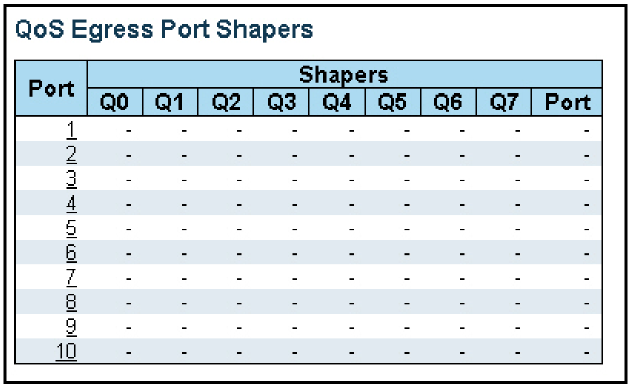
Scheduler Mode: Strict Priority

4. Select **Save** at the bottom of the menu to save the port scheduler configuration.

Configuring Egress Port Shapers via the GUI

Shapers can be configured on a per-port basis to aid in bandwidth allocation on the port. To configure a port shaper, complete these steps:

1. Navigate to the **Configuration** tab, and select **QoS** > **Port Shaping**. The **QoS Egress Port Shapers** menu is displayed, which shows the queue shaper rate and the port shaper rate associated with each port.

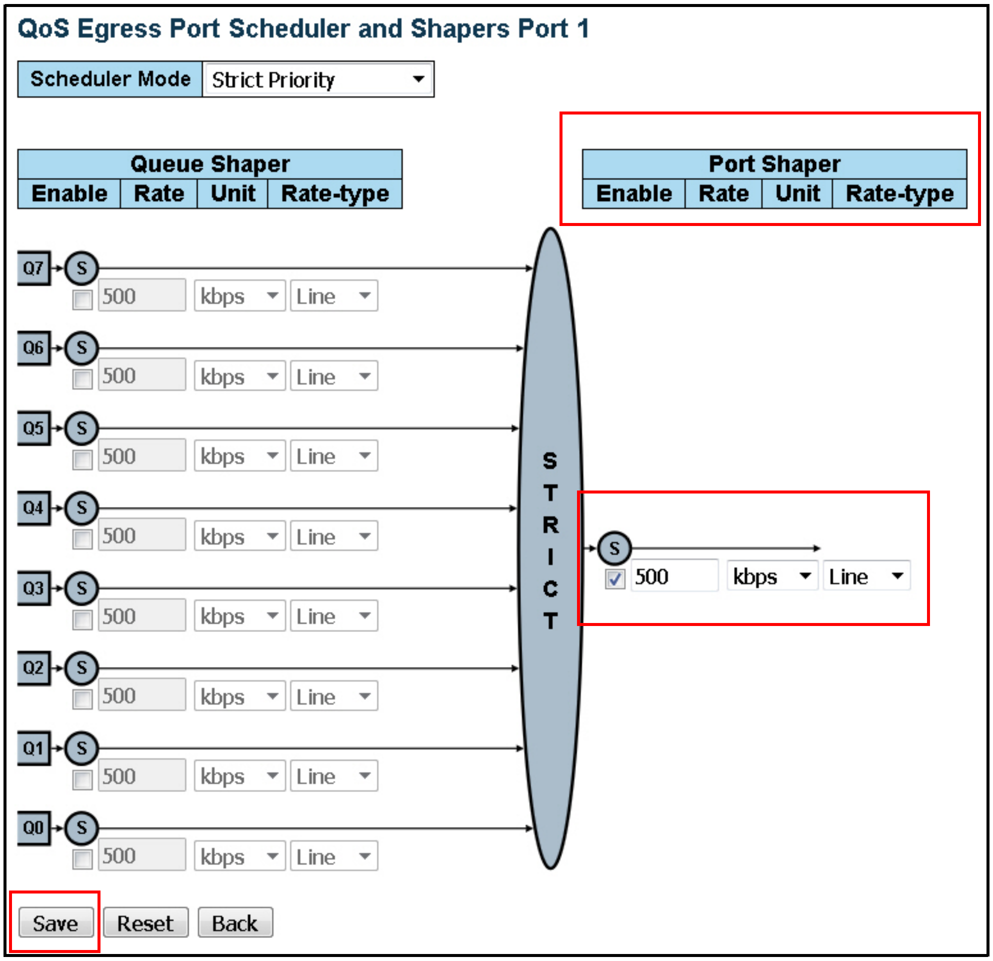


QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-

2. Select the port on which you want to configure the shaper from the **Port** list.
3. In the **QoS Egress Port Scheduler and Shapers** menu, enable the shaper on the port by selecting the **Enable** check box for the port shaper.
4. Specify the bandwidth rate used by the shaper in the **Rate** field and select the bandwidth rate unit by choosing the appropriate measurement (**Mbps** or **kbps**) from the drop-down menu. By default, the bandwidth rate for the shaper is set to **500 kbps**.

5. Next specify the **Rate-type** from the drop-down menu. You can choose either **Line** or **Data** rate, which specifies that the queue shaper measures either line bandwidth rates or data bandwidth rates. By default, the shaper will measure **Line** bandwidth rates.



QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Strict Priority

Queue Shaper				
	Enable	Rate	Unit	Rate-type
Q7	☐	500	kbps	Line
Q6	☐	500	kbps	Line
Q5	☐	500	kbps	Line
Q4	☐	500	kbps	Line
Q3	☐	500	kbps	Line
Q2	☐	500	kbps	Line
Q1	☐	500	kbps	Line
Q0	☐	500	kbps	Line

Port Shaper			
Enable	Rate	Unit	Rate-type
☑	500	kbps	Line

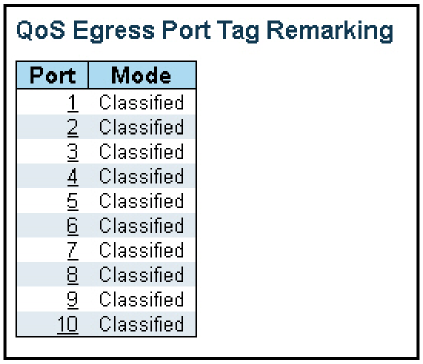
6. Once you have configured the shaper for the port, select **Save** at the bottom of the menu to save the shaper's configuration on the port.

Configuring Egress Port Tag Remarking Using the GUI

Egress traffic can be classified on the port by remarking the tags on the traffic. Tags can be set to one of three marking strategies. The first is **Classified**, which specifies that the PCP and DEI values on the egress frames are updated with the classified tag values specified at ingress (refer to *Configuring Ingress Port Traffic Classification Via the GUI on page 11*). The second is **Default**, which specifies that the PCP and DEI values on the egress frames are updated to the default values defined on the port (set with this configuration). The third is **Mapped**, which specifies that the PCP and DEI values on the egress frames are updated based on the CoS/DPL to PCP/DEI mapping configured on the port (set with this configuration).

To configure tag remarking for egress traffic on the port, complete these steps:

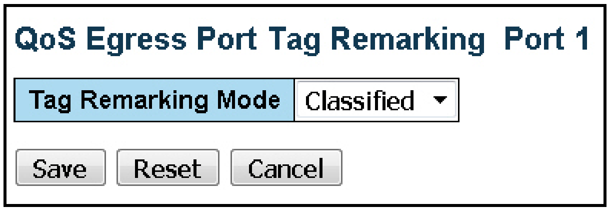
1. Navigate to the **Configuration** tab and select **QoS** > **Port Tag Remarking**. The **QoS Egress Port Tag Remarking** menu appears, and indicates the remarking mode for each port on the switch. By default, each port is set to **Classified**, indicating they use the PCP and DEI values configured at ingress.



QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified

2. Select the port on which you want to configure tag remarking from the **Port** list. The **QoS Egress Port Tag Remarking** configuration menu for the port is displayed.

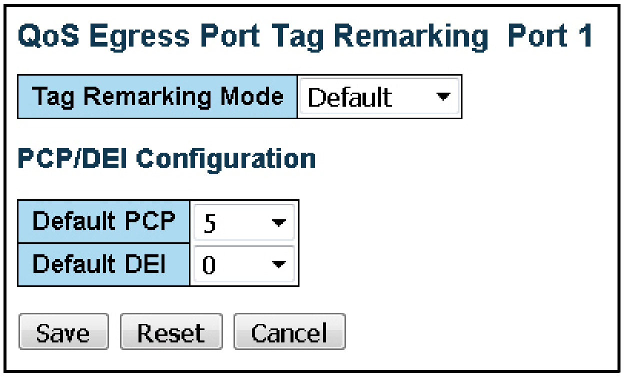


QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode: Classified

3. Select the appropriate mode from the **Tag Remarking Mode** drop-down menu. Mode choices are **Classified**, **Default**, and **Mapped** and indicate from where the PCP and DEI values for the egress frames are selected (ingress classification values, default values, or mapped values, respectively). The **Tag Remarking Mode** is set to **Classified** by default.

   Specifying **Default** from the **Tag Remarking Mode** menu allows you to specify the default PCP and DEI values for the port. In the example below, **Port 1** is configured with a PCP default value of **5**, and a DEI default value of **0**.



QoS Egress Port Tag Remarking Port 1

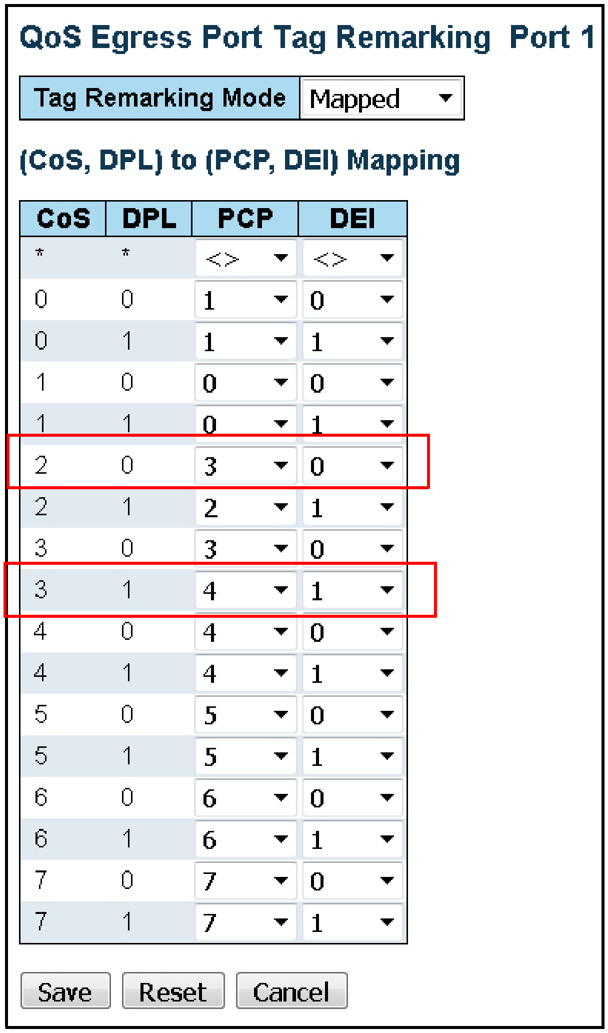
Tag Remarking Mode: Default

PCP/DEI Configuration

Default PCP: 5

Default DEI: 0

Specifying **Mapped** from the **Tag Remarking Mode** menu allows you to configure the CoS/DPL to PCP/DEI mapping for the port. In the example below, **Port 1** is configured with **CoS 2/DPL 0** mapped to **PCP 3/DEI 0**, and **CoS 3/DPL 1** mapped to **PCP 4/DEI 1**.All other CoS/DPL mappings are the default values.



QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode: Mapped

(CoS, DPL) to (PCP, DEI) Mapping

CoS	DPL	PCP	DEI
*	*	<>	<>
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	3	0
2	1	2	1
3	0	3	0
3	1	4	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0
7	1	7	1

4. After specifying the **Tag Remarking Mode** on the port, and configuring any PCP or DEI values, select **Save** at the bottom of the menu to save these settings on the port.

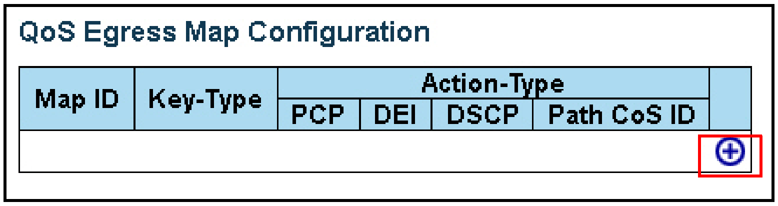
After configuring and applying any tag remarking for the QoS egress traffic, you can begin to configure the QoS egress map.

Configuring the QoS Egress Map via the GUI

The last step in configuring QoS egress parameters is to configure the QoS egress map. Egress maps function in the same way as ingress map, but they are applied to egress traffic on the port. Egress maps are used to control the rewriting of packets at egress, where PCP, DEI, and DSCP values can be updated based on their classified key values. Egress maps are configured by specifying which part of the packet is used for matching (CoS ID, CoS ID-DPL, DSCP, or DSCP-DPL), specifying the actions taken once the packet information is processed, and specifying which values are mapped to the packet information.

To begin configuring a QoS egress map, complete these steps:

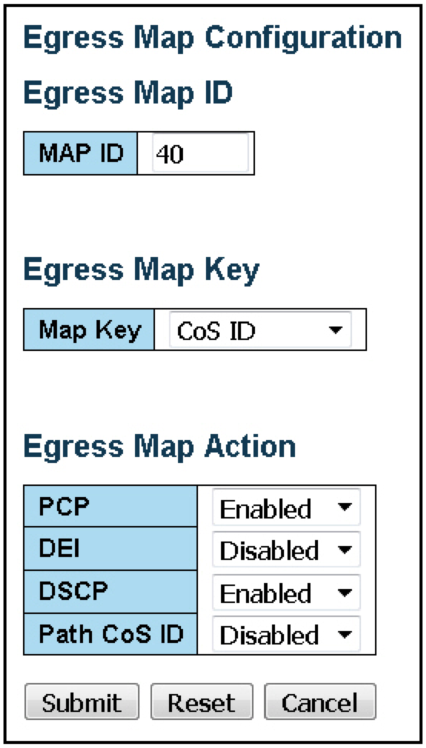
1. Navigate to the **Configuration** tab, and then select **QoS** > **Egress Map**. The **QoS Egress Map Configuration** menu is displayed, where all configured egress maps are listed.



QoS Egress Map Configuration

Map ID	Key-Type	Action-Type				
		PCP	DEI	DSCP	Path CoS ID	
						⊕

2. To configure a new QoS egress map, select the **plus** sign at the bottom right of the **QoS Egress Map Configuration** menu. This action will open the **Egress Map Configuration** menu.



Egress Map Configuration

Egress Map ID

MAP ID	40

Egress Map Key

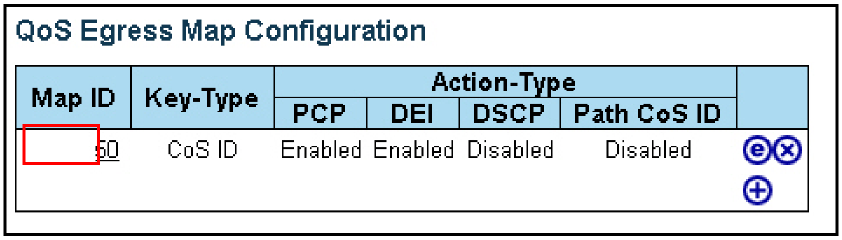
Map Key	CoS ID

Egress Map Action

PCP	Enabled
DEI	Disabled
DSCP	Enabled
Path CoS ID	Disabled

3. Specify the ID number for the ingress map in the **MAP ID** field.
4. Next, specify the **Map Key** from the drop-down menu. The map key is the part of the packet header used for matching purposes. The key type choices are **CoS ID** (default), **CoS ID-DPL**, **DSCP**, or **DSCP-DPL**. Selecting **CoS ID** indicates the map applies mapping actions to egress traffic based on the CoS ID, **CoS ID-DPL** indicates mapping actions take place based on both CoS ID and DPL information from the packet, **DSCP** indicates mapping actions take place based on the DSCP value in the packet, and **DSCP-DPL** indicates both DSCP and DPL values are used to determine mapping actions.
5. Lastly, enable rewriting actions for traffic that matches the defined key. Each parameter, **PCP**, **DEI**, **DSCP**, and **Path CoS ID**, specifies the type of rewriting you are enabling for matched traffic and can be enabled or disabled independently. When enabled, these values can be rewritten and replaced with new values specified in the egress map's mapping rules configuration.
6. Select **Submit** to create the egress map. Once created, the map will be displayed in the **QoS Egress Map Configuration** menu.

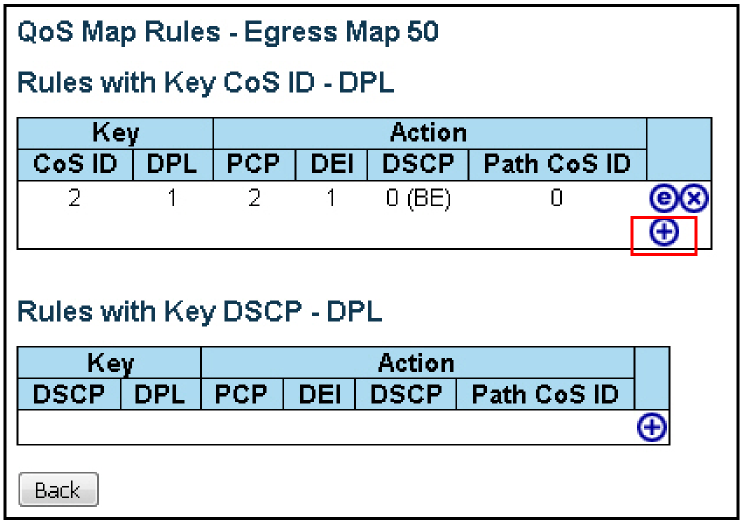
7. Configure the mapping rules for each map by selecting the **Map ID** from the list in the **QoS Egress Map Configuration** menu. These rules are used to define the new values that will be assigned to traffic that matches the egress map's criteria.



QoS Egress Map Configuration

Map ID	Key-Type	Action-Type				
		PCP	DEI	DSCP	Path CoS ID	
50	CoS ID	Enabled	Enabled	Disabled	Disabled	

8. In the **QoS Map Rules - Egress Map** configuration menu, select the **plus** sign at the bottom of the **Rules with Key** menus to configure new rules for the keys you selected for the map (refer to Step 4 above).



QoS Map Rules - Egress Map 50

Rules with Key CoS ID - DPL

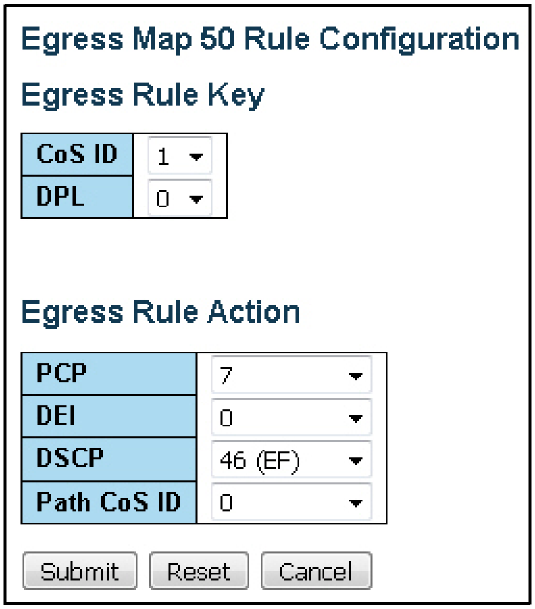
Key		Action				
CoS ID	DPL	PCP	DEI	DSCP	Path CoS ID	
2	1	2	1	0 (BE)	0	

Rules with Key DSCP - DPL

Key		Action				
DSCP	DPL	PCP	DEI	DSCP	Path CoS ID	

9. Once the **Egress Map Rule Configuration** menu is displayed, you can specify the **Egress Rule Key** for the keys you selected for the map (refer to Step 4 above) from the appropriate drop-down menu. Here you are defining the new values to be mapped to the values defined in the map's keys and for which you enabled rewrite actions. In addition, specify the **Egress Rule Action** by selecting the appropriate value from the action drop-down menus. Here you are specifying the new values for traffic that matches the egress map. For example, you can specify the egress rule action for CoS ID **1** includes specifying a PCP

value of **7** and a DSCP value of **46 (EF)**. Once you have configured the rule keys and actions, select **Submit**.



Egress Map 50 Rule Configuration

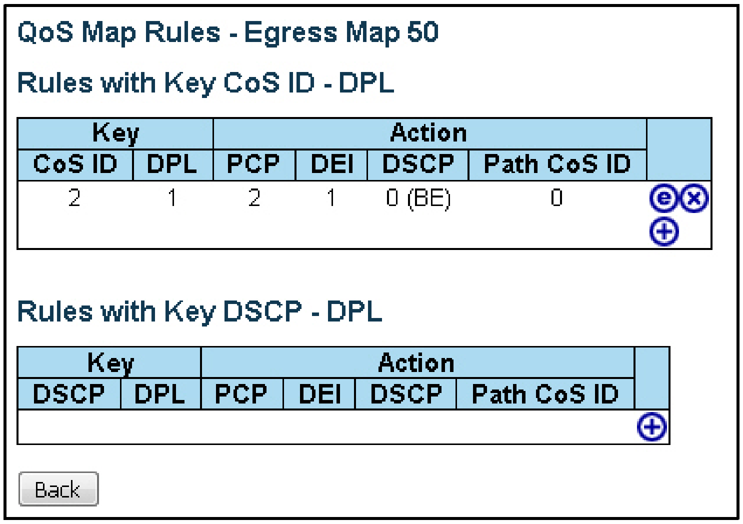
Egress Rule Key

CoS ID	1
DPL	0

Egress Rule Action

PCP	7
DEI	0
DSCP	46 (EF)
Path CoS ID	0

10. Once you select **Submit**, the configured map rules are shown in the **QoS Map Rules** configuration menu for the specific map. You can add as many rules as necessary to define the proper traffic matching and mapping properties for the QoS egress map.



QoS Map Rules - Egress Map 50

Rules with Key CoS ID - DPL

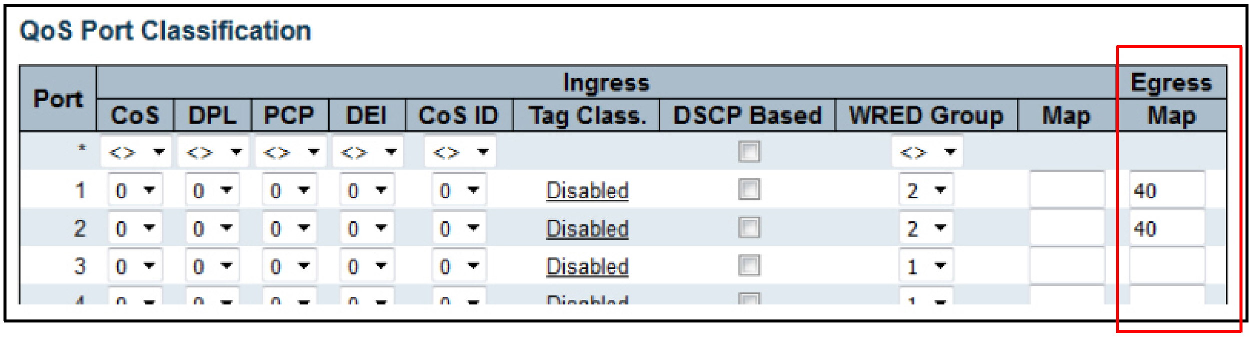
Key		Action				
CoS ID	DPL	PCP	DEI	DSCP	Path CoS ID	
2	1	2	1	0 (BE)	0	

Rules with Key DSCP - DPL

Key		Action				
DSCP	DPL	PCP	DEI	DSCP	Path CoS ID	

11. Once the map and its rules have been configured, the map must be applied for it to take effect. You can apply the egress map to a specific port, using the **QoS Port Classification** menu (refer to *Configuring*

Ingress Port Traffic Classification Via the GUI on page 11), or you can apply the map to a QoS Control List, as described in *Configuring the QoS Control List via the GUI (Optional) on page 38*.



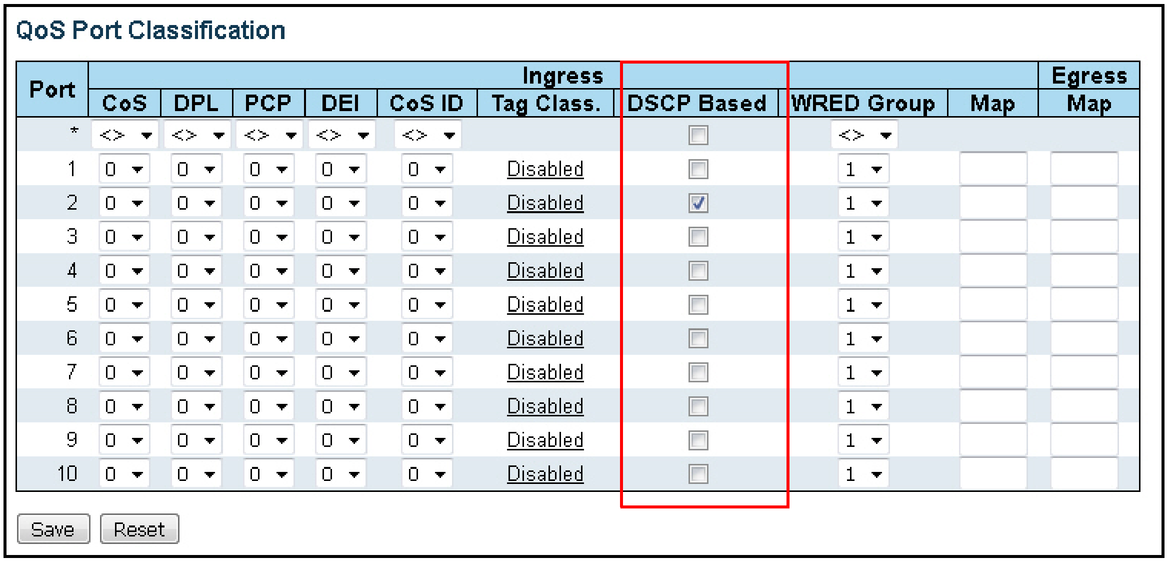
QoS Port Classification

Port	Ingress									Egress
	CoS	DPL	PCP	DEI	CoS ID	Tag Class.	DSCP Based	WRED Group	Map	Map
*	<>	<>	<>	<>	<>		□	<>		
1	0	0	0	0	0	Disabled	□	2		40
2	0	0	0	0	0	Disabled	□	2		40
3	0	0	0	0	0	Disabled	□	1		
4	0	0	0	0	0	Disabled	□	1		

With the finished configuration of the QoS egress map, and its application to the appropriate ports, the basic QoS configurations are complete. You can now choose to optionally configure DSCP translation and classification, QoS control list entries, or storm policing features.

8. Configuring QoS DSCP via the GUI (Optional)

QoS on the ASE device can include DSCP configuration for packet classification, translation, rewriting, or remapping purposes. These features can be applied on a per-port basis for both ingress traffic classification and translation and egress traffic rewriting and remapping. The following sections outline how to configure DSCP on the ASE device for QoS purposes.



QoS Port Classification

Port	Ingress									Egress
	CoS	DPL	PCP	DEI	CoS ID	Tag Class.	DSCP Based	WRED Group	Map	Map
*	<>	<>	<>	<>	<>		□	<>		
1	0	0	0	0	0	Disabled	□	1		
2	0	0	0	0	0	Disabled	☑	1		
3	0	0	0	0	0	Disabled	□	1		
4	0	0	0	0	0	Disabled	□	1		
5	0	0	0	0	0	Disabled	□	1		
6	0	0	0	0	0	Disabled	□	1		
7	0	0	0	0	0	Disabled	□	1		
8	0	0	0	0	0	Disabled	□	1		
9	0	0	0	0	0	Disabled	□	1		
10	0	0	0	0	0	Disabled	□	1		

NOTE

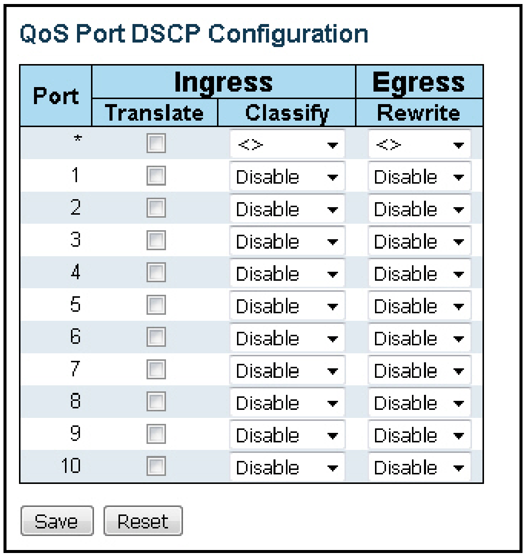
For all DSCP configurations used in QoS, you must first enable DSCP-based QoS on the port. Navigate to the ***Configuration*** *tab, and select* ***QoS*** *>* ***Port Classification****, and select the* ***DSCP Based*** *check box for the appropriate port(s). Then select the* ***Save*** *button at the bottom of the menu before moving forward with DSCP configuration.*

Configuring Port DSCP Values via the GUI

DSCP can be configured on a per-port basis to apply to both ingress and egress traffic. Ingress traffic can use DSCP configurations for translation and classification purposes, and egress traffic can use DSCP configurations for rewriting and remapping purposes.

To begin configuring DSCP values for both ingress and egress traffic on the port, complete these steps:

1. Navigate to the **Configuration** tab, and select **QoS** > **Port DSCP**. The **QoS Port DSCP Configuration** menu appears.



QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	□	<>	<>
1	□	Disable	Disable
2	□	Disable	Disable
3	□	Disable	Disable
4	□	Disable	Disable
5	□	Disable	Disable
6	□	Disable	Disable
7	□	Disable	Disable
8	□	Disable	Disable
9	□	Disable	Disable
10	□	Disable	Disable

2. You can enable DSCP translation for ingress traffic on the port by selecting the **Translate** check box next to the appropriate port. When enabled, DSCP translation is completed for ingress traffic based on the settings in the DSCP translation table. When enabled, you must also configure the DSCP translation table settings (refer to *Configuring DSCP Translation via the GUI on page 35*), and enable DSCP-based QoS on the port.

3. Next, you can configure the DSCP classification for ingress traffic on the port by selecting an option from the **Classify** drop-down menu next to the appropriate port. This type of traffic classification is used for DSCP rewriting upon traffic egress. By default, DSCP classification is disabled (**Disable**), indicating that no DSCP classification is completed for ingress traffic. Other options include:

   - **DSCP=0**: indicating that incoming DSCP traffic is classified with a DSCP value of **0**.
   - **Selected**; indicating that only traffic with specific, trusted DSCP values are classified. The DSCP values used for traffic classification are specified in the DSCP classification table, as described in *Configuring DSCP Classification via the GUI on page 36*.
   - **All**: indicating that all DSCP traffic is classified.

4. Lastly, you can configure the DSCP rewrite process for outgoing classified DSCP traffic by selecting an option from the **Rewrite** drop-down menu for the appropriate port. By default, DSCP rewrite functionality is disabled (**Disable**), indicating that no rewriting occurs on traffic egress. Other options include:

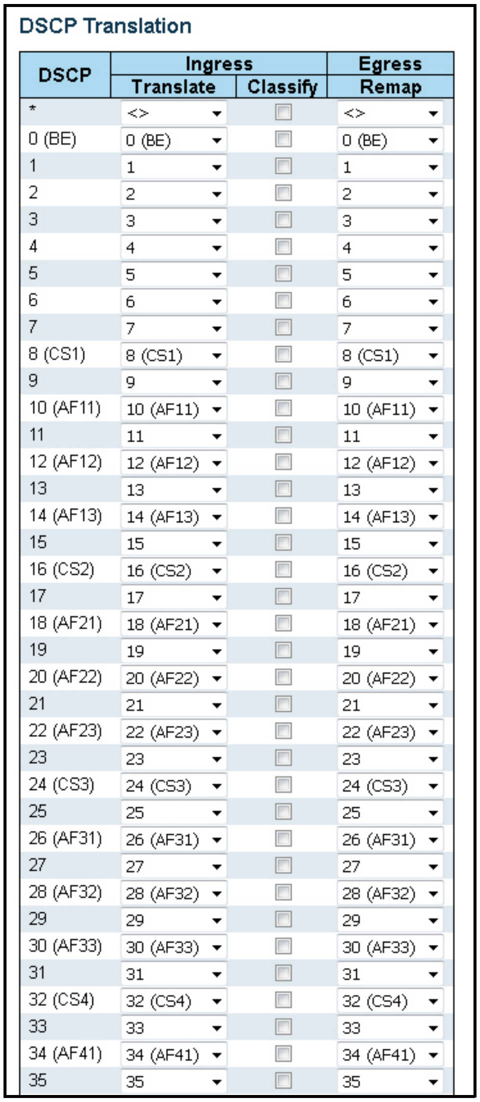
   - **Enable**: indicating rewriting of the DSCP traffic occurs, but without traffic remapping.
   - **Remap**: indicating that egress traffic is remapped upon egress, using the values specified in the DSCP translation table (refer to *Configuring DSCP Translation via the GUI on page 35*).

5. Once the DSCP translation, classification, and rewrite settings have been configured for the port, select **Save** at the bottom of the menu to save these settings.

Configuring DSCP Translation via the GUI

DSCP translation configuration is used to populate the DSCP translation table, which in turn is used by DSCP classification and rewriting processes on the port. Both ingress and egress traffic DSCP translation tables are configured from a single menu. To configure DSCP translation parameters, complete these steps:

1. Navigate to the **Configuration** tab, and select **QoS** > **DSCP Translation**. The **DSCP Translation** menu appears, displaying all DSCP values (from **0** to **63**, and * for all), and allows you to specify DSCP translation and classification settings for ingress traffic, as well as DSCP remapping settings for egress traffic.



DSCP Translation

DSCP	Ingress		Egress
	Translate	Classify	Remap
*	<>	☐	<>
0 (BE)	0 (BE)	☐	0 (BE)
1	1	☐	1
2	2	☐	2
3	3	☐	3
4	4	☐	4
5	5	☐	5
6	6	☐	6
7	7	☐	7
8 (CS1)	8 (CS1)	☐	8 (CS1)
9	9	☐	9
10 (AF11)	10 (AF11)	☐	10 (AF11)
11	11	☐	11
12 (AF12)	12 (AF12)	☐	12 (AF12)
13	13	☐	13
14 (AF13)	14 (AF13)	☐	14 (AF13)
15	15	☐	15
16 (CS2)	16 (CS2)	☐	16 (CS2)
17	17	☐	17
18 (AF21)	18 (AF21)	☐	18 (AF21)
19	19	☐	19
20 (AF22)	20 (AF22)	☐	20 (AF22)
21	21	☐	21
22 (AF23)	22 (AF23)	☐	22 (AF23)
23	23	☐	23
24 (CS3)	24 (CS3)	☐	24 (CS3)
25	25	☐	25
26 (AF31)	26 (AF31)	☐	26 (AF31)
27	27	☐	27
28 (AF32)	28 (AF32)	☐	28 (AF32)
29	29	☐	29
30 (AF33)	30 (AF33)	☐	30 (AF33)
31	31	☐	31
32 (CS4)	32 (CS4)	☐	32 (CS4)
33	33	☐	33
34 (AF41)	34 (AF41)	☐	34 (AF41)
35	35	☐	35

2. To configure the DSCP translation mapping for ingress traffic, select the appropriate new DSCP value next to the DSCP value you are mapping from the **Translate** drop-down menu. DSCP values can be

mapped to any DSCP values in the **0** to **63** value range. In addition, you can select the **Classify** check box to enable DSCP classification in addition to translation for ingress traffic.

> **NOTE**
>
> *DSCP translation and classification, when used, should be enabled on the appropriate port before being configured. To enable these DSCP features on the port for ingress traffic, follow the instructions detailed in Configuring Port DSCP Values via the GUI on page 34.*

3. To configure DSCP remapping for egress traffic, select the appropriate new DSCP value next to the DSCP value you are remapping from the **Remap** drop-down menu. DSCP values can remapped to any of DSCP values in the **0** to **63** value range.

> **NOTE**
>
> *DSCP remapping, when used, should be enabled on the appropriate port before being configured. To enable this DSCP feature on the port for egress traffic, follow the instructions detailed in Configuring Port DSCP Values via the GUI on page 34.*

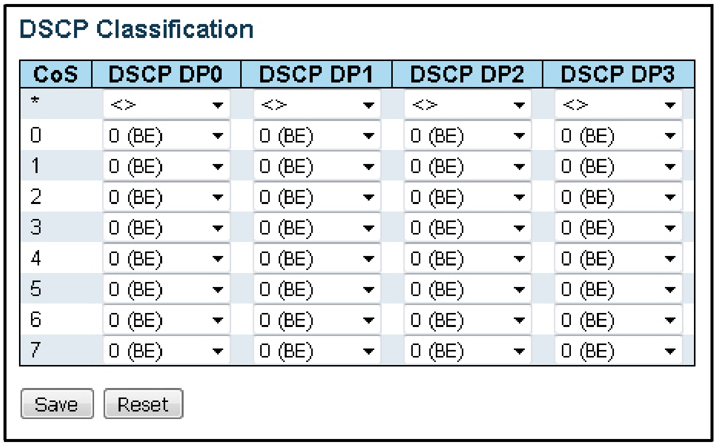
4. Once the DSCP translation settings have been configured for ingress and egress traffic, select **Save** at the bottom of the menu to save these settings in the DSCP translation table.

Configuring DSCP Classification via the GUI

DSCP classification occurs for ingress traffic on the port and is used for DSCP rewriting on egress traffic. By default, DSCP classification is disabled, indicating that no DSCP classification is completed for ingress traffic. When DSCP classification is enabled, and set to **Selected** (as described in *Configuring Port DSCP Values via the GUI on page 34*), specific, trusted DSCP values are classified according to the values configured in the DSCP classification table.

To configure the DSCP values in the classification table for ingress traffic, complete these steps:

1. Navigate to the **Configuration** tab, and select **QoS** > **DSCP Classification**. The **DSCP Classification** menu appears.



DSCP Classification

CoS	DSCP DP0	DSCP DP1	DSCP DP2	DSCP DP3
*	<>	<>	<>	<>
0	0 (BE)	0 (BE)	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)	0 (BE)	0 (BE)
3	0 (BE)	0 (BE)	0 (BE)	0 (BE)
4	0 (BE)	0 (BE)	0 (BE)	0 (BE)
5	0 (BE)	0 (BE)	0 (BE)	0 (BE)
6	0 (BE)	0 (BE)	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)	0 (BE)	0 (BE)

2. Select the appropriate DSCP values from the appropriate **DSCP DP** drop-down menu, for the desired CoS ID. Valid **DSCP DP** range is **0** to **63**.

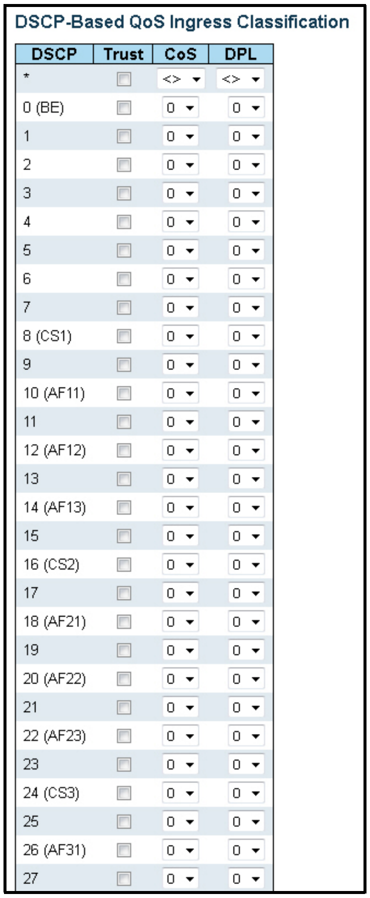
3. Once the DSCP classification values have been specified for the appropriate CoS ID, select **Save** at the bottom of the menu.

Configuring DSCP-Based QoS via the GUI

QoS can be configured to use trusted DSCP values as part of the QoS and DPL classification for ingress traffic. Configuring this option allows you to specify the trusted DSCP value, and assign that value a QoS class and DPL value so that as traffic comes into the switch it is automatically classified by QoS and DPL value, based on its DSCP value. Configuring this feature can be easier than configuring DSCP translation and classification at ingress, if those configurations are not necessary.

To configure DSCP-based QoS classification for ingress traffic, complete these steps:

1. Ensure that DSCP-based QoS port classification is enabled, as described in *Configuring QoS DSCP via the GUI (Optional) on page 33*.
2. Next, navigate to the **Configuration** tab and select **QoS** > **DSCP-Based QoS**. The **DSCP-Based QoS Ingress Classification** menu appears.



DSCP-Based QoS Ingress Classification

DSCP	Trust	CoS	DPL
*	□	<>	<>
0 (BE)	□	0	0
1	□	0	0
2	□	0	0
3	□	0	0
4	□	0	0
5	□	0	0
6	□	0	0
7	□	0	0
8 (CS1)	□	0	0
9	□	0	0
10 (AF11)	□	0	0
11	□	0	0
12 (AF12)	□	0	0
13	□	0	0
14 (AF13)	□	0	0
15	□	0	0
16 (CS2)	□	0	0
17	□	0	0
18 (AF21)	□	0	0
19	□	0	0
20 (AF22)	□	0	0
21	□	0	0
22 (AF23)	□	0	0
23	□	0	0
24 (CS3)	□	0	0
25	□	0	0
26 (AF31)	□	0	0
27	□	0	0

3. Specify the DSCP value is trusted by selecting the **Trust** check box next to the appropriate DSCP value. DSCP values range from **0** to **63**.
4. Next, specify the CoS ID to be associated with the trusted DSCP value by selecting the appropriate CoS ID from the **CoS** drop-down menu. Valid range is **0** to **7**.
5. Lastly, specify the DPL value to be associated with the trusted DSCP value by selecting the appropriate DPL value (**0** to **3**) from the **DPL** drop-down menu.

6. When the trusted DSCP values have been configured with a CoS and DPL value, select **Save** at the bottom of the menu to save these setting.

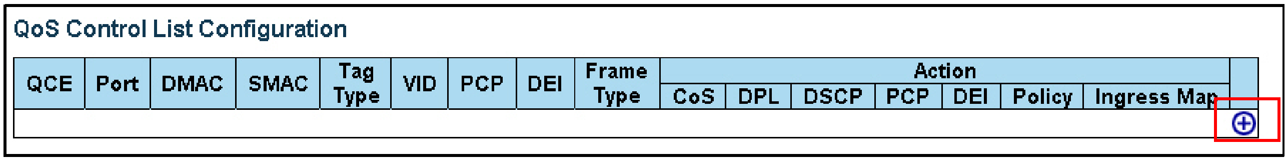
DSCP configurations for QoS are complete once you have configured the ingress and egress translation, classification, and rewriting/remapping behaviors. You can now optionally configure QoS control lists or storm policers.

9. Configuring the QoS Control List via the GUI (Optional)

QoS control lists (QCLs) can be used to configure flexible classification for Layer 2 through Layer 4 traffic, and can perform reclassification of traffic based on CoS, DPL, PCP, DEI, DSCP, and access control list (ACL) values. The QCL is comprised of various QoS control entries (QCEs), which are applied on a per-port basis, and can specify source and destination media access control (MAC) addresses, traffic types, VLAN IDs, PCP values, and frame types that receive certain classifications if the incoming traffic matches the QCE criteria. Up to **1024** QCEs can be created for the ASE device, and each are applied to incoming traffic from the QCE configuration menu.

To configure the QCL, and various QCEs, complete these steps:

1. Navigate to the **Configuration** tab, and select **QoS** > **QoS Control List**. The **QoS Control List Configuration** menu appears, and will display any configured QCEs.

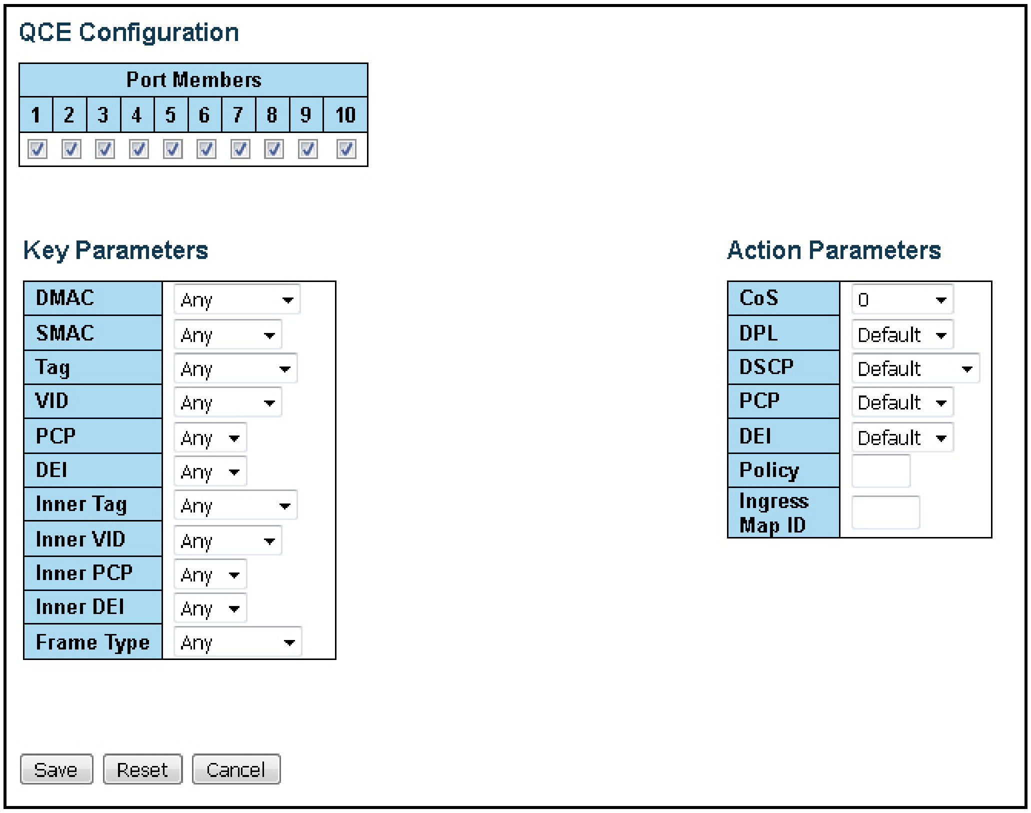


QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action							
									CoS	DPL	DSCP	PCP	DEI	Policy	Ingress Map	
																⊕

2. To create a new QCE, select the **plus** icon at the bottom right of the **QoS Control List Configuration** menu, and the **QCE Configuration** menu appears. In this menu, you can specify the QCE ID, the ports to

which it is applied, the ingress traffic parameters used for matching, and the reclassification actions taken on matching traffic.



QCE Configuration

Port Members									
1	2	3	4	5	6	7	8	9	10
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Key Parameters

DMAC	Any
SMAC	Any
Tag	Any
VID	Any
PCP	Any
DEI	Any
Inner Tag	Any
Inner VID	Any
Inner PCP	Any
Inner DEI	Any
Frame Type	Any

Action Parameters

CoS	0
DPL	Default
DSCP	Default
PCP	Default
DEI	Default
Policy	
Ingress Map ID	

3. First, specify the port(s) to which the QCE applies by selecting the appropriate port check box in the **Port Members** menu.

4. Next, specify the parameters on which you want to match traffic, using the drop-down menus in the **Key Parameters** menu. Available parameters on which to match traffic include the following:

- **DMAC**: Specifies the destination MAC address for the incoming traffic used as matching criteria. Drop-down menu options include **Any** (matches on all MAC addresses), **Unicast** (matches on unicast MAC addresses), **Multicast** (matches on multicast MAC addresses), **Broadcast** (matches on broadcast MAC addresses), or **Specific** (matches on a specific MAC address). By default, the QCE matches on **Any** MAC address. If the **Specific** option is chosen, you will prompted to enter the MAC address to be used for matching.

- **SMAC**: Specifies the source MAC address of the incoming traffic used as matching criteria. Drop-down menu options include **Any** (matches on all MAC addresses) or **Specific** (matches on a specific MAC address). By default, the QCE matches on **Any** MAC address. If the **Specific** option is chosen, you will prompted to enter the MAC address to be used for matching.

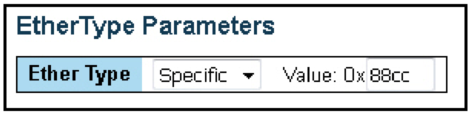
- **Tag**: Specifies the tag type associated with the incoming traffic used as matching criteria. Drop-down menu items include **Any** (matches on all traffic, whether tagged or untagged), **Untagged** (matches on all untagged traffic), **C-Tagged** (matches on C-tagged traffic), **S-Tagged** (matches on all S-tagged traffic), or **Tagged** (matches on all tagged traffic). By default, the QCE matches on **Any** type of traffic.

- **VID**: Specifies the VLAN ID of the incoming traffic used as matching criteria. Drop-down menu options include **Any** (matches on any VLAN ID), **Specific** (matches on a specific VLAN ID), or **Range** (matches on a range of VLAN IDs). By default, the QCE matches on **Any** VLAN ID. If **Specific** or **Range** are selected, you will be prompted to enter the single VLAN ID, or the range of VLAN IDs. Valid VLAN ID range is **1** to **4095**.

- **PCP**: Specifies the PCP value of the incoming traffic used as matching criteria. Drop-down menu options include **Any** (matches on any PCP value), a specific PCP value between **0** to **7** (matches on that single PCP value), or a range that includes **0-1**, **2-3**, **4-5**, **6-7**, **0-3**, and **4-7** (matches on the specified PCP value range). By default, the QCE matches on **Any** PCP value.
- **DEI**: Specifies the DEI value of the incoming traffic used as matching criteria. Drop-down menu options include: **Any** (matches on any DEI value), **0** (matches on a DEI value of zero), or **1** (matches on a DEI value of one). By default, the QCE matches on **Any** DEI value.
- **Inner Tag**: Specifies the inner tag of the incoming traffic used as matching criteria. Drop-down menu options include: **Any** (matches on all traffic, whether tagged or untagged), **Untagged** (matches on all untagged traffic), **C-Tagged** (matches on C-tagged traffic), **S-Tagged** (matches on all S-tagged traffic), or **Tagged** (matches on all tagged traffic). By default, the QCE matches on **Any** type of inner tag in the traffic.
- **Inner VID**: Specifies the inner VLAN ID value of the incoming traffic used as matching criteria. Drop-down menu options include **Any** (matches on any VLAN ID), **Specific** (matches on a specific VLAN ID), or **Range** (matches on a range of VLAN IDs). By default, the QCE matches on **Any** VLAN ID. If **Specific** or **Range** are selected, you will be prompted to enter the single VLAN ID, or the range of VLAN IDs. Valid VLAN ID range is **1** to **4095**.
- **Inner PCP**: Specifies the inner PCP value of the incoming traffic used as matching criteria. Drop-down menu options include **Any** (matches on any PCP value), a specific PCP value between **0** to **7** (matches on that single PCP value), or a range that includes **0-1**, **2-3**, **4-5**, **6-7**, **0-3**, and **4-7** (matches on the specified PCP value range). By default, the QCE matches on **Any** PCP value.
- **Inner DEI**: Specifies the inner DEI value of the incoming traffic used as matching criteria. Drop-down menu options include: **Any** (matches on any DEI value), **0** (matches on a DEI value of zero), or **1** (matches on a DEI value of one). By default, the QCE matches on **Any** DEI value.
- **Frame Type**: Specifies the frame type of the incoming traffic used as matching criteria. Drop-down menu options include: **Any** (matches on any frame type), **EtherType** (matches on Ethernet frames), **LLC** (matches on Logical Link Control (LLC) frames), **SNAP** (matches on Subnetwork Access Protocol (SNAP) frames), **IPv4** (matches on IPv4 frames), or **IPv6** (matches on IPv6 frames). By default, the QCE matches on **Any** frame type.

If you select **EtherType**, **LLC**, **SNAP**, **IPv4**, or **IPv6**, you will be prompted for the following additional information:

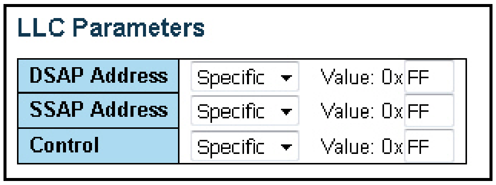
- **EtherType**: Select **Any** or **Specific** from the **EtherType Parameters** drop-down menu. If you select **Specific**, you will be prompted to enter the two-octet value for the Ethernet frame type.



EtherType Parameters

Ether Type	Specific	Value: 0x 88cc

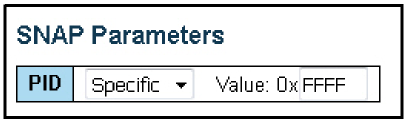
- **LLC**: Select **Any** or **Specific** from the **DSAP Address**, **SSAP Address**, and **Control** drop-down menus in the **LLC Parameters** menu. If you select **Specific**, you will be prompted to enter the destination service access point (DSAP), source service access point (SSAP), or control addresses.



LLC Parameters

DSAP Address	Specific	Value: 0x FF
SSAP Address	Specific	Value: 0x FF
Control	Specific	Value: 0x FF

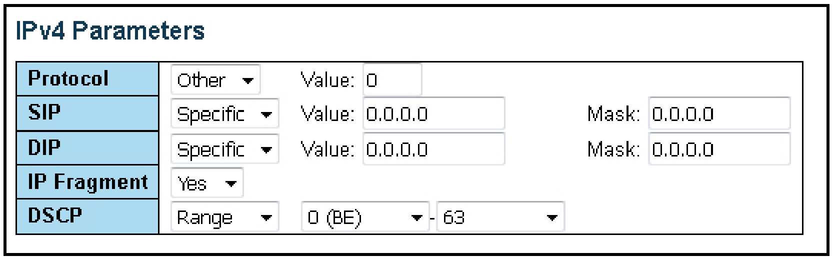
- **SNAP**: Select **Any** or **Specific** from the Protocol ID (**PID**) drop-down menu in the **SNAP Parameters** menu. If you select **Specific**, you will be prompted to enter the PID.



SNAP Parameters

PID	Specific	Value: 0x FFFF

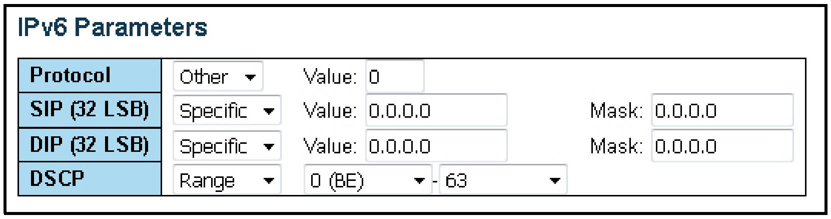
- **IPv4**: Select the proper values from the **Protocol**, source IP address (**SIP)**, destination IP address (**DIP**), **IP Fragment**, and **DSCP** drop-down menus in the **IPv4 Parameters** menu. Protocol choices are **Any**, User Datagram Protocol (**UDP**), Transmission Control Protocol (**TCP**), and **Other**. For **UDP** and **TCP**, you will additionally need to specify the source and destination port information; for **Other** you will also need to specify the protocol number. **SIP** and **DIP** menu choices are **Any** or **Specific**; if you select **Specific**, you will also need to inter an IPv4 address and subnet mask. **IP Fragment** menu choices are **Any**, **Yes**, or **No**. The **DSCP** menu includes the **Any**, **Specific**, or **Range** options.



IPv4 Parameters

Protocol	Other	Value: 0	
SIP	Specific	Value: 0.0.0.0	Mask: 0.0.0.0
DIP	Specific	Value: 0.0.0.0	Mask: 0.0.0.0
IP Fragment	Yes		
DSCP	Range	0 (BE) - 63	

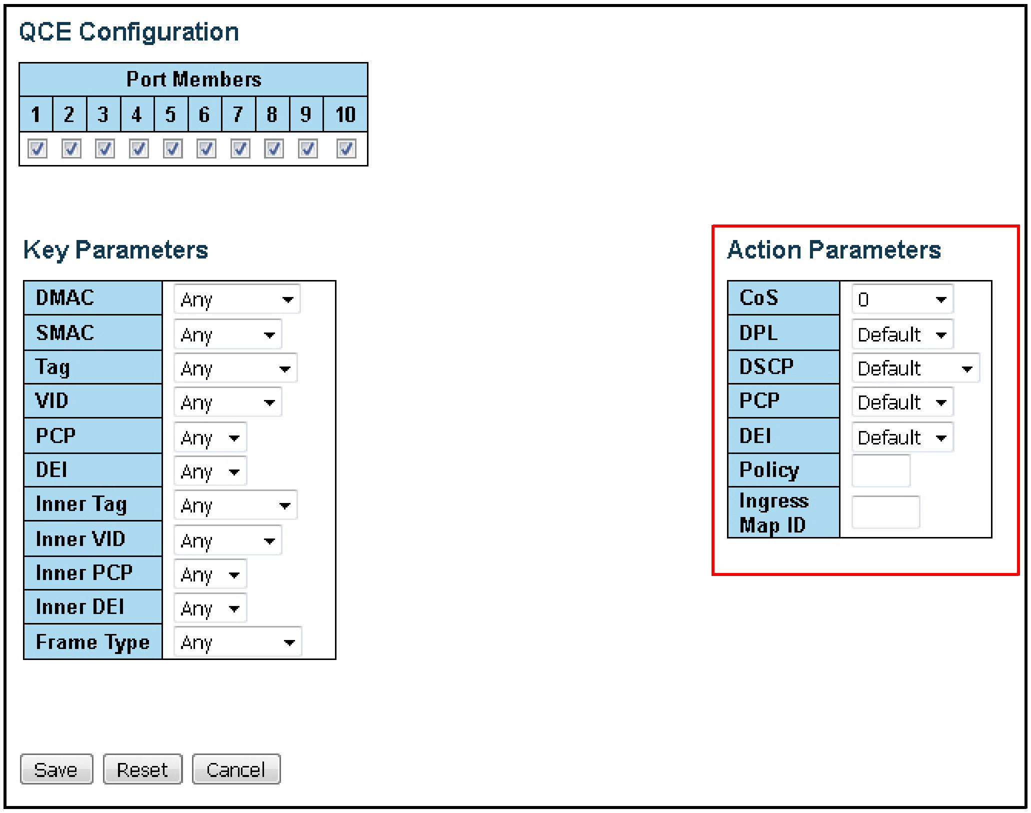
- **IPv6**: Select the proper values from the **Protocol**, **SIP (32 LSB)**, **DIP (32 LSB)**, and **DSCP** drop-down menus in the **IPv6 Parameters** menu. Protocol choices are **Any**, **UDP**, **TCP**, and **Other**. For **UDP** and **TCP**, you will additionally need to specify the source and destination port information; for **Other** you will also need to specify the protocol number. **SIP (32 LSB)** and **DIP (32 LSB)** menu choices are **Any** or **Specific**; if you select **Specific**, you will also need to inter an IPv6 address and subnet mask. The **DSCP** menu includes the **Any**, **Specific**, or **Range** options.



IPv6 Parameters

Protocol	Other	Value: 0	
SIP (32 LSB)	Specific	Value: 0.0.0.0	Mask: 0.0.0.0
DIP (32 LSB)	Specific	Value: 0.0.0.0	Mask: 0.0.0.0
DSCP	Range	0 (BE) - 63	

5. After you have specified the ports on which the QCE is active, and configured the QCE's traffic matching criteria, you can specify the actions to be taken on traffic that matches the criteria using the **Action Parameters** menu of the **QCE Configuration** menu.



QCE Configuration

Port Members									
1	2	3	4	5	6	7	8	9	10
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Key Parameters

DMAC	Any
SMAC	Any
Tag	Any
VID	Any
PCP	Any
DEI	Any
Inner Tag	Any
Inner VID	Any
Inner PCP	Any
Inner DEI	Any
Frame Type	Any

Action Parameters

CoS	0
DPL	Default
DSCP	Default
PCP	Default
DEI	Default
Policy	
Ingress Map ID	

6. Specify the CoS classification for ingress traffic that matches the QCE criteria using the **CoS** drop-down menu in the **Action Parameters** menu. Valid range is **0** to **7**, or you can select **Default**.

7. Specify the DPL classification for ingress traffic that matches the QCE criteria using the **DPL** drop-down menu in the **Action Parameters** menu. Valid range is **0** to **3**, or you can select **Default**.

8. Specify the DSCP classification for ingress traffic that matches the QCE criteria using the **DSCP** drop-down menu in the **Action Parameters** menu. Valid range is **0** to **63**, or you can select **Default**.

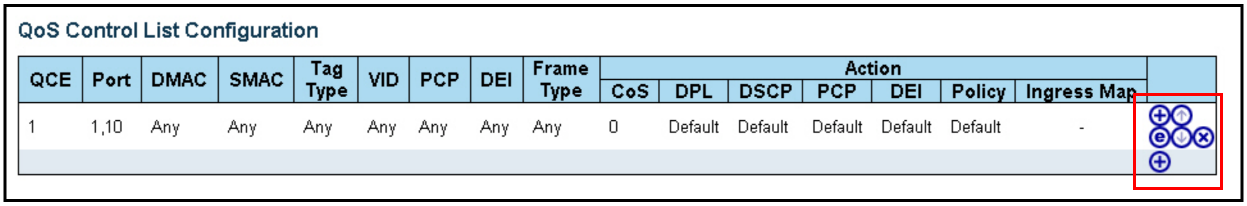
9. Specify the PCP classification for ingress traffic that matches the QCE criteria using the **PCP** drop-down menu in the **Action Parameters** menu. Valid range is **0** to **7**, or you can select **Default**.

10. Specify the DEI classification for ingress traffic that matches the QCE criteria using the **DEI** drop-down menu in the **Action Parameters** menu. Valid selection is **0**, **1**, or **Default**.

11. Associate a previously configured ACL with ingress traffic that matches the QCE by entering an ACL ID in the **Policy** field of the **Action Parameters** menu. By default, an ACL is not associated with the QCE.

12. Associate a previously configured QoS ingress map with traffic that matches the QCE by entering a map ID in the **Ingress Map ID** field of the **Action Parameters** menu. By default, no QoS ingress map is associated with the QCE.

13. Once the QCE parameters have been configured, select **Save** at the bottom of the menu to create the QCE. Newly created QCEs appear listed in the **QoS Control List Configuration** menu. You can reorder, edit, delete, or create QCE entries using the buttons at the right of the menu.



QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action							
									CoS	DPL	DSCP	PCP	DEI	Policy	Ingress Map	
1	1,10	Any	Any	Any	Any	Any	Any	Any	0	Default	Default	Default	Default	Default	-	

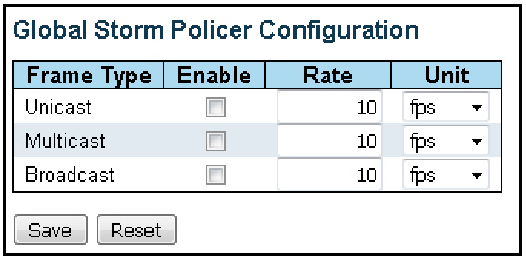
Once the necessary QCE entries have been created, the QoS control list configuration is complete.

10. Configuring Global Storm Policers via the GUI (Optional)

You can optionally choose to configure global-level storm policers on the ASE device to aid in QoS functionality. Global storm policers apply to the entire switch, and can be used to restrict the amount of flooded frames, those without previously-learned source MAC addresses, from entering the device. Global policers can be configured to limit unicast, multicast, or broadcast packets.

To configure global storm policers on the ASE device, complete these steps:

1. Navigate to the **Configuration** tab and select **QoS** > **Storm Policing**. You can configure the storm policers using the **Global Storm Policer Configuration** menu.



Global Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unicast	□	10	fps
Multicast	□	10	fps
Broadcast	□	10	fps

2. Enable the type of storm policer you want to configure by selecting the **Enable** check box next to the appropriate frame type (**Unicast**, **Multicast**, or **Broadcast**).
3. Next, specify the rate at which flooded frames of the specified type are limited by entering a value in the **Rate** field and specifying a unit from the drop-down menu. Unit measurement selections are **kbps**, **Mbps**, **fps**, and **kfps**. By default, the **Rate** is set at **10** and the unit is set to **fps** (frames per second).
4. Once you have configured the appropriate policers, select **Save** at the bottom of the menu to save and apply the policers on the device.

After configuring the optional QoS parameters, all QoS configuration using the GUI has been completed. For information regarding viewing QoS statistics and configurations on the ASE device, or for additional QoS information, refer to *Troubleshooting on page 76* and *Additional QoS Information on page 80*.

11. Configuring Ingress QoS Parameters Using the CLI

The first steps in configuring the QoS feature on the ASE device is to specify how traffic is handled on the incoming port. To configure the ingress QoS parameters, configure the traffic classification on the ingress port, the port policer, and an ingress traffic map. To configure these settings, connect to the ASE CLI and complete the following tasks:

- *Configuring QoS on a Per-Port Basis Via the CLI on page 44*
- *Configuring the Ingress Port Policer via the CLI on page 47*
- *Configuring the QoS Ingress Map Via the GUI on page 16*

These actions serve to classify and police the incoming traffic on the ASE device.

NOTE

It is recommended to restore defaults on the ASE device before beginning any configuration. To restore the defaults on the device, connect to the CLI, and enter the **reload defaults** *command from the Enable mode prompt. Be aware this will erase the IP address of the switch itself.*

Configuring QoS on a Per-Port Basis Via the CLI

The first step in configuring the QoS feature is to specify how the ingress traffic is classified when it first enters the switch. There are several QoS features that are configured and applied on a per-port basis, including CoS classification and ID parameters, DEI, DPL, and PCP parameters, and ingress map classification. The following sections describe these QoS configurations on the port(s).

Configuring QoS CoS Settings on the Port via the CLI

Both the CoS classification and CoS ID can be configured on the port using commands executed from the interface configuration mode.

To configure the CoS classification for the port, enter the **[no] qos cos** *<value>* command from the interface's configuration mode. Valid *<value>* range is **0** to **7**, with a value of **0** being the lowest priority. Use the **no** form of this command to return to the default value of **0**.The CoS classification entered on the port applies to all incoming traffic on the port, and can only be overwritten by a QCE applied to the port. Enter the command from the interface configuration mode prompt as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos cos 5
```

To configure the CoS ID for the port, enter the **[no] qos class** *<id>* command from the interface's configuration mode. Valid *<id>* range **0** to **7**, and is configured as **0** by default. Use the **no** form of this command to return the CoS ID to the default value. Enter the command from the interface configuration mode prompt as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos class 3
```

Configuring DEI Settings on the Port via the CLI

DEI values are assigned to incoming traffic on the port using the **[no] qos dei** *<value>* command from the interface's configuration mode. Valid *<value>* range is **0** or **1**. Use the **no** form of this command to return the DEI settings to the default value (**0**). Enter the command from the interface configuration mode prompt as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos dei 1
```

Configuring DPL Settings on the Port via the CLI

DPL values are assigned to incoming traffic on the port using the **[no] qos dpl** *<value>* command. Valid *<value>* range is **0** to **3**, with a default value of **0**. Using the **no** form of this command indicates all incoming traffic is associated with the default DPL value. To change the DPL value for incoming traffic, enter the command from the interface configuration mode prompt as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos dpl 2
```

Configuring PCP Settings on the Port via the CLI

PCP values are assigned to all incoming traffic on the port using the **[no] qos pcp** *<value>* command. Valid *<value>* range is **0** to **7**. By default, all frames are classified using the default PCP value unless the port is VLAN-aware and the frame is tagged, in which case the PCP value given in the frame tag is used. Using the **no** form of this command indicates all incoming traffic is associated with the default PCP value. To change the PCP value for incoming traffic, enter the command from the interface configuration mode prompt as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos pcp 5
```

Configuring QoS Tag Mapping on the Port via the CLI

Tag mapping for incoming traffic on the port specifies how incoming tagged frames on the VLAN-aware port are handled. By default, this feature is disabled, which indicates that the default CoS and DPL values are used for tagged frames. When enabled, this feature specifies that PCP and DEI values, mapped from the CoS and DPL values in the frame tags, are used instead. Tag mapping settings are specified in the QoS Map/Table configuration on a per-port basis, using the **[no] qos map [cos-tag | tag-cos]** command from the interface configuration mode. Using the **no** form of this command removes the mapping configuration.

Using the **qos map cos-tag** command configures the mapping parameters for CoS-to-tag configurations. Once you've entered the **qos map cos-tag** command at the interface configuration mode prompt, you can configure the CoS and DPL values to map to the specified PCP and DEI parameters. The full syntax of the command is **[no] qos map cos-tag cos** *<value>* **dpl** *<value>* **pcp** *<value>* **dei** *<value>*. The **cos** *<value>* parameter specifies the CoS value you are mapping: valid range is **0** to **7** and can consist of a specific CoS class value or a range. The **dpl** *<value>* parameter is the DPL level you are mapping; valid range is **0** to **3**. The **pcp** *<value>* parameter is the PCP value to which you are mapping the specified CoS and DPL values; valid range is **0** to **7**. The **dei** *<value>* parameter is the DEI value to which you are mapping the specified CoS and DPL values; valid range is **0** to **1**. For example, to configure Cos-to-tag mapping of CoS **5** and DPL **1** to PCP **3** and DEI **0**, enter the command as follows from the interface configuration mode prompt:

```
(config)#interface gigabitethernet 1/1
```

```
(config-if)#qos map cos-tag cos 5 dpl 1 pcp 3 dei 0
```

Using the **qos map tag-cos** command, on the other hand, configures the mapping parameters for Tag-to-CoS configurations. Once you've entered the **qos map tag-cos** command at the interface configuration mode prompt, you can configure the PCP and DEI values to map to the specified CoS and DPL parameters. The full syntax of the command is **[no] qos map tag-cos pcp** *<value>* **dei** *<value>* **cos** *<value>* **dpl** *<value>*. The **pcp** *<value>* parameter is the PCP value you are mapping; valid range is **0** to **7** and can consist of a specific value or a range. The **dei** *<value>* parameter is the DEI value you are mapping; valid range is **0** to **1**. The **cos** *<value>* parameter specifies the CoS value to which you are mapping the PCP and DEI values, and has a valid range **0** to **7**. The **dpl** *<value>* parameter is the DPL level to which you are mapping the PCP and DEI values; valid range is **0** to **3**. For example, to configure Tag-to-CoS mapping of PCP **6** and DEI **0** to CoS **3** and DPL **1**, enter the command as follows from the interface configuration mode prompt:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos map tag-cos pcp 6 dei 0 cos 3 dpl 1
```

NOTE

Tag mapping configuration is only necessary for VLAN-aware ports and has no effect on ports that are not VLAN-aware.

Assigning the WRED Group to the Port via the CLI

The WRED group is part of the queue system used by the ASE switch to avoid traffic congestion, and is assigned to incoming traffic on a per-port basis using the **[no] qos wred-group** *<group id>* command. The *<group id>* parameter is the ID number of the WRED group being assigned to the port; valid range is **1** to **3**. By default, no WRED group is assigned to the port. Using the **no** form of this command removes the WRED group from the port's configuration. To assign a previously configured WRED group to the port, enter the command from the interface configuration command mode prompt as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos wred-group 2
```

NOTE

WRED groups are configured in the CLI at a global level. Refer to Configuring WRED via the CLI on page 51 for more information about WRED group configuration.

Specify an Ingress Map for the Port via the CLI

Previously configured ingress maps can be applied to incoming traffic on a per-port basis using the **[no] qos ingress-map** *<map id>* command. The *<map id>* parameter is the ID of the ingress map to be associated with the port; valid ID range is **0** to **127**. Using the **no** form of this command removes the ingress map from the port's QoS configuration. To associate a previously created ingress map with the port, enter the command from the interface configuration mode prompt as follows:

```
(config)#interface gigabit ethernet 1/1
(config-if)#qos ingress-map 12
```

NOTE

Ingress maps for QoS are configured at the global level on the ASE device. Refer to Configuring the QoS Ingress Map via the CLI on page 47 for ingress map configuration information.

Specify an Egress Map for the Port via the CLI

Previously configured egress maps can be applied to outgoing traffic on a per-port basis using the **`[no] qos egress-map`** *`<map id>`* command. The *`<map id>`* parameter is the ID of the egress map to be associated with the port; valid ID range is **0** to **255**. Using the **`no`** form of this command removes the egress map from the port's QoS configuration. To associate a previously created egress map with the port, enter the command from the interface configuration mode prompt as follows:

```
(config)#interface gigabit ethernet 1/1
(config-if)#qos egress-map 75
```

NOTE

Egress maps for QoS are configured at the global level on the ASE device. Refer to Configuring the QoS Egress Map via the GUI on page 29 for egress map configuration information.

Configuring the Ingress Port Policer via the CLI

After configuring the QoS ingress classification for traffic on the port, the next step in configuring QoS ingress parameters is to configure the port policer used by QoS for ingress traffic. This policer serves to classify even further the incoming traffic on the port. The policer is applied on a per-port basis, where it is either enabled or disabled, and the traffic rates and flow control are configured.

Configure the port policer using the **`[no] qos policer`** *`<rate>`* **`[flowcontrol] [fps | kbps |kfps | mbps]`** command. Valid *`<rate>`* range is **1** to **13128147**, with **500 kbps** as the default setting. The specified rate is internally rounded up to the nearest value supported by the port policer. The optional **`flowcontrol`** parameter enables flow control on the policer; this keyword can be entered prior to defining the rate unit, or after entering the rate unit. By default, flow control is disabled. When enabled, and the port is configured in flow control mode, the policer does not discard TCP traffic paused frames, but rather continues to send them. The **`fps`**, **`kbps`**, **`kfps`**, and **`mbps`** parameters of the command specify the rate unit for the policer, and correspond to frames per second, kilobits per second (default), kiloframes per second, and Megabits per second, respectively. Using the **`no`** form of this command disables the policer on the port. To configure a port policer for QoS, enter the command from the interface configuration mode prompt as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos policer
```

Configuring the QoS Ingress Map via the CLI

Ingress maps are used by QoS as a method for further classifying incoming traffic based on key values in the packet or frame header. Maps are configured by completing the following tasks:

- *Step One: Create the QoS Ingress Map on page 47*
- *Step Two: Specify the Ingress Map's Matching Criteria (Keys) on page 48*
- *Step Three: Enable Specific Ingress Map Traffic Classification Features (Actions) on page 48*
- *Step Four: Define New Values for Matching Traffic (Mapping) on page 48*
- *Step Five: Configure Ingress Map Presets (Optional) on page 50*
- *Step Six: Apply the QoS Ingress Map to the Port on page 50*

Step One: Create the QoS Ingress Map

Ingress map configuration begins by entering the **`[no] qos map ingress`** *`<map id>`* command from the Global Configuration mode prompt. This command creates an ingress QoS map, assigns it an ID, and enters the map's configuration mode. Valid *<map id>* range is **0** to **127**. Using the **no** form of this command deletes the QoS ingress map instance from the ASE configuration. To create a new QoS ingress map, with an ID of **20**, enter the command from the Global Configuration mode prompt as follows:

```
(config)#qos map ingress 20
(config-qos-map-ingress)#
```

Once you have created the ingress map instance, and entered the map's configuration mode, you can begin to configure the map's traffic matching criteria, actions, and mapping features.

Step Two: Specify the Ingress Map's Matching Criteria (Keys)

Specifying matching criteria for incoming traffic, or "keys" as they are called in the ASE device, consists of naming the part of the packet header used for matching purposes. Available packet information used for matching includes DSCP, PCP, and DEI values. Once a key is defined, actions and traffic matching can be associated to traffic that matches the key criteria.

To specify the keys used for packet matching, enter the **[no] key [dscp | dscp-pcp-dei | pcp | pcp-dei]** command from the ingress map's configuration mode. The **dscp** parameter of the command specifies that the frame's DSCP value is used as a key, and that no mapping is performed for non-IP frames. The **dscp-pcp-dei** parameter specifies that the frame's DSCP value is used as a key, and that non-IP frames use the classified PCP and DEI values as keys. The **pcp** parameter specifies that the classified PCP value is used as a key for all traffic; this is the default setting. The **pcp-dei** parameter specifies that the classified PCP and DEI values are used as keys for all traffic. Entering the **no** version of this command returns the key configuration to the default matching criteria (classified PCP values).

To configure an ingress map to match traffic based on DSCP values for IP traffic, and PCP and DEI values for non-IP traffic, enter the command from the ingress map's configuration mode prompt as follows:

```
(config)#qos map ingress 20
(config-qos-map-ingress)#key dscp-pcp-dei
```

Step Three: Enable Specific Ingress Map Traffic Classification Features (Actions)

Once the key has been defined for the ingress map, you can enable classification actions for traffic that matches the defined key using the **[no] action [class | cos | dei | dpl | dscp | path | pcp]** command from the ingress map's configuration mode. Each parameter specifies the type of classification you are enabling for matched traffic. For example, the **class** parameter enables classification of the CoS ID; the **cos** parameter enables classification of the CoS value; the **dei** parameter enables DEI classification, the **dpl** parameter enables DPL classification, the **dscp** parameter enables DSCP classification, the **path** parameter enables classification of the path CoS ID, and the **pcp** parameter enables PCP classification. These action parameters can be entered in any order and multiple parameters can be specified in a single command entry. Using the **no** form of this command disables classification for the specified action.

To enable classification of DEI and PCP values for incoming traffic that matches the **dscp-pcp-dei** key specified in ingress map **20**, enter the command as follows:

```
(config)#qos map ingress 20
(config-qos-map-ingress)#key dscp-pcp-dei
(config-qos-map-ingress)#action dei pcp
```

Step Four: Define New Values for Matching Traffic (Mapping)

After you have specified the matching criteria for incoming traffic (keys), and enabled the classification of specific values in the ingress map (actions), you can then specify the new values that will be assigned to traffic that matches the ingress map's criteria. You can configure new values to be assigned to traffic based on the traffic’s current DSCP or PCP values using the **[no] map [dscp** *<value>* **| pcp** *<value>***]** command from the ingress map’s configuration mode.

NOTE

Refer to the sections below for the full syntax of this command and the additional configurable options for the **dscp** *and* **pcp** *parameters.*

When this command is entered, you can then specify the new values that are applied to traffic when it matches the ingress map key and the specific classification action has been enabled. The **dscp** *<value>* parameter specifies the DSCP value used for traffic matching, and enters the mapping configuration for the new values assigned to traffic that matches the specified DSCP value. The **pcp** *<value>* parameter specifies the PCP value (or range) used for traffic matching, and enters the mapping configuration for the new values assigned to traffic that matches the specified PCP value. Using the **no** form of this command removes the mapping configuration from the ingress map.

DSCP Value Mapping Configuration

Traffic with specific DSCP values can be assigned new CoS ID, CoS, DEI, DPL, DSCP, path CoS ID or PCP values using the **map dscp** *<value>* **to [class** *<id>* **| cos** *<value>* **| dei** *<value>* **| dpl** *<value>* **| dscp** *<value>* **| path-cosid** *<id>* **| pcp** *<value>***]** command. The **to** keyword allows you to specify the classified values that are assigned when the key is matched and the action is enabled. The the **class** *<id>* parameter specifies the CoS ID value to be used by matching traffic (valid range is **0** to **7**); the **cos** *<value>* parameter specifies the CoS value to be used by matching traffic (valid range is **0** to **7**); the **dei** *<value>* parameter specifies the DEI value to be used by matching traffic (valid range is **0** to **1**), the **dpl** *<value>* parameter specifies the DPL value to be used by matching traffic (valid range is **0** to **3**), the **dscp** *<value>* parameter specifies the DSCP value to be used by matching traffic (valid range is **0** to **63**), the **path-cosid** *<id>* parameter specifies the path CoS ID value to be used by matching traffic (valid range is **0** to **7**), and the **pcp** *<value>* parameter specifies the PCP value to be used by matching traffic (valid range is **0** to **7**). These new values can be entered in any order and multiple value types can be specified in a single command entry.

To map the DSCP value of best effort (**be**) to a CoS ID value of **3** and a PCP value of **5** for traffic that matches the **dscp-pcp-dei** key specified in ingress map **20**, which is also configured with DEI and PCP value classification enabled, enter the command as follows:

```
(config)#qos map ingress 20
(config-qos-map-ingress)#key dscp-pcp-dei
(config-qos-map-ingress)#action dei pcp
(config-qos-map-ingress)#map dscp be to class 3 pcp 5
```

PCP Value Mapping Configuration

Traffic with specific PCP values can also be assigned new CoS ID, CoS, DEI, DPL, DSCP, path CoS ID or PCP values using the **map pcp** *<value>* **[dei** *<value>***] to [class** *<id>* **| cos** *<value>* **| dei** *<value>* **| dpl** *<value>* **| dscp** *<value>* **| path-cosid** *<id>* **| pcp** *<value>***]** command. The optional **dei** *<value>* allows you to optionally specify a DEI value to which mapping also occurs (valid range is **0** to **1**); if this parameter is not configured, then by default only mapping for DEI **0** is configured. The **to** keyword specifies the classified values that are assigned when the key is matched and the action is enabled. The the **class** *<id>* parameter specifies the CoS ID value to be used by matching traffic (valid range is **0** to **7**); the **cos** *<value>* parameter specifies the CoS value to be used by matching traffic (valid range is **0** to **7**); the **dei** *<value>* parameter specifies the DEI value to be used by matching traffic (valid range is **0** to **1**), the **dpl** *<value>* parameter specifies the DPL value to be used by matching traffic (valid range is **0** to **3**), the **dscp** *<value>* parameter specifies the DSCP value to be used by matching traffic (valid range is **0** to **63**), the **path-cosid** *<id>* parameter specifies the path CoS ID value to be used by matching traffic (valid range is **0** to **7**), and the **pcp** *<value>* parameter specifies the PCP value to be used by matching traffic (valid range is **0** to **7**). These new values can be entered in any order and multiple value types can be specified in a single command entry.

To map the PCP value of **4** and DEI value of **1** to a CoS ID value of **3** and a PCP value of **5** for traffic that matches the **dscp-pcp-dei** key specified in ingress map **20**, which is also configured with DEI and PCP value classification enabled, enter the command as follows:

```
(config)#qos map ingress 20
(config-qos-map-ingress)#key dscp-pcp-dei
(config-qos-map-ingress)#action dei pcp
(config-qos-map-ingress)#map pcp 4 dei 1 to cos 3 pcp 5
```

Step Five: Configure Ingress Map Presets (Optional)

You can optionally configure the ingress map to automatically apply to a specific number of traffic classes, using the **[no] preset classes** *<number>* **[color-aware]** command from the ingress map's configuration mode. The *<number>* parameter specifies the number of traffic classes to which to apply the ingress map; valid range is **1** to **8**. The optional **color-aware** parameter enables color awareness for traffic intercepted by the ingress map. By default, this feature is disabled. Using the **no** form of this command removes the traffic class preset configuration from the ingress map.

To add this ingress map to a number of traffic classes, enter the command as follows:

```
(config)#qos map ingress 20
(config-qos-map-ingress)#preset classes 5
```

Step Six: Apply the QoS Ingress Map to the Port

After the ingress map has been configured with the proper keys, actions, and mapping behavior, you must apply the map to the port before it will become active. To apply the ingress map **20** to port **1** of the Gigabit Ethernet interface, enter the **qos ingress-map** *<map id>* command from the interface's configuration mode prompt as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos ingress-map 20
```

NOTE

Refer to Specify an Ingress Map for the Port via the CLI on page 46 for more details about this command.

After configuring the QoS ingress map, the ingress portion of QoS configuration is completed. The next steps include configuring the QoS queue parameters and the QoS egress behaviors.

12. Configuring QoS Queue Parameters via the CLI

Configuring the QoS queue parameters on the ASE switch determines how traffic is handled to avoid or manage traffic congestions. Queues are managed by a queue policer, WRED algorithm, and a queue shaper. To configure the QoS queue parameters, complete the following tasks:

- *Configuring the Queue Policer via the CLI on page 51*
- *Configuring the Queue Shaper via the CLI on page 51*
- *Configuring WRED via the CLI on page 51*

Configuring the Queue Policer via the CLI

Configuration of the queue policers occurs on a per-port basis, and consists of enabling the queue policer and specifying the traffic rate for the enabled policer. The queue policers limit the bandwidth of received frames that exceed configured rates for the port.

To configure the queue policer, enter the **`[no] qos queue-policer queue`** *`<queue> <rate>`* **`[kbps | mbps]`** command from the interface configuration mode. Valid *<queue>* range is **0** to **7**, and can be entered as a single queue or a range of queues. Valid *<rate>* range is **1** to **13128147**, with **500 kbps** as the default setting. The specified rate is internally rounded up to the nearest value supported by the queue policer. The **`kbps`** and **`mbps`** parameters of the command specify the rate unit for the policer, and correspond to kilobits per second (default) and Megabits per second, respectively. Using the **`no`** form of this command returns the queue policer rate to the default value.

Enter the command from the interface configuration mode prompt as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos queue-policer queue 5 1500 mbps
```

Configuring the Queue Shaper via the CLI

The shaper available for queues configures bandwidth usage and traffic flow parameters for egress traffic on the ASE device. Shapers can also be applied at port-level (refer to *Configuring Egress Port Scheduling via the GUI on page 24*), however, queue-level shapers can be used to measure data rates or line rates of traffic from the queue associated with a port.

To configure the queue shaper, enter the **`[no] qos queue-shaper queue`** *`<queue> <rate>`* **`[kbps | mbps] rate-type [data | line]`** command from the interface configuration mode. Valid *<queue>* range is **0** to **7**, and can be entered as a single queue or a range of queues. Valid *<rate>* range is **1** to **13107100**, with **500 kbps** as the default setting. The **`kbps`** and **`mbps`** parameters specify the rate unit for the shaper itself, and correspond to kilobits per second (default) and Megabits per second, respectively. The specified rate is internally rounded up to the nearest value supported by the queue shaper. The **`rate-type`** parameters specify whether you are shaping the data rate (**`data`** parameter) or the line rate (**`line`** parameter). Using the **`no`** form of this command returns the queue shaper rate to the default value.

Enter the command from the interface configuration mode prompt as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos queue-shaper queue 3 1500 mbps rate-type data
```

Configuring WRED via the CLI

Congestion can be avoided in the QoS queue system by enabling and configuring the WRED function on the ASE device. WRED configuration includes creating a WRED group, associating it with a queue and DPL value, and specifying the minimum and maximum threshold for packets held within the queue. When the minimum threshold is reached, packets begin to be dropped from the queue. The maximum threshold, on the other hand, specifies that packets are dropped from the queue when the queue fill level reaches the threshold, or all packets are dropped when the queue is 100 percent full.

WRED is configured on a global level on the ASE device using the **`[no] qos wred group`** *`<group id>`* **`queue`** *`<queue>`* **`dpl`** *`<value>`* **`min-fl`** *`<number>`* **`max`** *`<number>`* **`[fill-level]`** command. The **`group`** *`<group id>`* parameter of the command creates the WRED group that will be associated with the queue specified using the **`queue`** *`<queue>`* parameter. Valid WRED *<group id>* range is **1** to **3**. Valid *`<queue>`* range is **0** to **7**, and can be entered as a specific queue, or a range of queues. The **`dpl`** *`<value>`* parameter associates a drop probability level with the queue, and is used by default as the fill maximum value for the queue. Valid **`dpl`** *`<value>`* rang is **1** to **3**. The **`min-fil`** *`<number>`* parameter specifies the minimum fill level (in percent) of the queue. Valid *<number>* range is **0** to **100** percent. The **`max`** *`<number>`*

parameter specifies the maximum threshold (in percent) for the queue. Valid *<number>* range is **1** to **100** percent. By default, the queue uses the drop probability setting to determine when packets begin to drop from the queue. To change this setting, enter the optional **fill-level** parameter, which specifies that packets are not dropped until the fill-level of the queue is reached, rather than when the drop probability percentage is reached. Use the **no** form of this command to return to the default queue values.

To configure a WRED group with an ID of **2**, for queue **3** with a DPL value of **2** and a minimum fill percentage of **75** percent and a maximum drop probability of **95**, enter the command from the Global Configuration mode as follows:

```
(config)#qos wred group 2 queue 3 dpl 2 min-fl 75 max 95
(config)#
```

13. Configuring QoS Egress Parameters Using the CLI

The last steps in configuring the QoS feature on the ASE device is to specify how traffic is handled on the egress port. To configure the egress QoS parameters, configure the traffic schedulers and shapers on the port, any packet or frame tag remarking on the port, and an egress traffic map. To configure these settings, complete the following tasks:

- *Configuring Egress Port Scheduling via the CLI on page 52*
- *Configuring Egress Port Shapers via the CLI on page 52*
- *Configuring Egress Port Tag Remarking via the CLI on page 53*
- *Configuring the QoS Egress Map via the CLI on page 53*

These actions serve to shape, schedule, and prepare the outgoing traffic on the ASE device.

Configuring Egress Port Scheduling via the CLI

As part of QoS configuration, you can configure port-level scheduling for egress traffic to help avoid or manage egress traffic congestion. Scheduling is performed by scheduling algorithms, which follow either strict priority scheduling, or deficit weighted round robin (DWRR) scheduling. Strict priority scheduling specifies that all queues adhere to the priority values applied to the egress traffic when deciding which packets and frames to send first. DWRR scheduling is based on the weights configured for each queue associated with the port.

Port scheduling is configured for egress traffic using the **[no] qos wrr** *<Q0 weight> <Q1 weight> <Q2 weight> <Q3 weight> <Q4 weight> <Q5 weight> <Q6 weight> <Q7 weight>* command from the interface configuration mode. Each *<weight>* parameter assigns a weight, from **1** to **100**, to queues **0** through **7**, respectively. The higher the weight, the higher the priority of the queue. Using the **no** form of this command removes the configured weight from the queue.

To configure the DWRR scheduling on the egress port, by specifying a that queue **0** has higher priority than queues **1** or **2**, enter the command from the interface configuration mode prompt as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos wrr 10 6 2
```

Configuring Egress Port Shapers via the CLI

Shapers can be configured on a per-port basis to aid in bandwidth allocation on the port for egress traffic. Port shapers are configured by entering the **[no] qos shaper** *<rate>* **[kbps | mbps] [rate-type [data | line]]** command from the interface configuration mode. Valid *<rate>* range is **1** to **13107100**, with **500 kbps** as the default setting. The **kbps** and **mbps** parameters specify the rate unit for the shaper itself, and correspond to kilobits per second (default) and Megabits per second, respectively. The specified rate is internally rounded up to the nearest value supported by the port shaper. The **rate-type** parameters specify whether you are shaping the data rate (**data** parameter) or the line rate (**line** parameter). Using the **no** form of this command returns the queue shaper rate to the default value.

To configure a shaper on the port for egress traffic, that shapes egress traffic to a rate of **1750 kbps**, and measures **line** data rates, enter the command as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos shaper 1750 kbps rate-type line
```

Configuring Egress Port Tag Remarking via the CLI

In the CLI, remarking tags on egress traffic at the port level is accomplished by applying mapped definitions for CoS/DPL to PCP/DEI values (refer to DSCP/CoS Mapping discussed in *Configuring DSCP-Based QoS via the CLI on page 59*), or by applying the configured default PCP and DEI values defined on the port.

To apply previously configured map values, or to configured the default PCP and DEI values to apply to egress traffic, enter the **qos tag-remark [mapped | pcp** *<value>* **dei** *<value>***]** command from the interface configuration mode. The **mapped** keyword specifies that tag remarking occurs using previously mapped CoS/DPL to PCP/DEI values (refer to DSCP/CoS Mapping discussed in *Configuring DSCP-Based QoS via the CLI on page 59*). The **pcp** *<value>* **dei** *<value>* parameters specify that tag remarking occurs on egress traffic using default PCP and DEI settings that are set with this command. Valid range of PCP values is **0** to **7**, and valid range of DEI values is **0** to **1**.

To configure port tag remarking to use newly specified PCP and DEI values, enter the command as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos tag-remark pcp 4 dei 0
```

To configure port tag remarking to use previously mapped tag values, enter the command as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos tag-remark mapped
```

Configuring the QoS Egress Map via the CLI

The last step in configuring QoS egress parameters is to configure the QoS egress map. Egress maps function in the same way as ingress maps, but they are applied to egress traffic on the port. Egress maps are used to control the rewriting of packets at egress, where PCP, DEI, and DSCP values can be updated based on their classified key values. Egress maps are configured by specifying which part of the packet is used for matching (CoS ID, CoS ID-DPL, DSCP, or DSCP-DPL), enabling the rewriting actions taken once the packet information is processed, and specifying which new values are mapped to the packet information. Maps are configured by completing the following tasks:

- *Step One: Create the QoS Egress Map on page 53*
- *Step Two: Specify the Egress Map's Matching Criteria (Keys) on page 54*
- *Step Three: Enable Specific Egress Map Rewriting Features (Actions) on page 54*
- *Step Four: Define New Values for Matching Traffic (Mapping) on page 54*
- *Step Five: Configure Egress Map Presets (Optional) on page 56*
- *Step Six: Apply the QoS Egress Map to the Port on page 56*

Step One: Create the QoS Egress Map

Egress map configuration begins by entering the **[no] qos map egress** *<map id>* command from the Global Configuration mode prompt. This command creates an egress QoS map, assigns it an ID, and enters the map's configuration mode. Valid *<map id>* range is **0** to **255**. Using the **no** form of this command deletes the QoS egress map instance from the ASE device's configuration. To create a new QoS egress map, with an ID of **75**, enter the command from the Global Configuration mode prompt as follows:

```
(config)#qos map egress 75
(config-qos-map-egress)#
```

Once you have created the egress map instance, and entered the map's configuration mode, you can begin to configure the map's traffic matching criteria, actions, and mapping features.

Step Two: Specify the Egress Map's Matching Criteria (Keys)

Specifying matching criteria (keys) for egress traffic, consists of naming the part of the packet header used for matching purposes. Available packet information used for matching egress traffic includes CoS, DSCP, and DPL values. Once a key is defined, actions and traffic mapping can be associated to traffic that matches the key criteria.

To specify the keys used for packet matching, enter the **[no] key [class | class-dpl | dscp | dscp-dpl]** command from the egress map's configuration mode. The **class** parameter of the command specifies that the classified CoS ID value is used as a key; this is the default egress map key. The **class-dpl** parameter specifies that the classified CoS ID and DPL value are used as keys. The **dscp** parameter specifies that the classified DSCP value is used as a key. The **dscp-dpl** parameter specifies that the classified DSCP and DPL values are used as keys. Entering the **no** version of this command returns the key configuration to the default matching criteria (classified CoS ID value).

To configure an egress map to match traffic based on DSCP values, enter the command from the egress map's configuration mode prompt as follows:

```
(config)#qos map egress 75
(config-qos-map-egress)#key dscp
```

Step Three: Enable Specific Egress Map Rewriting Features (Actions)

Once the key has been defined for the egress map, you can enable rewriting actions for traffic that matches the defined key using the **[no] action [dei | dscp | path | pcp]** command from the egress map's configuration mode. Each parameter specifies the type of rewriting you are enabling for matched traffic. For example, the **dei** parameter enables rewriting of the DEI value in the packet; the **dscp** parameter enables rewriting of the DSCP value; the **path** parameter enables rewriting of the path CoS ID value, and the **pcp** parameter enables rewriting of the PCP value. These action parameters can be entered in any order and multiple parameters can be specified in a single command entry. Using the **no** form of this command disables rewriting for the specified action.

To enable rewriting of DEI and PCP values for egress traffic that matches the **dscp** key specified in egress map **75**, enter the command as follows:

```
(config)#qos map egress 75
(config-qos-map-egress)#key dscp
(config-qos-map-egress)#action dei pcp
```

Step Four: Define New Values for Matching Traffic (Mapping)

After you have specified the matching criteria for egress traffic (keys), and enabled the rewriting of specific values in the egress map (actions), you can then specify the new values that will be assigned to traffic that matches the egress map's criteria. You can configure new values to be assigned to traffic based on the traffic's current CoS class or DSCP values using the **[no] map [class** *<id>* **| dscp** *<value>***]** command from the egress map's configuration mode.

NOTE

Refer to the sections below for the full syntax of this command and the additional configurable options for the **class** *and* **dscp** *parameters.*

When this command is entered, you can then specify the new values that are applied to traffic when it matches the egress map key and the specific rewriting action has been enabled. The **class** *<id>* parameter specifies the CoS ID value (or range) used for traffic matching, and enters the mapping configuration for the new values assigned to traffic that matches the specified CoS ID value. The **dscp** *<value>* parameter specifies the DSCP value used for traffic matching, and enters the mapping configuration for the new values assigned to traffic that matches the specified DSCP value. Using the **no** form of this command removes the mapping configuration from the egress map.

CoS ID Value Mapping Configuration

Traffic with specific CoS ID values can also be assigned new DEI, DSCP, path CoS ID or PCP values using the **map class** *<id>* **[dpl** *<value>***] to [dei** *<value>* **| dscp** *<value>* **| path-cosid** *<id>* **| pcp** *<value>***]** command. The optional **dpl** *<value>* allows you to specify a DPL value to which mapping also occurs (valid range is **0** to **3**); if this parameter is not configured, then by default only mapping for DPL **0** is configured. The **to** keyword specifies the values that are written to the frame when the key is matched and the action is enabled. The **dei** *<value>* parameter specifies the DEI value to be written to matching traffic (valid range is **0** to **1**), the **dscp** *<value>* parameter specifies the DSCP value to be written to matching traffic (valid range is **0** to **63**), the **path-cosid** *<id>* parameter specifies the path CoS ID value to be written to matching traffic (valid range is **0** to **7**), and the **pcp** *<value>* parameter specifies the PCP value to be written to matching traffic (valid range is **0** to **7**). These new values can be entered in any order and multiple value types can be specified in a single command entry.

To map the DEI value of **1** and the PCP value of **5** to the CoS ID of **3** and a DPL value of **2**, for traffic that matches the **dscp** key specified in egress map **75**, which is also configured with DEI and PCP rewrite actions enabled, enter the command as follows:

```
(config)#qos map egress 75
(config-qos-map-egress)#key dscp
(config-qos-map-egress)#action dei pcp
(config-qos-map-egress)#map class 3 dpl 2 to dei 1 pcp 5
```

DSCP Value Mapping Configuration

Traffic with specific DSCP values can be assigned new CoS ID, CoS, DEI, DPL, DSCP, path CoS ID or PCP values using the **map dscp** *<value>* **[dpl** *<value>***] to [dei** *<value>* **| dscp** *<value>* **| path-cosid** *<id>* **| pcp** *<value>***]** command. The optional **dpl** *<value>* allows you to specify a DPL value to which mapping also occurs (valid range is **0** to **3**); if this parameter is not configured, then by default only mapping for DPL **0** is configured. The **to** keyword allows you to specify the values that are written to the frame when the key is matched and the action is enabled. The **dei** *<value>* parameter specifies the DEI value to be written to matching traffic (valid range is **0** to **1**), the **dscp** *<value>* parameter specifies the DSCP value to be written to matching traffic (valid range is **0** to **63**), the **path-cosid** *<id>* parameter specifies the path CoS ID value to be written to matching traffic (valid range is **0** to **7**), and the **pcp** *<value>* parameter specifies the PCP value to be written to matching traffic (valid range is **0** to **7**). These new values can be entered in any order and multiple value types can be specified in a single command entry.

To map the DSCP value of best effort (**be**) and a DPL value of **2** to a DEI value of **1** and a PCP value of **5** for traffic that matches the **`dscp`** key specified in egress map **75**, which is also configured with DEI and PCP value classification enabled, enter the command as follows:

```
(config)#qos map egress 75
(config-qos-map-egress)#key dscp
(config-qos-map-egress)#action dei pcp
(config-qos-map-egress)#map dscp be dpl 2 to dei 1 pcp 5
```

Step Five: Configure Egress Map Presets (Optional)

You can optionally configure the egress map to automatically apply to a specific number of traffic classes, using the **`[no] preset classes`** *`<number>`* **`[color-aware]`** command from the egress map's configuration mode. The *`<number>`* parameter specifies the number of traffic classes to which to apply the egress map; valid range is **1** to **8**. The optional **`color-aware`** parameter enables color awareness for traffic intercepted by the egress map. By default, this feature is disabled. Using the **`no`** form of this command removes the traffic class preset configuration from the egress map.

To add this egress map to a number of traffic classes, enter the command as follows:

```
(config)#qos map egress 75
(config-qos-map-egress)#preset classes 5
```

Step Six: Apply the QoS Egress Map to the Port

After the egress map has been configured with the proper keys, actions, and mapping behavior, you must apply the map to the port before it will become active. To apply the egress map **75** to port **1** of the Gigabit Ethernet interface, enter the **`qos egress-map`** *`<map id>`* command from the interface's configuration mode prompt as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos egress-map 75
```

> **NOTE**
>
> *Refer to Specify an Egress Map for the Port via the CLI on page 47 for more details about this command.*

With the finished configuration of the QoS egress map, and its application to the appropriate ports, the basic QoS configurations are complete. You can now choose to optionally configure DSCP translation and classification, QoS control list entries, or storm policing QoS features.

14. Configuring QoS DSCP via the CLI (Optional)

QoS on the ASE device can include DSCP configuration for packet classification, translation, rewriting, or remapping purposes. These features can be applied on a per-port basis for both ingress traffic classification and translation and egress traffic rewriting and remapping. The following sections outline how to configure DSCP on the ASE device for QoS purposes. Typical DSCP configuration tasks include:

- *Enabling DSCP Features on the Port via the CLI on page 57*
- *Configure the DSCP Classify Map (Global) via the CLI on page 57*
- *Configure the DSCP Ingress Translation Map (Global) via the CLI on page 58*
- *Configuring DSCP-Based QoS via the CLI on page 59*

Enabling DSCP Features on the Port via the CLI

DSCP features can be enabled on a per-port basis for both ingress and egress traffic. Ingress traffic can use DSCP for packet translation and classification purposes, and egress traffic can use DSCP for rewriting and remapping purposes. DSCP configurations (such as translation, classification, and rewriting or remapping) are actually configured at the global level on the ASE device. DSCP commands at the port-level enable or apply the global-level DSCP configurations (refer to *Configure the DSCP Classify Map (Global) via the CLI on page 57*, *Configure the DSCP Ingress Translation Map (Global) via the CLI on page 58*, or *Configure the DSCP Egress Translation Map (Global) via the CLI on page 58*).

Enable DSCP translation for ingress traffic using the **[no] qos dscp-translate** command from the interface configuration mode prompt. Use the **no** form of this command to disable DSCP translation for ingress traffic on the port. Enter the command as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos dscp-translate
```

Enable DSCP classification for ingress traffic using the **[no] qos dscp-classify [any | selected | zero]** command from the interface configuration mode prompt. The **any** parameter specifies that incoming traffic is always classified to a new DSCP value. The **selected** parameter specifies that incoming traffic of a specific DSCP value is classified to a new DSCP value only if DSCP classification is enabled for that specific DSCP value in the global DSCP classify map (refer to *Configure the DSCP Classify Map (Global) via the CLI on page 57*). The **zero** parameter specifies that incoming traffic is classified to a new DSCP value if the current DSCP value is zero. Use the **no** form of this command to disable DSCP classification on the port. To enable DSCP classification for all DSCP traffic incoming on the port, enter the command as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos dscp-classify any
```

Enable DSCP rewriting and remapping of egress traffic on the port using the **[no] qos dscp-remark [remap | rewrite]** command from the interface configuration mode prompt. The **remap** parameter of this command specifies that the DSCP field of egress traffic is rewritten using classified DSCP values that have been mapped through the global DSCP egress translation map (refer to *Configure the DSCP Egress Translation Map (Global) via the CLI on page 58*). The **rewrite** parameter specifies that the DSCP field of egress traffic is rewritten with a classified DSCP value without any DSCP translation. Use the **no** form of this command to disable DSCP rewriting and remapping features on the port. To enable DSCP rewrites based on the global DSCP egress translation map, enter the command as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos dscp-remark remap
```

Configure the DSCP Classify Map (Global) via the CLI

DSCP classification is used for additional classification of ingress traffic on the port, as well as rewriting DSCP values on egress traffic. By default, DSCP classification is disabled, indicating that no DSCP classification is completed for ingress traffic and is not applied to egress traffic. When DSCP classification is enabled on the port (using the **qos dscp-classify** command, as described in *Enabling DSCP Features on the Port via the CLI on page 57*), specific, trusted DSCP values are configured as “classified,” and can be used to further classify ingress traffic or to rewrite egress traffic. DSCP values are configured as trusted and classified using the globally-configured DSCP Classify Map.

The DSCP Classify Map is configured from the Global Configuration mode prompt, and only requires the use of a single command. This command, **[no] qos map dscp-classify** *<dscp value>*, can be entered multiple times to specify that particular DSCP values are classified as trustworthy and can be used by other QoS processes (ingress traffic classification and egress traffic rewriting). The *<dscp value>* parameter is used to specify the DSCP value; valid range is **0** to **63**. Using the **no** form of this command removes the

DSCP value from the DSCP classification table. When the DSCP values are entered using this command, those same values can be used in port-level DSCP classification and rewriting functions.

NOTE

Refer to DSCP Values Explained on page 80 for more information about DSCP values and their use in QoS.

To globally configure DSCP classification of specific DSCP values for use with other QoS features, such as best effort (**0**) or assured forwarding (**10**) DSCP values, enter the command from the Global Configuration mode prompt as follows:

```
(config)#qos map dscp-classify 0
(config)#qos map dscp-classify 10
```

Configure the DSCP Ingress Translation Map (Global) via the CLI

DSCP translation is used to populate the DSCP translation table, which in turn is used by QoS to further classify ingress traffic by remapping DSCP values. You can specify the global ingress DSCP translation parameters using the **`[no] qos map dscp-ingress-translation`** *`<dscp value>`* **`to`** *`<dscp value>`* command from the Global Configuration mode prompt. When DSCP translation is enabled on the port (using the **`qos dscp-translate`** command as described in *Enabling DSCP Features on the Port via the CLI on page 57*), the DSCP translation parameters configured globally are applied to incoming traffic on the port. Use the **`no`** form of this command to remove the specific DSCP value from DSCP translation. The *`<dscp value>`* parameter is used to specify the DSCP value; valid range is **0** to **63**. This command can be entered multiple times to specify multiple DSCP translation configurations.

To configure specific DSCP values are translated to different DSCP values when DSCP translation is enabled for incoming traffic, enter the command as follows:

```
(config)#qos map dscp-ingress-translation 14 to 34
(config)#qos map dscp-ingress-translation 0 to 10
```

Configure the DSCP Egress Translation Map (Global) via the CLI

DSCP egress translation is configured for the same purposes as DSCP ingress translation. QoS uses the values specified in the DSCP egress translation map to remap the DSCP values of egress traffic on the port. You can specify the global egress DSCP translation parameters using the **`[no] qos map dscp-egress-translation`** *`<dscp value>`* **`to`** *`<dscp value>`* command from the Global Configuration mode prompt. When DSCP translation is enabled for remapping values of egress traffic on the port (using the **`qos dscp-remark remap`** command as described in *Enabling DSCP Features on the Port via the CLI on page 57*), the DSCP translation and remapping parameters configured globally are applied to egress traffic on the port. Use the **`no`** form of this command to remove the specific DSCP value from DSCP translation. The *`<dscp value>`* parameter is used to specify the DSCP value; valid range is **0** to **63**. This command can be entered multiple times to specify multiple DSCP translation configurations.

To configure specific DSCP values to be used for remapping egress traffic, enter the command as follows:

```
(config)#qos map dscp-egress-translation 34 to 14
(config)#qos map dscp-egress-translation 10 to 0
```

Configuring DSCP-Based QoS via the CLI

QoS can be configured to use trusted DSCP values as part of the QoS and DPL classification for ingress traffic. Configuring this option allows you to specify the trusted DSCP value, and assign that value a QoS class and DPL value so that as traffic comes into the switch it is automatically classified by QoS and DPL value, based on its DSCP value. Configuring this feature requires the completion of three tasks:

- *Specifying Trusted DSCP Values on the Port on page 59*
- *Configuring the Global CoS to DSCP Map on page 59*
- *Configuring the Global DSCP to CoS Map on page 59*

Specifying Trusted DSCP Values on the Port

To configure DSCP-based QoS on the ASE device, you must enable trust for DSCP and VLAN tagged traffic. Trust for these values is enabled on a per-port basis using the **`[no] qos trust [dscp | tag]`** command. The **`dscp`** parameter specifies that DSCP values defined in the DSCP to CoS map are trusted, and can be used for DSCP-based QoS. The **`tag`** parameter specifies that traffic tagged with VLAN IDs defined in the CoS to DSCP map are trusted, and can be used for DSCP-based QoS. Using the **`no`** form of this command disables trust for DSCP and/or VLAN tagged incoming traffic, and disables DSCP-based QoS.

To enable trust on the port for incoming traffic with associated DSCP values, enter the command from the interface configuration mode prompt as follows:

```
(config)#interface gigabitethernet 1/1
(config-if)#qos trust dscp
```

Configuring the Global CoS to DSCP Map

CoS values can be mapped to DSCP values for use with DSCP-based QoS. When this option is configured, traffic coming into the switch is automatically classified by its CoS and DPL value, and then assigned a corresponding DSCP value. The DSCP value can then be used to classify, remark, or rewrite traffic as it moves through the ASE device.

CoS values are mapped to DSCP values using the **`[no] qos map cos-dscp`** *`<value>`* **`dpl`** *`<value>`* **`dscp`** *`<value>`* command from the Global Configuration mode prompt. The **`cos-dscp`** *`<value>`* parameter specifies the CoS class value you are mapping to the DSCP value. Valid range is **0** to **7**, and can be entered as a single class value or as a range. The **`dpl`** *`<value>`* parameter defines the DPL value associated with the CoS class; valid range is **0** to **3**, and can be entered as a single value or as a range. The **`dscp`** *`<value>`* parameter specifies the DSCP value that you are associating with the specified CoS class. Valid **`dscp`** *`<value>`* range is **0** to **63**. You can enter this command as many times as necessary to associate the required DSCP values with the appropriate CoS classes. Using the **`no`** form of this command removes the specified CoS to DSCP mapping from the ASE switch.

To configure the CoS to DSCP map to associate the DSCP value **10** with the CoS class **5**, enter the command from the Global Configuration mode prompt as follows:

```
(config)#qos map cos-dscp 5 dpl 2 dscp 10
```

Configuring the Global DSCP to CoS Map

DSCP values can be mapped to CoS values for use with DSCP-based QoS. When this option is configured, traffic coming into the switch is automatically classified by its DSCP value and then assigned corresponding CoS and DPL values. The CoS and DPL values can then be used to classify, remark, or rewrite traffic as it moves through the ASE device.

DSCP values are mapped to CoS values using the **`[no] qos map dscp-cos`** *`<value>`* **`cos`** *`<value>`* **`dpl`** *`<value>`* command from the Global Configuration mode prompt. The **`dscp-cos`** *`<value>`* parameter specifies the DSCP value you are mapping to the CoS class value. Valid range is **0** to **63**. The **`cos`** *`<value>`*

parameter defines the CoS class value that you are associating with the specified DSCP value; valid range is **0** to **7**, and can be entered as a single value or as a range. The **dpl** *<value>* parameter specifies the DPL value that is associated with the specified CoS class. Valid **dpl** *<value>* range is **0** to **3**. You can enter this command as many times as necessary to associate the required CoS class values with the appropriate DSCP values. Using the **no** form of this command removes the specified DSCP to CoS mapping from the ASE switch.

To configure the DSCP to CoS map to associate the DSCP value **10** with the CoS class **5**, enter the command from the Global Configuration mode prompt as follows:

```
(config)#qos map dscp-cos 10 cos 5 dpl 2
```

15. Configuring the QoS Control List via the CLI (Optional)

QoS control lists (QCLs) can be used to configure flexible classification for Layer 2, 3, and 4 network traffic, and can perform reclassification of traffic based on CoS, DPL, PCP, DEI, DSCP, and ACL values. The QCL is comprised of various QoS control entries (QCEs), which are applied on a per-port basis, and can specify source and destination MAC addresses, traffic types, VLAN IDs, PCP values, and frame types that receive certain classifications if the incoming traffic matches the QCE criteria. Up to **255** QCEs can be created for the ASE device.

Configuring QCEs relies on creating the QCE, specifying the criteria used to match incoming traffic (key parameters), configuring the actions taken on matching traffic, associating the QCE with any ingress maps or ACLs, and applying the QCE to the appropriate interface. These configurations are all completed using a single command from the Global Configuration mode prompt. This top level command, and its subsequent configuration keywords and parameters are described in the following sections.

QCE Configuration Command Overview

There are several command parameters used to configure QCEs. These command parameters are all available as part of a single command used to create the QCE, define key parameters for matching traffic, specify actions to be taken on matching traffic, and apply the QCE to the appropriate port.

The full syntax of the QCE configuration command appears as follows:

```
[no] qos qce <qce id> [refresh | update <qce id>] [action <action>] [<matching
criteria>] [<qce operation>]
```

Using the **no** form of this command to remove the specified QCE from the ASE device configuration.

The basic parameters of this top level command include:

- *<qce id>:* Specifies the ID number of the QoS control list entry. Valid range is **1** to **256**. When used alone, it creates the QCE with the specified ID number. When used in conjunction with the **update** parameter, it specifies the QCE ID to which you are editing/updating.
- **refresh**: Refreshes the QCE tables in hardware.
- **update**: Specifies you will be updating a previously configured QCE.
- **action** *<action>* : Enables CoS, DPL, DSCP, ingress map, PCP-DEI, and policy classification for traffic that matches the QCE matching criteria.
- *<matching criteria>*: Specifies the key values that are compared to the values included in incoming traffic packets and frames.
- *<qce operations>*: Specifies the location of the QCE in the QCE list and can apply the QCE to an interface.

Many of these parameters, when entered in the command, will unlock several additional configuration options. For example, when entering the command to begin configuring the actions to take on any matching traffic, the command might look like the following:

```
(config)#qos qce 5 action
```

You can then configure CoS, DPL, DSCP, ingress map, PCP-DEI, and ACL policy actions using one of those keywords (**cos**, **dpl**, **dscp**, **ingress-map**, **pcp-dei**, **policy**), so that the command might look like the following:

```
(config)#qos qce 5 action dscp
```

In turn, each of those keywords has additional configuration parameters available. For example, configurable options for the **dscp** keyword include **[***<value>* **| default]**, indicating a specific DSCP value (range is **0** to **63**), or the use of the existing DSCP value of the frame. So, the command would look like the following if you were configuring actions based on the DSCP value **10**:

```
    (config)#qos qce 5 action dscp 10
```

You could then continue to configure actions, entering any of the additional action keywords and their additional configuration parameters. Or, you could begin configuring matching criteria, in which case the command might look like the following:

```
    (config)#qos qce 5 action dscp 10 dmac any inner-tag vid
```

This process could continue until you have configured all desired matching criteria, actions, and associations for the QCE in a single, lengthy command. In addition, these parameters (actions, matching criteria, associations, positioning instructions, etc.) can be entered in almost any order from any configuration area (for example, you can enter the **action** keyword, specify the action parameter, specify the QCE is the last QCE in the list (using the **last** keyword) and then immediately begin entering matching criteria). The following sections describe each of the configuration parameters and their subsequent configuration options; however, note that these parameters and options can be entered in multiple places within the single command.

Configuring QCE Actions ([*<action>*] Parameter)

QCE actions include enabling CoS, DPL, DSCP, ingress map, PCP, DEI, and policy classification for traffic that matches the specified criteria in the QCE (refer to *Configuring QCE Matching Criteria ([<matching criteria>] Parameter) on page 62* for information about matching key parameters). The QCE *<action>* parameter is configured by entering one (or more) of the following keywords and their parameters: The command syntax for specifying QCE actions appears as follows:

```
    (config)#qos qce 5 action <action>
```

After entering the **action** keyword in the QCE configuration command, you can specify one of the following *<action>* parameters:

- **cos [***<value>* **| default]**: Configures CoS class actions. Specifying *<value>* assigns a single CoS class ID. Valid range is **0** to **7**. Using the **default** parameter specifies that matching traffic keeps the existing setting.
- **dpl [***<value>* **| default]**: Configures DPL actions. Specifying *<value>* assigns a single DPL value. Valid range is **0** to **3**. Using the **default** parameter specifies that matching traffic keeps the existing setting.
- **dscp [***<value>* **| default]**: Configures DSCP actions. Specifying *<value>* assigns a single DSCP value. Valid range is **0** to **63**. Using the **default** parameter specifies that matching traffic keeps the existing setting.

- **ingress-map** [*<map id>* | **default**]: Assigns a QoS ingress map to the incoming traffic. Specifying *<map id>* assigns a single ingress map to the traffic. Valid range is **0** to **127**. Using the **default** parameter specifies that matching traffic keeps the existing ingress map setting.
- **pcp-dei** [*<pcp value> <dei value>* | **default**]: Configures PCP and DEI actions. Using the *<pcp value> <dei value>* parameter assigns a new PCP value (range is **0** to **7**) and DEI value (range is **0** to **1**. Using the **default** parameter specifies that matching traffic keeps the existing setting.
- **policy** [*<acl id>* | **default**]: Assigns an ACL to the incoming traffic. Specifying *<acl id>* assigns a single ACL to the traffic. Valid range is **0** to **127**. Using the **default** parameter specifies that matching traffic keeps the existing ACL setting.

Each of these *<action>* can be entered multiple times, and in any order. The following is an example of configuring QCE **5** with a CoS action:

```
(config)#qos qce 5 action cos 2
```

After specifying an *<action>* parameter for the QCE, you can begin specifying the QCE *<matching criteria>* parameters.

Configuring QCE Matching Criteria ([*<matching criteria>*] Parameter)

QCE matching criteria are specified key values that are compared to the values included in incoming traffic packets and frames. Multiple types of matching criteria can be used in a single QCE entry, and can be entered in any order. The same *<matching criteria>* parameters are available in almost every area of the QCE configuration.

Table 2 below displays the *<matching criteria>* parameters available in QCE configuration, listing the criteria keywords, the additional configurable parameters for each keyword, and a description of the matching action they perform.

Table 2. Available Parameters for QCE *<matching criteria>*

Keyword	Parameters	Description
<action>	Refer to *Configuring QCE Actions ([<action>] Parameter) on page 61*	Actions can be included after a specified matching criteria is defined, without having to use the **action** keyword.
dmac	[*<mac_address>* | **any** | **broadcast** | **multicast** | **unicast**]	Configures traffic matching based on destination MAC address. Enter *<mac_address>* in the **xx-xx-xx-xx-xx** format. The **any** keyword indicates any destination MAC address matches. The **broadcast**, **multicast**, and **unicast** keywords indicate broadcast, multicast, or unicast destination MAC addresses match, respectively.
frame-type	[**any** | **etype** | **ipv4** | **ipv6** | **llc** | **snap**] **Note**: Each of these parameters has additional configuration for matching parameters. Refer to *Configuring Frame-Type [<matching criteria>] on page 63*.	Configures traffic matching based on the specific frame type. The **any** keyword specifies any frame type is matched. The **etype** keyword specifies the Ether type of frame to match. The **ipv4** keyword specifies that IPv4 packets are matched.The **ipv6** keyword specifies that IPv6 packets are matched. The **llc** keyword specifies that LLC frames are matched. The **snap** keyword indicates that SNAP frames are matched.

Table 2. Available Parameters for QCE *<matching criteria>* (Continued)

Keyword	Parameters	Description
inner-tag	**dei [***<value>* **| default]** **pcp [***<value>* **| default]** **type [any | c-tagged | s-tagged | tagged | untagged]** **vid [***<id>* **| any]**	Configures traffic matching based on the inner tag of the traffic. The **dei** *<value>* parameter specifies the DEI value; valid range is **0** to **1**. The **pcp** *<value>* parameter specifies the PCP value; valid range is **0** to **7**. The **default** keyword indicates the existing DEI or PCP value is used for matching. The **any** keyword indicates any type of tag or VLAN ID matches. The **c-tagged**, **s-tagged**, **tagged,** and **untagged** keywords indicate C-tagged, S-tagged, tagged, or untagged traffic matches, respectively. The **vid** *<id>* parameter specifies the VLAN ID, or ID range, of the inner tag to use for matching.
smac	**[***<mac_address>* **| any]**	Configures traffic matching based on source MAC address. Enter *<mac_address>* in the **xx-xx-xx-xx-xx** format. The **any** keyword indicates any source MAC address matches.
tag	**dei [***<value>* **| default]** **pcp [***<value>* **| default]** **type [any | c-tagged | s-tagged | tagged | untagged]** **vid [***<id>* **| any]**	Configures traffic matching based on the tag of the traffic. The **dei** *<value>* parameter specifies the DEI value; valid range is **0** to **1**. The **pcp** *<value>* parameter specifies the PCP value; valid range is **0** to **7**. The **default** keyword indicates the existing DEI or PCP value is used for matching. The **any** keyword indicates any type of tag or VLAN ID matches. The **c-tagged**, **s-tagged**, **tagged,** and **untagged** keywords indicate C-tagged, S-tagged, tagged, or untagged traffic matches, respectively. The **vid** *<id>* parameter specifies the VLAN ID tag, or ID range, to use for matching.

Each of these *<matching criteria>* parameters can be entered multiple times, and in any order. The following is an example of configuring QCE **5** with a CoS action, and matching based on destination MAC addresses and VLAN ID tags:

```
(config)#qos qce 5 action cos 2 dmac any tag vid 100
```

After specifying the *<matching criteria>* parameter for the QCE, you can begin specifying the QCE *<qce operations>* parameters, as defined in *Configuring QCE Operations ([<qce operations>] Parameter) on page 66*.

NOTE

If you are defining the <matching criteria> based on **frame-type***, continue to Configuring Frame-Type [<matching criteria>] on page 63 for more information and configurable options.*

Configuring Frame-Type [*<matching criteria>*]

The **frame-type** matching criteria for QCEs includes several additional parameters and configuration options. The frame types available to use as matching criteria include specific Ethernet frames, IPv4 and IPv6 packets, LLC frames, and SNAP frames. You can specify additional parameters for each of these options to use as matching criteria for the QCE. The command syntax for specifying matching criteria by frame type appears as follows:

```
(config)#qos qce <qce id> frame-type [any | etype | ipv4 | ipv6 | llc | snap]
```

The syntax of the **frame-type** keywords, and their additional parameters, are defined below:

- **any**: Specifies that matching occurs for traffic of any frame type.
- **etype** *<value>*: Specifies the EtherType frame used for traffic matching. Valid *<value>* ranges are **0x600** to **0x7ff**, **0x801** to **0x86dc**, **0x86de** to **0xfff**.
- **ipv4**: Specifies IPv4 information is used for traffic matching. This frame type has additional configuration parameters for specific IPv4 criteria to use for matching purposes. Refer to *Table 3 on page 64*.
- **ipv6**: Specifies IPv6 information is used for traffic matching. This frame type has additional configuration parameters for specific IPv6 criteria to use for matching purposes. Refer to *Table 3 on page 64*.
- **llc**: Specifies LLC frame information is used for traffic matching. This frame type has additional configuration parameters for specific LLC frame types to use for matching purposes. Refer to *Table 4 on page 65*.
- **snap [***<value>* **| any]**: Specifies SNAP frame information is used for traffic matching. Valid *<value>* range is **0** to **0xfff**. The **any** keyword indicates matching occurs for any SNAP frame.

The following tables display the additional configurable parameters for the IPv4, IPv6, and LLC frame types. These additional parameters are configured after entering the frame type keyword, and can be followed by specifying additional *<actions>*, *<matching criteria>*, or *<qce operations>* parameters.

NOTE

Although the **any**, **etype**, *and* **snap** *keywords do not have any additional configuration parameters, you can also specify additional <actions>, <matching criteria>, or <qce operations> parameters after entering these keywords.*

Table 3. Additional Parameters for IPv4 and IPv6 Frame Type *<matching criteria>*

Keyword	Parameters	Description
dip	[*<ipv4 address> <subnet mask>* | **any**] [*<ipv6 address>* | **any**]	Configures traffic matching based on destination IP address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). IPv4 subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**). IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**. The **any** keyword indicates any destination IP address matches.
dport	[*<port>* | **any**]	Configures traffic matching based on UDP/TCP destination port. Valid *<port>* range is **0** to **65535**. The **any** keyword indicates any destination TCP or UDP port matches.
fragment (Note: Applies to **ipv4** only)	[**any** | **no** | **yes**]	Configures traffic matching based on IPv4 packet fragments. The **any** keyword indicates any IPv4 packet fragment matches. The **no** keyword indicates matches occur only on non-fragmented IPv4 traffic. The **yes** keyword indicates matches occur on IPv4 fragments.

Table 3. Additional Parameters for IPv4 and IPv6 Frame Type *<matching criteria>* (Continued)

Keyword	Parameters	Description
proto	[*<number>* | **any** | **tcp** | **udp**]	Configures traffic matching based on IP protocol. The *<number>* parameter indicates a specific protocol number. Valid range is **0** to **255**. The **any** keyword indicates any IP protocol matches. The **tcp** keyword indicates matches occur on TCP protocol packets. The **udp** keyword indicates matches occur on UDP protocol packets.
sip	[*<ipv4 address> <subnet mask>* | **any**] [*<ipv6 address>* | **any**]	Configures traffic matching based on source IP address. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**). IPv4 subnet masks can be expressed in dotted decimal notation (for example, **255.255.255.0**) or as a prefix length (for example, **/24**). IPv6 addresses should be expressed in colon hexadecimal format (**X:X:X:X::X**), for example, **2001:DB8:1::1**. The **any** keyword indicates any source IP address matches.
sport	[*<port>* | **any**]	Configures traffic matching based on UDP/TCP source port. Valid *<port>* range is **0** to **65535.** The **any** keyword indicates any source TCP or UDP port matches.
<action>	Refer to *Configuring QCE Actions ([<action>] Parameter) on page 61*	Actions can be specified after entering the additional IPv4 or IPv6 traffic matching specifications, without having to use the **action** keyword.
<matching criteria>	Refer to *Configuring QCE Matching Criteria ([<matching criteria>] Parameter) on page 62*	Additional matching criteria can be specified after entering the additional IPv4 or IPv6 traffic matching specifications.
<qce operations>	Refer to *Configuring QCE Operations ([<qce operations>] Parameter) on page 66*	QCE operations can be specified after entering the additional IPv4 or IPv6 traffic matching specifications.

Table 4. Additional Parameters for LLC Frame Type *<matching criteria>*

Keyword	Parameters	Description
control	[*<value>* | **any**]	Configures traffic matching based on LLC control bytes. The <value> parameter specifies a single control byte; valid range is **0** to **0xff**. The **any** keyword indicates any LLC control byte matches.
dsap	[*<value>* | **any**]	Configures traffic matching based on LLC destination SAP bytes. The <value> parameter specifies a single destination SAP byte; valid range is **0** to **0xff**. The **any** keyword indicates any LLC destination SAP byte matches.
ssap	[*<value>* | **any**]	Configures traffic matching based on LLC source SAP bytes. The <value> parameter specifies a single source SAP byte; valid range is **0** to **0xff**. The **any** keyword indicates any LLC source SAP byte matches.

Table 4. Additional Parameters for LLC Frame Type *<matching criteria>* (Continued)

Keyword	Parameters	Description
<action>	Refer to *Configuring QCE Actions ([<action>] Parameter) on page 61*	Actions can be specified after entering the additional LLC traffic matching specifications, without having to use the **action** keyword.
<matching criteria>	Refer to *Configuring QCE Matching Criteria ([<matching criteria>] Parameter) on page 62*	Additional matching criteria can be specified after entering the additional LLC traffic matching specifications.
<qce operations>	Refer to *Configuring QCE Operations ([<qce operations>] Parameter) on page 66*	QCE operations can be specified after entering the additional LLC traffic matching specifications.

Configuring QCE Operations ([*<qce operations>*] Parameter)

QCE operations are values that act on the QCE entry itself, to specify the location of the QCE entry. This parameter is configured by entering one (or more) of the following keywords and their parameters:

- **interface** *<interface>*: Associates the QCE with an interface. The *<interface>* parameter is specified in the format **GigabitEthernet** *<slot/port>* or **10GigabitEthernet** *<slot/port>*.
- **last**: Specifies this QCE is placed at the end of the list of configured QCEs.
- **next** *<qce id>*: Specifies this QCE is placed in the QCE list before the specified QCE ID. Valid *<qce id>* range is **1** to **256**.

To configure a QCE (**5**), that applies CoS and DSCP values to IPv4 traffic with a destination TCP port of **443**, and appears last in the QCE list, enter the command as follows:

```
(config)#qos qce 5 action cos 2 dscp 10 frame-type ipv4 dport 443 last
```

To associate the QCE with an interface, enter the command as follows:

```
(config)#qos qce 5 interface GigabitEthernet 1/1
```

16. Configuring Global Storm Policers via the CLI (Optional)

You can optionally choose to configure global-level storm policers on the ASE device to aid in QoS functionality. Global storm policers apply to the entire switch, and can be used to restrict the amount of flooded frames, those without previously-learned source MAC addresses, from entering the device. Global policers can be configured to limit unicast, multicast, or broadcast packets.

Configure global storm policers by entering the **[no] qos storm [broadcast | multicast | unicast]** *<rate>* **[fps | kbps | kfps | mbps]** command from the Global Configuration mode prompt. The **broadcast**, **multicast**, and **unicast** keywords specify that the policer is applied to broadcast, multicast, or unicast traffic, respectively. The *<rate>* parameter specifies the rate limit of the policer; valid range is **1** to **13128147**. The **fps**, **kbps**, **kfps**, and **mbps** parameters of the command specify the rate unit for the policer, and correspond to frames per second, kilobits per second (default), kiloframes per second, and Megabits per second, respectively. By default, the global storm policer is set to a rate limit **10 fps**.

To configure the QoS global storm policer to limit unicast traffic, enter the command as follows:

```
(config)#qos storm unicast 100 mbps
```

After configuring the global storm policer, the QoS configuration is complete. To view CLI configuration examples, refer to *QoS Configuration Examples Using the CLI on page 67*.

17. QoS Configuration Examples Using the CLI

The example scenarios contained in this section are designed to enhance understanding of QoS configurations on ASE devices. All configurations provided in this section use the CLI.

NOTE

The configuration parameters entered in these examples are sample configurations only. These applications should be configured in a manner consistent with the needs of your particular network. CLI prompts have been removed from the configuration examples to provide a method of copying and pasting configurations directly from this configuration guide into the CLI. These configurations should not be copied without first making the necessary adjustments to ensure they will function properly in your network.

Classifying Ingress Traffic by Class

The following example specifies that all incoming traffic on Port **1** is assigned a CoS value of **2**, and a PCP value of **1**:

```
interface GigabitEthernet 1/1
  qos cos 2
  qos pcp 1
  end
```

Classifying Ingress Traffic by Frame Tags

The following example enables tag classification for ingress traffic on port **2**. In this configuration, traffic with a PCP value of **0** and a DEI value of **0** is assigned the CoS value of **2** and DPL value of **0**, and traffic with a PCP value of **0** and a DEI value of **1** is assigned the CoS value of **3** and DPL value of **1**:

```
interface GigabitEthernet 1/2
  qos trust tag
  qos map tag-cos pcp 0 dei 0 cos 2 dpl 0
  qos map tag-cos pcp 0 dei 1 cos 3 dpl 1
  end
```

QoS Traffic Mapping

The following example maps CoS **2** and DPL **0** values to PCP **3** and DEI **0** values, and CoS **3** and DPL **1** values to PCP **4** and DEI **1** values on port **2**:

```
interface GigabitEthernet 1/2
  qos tag-remark mapped
  qos map cos-tag cos 2 dpl 0 pcp 3 dei 0
  qos map cos-tag cos 3 dpl 1 pcp 4 dei 1
  end
```

Configuring DSCP to QoS Classification

The following example assigns trusted DSCP values **4** and **5** on port **2** to CoS class **6**:

```
interface GigabitEthernet 1/2
  qos trust dscp
  exit
```

```
!
qos map dscp-cos 4 cos 6 dpl 0
qos map dscp-cos 5 cos 6 dpl 0
end
```

Configuring DSCP Translation for Ingress Traffic

The following example enables translation of DSCP values for ingress traffic on port **2**, enables rewriting of DSCP values for egress traffic on port **3**, and creates a DSCP translation map for ingress traffic that maps DSCP values of **1** and **2** to DSCP values of **5** and **6**, respectively:

```
interface GigabitEthernet 1/2
  qos trust dscp
  qos dscp-translate
  exit
!
interface GigabitEthernet 1/3
  qos trust dscp
  qos dscp-remark rewrite
  exit
!
qos map dscp-ingress-translation 1 to 5
qos map dscp-ingress-translation 2 to 6
!
```

Configuring Queue Shaper to Measure Data Rate

The following example configures shaping for Queues **3** and **4** at different rates on port **3**. The queues are also configured to measure data rates instead of line rates.

```
interface GigabitEthernet 1/3
  qos queue-shaper queue 3 4 mbps rate-type data
  qos queue-shaper queue 4 8 mbps rate-type data
  end
```

Configuring WRED Maximum Threshold

The following example configures WRED on Group **1**, Queue **4**, and DPL **1** with a minimum threshold of **10** percent and maximum threshold of **50** percent:

```
qos wred group 1 queue 4 dpl 1 min-fl 10 max 50
```

NOTE

Please note that ports are in WRED Group 1 by default. This is why further configuration is not necessary.

Configuring the QoS Ingress Map

The following example configures QoS ingress map **20** with the following characteristics:

- Tagged frames with PCP **0-3** are mapped to CoS **0** and CoS ID **0** (default mapping).
- Tagged frames with PCP **4-7** are mapped to CoS **1** and CoS ID **1**.

The map is then applied to ports **1** and **2**, and associated with QCE **123**, which matches all traffic from all ports where the destination MAC address is a multicast address.

```
qos map ingress 20
  action cos class
  map pcp 4 to class 1 cos 1
  map pcp 5 to class 1 cos 1
  map pcp 6 to class 1 cos 1
  map pcp 7 to class 1 cos 1
  exit
!
interface GigabitEthernet 1/1-2
  qos ingress-map 20
  exit
!
qos qce 123 dmac multicast action ingress-map 20
end
```

Configuring the QoS Egress Map

The following example creates QoS egress map **40** with the following characteristics:

- PCP is set to **7** and DSCP to **46** on frames classified to CoS ID **1**.
- PCP and DSCP are set to **0** on frames classified to all other CoS ID values (default mapping).

The map is then applied to ports **1** and **2**.

```
qos map egress 40
  action dscp pcp
  map class 1 to dscp 46 pcp 7
  exit
!
interface GigabitEthernet 1/1-2
  qos egress-map 40
  end
```

18. QoS Configuration Command Summary

The following tables summarize the commands used in conjunction with QoS configurations on the ASE device.

Table 5. QoS Ingress Configuration Commands

Prompt	Command	Description
(config-if)#	**[no] qos cos** *<value>*	Specifies the CoS classification for all incoming traffic on the port. Valid *<value>* range is **0** to **7**, with a default value of **0**. Using the **no** form of the command returns the CoS classification to the default value.
(config-if)#	**[no] qos class** *<id>*	Specifies the CoS ID for all incoming traffic on the port. Valid *<value>* range is **0** to **7**, with a default value of **0**. Using the **no** form of the command returns the CoS ID to the default value.

Table 5. QoS Ingress Configuration Commands (Continued)

Prompt	Command	Description
(config-if)#	**[no] qos dei** *<value>*	Specifies the DEI bit for incoming traffic on the port. Valid *<value>* range is **0** to **1**. Using the **no** form of the command returns the DEI value to the default setting.
(config-if)#	**[no] qos dpl** *<value>*	Specifies the DPL value assigned to incoming traffic on the port. Valid *<value>* range is **0** to **3**. Using the **no** form of the command returns the DPL value to the default setting.
(config-if)#	**[no] qos pcp** *<value>*	Specifies the PCP value assigned to incoming traffic on the port. Valid *<value>* range is **0** to **7**. Using the **no** form of the command returns the PCP value to the default setting.
(config-if)#	**[no] qos map [cos-tag cos** *<value>* **dpl** *<value>* **pcp** *<value>* **dei** *<value>***| tag-cos pcp** *<value>* **dei** *<value>* **cos** *<value>* **dpl** *<value>***]**	Specifies the per-port mapping settings for Cos-to-Tag mapping (cos-tag parameter) or for Tag-to-CoS mapping (tag-cos parameter). Using the **no** form of the command removes the map configuration from the port. Valid **cos** *<value>* range is **0** to **7**. Valid **dpl** *<value>* range is **0** to **3**. Valid **pcp** *<value>* range is **0** to **7**. Valid **dei** *<value>* range is **0** to **1**.
(config-if)#	**[no] qos wred-group** *<group id>*	Specifies the WRED group assigned to incoming traffic on the port. Valid *<group id>* range is **1** to **3**. Using the **no** form of the command removes the WRED group from the port's configuration.
(config-if)#	**[no] qos ingress-map** *<map id>*	Specifies the QoS ingress map assigned to the port. Valid *<map id>* range is **0** to **127**. Using the **no** form of the command removes the map from the port's configuration.
(config-if)#	**[no] qos egress-map** *<map id>*	Specifies the QoS egress map assigned to the port. Valid *<map id>* range is **0** to **255**. Using the **no** form of the command removes the map from the port's configuration.

Table 6. QoS Ingress Map Configuration Commands

Prompt	Command	Description
(config)#	**[no] qos map ingress** *<map id>*	Creates a QoS ingress map and enters the map's configuration mode. Valid *<map id>* range is **0** to **127**. Using the **no** form of the command removes the map from the device's configuration.
(config-qos-map-ingress)#	**[no] key [dscp | dscp-pcp-dei | pcp | pcp-dei]**	Specifies the packet header value used for traffic matching in the ingress map. The **dscp** parameter specifies the frame's DSCP value is used for matching. The **dscp-pcp-dei** parameter specifies the frame's DSCP value is used for matching IP frames, and that PCP and DEI values are used for matching non-IP frames. The **pcp** parameter specifies the traffic's PCP value is used for matching. The **pcp-dei** parameter specifies that both the PCP and DEI values are used for matching. Using the **no** form of the command removes the criteria from the map's configuration.

Table 6. QoS Ingress Map Configuration Commands (Continued)

Prompt	Command	Description
(config-qos-map-ingress)#	**[no] action [class | cos | dei | dpl | dscp | path | pcp]**	Enables the classification action performed on traffic that matches the map's criteria. The **class** parameter enables CoS ID classification, the **cos** parameter enables CoS value classification, the **dei** parameter enables DEI classification, the **dpl** parameter enables DPL classification, the **dscp** parameter enables DSCP classification, the **path** parameter enables path CoS ID classification, and the **pcp** parameter enables PCP classification. Using the **no** form of the command removes the criteria from the map's configuration.
(config-qos-map-ingress)#	**[no] map dscp** *<value>* **to [class** *<id>* **| cos** *<value>* **| dei** *<value>* **| dpl** *<value>* **| dscp** *<value>* **| path-cosid** *<id>* **| pcp** *<value>***]**	Specifies the newly assigned values for traffic matching the specified DSCP values. To assign these new values, the same parameters must first be enabled using the **action** command from the map's configuration mode prompt. Valid **dscp** *<value>* range is **0** to **63**. Valid **class** *<id>* range is **0** to **7**. Valid **cos** *<value>* range is **0** to **7**. Valid **dei** *<value>* range is **0** to **1**. Valid **dpl** *<value>* range is **0** to **7**. Valid **path-cosid** *<id>* range is **0** to **1**. Valid **pcp** *<value>* range is **0** to **7**. Using the **no** form of the command removes the criteria from the map's configuration.
(config-qos-map-ingress)#	**[no] map pcp** *<value>* **[dei** *<value>***] to [class** *<id>* **| cos** *<value>* **| dei** *<value>* **| dpl** *<value>* **| dscp** *<value>* **| path-cosid** *<id>* **| pcp** *<value>***]**	Specifies the newly assigned values for traffic matching the specified PCP value, or optionally both PCP and DEI values. To assign these new values, the same parameters must first be enabled using the **action** command from the map's configuration mode prompt. Valid **pcp** *<value>* range is **0** to **7**. Valid **dei** *<value>* range is **0** to **1**. Valid **class** *<id>* range is **0** to **7**. Valid **cos** *<value>* range is **0** to **7**. Valid **dpl** *<value>* range is **0** to **7**. Valid **dscp** *<value>* range is **0** to **63**. Valid **path-cosid** *<id>* range is **0** to **1**. Valid **pcp** *<value>* range is **0** to **7**. Using the **no** form of the command removes the criteria from the map's configuration.
(config-qos-map-ingress)#	**[no] preset classes** *<number>* **[color-aware]**	Applies the ingress map to a specific number of traffic classes. Valid *<number>* range is **1** to **8**. The optional **color-aware** parameter enables color awareness for traffic intercepted by the ingress map; this feature is disabled by default. Using the **no** form of the command removes the criteria from the map's configuration.

Table 7. QoS Queue Configuration Commands

Prompt	Command	Description
`(config-if)#`	**[no] qos queue-policer queue** *<queue> <rate>* **[kbps | mbps]**	Configures a queue policer on a per-port basis. Queue policers limit the bandwidth of received frames that exceed configured rates for the port. Valid *<queue>* range is **0** to **7**, and specifies the queue ID to which the policer applies. Valid *<rate>* range is **1** to **13128147**. The **kbps** and **mbps** parameters specify the unit of measurement for the rate of the policer, and correspond to kilobits per second and Megabits per second, respectively. By default, the policer rate is set to **500 kbps**. Using the **no** form of the command removes the queue policer from the queue's configuration.
`(config-if)#`	**[no] qos queue-shaper queue** *<queue> <rate>* **[kbps | mbps] rate-type [data | line]**	Configures a queue shaper on a per-port basis. Queue shapers limit the bandwidth and traffic flow parameters of egress traffic on the port. Valid *<queue>* range is **0** to **7**, and specifies the queue ID to which the shaper applies. Valid *<rate>* range is **1** to **13107100**. The **kbps** and **mbps** parameters specify the unit of measurement for the rate of the shaper, and correspond to kilobits per second and Megabits per second, respectively. By default, the shaper rate is set to **500 kbps**. The **rate-type** parameter specifies whether data rate (**data** keyword) or line rate (**line** keyword) is being shaped. Using the **no** form of the command removes the queue shaper from the queue's configuration.
`(config)#`	**[no] qos wred-group** *<group id>* **queue** *<queue>* **dpl** *<value>* **min-fl** *<number>* **max** *<number>* **[fill-level]**	Configures the WRED functionality for queues on the ASE device. The **group** *<group id>* parameter specifies the WRED group ID; valid range is **1** to **3**. The **queue** *<queue>* parameter specifies the queue to which the WRED group is applied; valid range is **0** to **7**. The **dpl** *<value>* parameter associates a DPL with the queue, and is used by default as the fill maximum value for the queue; valid range is **1** to **3**. The **min-fl** *<number>* parameter specifies the minimum fill level (in percent) of the queue; valid range is **0** to **100** percent. The **max** *<number>* parameter specifies the maximum threshold (in percent) for the queue; valid range is **1** to **100** percent. The optional **fill-level** parameter specifies that packets are not dropped until the fill level of the queue is reached. By default, the queue uses the DPL setting to determine when packets begin to drop from the queue. Using the **no** form of the command removes the WRED group from the ASE device configuration.

Table 8. QoS Policer Configuration Commands

Prompt	Command	Description
(config)#	**[no] qos storm [broadcast | multicast | unicast]** *<rate>* **[fps | kbps | kfps | mbps]**	Configures the global storm policer on the ASE device. The storm policer restricts the amount of flooded frames from entering the switch. The **broadcast**, **multicast**, and **unicast** parameters specify whether the policer is applied to broadcast, multicast, or unicast traffic, respectively. The *<rate>* parameter specifies the rate limit of the policer; valid range is **1** to **13128147**. The optional **fps**, **kbps**, **kfps**, **mbps** parameters specify the unit of measurement for the rate (frames per second, kilobits per second, kiloframes per second, and Megabits per second, respectively). By default, the policer rate is set to **10 fps**. Using the **no** form of the command removes the policer from the switch's configuration.
(config-if)#	**[no] qos policer** *<rate>* **[flowcontrol] [fps | kbps | kfps | mbps]**	Configures and assigns a QoS policer to the port. Valid *<rate>* range is **1** to **13128147**. The optional **fps**, **kbps**, **kfps**, **mbps** parameters specify the unit of measurement for the rate (frames per second, kilobits per second, kiloframes per second, and Megabits per second, respectively). By default, the policer rate is set to **500 kbps**. The optional **flowcontrol** parameter enables flow control for the policer; this feature is disabled by default. Using the **no** form of the command removes the policer from the port's configuration.

Table 9. QoS Egress Configuration Commands

Prompt	Command	Description
(config-if)#	**[no] qos wrr** *<Q0 weight> <Q1 weight> <Q2 weight> <Q3 weight> <Q4 weight> <Q5 weight> <Q6 weight> <Q7 weight>*	Configures DWRR port scheduling for egress traffic. Each *<weight>* parameter assigns a weight, from **1** to **100** to each queue (Q0 through Q7). The higher the weight, the higher the priority of the queue. Using the **no** form of the command removes the configured weight from the queue.
(config-if)#	**[no] qos shaper** *<rate>* **[kbps | mbps] [rate-type [data | line]]**	Configures a shaper on a per-port basis for egress traffic. Valid *<rate>* range is **1** to **13107100**. The **kbps** and **mbps** parameters specify the unit of measurement for the rate of the shaper, and correspond to kilobits per second and Megabits per second, respectively. By default, the shaper rate is set to **500 kbps**. The optional **rate-type** parameter specifies whether data rate (**data** keyword) or line rate (**line** keyword) is being shaped. Using the **no** form of the command returns the port shaper configuration to the default value.
(config-if)#	**[no] qos tag-remark [mapped | pcp <***value>* **dei** *<value>***]**	Applies previously configured mapped, or default PCP and DEI, values to tags on egress traffic. The **mapped** keyword specifies that tag remarking occurs using previously mapped CoS/DPL to PCP/DEI values. The **pcp** *<value>* **dei** *<value>* parameters specify that tag remarking occurs on egress traffic using the PCP and DEI settings specified with this command. Valid range for PCP values is **0** to **7**, and valid range of DEI values is **0** to **1**. Using the **no** form of the command disables tag remarking for egress traffic on the port.

Table 10. QoS Egress Map Configuration Commands

Prompt	Command	Description
(config)#	**[no] qos map egress** *<map id>*	Creates a QoS egress map and enters the map's configuration mode. Valid *<map id>* range is **0** to **255**. Using the **no** form of the command removes the map from the device's configuration.
(config-qos-map-egress)#	**[no] key [class | class-dpl | dscp | dscp-dpl]**	Specifies the packet header value used for traffic matching in the egress map. The **class** parameter specifies the frame's CoS ID is used for matching. The **class-dpl** parameter specifies the packet's CoS ID and DPL value are used for matching. The **dscp** parameter specifies the frame's DSCP value is used for matching. The **dscp-dpl** parameter specifies that both the DSCP and DPL values are used for matching. Using the **no** form of the command removes the criteria from the map's configuration.
(config-qos-map-egress)#	**[no] action [dei | dscp | path | pcp]**	Enables the rewriting action performed on traffic that matches the map's criteria. The **dei** parameter allows DEI values to be rewritten, the **dpl** parameter allows DPL values to be rewritten, the **dscp** parameter allows DSCP values to be rewritten, the **path** parameter allows path CoS ID values to be rewritten, and the **pcp** parameter allows PCP values to be rewritten. Using the **no** form of the command removes the criteria from the map's configuration.
(config-qos-map-egress)#	**[no] map class** *<id>* **[dpl** *<value>***] to [dei** *<value>* **| dscp** *<value>* **| path-cosid** *<id>* **| pcp** *<value>***]**	Specifies the newly assigned values for traffic matching the specified CoS ID, or optionally both CoS ID and DPL values. To assign these new values, the same parameters must first be enabled using the **action** command from the map's configuration mode prompt. Valid **class** *<id>* range is **0** to **7**. Valid **dpl** *<value>* range is **0** to **7**. Valid **dei** *<value>* range is **0** to **1**. Valid **dscp** *<value>* range is **0** to **63**. Valid **path-cosid** *<id>* range is **0** to **1**. Valid **pcp** *<value>* range is **0** to **7**. Using the **no** form of the command removes the criteria from the map's configuration.
(config-qos-map-egress)#	**[no] map dscp** *<value>* **[dpl** *<value>***] to [dei** *<value>* **| dscp** *<value>* **| path-cosid** *<id>* **| pcp** *<value>***]**	Specifies the newly assigned values for traffic matching the specified DSCP value, or optionally both DSCP and DPL values. To assign these new values, the same parameters must first be enabled using the **action** command from the map's configuration mode prompt. Valid **dscp** *<value>* range is **0** to **63**. Valid **dpl** *<value>* range is **0** to **7**. Valid **dei** *<value>* range is **0** to **1**. Valid **path-cosid** *<id>* range is **0** to **1**. Valid **pcp** *<value>* range is **0** to **7**. Using the **no** form of the command removes the criteria from the map's configuration.
(config-qos-map-egress)#	**[no] preset classes** *<number>* **[color-aware]**	Applies the egress map to a specific number of traffic classes. Valid *<number>* range is **1** to **8**. The optional **color-aware** parameter enables color awareness for traffic intercepted by the egress map; this feature is disabled by default. Using the **no** form of the command removes the criteria from the map's configuration.

Table 11. QoS DSCP Configuration Commands

Prompt	Command	Description
(config-if)#	**[no] qos dscp-translate**	Enables DSCP translation for ingress traffic on the port. Using the **no** form of the command disables the DSCP translation feature.
(config-if)#	**[no] qos dscp-classify [any | selected | zero]**	Enables DSCP classification for ingress traffic on the port. The **any** parameter specifies that all incoming traffic always classified to a new DSCP value. The **selected** parameter specifies that incoming traffic with DSCP values for which classification is enabled (via the global DSCP classify map) are classified to new DSCP values. The **zero** parameter specifies that incoming traffic is classified to a new DSCP value if the current DSCP value is **zero**. Using the **no** form of the command disables the DSCP classification feature.
(config-if)#	**[no] qos dscp-remark [remap | rewrite]**	Enables rewriting and remapping of egress traffic on the port. The **remap** parameter specifies that the DSCP field of egress traffic is rewritten using classified DSCP values that have been mapped through the global DSCP egress translation map. The **rewrite** parameter specifies that the DSCP field of egress traffic is rewritten with a classified DSCP value without any DSCP translation. Using the **no** form of the command disables the DSCP rewriting and remapping feature.
(config)#	**[no] qos map dscp-classify** *<dscp value>*	Specifies that a DSCP value is classified and trustworthy and can be used by other QoS processes, such as ingress traffic classification and egress traffic rewriting. The *<dscp value>* parameter specifies the classified and trusted DSCP value; valid range is **0** to **63**. Enter the command multiple times to specify more than one trusted DSCP value. Using the **no** form of the command removes the DSCP value from the DSCP classification table.
(config)#	**[no] qos map dscp-ingress-translation** *<dscp value>* **to** *<dscp value>*	Specifies DSCP translation values for ingress traffic when DSCP translation is enabled on the port. The *<dscp value>* parameters specify which DSCP values are being translated to which other DSCP values. Valid *<dscp value>* range is **0** to **63**. Using the **no** form of the command removes the DSCP values from DSCP translation.
(config)#	**[no] qos map dscp-egress-translation** *<dscp value>* **to** *<dscp value>*	Specifies DSCP translation values for egress traffic when DSCP translation is enabled for remapping values of egress traffic on the port. The *<dscp value>* parameters specify which DSCP values are being translated to which other DSCP values. Valid *<dscp value>* range is **0** to **63**. Using the **no** form of the command removes the DSCP values from DSCP translation.
(config-if)#	**[no] qos trust [dscp | tag]**	Specifies that ingress traffic with DSCP values defined in the DSCP to CoS map are trusted (**dscp** keyword) or that ingress traffic tagged with VLAN IDs defined in the CoS to DSCP map are trusted (**tag** keyword). Using the **no** form of the command disables trust for DSCP and/or VLAN tagged incoming traffic.

Table 11. QoS DSCP Configuration Commands (Continued)

Prompt	Command	Description
(config)#	**[no] qos map cos-dscp** *<value>* **dpl** *<value>* **dscp** *<value>*	Configures the global CoS to DSCP mapping parameters. The **cos-dscp** *<value>* parameter specifies the CoS class value being mapped to the DSCP value; valid range is **0** to **7**. The **dpl** *<value>* parameter defines the DPL value associated with the CoS class; valid range is **0** to **3**. The **dscp** *<value>* parameter specifies the DSCP value that will be associated with the CoS class; valid range is **0** to **63**. Using the **no** form of the command removes the specified CoS to DSCP mapping from the switch.
(config)#	**[no] qos map dscp-cos** *<value>* **cos** *<value>* **dpl** *<value>*	Configures the global DSCP to CoS mapping parameters. The **dscp-cos** *<value>* parameter specifies the DSCP value being mapped to the CoS class value; valid range is **0** to **63**. The **cos** *<value>* parameter defines the CoS class value that will be associated with the DSCP value; valid range is **0** to **7**. The **dpl** *<value>* parameter specifies the DPL value that is associated with the CoS class; valid range is **0** to **3**. Using the **no** form of the command removes the specified DSCP to CoS mapping from the switch.

Table 12. QoS QCE Configuration Commands

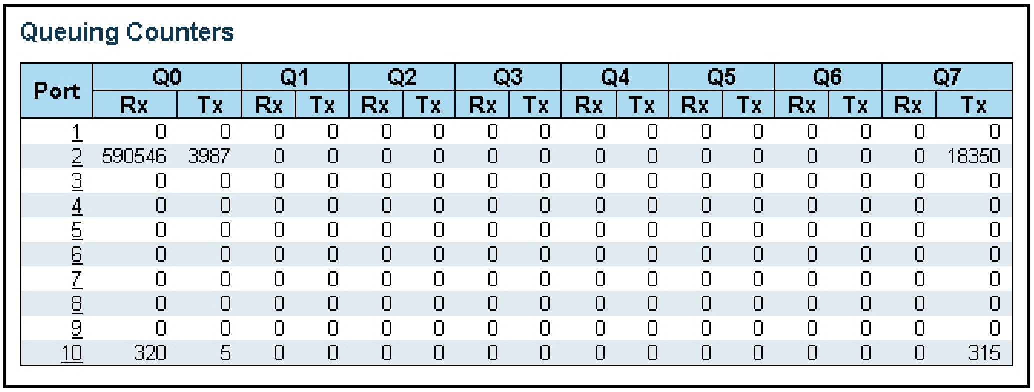
Prompt	Command	Description
(config)#	**[no] qos qce** *<qce id>* **[action** *<action>***]** **[***<matching criteria>***]** **[***<qce operation>***]**	Creates a QoS control list entry (QCE) that defines QoS actions (**action** *<action>*) taken on traffic that matches certain criteria (*<matching criteria>*), and configures where the QCE appears in the QCE list (*<qce operation>*). The *<qce id>* parameter specifies the QCE ID; valid range is **1** to **256**. The **qos qce** command configures all parameters of the QCE in a single command. For all available parameters and their details, refer to *Configuring the QoS Control List via the CLI (Optional) on page 60*.

19. Troubleshooting

You can view several types of QoS statistics on the ASE device that can aid in troubleshooting QoS configurations. Port and QoS statistics can be used to aid in debug procedures and other troubleshooting measures. QoS statistics and configurations can be viewed using either the GUI or the CLI.

Viewing QoS Statistics Using the GUI

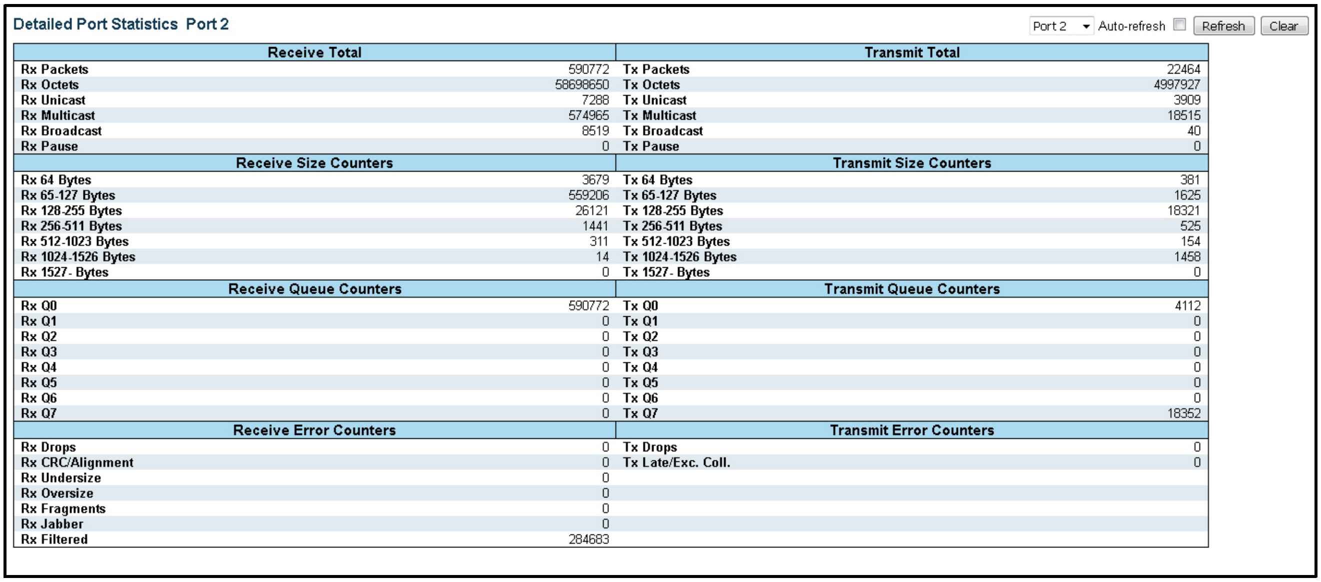
Detailed information about ports on which queues are configured can be viewed by navigating to the **Monitor** tab and selecting **Ports** > **QoS Statistics**. Queue information, such as packets received and transmitted in each queue, are displayed in the **Queuing Counters** menu.



Queuing Counters

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	590546	3987	0	0	0	0	0	0	0	0	0	0	0	0	0	18350
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	320	5	0	0	0	0	0	0	0	0	0	0	0	0	0	315

If you select a port from the list in the **Queuing Counter** menu, the **Detailed Port Statistics** menu is displayed for the chosen port. This menu displays specific traffic information for the port, including transmitted and received packet information, queue counters and statistics, and traffic errors.



Detailed Port Statistics Port 2

Receive Total		Transmit Total	
Rx Packets	590772	Tx Packets	22464
Rx Octets	58698650	Tx Octets	4997927
Rx Unicast	7288	Tx Unicast	3909
Rx Multicast	574965	Tx Multicast	18515
Rx Broadcast	8519	Tx Broadcast	40
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	3679	Tx 64 Bytes	381
Rx 65-127 Bytes	559206	Tx 65-127 Bytes	1625
Rx 128-255 Bytes	26121	Tx 128-255 Bytes	18321
Rx 256-511 Bytes	1441	Tx 256-511 Bytes	525
Rx 512-1023 Bytes	311	Tx 512-1023 Bytes	154
Rx 1024-1526 Bytes	14	Tx 1024-1526 Bytes	1458
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	590772	Tx Q0	4112
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	18352
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	284683		

Viewing QoS Statistics and Configurations Using the CLI

The CLI can also be used to view various QoS statistics, including QoS configurations on a per-port basis, QoS map configurations, QCE configurations, storm policer configurations and statistics, and WRED statistics. Use the following **show** commands to view QoS information in the CLI. All **show** commands are entered from the Enable mode prompt.

NOTE

The output of all **show** *commands can be limited by appending the following modifiers to the end of the command:* **| begin** *<text>*, **| exclude** *<text>, and* **| include** *<text>. The* **include** *modifier limits output to lines that contain the specified text, the* **exclude** *modifier excludes any lines with the specified text, and the* **begin** *modifier displays the first line of output with the specified text and all lines thereafter.*

Use the **show qos interface [* | gigabitethernet | 10gigabitethernet]** *<slot/port>* command to display QoS configurations on a per-port basis. Enter the command from the Enable mode prompt as follows:

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

Use the **show qos maps [cos-dscp | dscp-classify | dscp-cos | dscp-egress-translation | dscp-ingress-translation | egress | ingress]** command to display QoS map configurations. The **cos-dscp** parameter displays configured CoS to DSCP maps, the **dscp-classify** parameter displays configured DSCP classification maps for ingress traffic, the **dscp-cos** parameter displays configured DSCP to CoS maps, the **dscp-egress-translation** and **dscp-ingress-translation** parameters display configured DSCP translation maps for ingress or egress traffic are displayed, and the **egress** and **ingress** parameters display configured QoS egress or ingress maps.

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

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

Use the **show qos qce [**_<qce id>_**]** command to display all configured QCEs. The optional _<qce id>_ parameter limits output to a single QCE. Valid range is **1** to **256**. The following is sample output from the **show qos qce** command:

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

Use the **show qos storm** command to display configured QoS storm policer. Enter the command as follows from the Enable mode prompt:

```
#show qos storm
```

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

Use the **show qos wred** command to display any WRED configurations and statistics. Enter the command as follows from the Enable mode prompt:

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

20. Additional QoS Information

The following sections describe in detail the function of several QoS features, including DSCP values and WRED queue management.

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 bits shown in *Figure 3*:

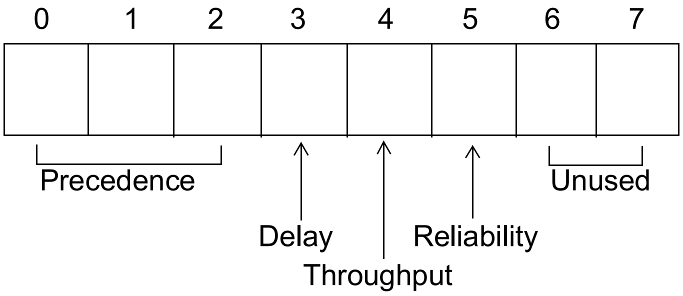


Figure 3. Type of Service Field Bits

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

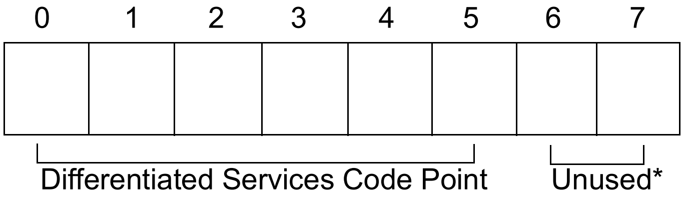
Table 13. IP Precedence Values

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

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 bits as shown in *Figure 4*:



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

Figure 4. 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 to 0. This compatibility requires DiffServ nodes to provide the same data services as are provided by nodes implementing IP precedence. *Table 14* provides a comparison of IP precedence values to their corresponding DSCP values.

Table 14. 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 15*).

Table 15. 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 16*.

Table 16. Assured Forwarding PHB Subclasses

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

Table 17 lists the AF PHB subclasses and their corresponding DSCP bits and values.

Table 17. 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

Table 17. Assured Forwarding PHB Subclasses and Corresponding DSCP Values

Class	Subclass	DSCP Bits	DSCP Value
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 18* provides the command line interface (CLI) entries to use when entering AF values and their corresponding DSCP value.

Table 18. Assured Forwarding DSCP Values

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

WRED Queue Management

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, the ASE device 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). 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 5 on page 85 illustrates queue management when no congestion is present. Ingress packets are queued and transmitted in a FIFO manner.

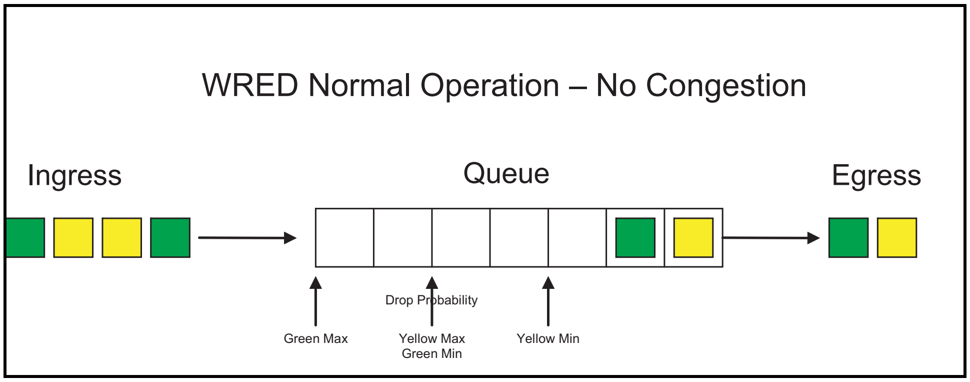


Figure 5. WRED Queue, No Congestion

Figure 6 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.

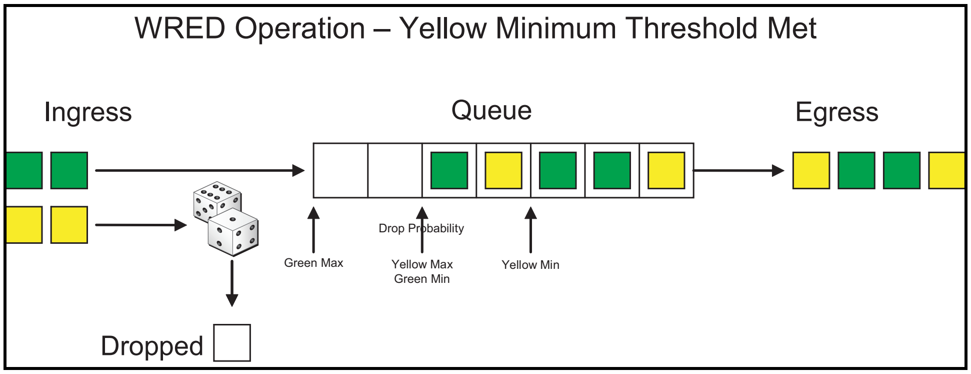


Figure 6. WRED Queue Yellow Minimum Threshold

Figure 7 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.

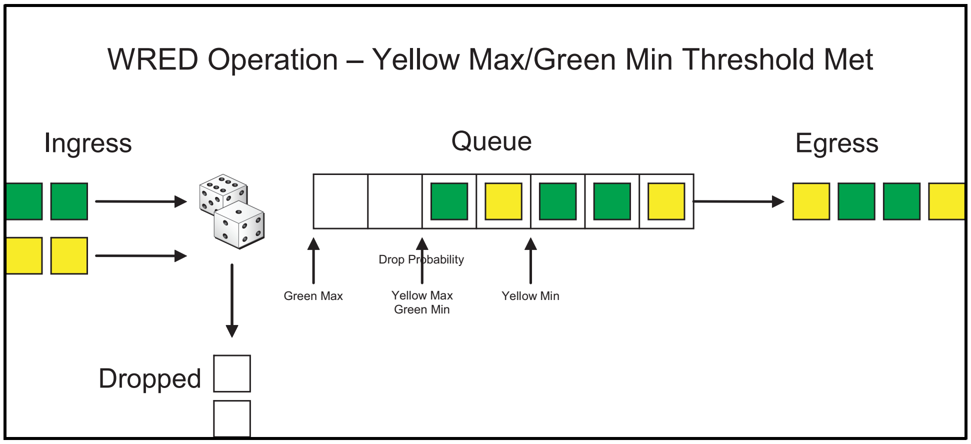


Figure 7. WRED Queue Yellow Maximum and Green Minimum Threshold

In *Figure 8*, once the maximum configured green threshold is reached, all packets are discarded until congestion is relieved.

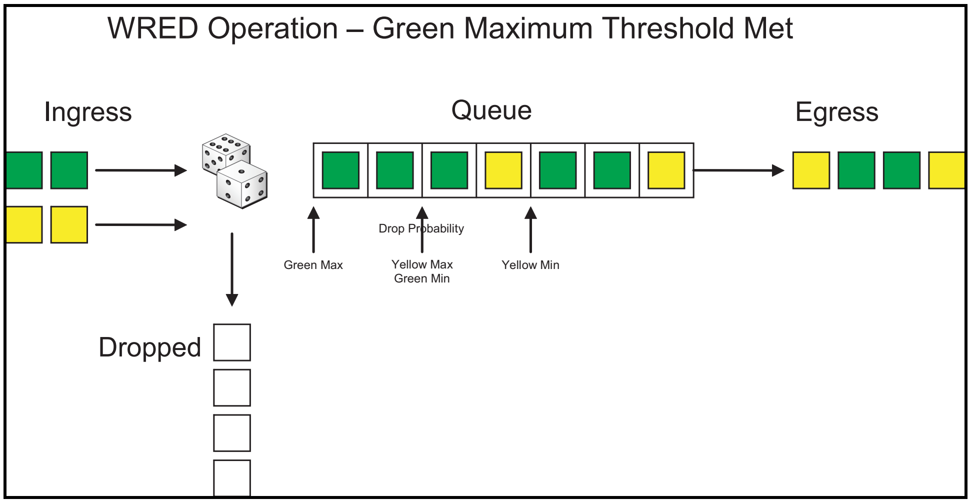


Figure 8. WRED Queue Green Maximum Threshold

NOTE

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

Figure 9 on page 87 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.

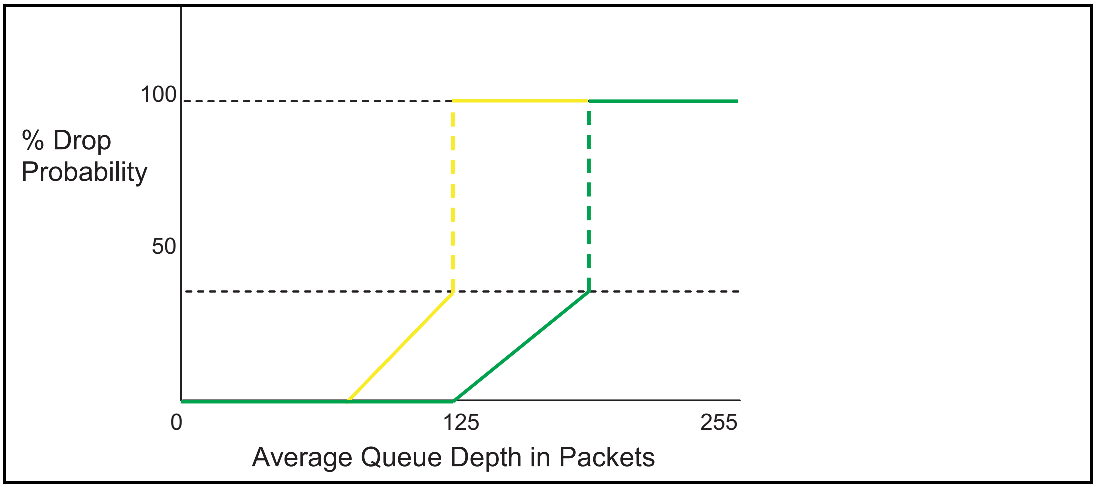


Figure 9. Drop Probability for WRED Slopes

NOTE

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

21. Warranty and Contact Information

Warranty

Warranty information can be found at:

www.adtran.com/warranty.

Contact Information

For all customer support inquiries, please contact ADTRAN Customer Care:

Contact	Support	Contact Information
Customer Care	From within the U.S. From outside the U.S. Technical Support: • Web: Training: • Email: • Web:	1-888-4ADTRAN (1-888-423-8726) + 1 (256) 963-8716 www.adtran.com/support training@adtran.com www.adtran.com/training www.adtranuniversity.com
Sales	Pricing and Availability	1-800-827-0807