Configuration — Quality of Service Avaya Ethernet Routing Switch 4500 Series

5.4
NN47205-504, 06.03
May 2011

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: New in this release....9
- Navigation....9
- Features....9
  - Enterprise Device Manager....9
  - Automatic QoS 802.1AB MED interoperability....10
  - Automatic QoS and ADAC interoperability....10
  - QoS Queue Set Support....10
  - QoS agent disable or enable....10
  - QoS traffic profile filter set support....11
  - QoS Egress Queue Shaping....11
  - QoS DSCP mutation....12
  - QoS IP and L2 Filter Options....12
- Other changes....13
  - Multiple Port Configuration....13
  - Precedence limitations....13

Chapter 2: Introduction....15
- ACLI command modes....15
- Navigation....16

Chapter 3: Policy-based Network Fundamentals....17
- Policy-based networks....17
  - Port-based and Role-based QoS policies....17
- QoS overview....18
- DiffServ Concepts....18
- QoS components....19
- Automatic QoS....20
- Automatic QoS 802.1AB MED interoperability....21
- Automatic QoS and ADAC interoperability....21
- Specifying interface groups....21
- Interface shaping....22
- Egress queue shaping....22
- ADAC for Avaya IP phones....23
- NSNA solution....23
- Rules....24
  - Classifier definition....24
  - IP classifier elements....25
  - Layer 2 classifier elements....26
  - System classifier elements....26
  - Classifiers and classifier blocks....27
- QoS traffic profile filter sets....28
  - Traffic profile filter set metering....29
- Specifying actions....29
- Specifying interface action extensions....31
- Specifying meters....32
- Trusted, untrusted, and unrestricted interfaces....33
  - QoS DSCP mutation....35
- Specifying policies....36

Packet flow using QoS....37
Queue sets....39
Modifying CoS-to-queue priorities....40
QoS configuration guidelines....40
QoS agent disable or enable....42

Chapter 4: Configuring Quality of Service using ACLI....43
Viewing QoS Parameters using ACLI....43
Configuring QoS Access Lists....47
Assigning ports to an access list....47
Creating an IP access list....48
Creating a Layer 2 access list....49
Configuring the CoS-to-Queue Assignments....51
Configuring CoS-to-Queue assignments....51
Configuring QoS Interface Groups....52
Adding ports to an interface group....52
Creating an interface group....52
DSCP and 802.1p and queue association configuration using ACLI....53
Configuring egress mapping using ACLI....53
Resetting egress mapping values....54
Configuring ingress mapping values....55
Resetting ingress mapping values....55
Configuring QoS for the NSNA solution....55
Configuring QoS for NSNA filters....56
Deleting a classifier, classifier block, or an entire filter set....59
QoS IP classifier element management using ACLI....60
Configuring an IP classifier element using ACLI....60
Deleting an IP classifier element using ACLI....62
Viewing IP classifier element information using ACLI....62
QoS L2 classifier element management using ACLI....63
Configuring a Layer 2 classifier element using ACLI....63
Deleting a Layer 2 classifier element using ACLI....65
Viewing Layer 2 classifier element information using ACLI....66
QoS system classifier element management using ACLI....66
Configuring a QoS system classifier element using ACLI....66
Deleting a QoS system classifier element using ACLI....68
Viewing system classifier element information using ACLI....69
QoS classifier management using ACLI....69
Configuring a QoS classifier using ACLI....69
Deleting a QoS classifier using ACLI....70
Viewing QoS classifier information using ACLI....71
QoS classifier block management using ACLI....72
Configuring classifier block entries using ACLI....72
Deleting a classifier block entry using ACLI....73
Viewing a classifier block entry using ACLI....74
QoS traffic profile filter set configuration using ACLI....74
Configuring a QoS traffic profile filter set classifier using ACLI....75
Deleting a QoS traffic profile filter set classifier using ACLI....78
Configuring a QoS traffic profile filter set using ACLI....79
Disabling a QoS traffic profile filter set using ACLI....81
Viewing QoS traffic profile filter set classifier information using ACLI....82

Viewing QoS traffic profile filter set information using ACLI....82
Viewing QoS traffic profile filter set interface information using ACLI....83
Viewing QoS traffic profile filter set statistics information using ACLI....83
Configuring QoS actions....84
Configuring interface action extension entries....86
Configuring QoS meters....87
Configuring QoS Interface Shaper....88
Creating a QoS interface queue shaper using ACLI....89
Deleting a QoS interface queue shaper using ACLI....90
Viewing QoS interface queue shaper information using ACLI....91
Configuring QoS Policies....92
Maintaining the QoS agent using ACLI....93
Enabling the QoS agent using ACLI....94
Disabling the QoS agent using ACLI....94
Configuring QoS resource buffer sharing using ACLI....94
Changing the QoS resource buffer size to default using ACLI....95
Configuring Automatic QoS support using ACLI....95
Configuring NVRAM parameters using ACLI....96
Resetting NVRAM parameters using ACLI....96
Changing the QoS CoS queue set using ACLI....97
Changing the QoS CoS queue set to default using ACLI....97
Changing the QoS agent to factory defaults using ACLI....98
Configuring QoS statistics tracking using ACLI....98
Changing QoS statistics tracking to default using ACLI....99
Viewing QoS agent configuration information using ACLI....99
Viewing QoS agent configuration details using ACLI....99

Chapter 5: Configuring Quality of Service using Enterprise Device Manager....101

Prerequisites....101
Displaying interface queues using EDM....101
Interface group configuration using EDM....102
Displaying interface groups using EDM....103
Deleting ports from an interface group using EDM....104
Adding interface groups using EDM....104
Deleting interface groups using EDM....105
Assigning ports to an interface group using EDM....105
Interface ID configuration using EDM....106
Displaying an interface ID using EDM....106
Filtering Interface ID Assignments table using EDM....107
Displaying priority queue assignments using EDM....108
Displaying priority mapping using EDM....109
Egress mapping configuration using EDM....109
Viewing egress mapping information using EDM....110
Configuring egress mapping using EDM....111
Displaying Meter Capability using EDM....112
Displaying Shaper Capability using EDM....113
QoS IP classifier element management using EDM....113
Viewing IP classifier element configuration using EDM....114
Creating an IP classifier element using EDM....116
Deleting IP classifier elements using EDM....119
QoS L2 classifier element management using EDM....120

Viewing L2 classifier element information using EDM....120
Creating an L2 classifier element using EDM....122
Deleting L2 classifier elements using EDM....123
QoS system classifier element management using EDM....124
Viewing QoS system classifier elements using EDM....124
Viewing the QoS system classifier pattern using EDM....127
Configuring a QoS system classifier element using EDM....127
Deleting QoS system classifier elements using EDM....129
QoS classifier management using EDM....129
Displaying classifiers using EDM....130
Adding classifiers using EDM....130
Deleting classifiers using EDM....131
Filtering classifiers using EDM....132
QoS classifier block management using EDM....133
Displaying classifier blocks using EDM....133
Appending classifier blocks using EDM....134
Adding classifier blocks using EDM....134
Deleting classifier blocks using EDM....135
Filtering classifier blocks using EDM....136
QoS action configuration using EDM....136
Displaying QoS actions using EDM....136
Adding QoS actions using EDM....137
Deleting QoS actions using EDM....138
QoS interface action extension configuration using EDM....138
Displaying Interface action extensions using EDM....139
Adding Interface action extensions using EDM....139
Deleting Interface action extensions using EDM....140
QoS meter configuration using EDM....140
Displaying QoS meters using EDM....141
Adding QoS meters using EDM....141
Deleting QoS meters using EDM....142
QoS interface shaper configuration using EDM....142
Viewing QoS interface shaper information using EDM....142
Creating a QoS interface shaper using EDM....143
Deleting a QoS interface shaper using EDM....144
QoS interface queue shaper configuration using EDM....145
Viewing QoS interface queue shaper information using EDM....145
Creating a QoS interface queue shaper using EDM....146
Deleting a QoS interface queue shaper using EDM....147
QoS policy configuration using EDM....148
Displaying QoS policies using EDM....148
Adding QoS policies using EDM....150
Deleting QoS policies using EDM....150
QoS Policy Stats using EDM....151
QoS traffic profile filter classifier configuration using EDM....152
Viewing QoS traffic profile filter classifier information using EDM....152
Filtering QoS traffic profile filter classifier information using EDM....157
Creating a QoS traffic profile filter classifier using EDM....158
Deleting a QoS traffic profile filter classifier using EDM....163
QoS traffic profile filter set configuration using EDM....163
Viewing QoS traffic profile filter set information using EDM....164

Creating a QoS traffic profile filter set using EDM....165
Deleting a QoS traffic profile filter set using EDM....166
Filtering QoS traffic profile filter set information using EDM....167
Configuring the QoS agent using EDM....168
QoS policy class support management using EDM....170
Displaying policy class support using EDM....171
Filtering the resource allocation table using EDM....171
Displaying policy device identification using EDM....172
Displaying resource allocation using EDM....173

Chapter 1: New in this release

The following sections detail what is new in *Avaya Ethernet Routing Switch 4500 Series Configuration - Quality of Service*, NN47205-504 for Release 5.4.

Navigation

- Features on page 9
- Other changes on page 13

Features

See the following sections for information about feature changes:

- Enterprise Device Manager on page 9
- Automatic QoS 802.1AB MED interoperability on page 10
- Automatic QoS and ADAC interoperability on page 10
- QoS Queue Set Support on page 10
- QoS agent disable or enable on page 10
- QoS traffic profile filter set support on page 11
- QoS Egress Queue Shaping on page 11
- QoS DSCP mutation on page 12
- QoS IP and L2 Filter Options on page 12

Enterprise Device Manager

Enterprise Device Manager (EDM) replaces both the Java-based Device Manager and Web-based management user interfaces. EDM is an embedded element management and configuration application for Avaya Ethernet Routing Switch 4500 Series switches. EDM provides a Web-based graphical user interface through a standard web browser for the convenience of full configuration and management on the switch, and retains the look and feel of Device Manager.

Automatic QoS 802.1AB MED interoperability

Automatic QoS 802.1AB MED interoperability enhances automatic QoS implementation on the switch so you can use QoS and 802.1AB MED simultaneously. With the enhancement, if you configure 802.1AB MED, the switch publishes the private Automatic QoS DSCP value to the end device rather than the default value defined by the network policy.

Automatic QoS and ADAC interoperability

Automatic QoS and ADAC interoperability enhances automatic QoS implementation on the switch so you can use Automatic QoS and ADAC simultaneously. With Release 5.4 you can enable ADAC and configure Avaya Automatic QoS on the port so that ADAC can use the Automatic QoS DSCP markings.

QoS Queue Set Support

Starting with release 5.4, you can use QoS Queue Set Support to configure the queue set that is associated with switch interfaces. The level of resource sharing across ports may also be specified. The queue set determines the number of egress queues and how they are serviced. One to eight queues can be used. The default queue set and buffer allocation defines two egress queues with a medium level of resource sharing. For more information, see:

- Queue sets on page 39
- Changing the QoS CoS queue set using ACLI on page 97
- Changing the QoS CoS queue set to default using ACLI on page 97
- Configuring QoS resource buffer sharing using ACLI on page 94
- Changing the QoS resource buffer size to default using ACLI on page 95
- Configuring the QoS agent using EDM on page 168

QoS agent disable or enable

QoS agent disable or enable provides a straightforward method to enable or disable all QoS functions on a switch or stack to allow easier repair of QoS configurations. For more information, see:

- QoS agent disable or enable on page 42
- Enabling the QoS agent using ACLI on page 94

- Disabling the QoS agent using ACLI on page 94
- Configuring the QoS agent using EDM on page 168

QoS traffic profile filter set support

QoS traffic profile filter set support offers the advantages of generic filter sets that combine Layer 2 and Layer 3 options into a single set. The following are some characteristics of QoS traffic profile filter set support:

- The filter sets can be associated with policy-based or classifier-based metering criteria (for either individual filters or blocks of filters).
- Filter set components (filters and actions) can be added or deleted while the filter set is associated with a port.
- Multiple filter sets can be applied to a port.
- Streamlined filter, meter and action definition.
- Automatic precedence assignment.

Traffic profile filter set metering

You can use policy-based and classifier-based metering modes with traffic profile sets, for either individual filters or blocks of filters.

For more information about QoS traffic profile filter set support and Traffic profile filter set metering, see:

- QoS traffic profile filter sets on page 28
- QoS traffic profile filter set configuration using ACLI on page 74
- QoS traffic profile filter classifier configuration using EDM on page 152
- QoS traffic profile filter set configuration using EDM on page 163

QoS Egress Queue Shaping

You can use QoS Egress Queue Shaping to configure egress shaping on a port by port and queue by queue basis. For more information, see:

- Egress queue shaping on page 22
- Creating a QoS interface queue shaper using ACLI on page 89
- Deleting a QoS interface queue shaper using ACLI on page 90
- Viewing QoS interface queue shaper information using ACLI on page 91
- QoS interface queue shaper configuration using EDM on page 145

QoS DSCP mutation

Quality of Service (QoS) DSCP mutation extends QoS trusted interface support by allowing DSCP values to be remarked at egress. The enhancement adds an egress DSCP value to the DSCP-to-COS mapping table. The switch uses this egress DSCP value to remark trusted IP traffic at egress. For more information, see:

- QoS DSCP mutation on page 35
- Configuring egress mapping using ACLI on page 53
- Viewing QoS Parameters using ACLI on page 43
- Configuring egress mapping using EDM on page 111

QoS IP and L2 Filter Options

Starting with Release 5.4, you can use QoS IP and L2 Filter Options to configure the following additional filter options based on IP and Layer 2 criteria:

- IPv4 flags
- TCP control flags
- IPv4 options
- frame type
- unknown IP multicast
- known IP multicast
- unknown non-IP multicast
- known non-IP multicast
- non-IP traffic

For more information, see:

- IP classifier elements on page 25
- Layer 2 classifier elements on page 26
- System classifier elements on page 26
- QoS IP classifier element management using ACLI on page 60
- QoS L2 classifier element management using ACLI on page 63
- QoS system classifier element management using ACLI on page 66
- QoS IP classifier element management using EDM on page 113

- QoS L2 classifier element management using EDM on page 120
- QoS system classifier element management using EDM on page 124

Other changes

See the following sections for information about changes that are not feature-related:

Multiple Port Configuration

Among the many functions available in EDM, you can configure port-specific features for a single port, a group of ports, or all ports. Multiple Port Configuration appears as a pane in the work area wherever this function is available. By default the pane appears and you can close and open it with a click of the task bar.

For more information about EDM, see *Avaya Ethernet Routing Switch 4500 Series Fundamentals,* NN47205-102.

Precedence limitations

Updates are made to precedence value limitations as they apply to QoS configuration.

Chapter 2: Introduction

This document provides information you need to configure Quality of Service (QoS) for the Avaya Ethernet Routing Switch 4500 Series.

ACLI command modes

ACLI provides the following command modes:

- User EXEC
- Privileged EXEC
- Global Configuration
- Interface Configuration

Mode access is determined by access permission levels and password protection.

If no password is set, you can enter ACLI in User EXEC mode and use the **`enable`** command to move to the next level (Privileged EXEC mode). However, if you have read-only access, you cannot progress beyond User EXEC mode, the default mode. If you have read-write access you can progress from the default mode through all of the available modes.

With sufficient permission, you can use the rules in the following table to move between the command modes.

Command mode and sample prompt	Entrance commands	Exit commands

User EXEC `4526T>`	No entrance command, default mode	`exit`
		or
		`logout`

Privileged EXEC `4526T#`	`enable`	`exit`
		or
		`logout`

Global Configuration
`4526T(config)#`
	`configure`	To return to Privileged EXEC mode, enter:
		`end`
		or
		`exit`
		To exit ACLI completely, enter:

Command mode and sample prompt	Entrance commands	Exit commands
		`logout`

Interface Configuration
`4526T(config-if)#`
	From Global Configuration mode: To configure a port, enter: `interface fastethernet <port number>` To configure a VLAN, enter: `interface vlan <vlan number>`	To return to Global Configuration mode, enter:
		`exit`
		To return to Privileged EXEC mode, enter:
		`end`
		To exit ACLI completely, enter:
		`logout`

See *Avaya Ethernet Routing Switch 4500 Series Fundamentals,* NN47205-102.

Navigation

This document contains the following chapters:

- Policy-based Network Fundamentals on page 17
- Configuring Quality of Service using ACLI on page 43
- Configuring Quality of Service using Enterprise Device Manager on page 101

Chapter 3: Policy-based Network Fundamentals

This chapter provides an overview of the Differentiated Services (DiffServ) Quality of Service (QoS) network architecture. The Avaya Ethernet Routing Switch 4500 Series provides a Command Line Interface (ACLI) and Enterprise Device Manager (EDM) to configure QoS.

Policy-based networks

System administrators can use Policy-enabled networks to prioritize the network traffic. Prioritizing network traffic provides improved service for selected applications. The system administrators can use QoS, to establish service level agreements (SLA) with network customers.

In general, QoS helps with two network issues: bandwidth and time-sensitivity. QoS can help you allocate bandwidth to critical applications, and limit bandwidth for noncritical applications. Applications, such as video and voice, must have a certain amount of bandwidth to work correctly; using QoS, you can provide that bandwidth, when necessary. Also, you can place a high priority on applications that are sensitive to timing or that cannot tolerate delay by assigning that traffic to a high-priority queue.

Avaya uses Differentiated Services (DiffServ) to provide QoS functionality. A DiffServ architecture enables service discrimination of traffic flows by offering network resources to high classes at the expense of low classes of service. With this architecture you can prioritize or aggregate flows and provides scalable QoS.

Briefly, with DiffServ, you can use policies to identify traffic to forward or drop, meter, re-mark, and assign to certain interfaces. The system marks the DiffServ (DS) field of IP packets to define packet treatment as it moves through the network. Flow prioritization is facilitated by identifying, metering, and re-marking. You can specify a number of policies, and each policy can match one or many flows to support complex classification scenarios.

Port-based and Role-based QoS policies

Software Release 5.4 supports both port-based and role-based Quality of Service (QoS) policies. In a port-based Quality of Service environment, apply policies directly to individual ports. In a role-based Quality of Service environment, individual ports are first assigned to a role and that role is assigned a policy.

A port-based Quality of Service environment provides direct application of Quality of Service policies and eliminates the need to group ports when you assign policies.

You can apply port-based and role-based policies to the same port; however, the switch administrator must divide resources across the individual policies.

QoS overview

Differentiated services (DiffServ) is a QoS network architecture that offers different levels of service for various types of data traffic. DiffServ designates a specific level of performance on a packet-by-packet basis, instead of using the best-effort model for data delivery. Preferential treatment (prioritization) can apply to applications that require high performance and reliable service, such as voice and video over IP.

To differentiate between traffic flows, the DiffServ (DS) field, as defined in RFCs 2474 and 2475, is marked. The DS field in the IP header is an octet, and the DS architecture uses the first 6 bits, called the DS codepoint (DSCP). The DSCP marking dictates the forwarding treatment given to the packet at each hop. This marking occurs at the edge of the DiffServ domain, and is based on the policy or filter for the particular microflow or an aggregate flow. The QoS system also can interact with 802.1p and Layer 2 QoS.

Within the DiffServ network, the marked packets are placed in a queue according to the marking, which, in turn, determines the per-hop behavior (PHB) of that packet. For example, if a video stream is marked as high priority, then it is placed in a high-priority queue. As those packets traverse the DiffServ network, the video stream is forwarded before any other packets.

To ensure that the traffic stream conforms to the bandwidth assigned, policing within the network is necessary.

DiffServ Concepts

DiffServ is described in IETF RFCs 2474 and 2475. This architecture is flexible and allows for either end-to-end QoS or intradomain QoS by implementing complex classification and mapping functions at the network boundary or access points. Within a DiffServ domain, the packet treatment is regulated by this classification and mapping.

The DiffServ basic elements are implemented within the network and include

- packet classification functions
- a small set of per-hop forwarding behaviors
- traffic metering and marking

Traffic is classified as it enters the DS network, and is then assigned the appropriate PHB based on that classification. Within the IP packet, the 6 bits in the DSCP are marked to identify how the packet is treated at each subsequent network node.

DiffServ assumes the existence of a Service Level Agreement (SLA) between DS domains that share a border. The SLA defines the profile for the aggregate traffic flowing from one network to the other, based on policy criteria. In a given traffic direction, the traffic is expected to be metered at the ingress point of the downstream network.

As the traffic moves within the DiffServ network, policies ensure that traffic, marked by the various DSCPs, is treated according to that marking.

QoS components

The Avaya Ethernet Routing Switch 4500 Series supports the following Avaya QoS classes:

- Critical and Network classes have the highest priority over all other traffic.
- Premium class is an end-to-end service that functions similarly to a virtual leased line. Traffic in this service class is normally guaranteed an agreed-upon peak bandwidth. Traffic requiring this service must be shaped at the network boundary to undergo a negligible delay and delay variance. This service class is suitable for real-time applications, such as video and voice over IP. The recommended PHB for this service is the Expedited Forwarding (EF) PHB.
- Platinum, Gold, Silver, and Bronze classes use the Assured Forwarding (AF) PHB. These classes are for real-time, delay-tolerant traffic and non-real-time, mission-critical traffic.
- Standard class is the best-effort IP service with an additional, optional use of traffic classification that is used at the network boundary to request optimal effort treatment for packets that are in-profile (packets that do not break the service agreements between the user and the service provider).

Table 1: Service Classes on page 19 describes the service classes and their required treatment.

Table 1: Service Classes

Traffic category	Service class	Application type	Required treatment
Real-time, delay-intolerant, fixed bandwidth	Premium	Real-time applications such as video and Voice over IP (VoIP).	Expedited Forwarding (EF) - end-to-end function similar to a virtual leased line. Guaranteed agreed peak bandwidth and 100% priority.

Traffic category	Service class	Application type	Required treatment
Critical and standard network control	Critical and Network	Critical and standard network control traffic.	Weighted Round Robin - 65% proportion
Real-time, delay-tolerant traffic and non-real-time, mission-critical traffic	Platinum, Gold, Silver, and Bronze	Communications requiring interaction with additional minimal delay (such as low-cost VoIP). Single human communication with no interaction (such as Web site streaming video). Transaction processing (such as Telnet, Web browsing), and. e-mail, FTP, SNMP.	Assured Forwarding (AF)
Non-real time, non-mission-critical	Standard	Bulk transfer (such as large FTP transfers, after-hours tape backup).	Best-effort delivery. Uses remaining available bandwidth. Optional use of traffic classification at the network boundary requests optimal treatment for in-profile packets.

Automatic QoS

When enabled, Avaya Automatic QoS (NAQ) support augments default interface class processing based on role type using filtering logic to identify traffic based on defined DSCP values. Identified traffic is given preferential treatment and is marked for downstream processing. The following table shows DSCP values used to identify traffic:

NT DSCP	Traffic type
0x2F (47)	VoIP Data (Premium)
0x29 (41)	VoIP Signaling (Platinum)
0x23 (35)	Video (Platinum)
0x1B (27)	Streaming (Gold)

AutoQoS mode may function in pure mode or in mixed mode. Depending on active AutoQoS mode, DSCP values may be maintained or remarked by AQ application. When AutoQoS mode is pure, packets are sent with DSCP value unchanged. When AutoQoS mode is mixed, DSCP

value is remarked and packets are sent with “Standard DSCP” (see the following table). The following table shows standard DSCP, CoS, and drop precedence values:

NT DSCP	CoS	Drop precedence	Standard DSCP
0x2F (47)	6	Low	0x2E (EF)
0x29 (41)	5	Low	0x28 (CS5)
0x23 (35)	5	Low	0x22 (AF41)
0x1B (27)	4	Low	0x1A (AF31)

Automatic QoS 802.1AB MED interoperability

Automatic QoS 802.1AB MED interoperability enhances automatic QoS implementation on the switch so you can use QoS and 802.1AB MED simultaneously. With the enhancement, if you configure 802.1AB MED, the switch publishes the private Automatic QoS DSCP value to the end device rather than the default value defined by the network policy.

Automatic QoS and ADAC interoperability

Automatic QoS and ADAC interoperability enhances automatic QoS implementation on the switch so you can use Automatic QoS and ADAC simultaneously. With Release 5.4 you can enable ADAC and configure Avaya Automatic QoS on the port so that ADAC can use the Automatic QoS DSCP markings.

Specifying interface groups

Interface groups are used to create role-based policies. Role-based policies differ from port-based policies in that role-based policies group ports to apply a common set of rules. Alternatively, port-based polices are used to apply rules to one port only.

Each port can belong to only one interface group. The web-based interface for QoS uses the term Interface Configurations for this function. One policy references only one interface group; however, you can configure several policies to reference the same interface group.

When you move a port to another interface group (role combination), the classification elements associated with the previous interface group are removed and the classifications elements associated with the new interface group are installed on the port.

Important:

If you assign a port that is part of a MultiLink Trunk (MLT) to an interface group, only that port joins the interface group. The other ports in the MLT do not automatically become part of the interface group (role combination).

By default, ports are assigned to the default interface group (role combination), which is named allQoSPolicyIfcs. Each port is associated with the default interface group, until a port is either associated with another interface group or the port is removed from all interface groups. Ports that are associated with no interface group are disabled for QoS; they remain disabled across reboots until that port is assigned to an interface group or the switch is reset to factory defaults (when it is reassigned to allQosPolicyIfcs).

Important:

You must remove all ports from an interface group before you delete the group. You must remove an interface group when it is referenced by a policy.

Interface shaping

Interface shaping involves limiting the rate at which all traffic egressing through a specific interface is transmitted on to the network.

Interface shaping ensures that the limited bandwidth resources are used efficiently by the traffic generation rate at egress.

Shaping for each interface provides full control over bandwidth or consumption on your networks. Interface-based shaping in conjunction with ingress flow metering, is a vital component of the overall bandwidth management solution.

Important:

Different results can be obtained using a meter and/or shaper with the same parameters. This is due to the adding of the VLAN encapsulation, when applicable. Metering is applied to packets received by a port before adding VLAN encapsulation. Shaping is applied to packets sent on a port, after the port has added the VLAN encapsulation to the packet.

Egress queue shaping

QoS shaper rate queue servicing on the Avaya Ethernet Routing Switch 4500 uses a weighted round robin algorithm to shape traffic. With egress queue shaping, you can specify the maximum and minimum egress shaping rates on an individual port and queue basis. You can configure shaping criteria for any or all egress queues associated with a switch port. The

number of egress queues available for a port is determined by the QoS agent egress queue set value.

You can use queue shaping in conjunction with interface shaping.

Bandwidth allocation for queues is done according to Strict Priority and WRR algorithm. When shapers on queues with minimum rate are configured, the system first tries to assure minimum rate for all queues. Then the system uses the remaining bandwidth according to Strict Priority, WRR and shape maximum rate configured for each queue. In case the sum of shape minimum rates configured (queue shapers) exceeds the line rate, minimum shape rate will be assured for queue 1 and then remaining bandwidth will be distributed to the rest of the queues using WRR algorithm in order to assure the minimum rates for the rest of queues. For the same scenario ERS5600 switches may use strict priority, WRR and RR algorithms, depending on the active queue set.

ADAC for Avaya IP phones

For information conceptual information relating to ADAC for Avaya IP phones, as well as procedures used to configure ADAC, see *Avaya Ethernet Routing Switch 4500 Series Configuration - VLANs, Spanning Tree and Multi-Link Trunking,* NN47205-501.

NSNA solution

The Avaya Ethernet Routing Switch 4500 Series can be configured as a network access device for the NSNA solution.

NSNA is a protective framework to secure the network completely from endpoint vulnerability. The NSNA solution addresses endpoint security and enforces policy compliance. NSNA delivers endpoint security by enabling only trusted, role-based access privileges premised on the security level of the device, user identity, and session context. NSNA enforces policy compliance, such as for Sarbanes-Oxley and COBIT, ensuring that the required antivirus applications or software patches are installed before users are granted network access.

The NSNA solution provides a policy-based, clientless approach to corporate network access. The NSNA solution provides both authentication and enforcement.

For more information about NSNA, see *Avaya Ethernet Routing Switch 4500 Series Configuration — Security*., NN47205-505.

Rules

Packet classifiers identify packets according to a particular content in the packet header, such as the source address, destination address, source port number, destination port number, and other data. Packet classifiers identify flows for additional processing.

Three types of classifier elements can be used to construct a classifier:

- Layer 2 (L2) classifier elements
- IP classifier elements
- System classifier

Classifier definition

A classifier is made up of one or more classifier elements. The classifier elements dictate the classification criteria of the classifiers. Only one element of each type, IP or L2 or System Classifier Element, can be used to construct a classifier.

Figure 1: Relationship of classifier elements, classifiers, and classifier blocks on page 25 displays the relationship between the classifier elements, classifiers, and classifier blocks.

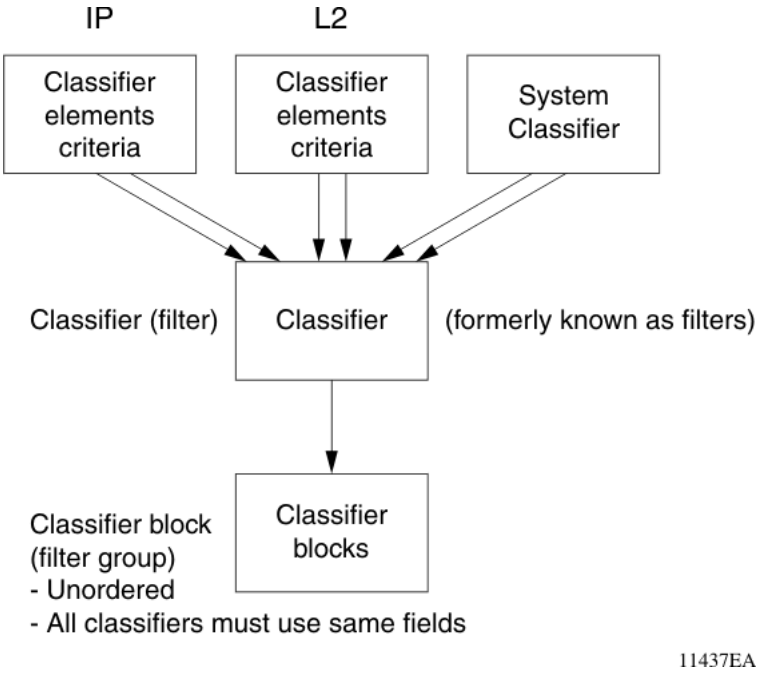

Figure 1: Relationship of classifier elements, classifiers, and classifier blocks

The system automatically creates some classifiers on untrusted ports. Additional classifiers are user-created.

When you assign a filter name to a VLAN (for example, redFilter), the switch automatically creates all the necessary QoS classifiers with the name you assigned (in this case, redFilter) if that filter does not already exist.

If you had previously defined the filter, then that pre-existent filter is used. Once a filter is created (either by you or automatically by the switch), it can be modified (that is, entries can be deleted or added).

IP classifier elements

The Avaya Ethernet Routing Switch 4500 Series classifies packets based on the following parameters in the IP header:

- IPv4/IPv6 address type
- IPv6 flow identifier
- IPv4/IPv6 source address/mask
- IPv4/IPv6 destination address/mask
- IPv4 protocol type/IPv6 next-header
- IPv4/IPv6 DSCP value
- IPv4/IPv6 Layer 4 source port number with TCP/UDP (range of)

- IPv4/IPv6 Layer 4 destination port number with TCP/UDP (range of)
- IP flags
- TCP control flags
- IPv4 options

Layer 2 classifier elements

The Avaya Ethernet Routing Switch 4500 Series classifies packets based on the following parameters in the Layer 2 header:

- source MAC address/mask
- destination MAC address/mask
- VLAN ID number (range of)
- VLAN tag
- EtherType
- IEEE 802.1p user priority values
- Packet type

Important:

Layer 2 classifier elements with an Ethernet Type of 0x0800 are treated as an IPv4 classifier, and those with an Ethernet Type of 0x86DD are treated as an IPv6 classifier.

System classifier elements

System classifier elements support pattern matching, also referred to as offset filtering. Offset filtering identifies fields within protocol headers, or portions thereof, on which to identify traffic for additional QoS processing. This eliminates the limitations that arise by supporting only certain protocol header fields, such as IP source address, IP protocol field, and VLAN ID for flow classification.

Fully customized classifiers can be created to match non-IP-based traffic, as well as to identify IP-based traffic using non-typical fields in Layers 2, 3, 4, and beyond.

The Avaya Ethernet Routing Switch 4500 Series Content Aware Processor (CAE) lookup engine supports selection of 16 bytes within the first 128 bytes of the packet.

Beginning with software release 5.4, the following system classifier elements are supported:

- unknown IP multicast
- known IP multicast

- unknown non-IP multicast
- known non-IP multicast
- non-IP packet

Classifiers and classifier blocks

Classifier elements can be combined into classifiers, and grouped into classifier blocks. Classifiers are created by referencing an L2 classifier element, IP element, a system classifier element, or one of each type.

Each classifier can have a maximum of a single IP classifier element, one L2 classifier element, one system classifier element or any combination of one IP, L2 and system classifier element.

Classifiers can be combined into classifier blocks. Each classifier block has one or more classifiers.

As classifier blocks are planned, keep in mind that only a single IP classifier element, a single L2 classifier element, and a single system classifier element can appear in each classifier. For example, to group five IP classifier elements create five separate classifiers, each with a unique IP classifier element, and then create a classifier block referencing those five classifiers.

When grouping IP Classifier Elements that match on layer 4 UDP or TCP port ranges all port ranges that are to be grouped must either satisfy or violate the following rule:

- Minimum value: even number
- Maximum value: minimum port number in binary with the right most consecutive 0s replaced with 1s using the formula: Port Maximum = ((Port minimum + 2^n) -1) where n is equal to the number of consecutive trailing zeros.

For example, if the requirement is to match the TCP port ranges 3460 to 3463 and 3470 to 3472, the range 3460 to 3463 is in compliance with the minimum /maximum rule. The second range 3470 to 3472 is not in compliance with the minimum /maximum rule. To group these two ranges into a single Classifier Block, the second range needs to be broken up into two separate ranges that are in compliance with the minimum /maximum rule.

The following Classifier Elements need to be created:

- IP Classifier Element 1 - Match TCP port range 3460-3463
- IP Classifier Element 2 - Match TCP port range 3470-3471
- IP Classifier Element 3 - Match TCP port range 3472-3472

These IP Classifier Elements can then be combined into a Classifier Block and associated with a Policy.

Also, if one of the classifier elements in a classifier block has associated actions or meters, then all classifier elements of that classifier block must also have associated actions or meters that are not necessarily identical.

A classifier or classifier block is associated through a policy with interface groups. Packets received from any port that is in an interface group are classified with the same filter criteria.

Each classifier or classifier block is associated with actions that are executed when the packet matches the filter criteria in the group. The filter criteria and the associated actions, metering criteria, and interface groups are referenced by a policy, which dictates the overall traffic treatment (refer to Figure 2: Flowchart of QoS Actions on page 30 for an illustration of the traffic treatment).

Classifier elements, through individual classifiers or a classifier block, are associated with an interface group, action, and metering through a policy. Multiple policies can be applied to a given flow. The policy evaluation order is determined by the policy precedence. The order of precedence is from the highest precedence value to the lowest precedence (that is, a value of 7 is evaluated before a value of 6).

Note:

Although there are 8 policy precedences available, the eighth precedence is permanently occupied by ARP, so, for practical purposes, 7 precedences are available.

In summary, classifiers combine different classifier elements. Classifier blocks combine classifiers to form an unordered set of classification data. Unordered data means that all classifiers associated with a policy are applied as if simultaneously, with no precedence.

QoS traffic profile filter sets

A filter set is a collection of policies that are identified as a single, named unit, with each policy referencing classifier and action criteria for identifying and processing traffic.

A filter set classifier element identifies the protocol fields and field content used for traffic identification. You can assign a unique identifier, or name, to a filter set classifier element, and all classifier elements that comprise a filter set share the same name.

Filter set classifier elements can be combined into a block when resources are limited. A single filter set (non-block) classifier element consumes one precedence level. Any number of filter set classifier elements combined in a block still only consumes one precedence level. Therefore, combining compatible filter set classifier elements into blocks can positively impact resource usage.

Policies within a set are applied to ingress traffic in a specific order. The evaluation order dictates the order in which classifier elements associated with the same filter set name are applied. Elements with a low evaluation order are applied before elements with a higher evaluation order. An evaluation order must be unique within a filter set. The evaluation order for a classifier block is determined by the lowest evaluation order of the elements that are members of the block.

The following are some characteristics of QoS traffic profile filter set support:

- Filter set components (filters and actions) can be added or deleted while the filter set is associated with a port.
- Multiple filter sets can be applied to a port.

Traffic profile filter set metering

You can use policy-based and classifier-based metering modes with traffic profile filter sets. Traffic metering can be applied to individual classifiers, blocks of classifiers and individual block members.

Policy-based metering associates a unique meter with each policy that comprises the filter set. Each meter can independently apply to an individual classifier or block of classifiers. There are two types of policy-based metering:

- uniform metering—each meter has the same characteristics derived from the filter set instance definition.
- individual metering—each meter has unique characteristics derived from the individual classifier or master block classifier member associated with the filter set policy.

Classifier-based metering associates a unique meter with each classifier for which you provide metering information. You can configure classifier-based meters for one, multiple, or all classifiers associated with a filter set. Each classifier-based meter has unique characteristics determined by classifier data. Without this classifier data, a meter is not associated with the classifier.

Specifying actions

Figure 2: Flowchart of QoS Actions on page 30 summarizes how QoS matches packets with actions.

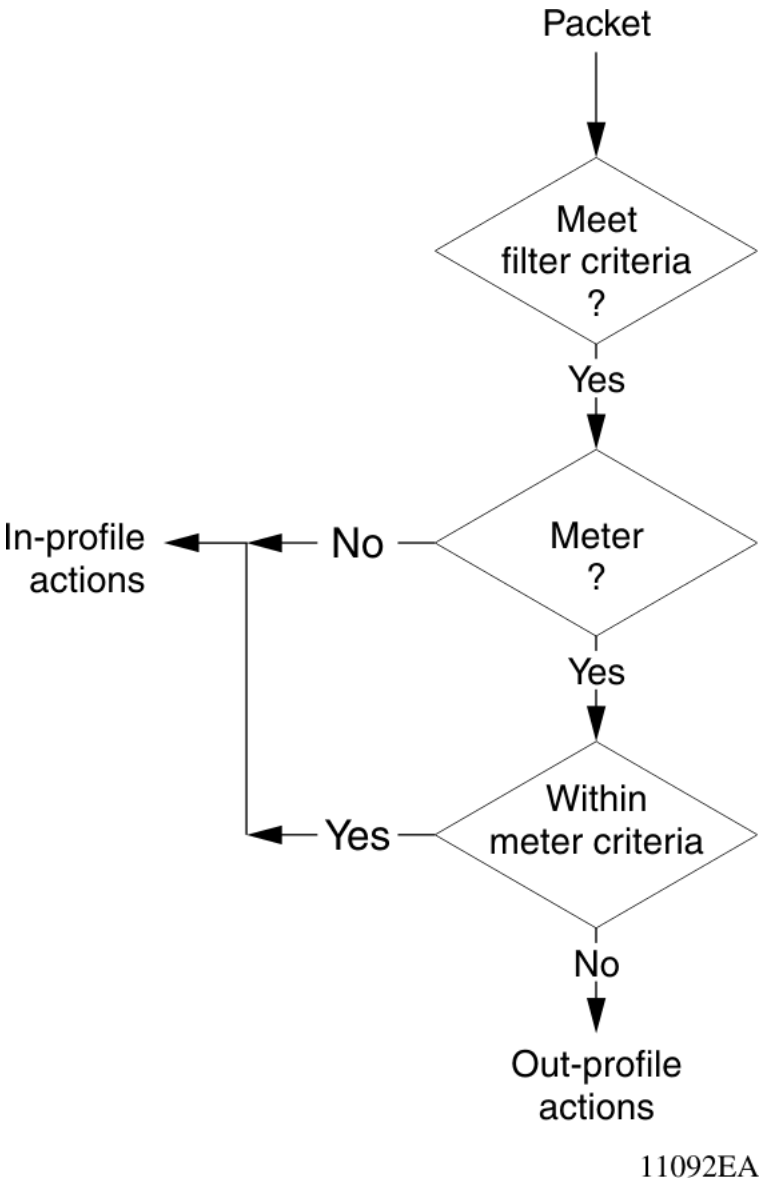

Figure 2: Flowchart of QoS Actions

Table 2: Summary of Allowable Actions on page 30 shows a summary of the allowable actions for different matching criteria.

Table 2: Summary of Allowable Actions

Actions	In-Profile	Out-Of-Profile
Drop/transmit	X	X
Update DSCP	X	X
Update 802.1p user priority	X	
Set drop precedence	X	X

The Avaya Ethernet Routing Switch 4500 Series filters collectively direct the system to initiate the following actions on a packet, depending on the configuration:

- Drop
- Re-mark the packet
  - Re-mark a new DiffServ Codepoint (DSCP)
  - Re-mark the 802.1p field
  - Assign a drop precedence

Important:
The 802.1p user priority value, used for out-of-profile packets, is derived from the associated in-profile action to prevent reordering at egress of packets from a single flow.

Packets received on an interface are matched against all policies associated with that interface. So, potentially, any number of policies--from none to many--are applied to the packet, depending on the policies associated with the specific interface. The set of actions applied to the packet is a result of the policies associated with that interface, ranging from no actions to many actions.

For example, if one policy associated with the specific interface specifies only a value updating the DSCP value, while another policy associated with that same interface specifies only a value for updating the 802.1p user priority value, both of these actions occur. If conflicts among actions are detected--for example, if two policies on the specified interface request that the DSCP be updated, but specify different values--the value from the policy with the higher precedence is used.

The actions applied to packets include those actions defined from user-defined policies and those actions defined from system default policies. The user-defined actions always carry higher precedences than the system default actions. This means that, if user-defined policies do not specify actions that overlap with the actions associated with system default policies (for example, the DSCP and 802.1p update actions installed on untrusted interfaces), the default policy actions with the lowest precedence will be included in the set of actions to be applied to the identified traffic.

Important:
You must define an additional wild card rule to enable native Non-Match support.

Specifying interface action extensions

The interface action extensions add to the base set of actions.

Table 3: Summary of allowable interface action extensions on page 32 shows a summary of the allowable interface action extensions for different matching criteria.

Table 3: Summary of allowable interface action extensions

Interface action extensions	In-Profile	Out-Of-Profile
Set egress unicast port	X	
Set egress non-unicast port	X	

The Avaya Ethernet Routing Switch 4500 Series does not initiate an action extension based packet type. So, user should redirect all incoming traffic, no matter of packet types (both unicast and non-unicast), towards same port, using interface action extension.

Important:

When specifying interface action extensions, you must use both options (Set egress unicast interface and Set egress non-unicast interface). Same port for both unicast and non-unicast packets redirection should be used.

Specifying meters

QoS metering, which operates at ingress, provides different levels of service to data streams through user-configurable parameters. A meter is used to measure the traffic stream against a traffic profile, which you create. Thus, creating meters yields In-Profile and Out-of-Profile traffic.

Different meters can be associated with different classifiers across a block of classifiers. Policies can be configured without metering, or policies can be configured with a single meter or match action that applies to all the classifiers associated with that policy. Meters and action criteria cannot be defined in both the policy definition and the individual classifier definition.

A policy can be created with a meter that is applied to all classifiers, and a policy can be created that has meters applied to individual classifiers; however, both types cannot be in the same policy or action.

A meter applied to a policy has that metering criteria applied to each port of the interface group (role combination). In other words, the specified bandwidth is allocated on each port, not distributed across all ports.

Using meters, a Committed Rate in Kb/s (1000 b/s in each Kb/s) can be set. All traffic within this Committed Rate is In-Profile. Additionally, a Maximum Burst Rate can be set that specifies an allowed data burst larger than the Committed Rate for a brief period. After this is set, the system offers suggestions in choosing the Duration for this burst. Combined, these parameters define the In-Profile traffic.

Important:

The range for the committed rate is 0 kb/s to 32 GB/s, if value of 0 is selected the specific rate will be ignored.

An example of traffic policing is limiting traffic entering a port to a specified bandwidth, such as 5000 Kb/s (Committed Rate). Instead of dropping all traffic that exceeds this threshold, a Maximum Burst Rate can be configured to exceed the threshold (Committed Rate), for a brief period of time (Duration), without being dropped.

Meter definitions where the committed burst size is too small, based on the requested committed rate, are rejected. The committed burst size can be only one of the following discrete values (in bytes): 4096 (4K), 8192 (8K), 16384 (16K), 32768 (32K), 65536 (64K), 131072 (128K), 262144 (256K), 524288 (512K), 1048576 (1024K), 16777216 (16384K), 2097152 (2048K), 4194304 (4096K), 8388608 (8192K).

Trusted, untrusted, and unrestricted interfaces

Avaya Ethernet Routing Switch 4500 Series ports are classified into three categories:

- trusted
- untrusted
- unrestricted

The classifications of trusted, untrusted, and unrestricted actually apply to groups of ports (interface groups). These three categories are also referred to as interface classes. In your network, trusted ports are usually connected to the core of the DiffServ network, and untrusted ports are typically access links that are connected to end stations. Unrestricted ports can be either access links or connected to the core network.

At factory default, all ports are considered untrusted. However, for those interface groups created, the default is unrestricted.

Because a port can belong to only one interface group, a port is classified as trusted, untrusted, or unrestricted. These types are also referred to as interface classes.

Trusted and untrusted ports are automatically associated with policies that initiate default traffic processing. This default processing occurs if:

no actions are initiated based on user-defined policy criteria that matches the traffic.

OR

the actions associated with the user-defined policy do not conflict with the default processing actions.

The default processing of trusted and untrusted interfaces is as follows:

- Trusted interfaces -- IPv4 traffic received on trusted interfaces is re-marked at the layer 2 level, that is, the 802.1p user priority value is updated based on the DSCP value in the packet at ingress and the installed DSCP-to-CoS mapping data. The DSCP value is not updated. Remapping occurs, by default, only for standardized DSCP values (for example, EF, AFXX) and any proprietary Avaya values. The DSCP values that are remapped are

associated with a non-zero 802.1p user priority value in the DSCP-to-COS Mapping Table.

- Untrusted interfaces -- IPv4 traffic received on untrusted interfaces is re-marked at the layer 3 level--that is, the DSCP value is updated. The new DSCP value is determined differently depending on whether the packet is untagged or tagged:

  - Untagged frames

    The DSCP value is derived using the default port priority of the interface receiving the ingressing packet. This default port priority is used to perform a lookup in the installed CoS-to-DSCP mapping table.

    The 802.1p user priority value is unchanged--that is, the default port priority determines this value.

    (Thus, the DSCP value on untagged frames on untrusted interfaces is updated using the default port priority of the ingress interface; the user sets the default port priority).

  - Tagged frames

    The DSCP value is re-marked to indicate best-effort treatment is all that is required for this traffic.

    The 802.1p user priority value is updated based on the DSCP-to-CoS mapping data associated with the best effort DSCP, which is 0.

Table 4: Default QoS fields by class of interface--IPv4 only on page 34 shows the default guidelines the switch uses to re-mark various fields of IPv4 traffic (and layer 2 traffic matching IPv4) based on the class of the interface. These actions occur if the user does not intervene at all; they are the default actions of the switch.

Table 4: Default QoS fields by class of interface--IPv4 only

Type of filter	Action	Trusted	Untrusted	Unrestricted
IPv4 filter criteria or Layer 2 filter criteria matching IPv4	DSCP	Does not change	• Tagged--Updates to 0 (Standard) • Untagged--Updates using mapping table and port's default value	Does not change
	IEEE 802.1p	Updates based on DSCP mapping table value	Updates based on DSCP mapping table value	Does not change

Important:

The default for layer 2 non-IP traffic is to pass the traffic through all interface classes with the QoS values for 802.1p and drop precedence unchanged.

The Avaya Ethernet Routing Switch 4500 Series does not trust the DSCP of IPv4 traffic received from an untrusted port, however, it does trust the DSCP of IPv4 traffic received from a trusted port.

L2 non-IP traffic, received on either a trusted port or an untrusted port, traverses the switch with no change.

IPv4 traffic, received on a trusted port, has the 802.1p user priority value re-marked and the drop precedence set, based on the DSCP in the received IP packet.

If an IPv4 packet is received from a trusted port, and either it does not match any of the classifier elements installed by the user on this port or it does match a classifier element but is not dropped, the Avaya Ethernet Routing Switch 4500 Series uses default system classifiers to change the packet IEEE 802.1p and drop precedence based on the DSCP of the packet.

If an IPv4 packet is received from an untrusted port and it does not match any one of the classifier elements installed by the user on the port, the Avaya Ethernet Routing Switch 4500 Series uses default system classifiers to change the packet DSCP, IEEE 802.1p priority, and drop precedence as follows:

- If the packet is tagged, the 802.1p user priority value is derived from the DSCP-to-CoS mapping table using the best effort DSCP, which is 0.
- If an IPv4 packet is untagged, the Avaya Ethernet Routing Switch 4500 Series uses the default classifier to change the DSCP based on the default IEEE 802.1p priority of the ingress untrusted port to index into the DSCP-to-CoS mapping table to determine the DSCP value.

Table 5: System requirements for network service class definitions and mapping to DSCP

DiffServ Code Point (DSCP)	Logical queue number	Recommended scheduler	Network service class
CS7, CS6	2	Weighted	Network
EF, CS5	1	Priority	Premium
AF1x, CS1	3	Weighted	Bronze
AF4x, AF3x, AF2x, CS4, CS3, CS2, DF (CSO), all unspecified DSCPs	4	Weighted	Standard

QoS DSCP mutation

QoS DSCP mutation enables the recolor of DSCP values on packet egress. QoS trusted interface support is extended by adding an egress DSCP value to the DSCP-to-COS mapping table. The switch uses the ingress DSCP value to update the Class of Service (COS) and recolor the DSCP value on egress. By default, the DSCP value is left unchanged.

Specifying policies

Important:

Configure interface groups (role combinations), classification criteria, actions, and meters before attempting to reference that data in a policy.

When network traffic attributes match those specified in a traffic pattern, the policy instructs the network device to perform a specified action on each packet that passes through it. A policy is a set of rules and actions that are applied to specific ports.

Caution:

It is recommended that you configure all applications that assign filters (IP Source Guard, UDPForwarding) before you configure any QoS policies and QoS Access Lists.

When configuring policies, it is important to consider that the policy with the highest precedence is evaluated first, then the policy with the next lowest precedence and so on. The valid precedence range for QoS policies is 1 to 7. For example, with a precedence of 1 to 7, the system begins the evaluation with 7, moves on to 6, and so forth. Although there are 8 precedences available, the eighth precedence is permanently occupied by ARP, so, for practical purposes, 7 precedences are available.

The valid precedence range can change if certain features are enabled. QoS shares resources with other switch applications such as MAC Security and Port Mirroring. Allocations for non-QoS applications are dynamic. The following list describes how the precedence range is affected by enabling these features:

- When MAC Security is enabled, it uses the highest available precedence value.
- When Port Mirroring is enabled using one of the following modes, it uses the highest available precedence:
  - Asrc
  - Adst
  - AsrcBdst
  - AsrcBdstOrBsrcAdst
  - AsrcOrAdst
  - XrxYtxOrYrxXtx
  - XrxYtx

Caution:

Issuing "qos agent reset-default" will not free resources used by Port-Mirroring.

Other applications that use QoS include EAPOL, IP Source Guard and UDP Forwarding. In the case of EAPOL, this feature should be enabled prior to any other QoS application since functionality may be affected.

A policy can reference an individual classifier or a classifier block.

A policy is a network traffic-controlling mechanism that monitors the characteristics of the traffic (for example, its source, destination, and protocol), and performs a controlling action on the traffic when certain user-defined characteristics are matched. A policy action is the effect a policy has on network traffic that matches the traffic profile of the policy.

The policies tie together:

- Actions
- Meters
- Classifier elements or classifiers or classifier blocks
- Interface groups

The policies, by connecting these user-defined configurations, control the traffic on the switch.

Ports can be assigned to interface groups that are linked to policies. Port-based policies eliminate the need to create an interface group for a single port, and are used to directly apply a policy to a single port.

Although a single policy can reference only one interface group, you can configure several policies that reference the same interface group. The policies determine the traffic treatment of the flows.

Important:

Policies can be enabled and disabled. Policies do not have to be deleted to be disabled. To modify a policy, it must first be deleted and a new policy created.

Statistics can also be tracked for QoS. The Avaya Ethernet Routing Switch 4500 Series supports statistics for each policy and for each policy, classifier, or interface statistics tracking.

Packet flow using QoS

Using DiffServ and QoS, a specific performance level for packets can be designated. This system allows for network traffic prioritization. However, it requires some thought to configure the prioritization. Anumber of policies can be specified and each policy can match one or many flows, supporting complex classification scenarios.

This section contains a very simplified introduction to the many ways to prioritize packets using QoS. In simple terms, the methods of prioritizing packets depend on the DSCP and the 802.1 priority level and drop precedence.

The QoS class basically directs which group of packets receives the best network throughput, which group of packets receives the next best throughput, and so on. The level of service for each packet is determined by the configurable DSCP.

The available levels of QoS classes are currently named Network, Premium, Platinum, Gold, Silver, Bronze, and Standard. The level of service for each packet is determined by the configurable DSCP.

Classifier elements, classifiers, and classifier blocks basically sort the packets by various configurable parameters. These parameters include VLAN IDs, IP source and subnet address, IP protocol, and many others.

The classifiers/classifier blocks are associated with policies, and policies are organized into a hierarchy. The policy with the highest precedence is evaluated first. The classifier elements, classifiers, and classifier blocks are associated with interface groups, in that packets from a specific port will have the same classification parameters as all others in the particular interface group (role combination).

Note:

When configuring rate limiting, the user configures a percentage of port bandwidth based upon the current operational speed. Rate limiting is implemented in the hardware based on packet per second. Based upon an average packet size of 500 bytes the packet per second rate is computed. For example, if a user had specified to limit the forwarding rate of broadcast packets to 1000 packets/second, any additional broadcast packets are discarded when the broadcast packet rate exceeds the threshold value. During each second first 1000 broadcast packets are allowed, then any additional broadcast packets which arrives on this port until the next second are discarded.

Meters, operating at ingress, keep the sorted packets within certain parameters. A committed rate of traffic can be configured, allowing a certain size for a temporary burst, as In-Profile traffic. All other traffic is configured as Out-of-Profile traffic. If you choose not to meter the flow, you do not configure meters.

Actions determine how the traffic is treated.

The overall total of all the interacting QoS factors on a group of packets is a policy. Policies can be configured that monitor the characteristics of the traffic and perform a controlling action on the traffic when certain user-defined characteristics are matched.

Figure 3: QoS Policy Schematic on page 39 provides a schematic overview of QoS policies.

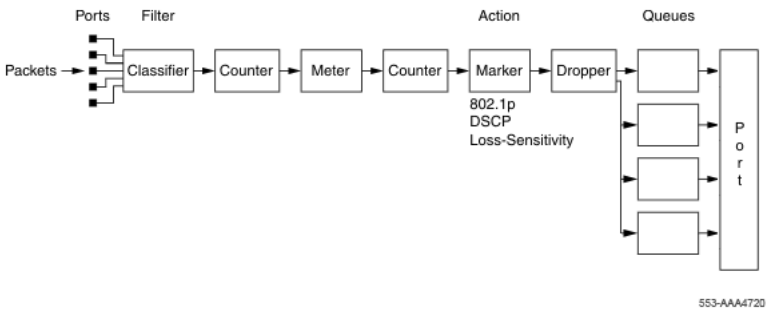

Figure 3: QoS Policy Schematic

Queue sets

A QoS queue set is used to logically represent the queuing capabilities that are associated with an egress QoS interface. A queue set is comprised of a number of related queuing components that dictate the queuing behavior supported by the set itself. These include:

- Queue count—the number of different CoS queues in the set.
- Queue service discipline—indicates the means through which queues (competing for limited transmission bandwidth) and the packets held in the queues are scheduled for transmission.
- Queue bandwidth allocation—indicates the absolute or relative amount of bandwidth that can be consumed by the queues in the set. When queues are serviced using a Weighted Round Robin (WRR) or Weighted Fair Queuing (WFQ) discipline, these values represent the weights associated with the queues.
- Queue service order—when multiple service disciplines are in use, the service order indicates service precedence assigned to individual queues (strict priority) or clusters of queues (WRR).
- Queue size—indicates the maximum buffering resources that can be consumed by the individual queue.

Each QoS egress port has eight queue sets consisting of anywhere from 1 to 8 queues, depending on the queue set you assign to the QoS interfaces. Packets are assigned to a queue based on the IEEE 802.1p, or Class of Service (CoS), value associated with that packet. Depending on the queue set you configure, some queues are serviced in an absolute priority fashion and some queues can be serviced in a Weighted Round Robin (WRR) fashion.

Beginning with software release 5.4, the queue set, the number of queues per QoS interface, the buffer allocation of the queue set, and the CoS-to-queue priority for each queue within the queue set can be configured.

Important:

Egress queuing and buffering characteristics and the CoS-to-queue priorities are the same across all QoS ports. The Avaya Ethernet Routing Switch 4500 has factory default queue set and buffer allocation mode values based on the following parameters:

- factory default queue set: queue set 2
- buffer allocation mode: Medium

Modifying CoS-to-queue priorities

The association of 802.1p, or CoS, values to each queue within the queue set can be modified. Within the queue set a value of 0 to 7 can be assigned to each queue in the set.

Important:

Any modification to the CoS-to-queue values takes effect immediately; the system does have to be reset to modify these values.

QoS configuration guidelines

Classifiers can be installed that act on traffic destined for the switch, such as ICMP Echo Requests (ping) and SNMP messages. If the associated action is to drop the traffic, the switch is locked from further use.

When you use QoS on the switch, the system shares resources across groups of ports. The number of access lists, or policies, that you can apply to a port depends on the number of available precedences.

Precedences are a resource that the system shares between QoS and non-QoS applications. The number of resources available to share changes, depending on the number of applications you enable. Applications include MAC security, port mirroring, EAPOL, IP Source Guard, and UDP Forwarding.

Note:

Although there are 8 precedences available, the eighth precedence is permanently occupied by ARP, so, for practical purposes, 7 precedences are available.

Each hardware device (ASIC) contains a specific number of ports and supports the following scaling:

- Up to 128 classifiers for each mask precedence for each ASIC.
- Up to 62 meters for each mask precedence for each ASIC.
- Up to 64 counters for each mask precedence for each ASIC.

- Up to 8 precedence masks for each port (1 precedence is permanently occupied by ARP).
- Up to 16 range checkers for each ASIC.
- Up to 8 policies, composed of up to 128 rules each can be added for each ASIC.

To view QoS resources, use ACLI command **`show qos diag`**.

The following table describes the ports supported by each ASIC for each model in the ERS 4500 portfolio.

Model	ASIC Device 1	ASIC Device 2
4526FX	Port 1 - 26	
4550T	Port 1 - 24	Port 25 - 50
4550T-PWR	Port 1 - 24	Port 25 - 48
4548GT	Port 1 - 24	Port 25 - 48
4548GT-PWR	Port 1 - 24	Port 25 - 48
4526T	Port 1 - 26	
4526T-PWR	Port 1 - 26	
4524GT	Port 1 - 24	
4524GT-PWR	Port 1 - 24	
4526GTX	Port 1 - 26	
4526GTX-PWR	Port 1 - 26	

QoS configuration example

If you are using QoS on the Avaya Ethernet Routing Switch 4500 Series 4548GT switch, you can add up to 128 rules to any ports from 1 to 24, using policy preference 7. You can also add another 128 rules to any ports from 25 to 48, using the same policy preference (7).

Resources used by a QoS policy remain reserved, from the QoS perspective, even if you disable the policy. To release these resources, you must delete the policy.

Important:

A maximum of 16 port ranges are supported for each hardware device (ASIC).

Using unrestricted role for ports, traffic will be prioritized based on 802.1p priority, allowing filters to be configured based on specific application needs. For example, assign all packets marked with DSCP 46 (2E) priority, such as with VoIP, to the highest priority queue.

Example

```
qos if-group name "Trust_VoIP" class unrestricted

no qos if-assign port 2-50
```

```
qos if-assign port 1 name Trust_VoIP

qos ip-element 1 ds-field 46

qos classifier 1 set-id 1 name "Trust_VoIP" element-type ip element-
id 1

qos policy 1 name "Trust_VoIP" if-group "Trust_VoIP" clfr-type
classifier clfr-id 1 in-profile-action 7 precedence 7 track-
statistics
```

QoS agent disable or enable

You can use the QoS agent to temporarily disable and then enable all QoS functions on a switch or stack to simplify the repair of QoS configurations.

You cannot use the QoS agent to temporarily disable QoS when non-QoS applications are using the QoS functionality.

Chapter 4: Configuring Quality of Service using ACLI

This chapter discusses how to configure DiffServ and Quality of Service (QoS) parameters for policy-enabled networks using the Avaya Command Line Interface (ACLI).

Important:
When the ignore value is used in QoS, the system matches all values for that parameter.

Viewing QoS Parameters using ACLI

Use the following procedure to display QoS parameters and policy configuration.

Procedure steps

To display QoS parameters, use the following command from Privileged EXEC mode:

show qos
[acl-assign <1 - 65535> |
if-group |
if-assign [port <portlist>]|
queue-set |
queue-set-assignment |
ingressmap
egressmap
ip-element [user | system | all | <1-65535>] |
l2-element [user | system | all | <1-65535>] |
classifier [user | system | all | <1-65535>] |
classifier-block [user | system | all | <1-65535>] |

action [user | system | all] |
if-action-extension [user | system | all | <1-65535>] |
meter [user | system | all | <1-65535>] |
if-queue-shaper [port <portlist>]|
if-shaper [port <portlist>]|
policy [user | system | all | <1-65535>] |
agent |
diag [unit | <cr>] |
ip-acl <1 - 65535> |
l2-acl <1 - 65535> |
capability [meter | shaper] [port <portlist>]]
nsna [classifier | interface | name]
system-element [user | system | all | <1-65535>]
statistics <1-65535>
traffic-profile <classifier | interface | set | statistics>
port

Variable Definitions

Variable	Value
acl-assign <1 - 65535>	Displays the specified access list assignment entry.
if-group	Displays the interface groups.
if-assign [port <portlist>]	Displays the list of interface assignments.
queue-set	Displays the queue set configuration.
queue-set-assignment	Displays the association between the 802.1p priority to that of a specific queue.
ingressmap	Displays the 802.1p priority to DSCP mapping.
egressmap	Displays the association between DSCP, 802.1p priority, drop precedence, new DSCP, and the egress mapping name.

Variable	Value
ip-element [user | system | all | <1-65535>]	Displays the IP classifier element entries. • user - displays only user-created and default entries • system - displays only system entries • all - displays user-created, default, and system entries • <1-65535> - displays a particular entry The default setting is all.
l2-element [user | system | all | <1-65535>]	Displays the Layer 2 element entries. • user - displays only user-created and default entries • system - displays only system entries • all - displays user-created, default, and system entries • <1-65535> - displays a particular entry The default setting is all.
system-element [user | system | all | <1-65535>]	Displays the system classifier element entries.
classifier [user | system | all <1-65535>]	Displays the classifier set entries. • user - displays only user-created and default entries • system - displays only system entries • all - displays user-created, default, and system entries • <1-65535> - displays a particular entry The default setting is all.
classifier-block [user | system | all | <1-65535>]	Displays the classifier block entries. • user - displays only user-created and default entries • system - displays only system entries • all - displays user-created, default, and system entries • <1-65535> - displays a particular entry The default setting is all.
action [user | system | all | <1-65535>]	Displays the base action entries. • user - displays only user-created and default entries • system - displays only system entries

Variable	Value
	• all - displays user-created, default, and system entries • <1-65535> - displays a particular entry The default setting is all.
if-action-extension [user | system | all | <1-65535>]	Displays the interface action entries. • user - displays only user-created and default entries • system - displays only system entries • all - displays user-created, default, and system entries • <1-65535> - displays a particular entry The default setting is all.
meter [user | system | all | <1-65535>]	Displays the meter entries. • user - displays user-created and default entries • system - displays only system entries • all - displays user-created, default, and system entries • <1-65535> - displays a particular entry The default setting is all.
if-queue-shaper port <portlist>	Displays the interface egress queue shaping parameters.
if-shaper port <portlist>	Displays the interface shaping parameters.
policy [user | system | all | 1-65535>]	Displays the policy entries. • user - displays only user-created and default entries • system - displays only system entries • all - displays user-created, default, and system entries • <1-65535> - displays a particular entry The default setting is all.
statistics <1-65535>	Displays the policy and filter statistics values.
nsna [classifier | interface | name]	Displays the NSNA entries: • classifier - displays QoS NSNA classifier entries. • interface - displays QoS NSNA interface entries. • name - specify the label to display a particular NSNA template entry.

Variable	Value
agent	Displays the global QoS parameters.
ip-acl <1 - 65535>	Displays the specified IP access list assignment entry.
l2-acl <1 - 65535>	Displays the specified Layer 2 access list assignment entry.
capability [meter | shaper] [port <portlist>]	Displays QoS meter or shaper port capabilities.
traffic-profile <classifier | interface | set | statistics>	Displays QoS traffic profile entries.
port	Displays QoS port configurations.

Configuring QoS Access Lists

The ACLI commands described in this section allow for the configuration and management of QoS access lists. For information on displaying this information, refer to Viewing QoS Parameters using ACLI on page 43.

Assigning ports to an access list

Use the following procedure to assign ports to an access list.

Procedure steps

To assign ports to an access list, use the following command from Global Configuration mode:

```
[no] qos acl-assign [<1 - 55000>] [enable] | [port <port_list>]
acl-type {ip|l2} name <WORD>
```

Use the **no** form of this command to remove an access list assignment.

Variable Definitions

Variable	Value
<1 - 55000>	A unique identifier for the access list assignment.
enable	Enable the access-list assignment entry.

Variable	Value
port <port_list>	The list of ports assigned to the specified access list.
acl-type {ip | l2}	The type of access list used; IP or Layer 2.
name <WORD>	The name of the access list to be used. Access lists must be configured before ports can be assigned to them.

Creating an IP access list

Use the following procedure to create an IP access list.

Procedure steps

To create an IP access list, use the following command from Global Configuration mode:

```
[no] qos ip-acl   name <WORD>
[addr-type <addrtype>]
[src-ip <source_ip>]
[dst-ip <destination_ip>]
[ds-field <dscp>]
[{protocol <protocol_type> | next_header <header>}]
[src-port-min <port> src-port-max <port>]
[dst-port-min <port> dst-port-max <port>]
[session-id <sessionid>] [drop-action {enable | disable}]
[update-dscp <0 - 63>] [update-1p <0 - 7>]
[set-drop-prec {high drop | low drop}]
[block <block_name>]
```

Use the **no** form of this command to remove an access list.

Variable Definitions

Variable	Value
name <WORD>	The name assigned to this access list.
addr-type <addrtype>	The IP address type to use for the access list; range is ipv4 or ipv6.
src-ip <source_ip>	The source IP address and mask to use for this access list, in the form of a.b.c.d/x for IPv4, or x:x:x:x:x:x:x:x/z for IPv6.
dst-ip <destination_ip>	The destination IP address to use for this access list.
ds-field <dscp>	The DSCP value to use for this access list; range is 0-63.
{protocol <protocol_type> | next_header <header>}	The protocol type or IP header to use with this access list.

Variable	Value
src-port-min <port> src-port-max <port>	The minimum and maximum source ports to use with this access list. Both values must be specified.
dst-port-min <port> dst-port-max <port>	The minimum and maximum destination ports to use with the access list. Both values must be specified.
session-id <sessionid>	The flow ID to use with this access list.
drop-action {enable | disable}	The drop action to use for this access list. Enable specifies to drop packets and disable specifies to not drop packets.
update-dscp <0 - 63>	The DSCP value to update for this access list.
update-1p <0 - 7>	The 802.1p value to update for this access list.
set-drop-prec {high-drop | low-drop}	The drop precedence to configure for this access list.
block <block_name>	The block name to associate with the access list.

Creating a Layer 2 access list

Use the following procedure to create a Layer 2 access list.

Procedure steps

To create a Layer 2 access list, use the following command from Global Configuration mode:

```
[no] qos l2-acl     name <WORD>
                    [src-mac <source_mac_address>]
                    [src-mac-mask
                    <source_mac_address_mask>]
                    [dst-mac <destination_mac_address>]
                    [dst-mac-mask
                    <destination_mac_address_mask>
                    [vlan-min <vid_min>
                    vlan-max <vid_max>]
                    [vlan-tag <tagged | untagged>]
                    [ethertype <etype>]
```

```
[priority <ieee1p_seq>]
[drop-action {enable | disable}]
[update-dscp <0 - 63>]
[update-1p <0 - 7>]
[set-drop-prec {high-drop | low-
drop}]
[block <block_name>]
```

Use the **no** form of this command to remove a Layer 2 access list.

Variable Definitions

Variable	Value
name <WORD>	The name assigned to this access list.
src-mac <source_mac_address>	The source MAC address to use for this access list.
src-mac-mask <source_mac_address_mask>	The source MAC address mask to use for this access list.
[dst-mac <destination_mac_address>]	The destination MAC address to use for this access list.
dst-mac-mask <destination_mac_address_mask>	The destination MAC address mask to use for this access list.
vlan-min <vid_min> vlan-max <vid_max>	The minimum and maximum VLANs to use with this access list. Both values must be specified.
vlan-tag <tagged | untagged>	Specify the VLAN tag classifier criteria: • untagged • tagged The default is Ignore.
ethertype <etype>	The Ethernet protocol type to use with the access list.
priority <ieee1p_seq>	The priority value to use with this access list. Valid range is 0-7 or all.
drop-action {enable | disable}	The drop action to use for this access list. Enable specifies to drop packets and disable specifies to not drop packets.
update-dscp <0 - 63>	The DSCP value to update for this access list.

Variable	Value
update-1p <0 - 7>	The 802.1p value to update for this access list.
set-drop-prec {high-drop | low-drop}	The drop precedence to configure for this access list.
block <block_name>	The block name to associate with the access list.

Configuring the CoS-to-Queue Assignments

CoS-to-queue assignments can be queried and modified using the following ACLI procedures.

Configuring CoS-to-Queue assignments

Use the following procedure to associate the 802.1p priority values with a specific queue within a specific queue set. This association determines the egress scheduling treatment that traffic with a specific 802.1p priority value receives.

Procedure steps

To configure CoS-to-Queue assignments, use the following command from Global Configuration mode:

```
qos queue-set-assignment queue-set <1-8> 1p <0-7> queue <1-8>
```

Variable Definitions

Variable	Value
1p <0-7>	Enter the 802.1p priority value for which the queue association is being modified; range is between 0 and 7.
queue <1-8>	Enter a number from 1–8 to specify the queue within the identified queue set to assign the 802.1p priority traffic at egress.
queue-set <1-8>	Specifies the QoS queue set. Values range from 1 to 8.

Configuring QoS Interface Groups

Ports can be added or deleted to or from an interface group or add or delete the interface groups themselves. This section covers the following ACLI commands.

Adding ports to an interface group

Use the following procedure to add ports to an interface group.

Procedure steps

To add ports to an interface group, use the following command from Interface Configuration mode:

```
[no] qos if-assign [port <portlist>] name [<WORD>]
```

Use the **no** form of this command to remove ports.

Important:
The system automatically removes the port from an existing interface group to assign it to a new interface group.

Variable Definitions

Variable	Value
port <portlist>	Enter the ports to add to interface group.
name <WORD>	Specify name of interface group.

Creating an interface group

Use the following procedure to create an interface group.

Procedure steps

To create an interface group, use the following command from Global Configuration mode:

```
[no] qos if-group name <WORD> class <trusted | untrusted |
unrestricted>
```

Use the **no** form of this command to delete an interface group.

Important:
An interface group referenced by an installed policy cannot be deleted.

Variable Definitions

Variable	Value
name <WORD>	Enter the name of the interface group; maximum is 32 US-ASCII. Name must begin with a letter a..z or A..Z.
class field; QoS: trusted ports; QoS:untrusted ports; QoS: unrestricted ports; interfaces; QoS:interfaces class <trusted | untrusted | unrestricted>	Defines a new interface group and specifies the class of traffic received on interfaces associated with this interface group: • trusted • untrusted • unrestricted

DSCP and 802.1p and queue association configuration using ACLI

Use the information in this section to configure DSCP, IEEE802.1p priority, and queue set association.

Configuring egress mapping using ACLI

Use the following procedure to configure DSCP-to-802.1p priority and drop precedence associations that are used for assigning these values at packet egress, based on the DSCP in the received packet.

Procedure steps

To configure egress mapping, use the following command from Global Configuration mode:

```
qos egressmap [name <WORD>] [ds <0-63>] [1p <0-7>] [dp <low-drop | high-drop>] [ds-new <0-63>]
```

Variable Definitions

Variable	Value
name <WORD>	Specifies the label for the egress mapping.
ds <0-63>	Specifies the DSCP value used as a lookup key for 802.1p priority and drop precedence at egress when appropriate; range is between 0 and 63.
1p <0-7>	Specifies the 802.1p priority value associated with the DSCP. Values range from 0–7.
dp <low-drop | high-drop>	Enter the drop precedence values associated with the DSCP: • low-drop • high-drop
ds-new <0-63>	Specifies a new DSCP value to use when DSCP mutation is required. Values range from 0–63.

Resetting egress mapping values

Use the following procedure to reset the egress mapping entries to factory default values.

Procedure steps

To reset the entries, use the following command from Global Configuration mode:

```
default qos egressmap
```

Configuring ingress mapping values

Use the following procedure to configure 802.1p priority-to-DSCP associations that are used for assigning default values at packet ingress based on the 802.1p value in the ingressing packet.

Procedure steps

To configure ingress mapping values, use the following command from Global Configuration mode:

```
qos ingressmap [name <WORD>] 1p <0-7> ds <0-63>
```

Variable Definitions

Variable	Value
name <WORD>	Specify the label for the ingress mapping.
1p <0-7>	Enter the 802.1p priority used as lookup key for DSCP assignment at ingress; range is between 0 and 7.
ds <0-63>	Enter the DSCP value associated with the target 802.1p priority; range is between 0 and 63.

Resetting ingress mapping values

Use the following procedure to reset ingress mapping values to factory default values.

Procedure steps

To reset the value, use the following command from Global Configuration mode:

```
default qos ingressmap
```

Configuring QoS for the NSNA solution

When you assign a filter set name using the **nsna vlan <vid> color <red|yellow|green> filter <name>** command (for example, **nsna vlan 110 color red filter**

redFilter), the switch automatically creates all the necessary (default) QoS classifiers for the specified color with the name you assigned (in this case, redFilter) if that filter set does not already exist. If you had previously defined the filter set (using the **qos nsna** command), then that pre-existent filter set is used. Once a filter set is created, it can be modified using the **qos nsna** command. NSNA functionality applies QoS filter sets to NSNA-enabled ports. A user defines a filter set first by defining the individual filters, followed by the overall filter set itself. The individual filters and the filter set share the same name string.

Note:

You must make any modifications to NSNA QoS filters before you enable NSNA globally or on any switch port.

Note:

When the NSNA filters are applied to a port, any existing QoS filters on that port are disabled, and the NSNA filters are applied. Pre-existing policies are re-enabled when NSNA is disabled.

Important:

New entries on nsna qos filters need to be added before enable nsna globally or nsna on ports. Otherwise an error can be returned. If NSNA is enabled and if you need to add new nsna qos entries to existing nsna qos filters, you have to disable NSNA.

Configuring QoS for NSNA filters

Use the following procedure to configure QoS for NSNA filters.

Procedure steps

To configure QoS for NSNA filters, use the following command from Global Configuration mode:

```
qos nsna
```

Note:

When using NSNA along with other applications, such as IP Source Guard, you must ensure resources are available for each application. It is recommended that applications such as IP Source Guard be applied to a small number of ports when used along with the QoS NSNA solution.

Variable Definitions

Variable	Value
classifier name [addr-type {ipv4|ipv6}] [block] [drop-action] [ds-field] [dst-ip] [dst-mac] [dst-port-min] [ethertype] [eval-order] [flow-id] [next-header] [priority] [protocol] [set-drop-prec] [src-ip] [src-mac] [src-port-min] [update-1p] [update-dscp] [vlan-min] [vlan-tag]	Creates the QoS NSNA classifier entry. Optional parameters: • addr-type {ipv4|ipv6} specifies the type of IP address used by this classifier entry. The type is limited to IPv4 and IPv6 addresses. • block specifies the label to identify access list elements that are of the same block. • drop-action specifies whether or not to drop non-conforming traffic. • ds-field specifies the value for the DiffServ Codepoint (DSCP) in a packet. • dst-ip specifies the IP address to match against the destination IP address of a packet. • dst-mac specifies the MAC address against which the MAC destination address of incoming packets is compared. • dst-port-min specifies the minimum value for the layer 4 destination port number in a packet. • ethertype specifies a value indicating the version of Ethernet protocol being used. • eval-order specifies the evaluation order for all elements with the same name. • flow-id specifies the flow identifier for IPv6 packets. • next-header specifies the IPv6 next-header value. Values are in the range 0-255. • priority specifies a value for the 802.1p user priority. • protocol specifies the IPv4 protocol value. • set-drop-prec specifies automatic drop precendence • src-ip specifies the IP address to match against the source IP address of a packet. • src-mac specifies the MAC source address of incoming packets. • src-port-min specifies the minimum value for the Layer 4 source port number in a packet.

Variable	Value
	• update-1p specifies an 802.1p value used to update user priority. • update-dscp specifies a value used to update the DSCP field in an IPv4 packet. • vlan-min specifies the minimum value for the VLAN ID in a packet. • vlan-tag specifies the type of VLAN tagging in a packet.
set name [committed-rate] [drop-nm-action] [drop-out-action] [max-burst-rate] [max-burst-duration] [update-dscp-out-action]	Creates the QoS NSNA set. Optional parameters: • committed-rate specifies the commited rate in Kbps. • drop-nm-action specifies the action to take when the packet is non-matching. This action is applied to all traffic that was not previously matched by the specified filtering data. Options are **enable** (packet is dropped) and **disable** (packet is not dropped). • drop-out-action specifies the action to take when a packet is out-of-profile. This action is only applied if metering is being enforced, and if the traffic is deemed out of profile based on the level of traffic and the metering criteria. Options are **enable** (packet is dropped) and **disable** (packet is not dropped). • max-burst-rate specifies the maximum number of bytes allowed in a single transmission burst. • max-burst-duration specifies the maximum burst duration in milliseconds. • update-dscp-out-action specifies the action to take when a dscp filed in an IPv4 packet is out of profile.

Job aid: Using QoS NSNA commands

The following command is an example of adding a classifier to an existing filter set (in this example, the ALPHAYELLOW filter set):

```
qos nsna classifier name ALPHAYELLOW dst-ip 10.80.22.25/32 ethertype
0x0800 drop-action disable eval-order 70
```

The following commands are an example of adding a classifier block (remedial) to an existing filter set (ALPHAYELLOW):

Note:

To consume only one precedence level, group classifiers in a classifier block.

```
qos nsna classifier name ALPHAYELLOW dst-ip 10.80.22.25/32 ethertype
0x0800 drop-action disable block remedial eval-order 70

qos nsna classifier name ALPHAYELLOW dst-ip 10.16.50.30/32 ethertype
0x0800 drop-action disable block remedial eval-order 71

qos nsna classifier name ALPHAYELLOW dst-ip 10.81.21.21/32 ethertype
0x0800 drop-action disable block remedial eval-order 72
```

The following commands are an example of classifiers configured to allow various TCP/UDP destination ports in the red filter set, and configured as a classifier block (novell):

```
qos nsna classifier name red protocol 17 dst-port-min 427 dst-port-
max 427 ethertype 0x0800 drop-action disable block novell eval-order
101

qos nsna classifier name red protocol 6 dst-port-min 524 dst-port-max
524 ethertype 0x0800 drop-action disable block novell eval-order 102

qos nsna classifier name red protocol 6 dst-port-min 396 dst-port-max
396 ethertype 0x0800 drop-action disable block novell eval-order 103
```

Note:

To modify an entry in a filter set, you must delete the entry and add a new entry with the desired modifications.

Deleting a classifier, classifier block, or an entire filter set

Use the following procedure to classifier, classifier block or filter set.

Note:

You cannot delete all the classifiers in a filter set. There should always be at least one remaining.

Procedure steps

1. To delete an entire filter set, use the following command from the Global configuration mode:

   ```
   no qos nsna name <filter name>
   ```

2. To delete a classifier, use the following command from the Global configuration mode:

```
no qos nsna name <filter name> eval-order <value>
```

3. To delete a classifier block, use the command for deleting a classifier to delete all the classifier members in that block.

QoS IP classifier element management using ACLI

Use the information in this section to configure and manage QoS IP classifier elements.

Configuring an IP classifier element using ACLI

Use the following procedure to create and manage an IP classifier element.

Procedure steps

To configure an IP classifier element, use the following command from Global Configuration mode:

```
qos ip-element <1-55000> [addr-type <addrtype>] [ds-field
<0-63>] [dst-ip <dst-ip-info>] [dst-port-min <0-65535>] [flow-
id <0x00-0xfffff>] [ip-flag <ip-flags>] [ipv4-option <no-opt|
with-opt>] [name <WORD>] [next-header <0-255>] [protocol
<0-255>] [session-id <1-4294967295>] [src-ip <src-ip-info>]
[src-port-min <0-65535>] [tcp-control <a|f|p|r|s|u>]
```

Important:
An IP element that is referenced in a classifier cannot be deleted.

Variable Definitions

The following table defines parameters that you enter with the **`qos ip-element <1-55000> [addr-type <addrtype>] [ds-field <0-63>] [dst-ip <dst-ip-info>] [dst-port-min <0-65535>] [flow-id <0x00-0xfffff>] [ip-flag <ip-flags>] [ipv4-option <no-opt|with-opt>] [name <WORD>] [next-header <0-255>] [protocol <0-255>] [session-id <1-4294967295>] [src-ip <src-ip-info>] [src-port-min <0-65535>] [tcp-control <a|f|p|r|s|u>`** command.

Variable	Value
<1-55000>	Specifies the IP classifier element identification number. Values range from 1–55000.

Variable	Value
addr-type <addr_type>	Specify the address type, either ipv4 or ipv6. The default is ipv4.
ds-field <0-63>	Specifies the value for the DSCP in a packet. Values range from 0–63.
dst-ip <dst-ip-info>	Enter the source IP address and mask in the form of a.b.c.d/x or a.b.c.d x.x.x.x for IPv4, or x:x:x:x:x:x:x:x/z for IPv6. Default is 0.0.0.0.
dst-port-min <0-65535>	Specifies the minimum value permitted for the Layer 4 destination port number in a packet. Values range from 0–65535.
flow-id <0x00-0xfffff>	Specifies the flow identifier for IPv6 packets. Values range from -1–1048575 (0x00 to 0xfffff hexadecimal). A value of -1 indicates that the system ignores this parameter.
ip-flag <ip_flags>	Specifies the value of flags present in an IPv4 header.
ipv4-option <no-opt|with-opt>	Specifies whether the Option field is present in the packet header. Values include: • no-opt—indicates that only IPv4 packets without options match this classifier element. • with-opt—indicates that only IPv4 packets that include options match this classifier element.
name <WORD>	Specifies an alphanumeric label for the IP classifier element. Value is a character string from 1–16 characters in length.
next-header <0-255>	Specifies the IPv6 next header the classifier element will match. Values range from 0–255. A value of 255 indicates that the system ignores the parameter.
protocol <0-255>	Specifies the IPv4 protocol. Values range from 0–255.
session-id <1-4294967295>	Specifies the session identification number. Values range from 1–4294967295.
src-ip <src_ip_info>	Specifies the source IP address and mask in the form of a.b.c.d/x for IPv4, or x:x:x:x:x:x:x:x/z for IPv6. Default is 0.0.0.0.
src-port-min <0-65535>	Specifies the minimum value permitted for the Layer 4 source port number in a packet. Values range from 0–65535.
tcp-control <a|f|p|r|s|u>	Specifies the control flags present in an TCP header. Values include:

Variable	Value
	• a=Ack • f=Fin • p=Psh • r=Rst • s=Syn • u=Urg

Deleting an IP classifier element using ACLI

Use the following procedure to delete an IP classifier element.

Procedure steps

To delete an IP classifier element, use the following command from Global Configuration mode:

```
no qos ip-element <1-55000>
```

Important:
An IP element that is referenced in a classifier cannot be deleted.

Variable Definitions

The following table defines parameters that you enter with the **`no qos ip-element <1-55000>`** command.

Variable	Value
<1-55000>	Specifies the identification number of the IP classifier element to delete. Values range from 1–55000.

Viewing IP classifier element information using ACLI

Use the following procedure to display IP classifier configuration information.

Procedure steps

To display IP classifier element information, use the following command from the Privileged EXEC mode:

```
show qos ip-element
```

Variable Definitions

The following table defines optional parameters that you can enter with the **`show qos ip-element`** command.

Variable	Value
<*1-65535*>	Specifies the IP classifier element entry for which to display configuration information. Values range from 1–65535.
<*all*>	Displays information for all configured IP classifier element configuration information.
<*system*>	Displays information for only system related IP classifier element configuration information.
<*user*>	Displays information for only user-configured IP classifier element configuration information.

QoS L2 classifier element management using ACLI

Use the information in this section to configure and manage QoS L2 classifier elements.

Configuring a Layer 2 classifier element using ACLI

Use the following procedure to create and manage a Layer 2 (L2) classifier element.

Procedure steps

To configure Layer 2 element entries, use the following command from Global Configuration mode:

```
qos l2-element <1-55000> [dst-mac <dst_mac_addr>][dst-mac-mask
<dst_mac_mask>] [ethertype <0x00-0xffff>] [name <WORD>] [pkt-
```

```
type <etherII|llc|snap>] [priority <0-7|all>] [session-id
<1-4294967295>] [src-mac <src_mac_addr>] [src-mac-mask
<src_mac_mask>] [vlan-min <1-4094>] [vlan-tag <tagged|
untagged>]
```

Important:
A Layer 2 element referenced in a classifier cannot be deleted.

Variable Definitions

The following table defines parameters that you enter with the **`qos l2-element <1-55000> [dst-mac <dst_mac_addr>][dst-mac-mask <dst_mac_mask>] [ethertype <0x00-0xffff>] [name <WORD>] [pkt-type <etherII|llc|snap>] [priority <0-7|all>] [session-id <1-4294967295>] [src-mac <src_mac_addr>] [src-mac-mask <src_mac_mask>] [vlan-min <1-4094>] [vlan-tag <tagged| untagged>]`** command.

Variable	Value
<1-55000>	Specifies the L2 classifier element identification number. Values range from 1–55000.
dst-mac <dst_mac_addr>	Specifies the MAC address against which the MAC destination address of incoming packets is compared. Use the H.H.H format.
dst-mac-mask <dst_mac_mask>	Specifies the destination MAC address mask. Use the H.H.H format.
ethertype <0x00-0xffff>	Specifies a value for the Ethernet type. Values range from 0x00 to 0xffff. If you enter a value of 0xffff, the system ignores this parameter. Default is ignore.
name <WORD>	Specifies an alphanumeric label for the L2 classifier entry. Value is a character string from 1–16 characters in length.
pkt-type <etherII|llc|snap>	Specifies the data link layer frame format that frames must have to match this L2 classifier entry. Values include: • ethernetII—only EthernetII format frames can match this classifier • snap—only IEEE 802 SNAP format frames can match this classifier • llc—only IEEE 802 LLC format frames can match this classifier
priority <0-7|all>	Specifies a value for the 802.1p user priority.

Variable	Value
	• 0-7—selects a specific priority value from 0–7 • all—selects all priority values
session-id <1-4294967295>	Specifies the session identification number. Values range from 1–4294967295.
src-mac <src_mac_addr>	Specifies the source MAC address of incoming packets. Use the H.H.H format.
src-mac-mask <src_mac_mask>	Specifies a mask identifying the source MAC address. Use the H.H.H format.
vlan-min <1-4094>	Specifies the minimum VLAN ID range for the L2 classifier element. Values range from 1–4094.
vlan-tag <tagged|untagged>	Specifies the type of VLAN tagging in a packet. Values include: • untagged • tagged

Deleting a Layer 2 classifier element using ACLI

Use the following procedure to delete an L2 classifier element.

Procedure steps

To delete an IP classifier element, use the following command from Global Configuration mode:

```
no qos l2-element <1-55000>
```

Important:
An IP element that is referenced in a classifier cannot be deleted.

Variable Definitions

The following table defines parameters that you enter with the **`no qos l2-element <1-55000>`** command.

Variable	Value
<1-55000>	Specifies the identification number of the L2 classifier element to delete. Values range from 1–55000.

Viewing Layer 2 classifier element information using ACLI

Use the following procedure to display Layer 2 classifier configuration information.

Procedure steps

To display Layer 2 classifier element information, use the following command from the Privileged EXEC mode:

```
show qos l2-element
```

Variable Definitions

The following table defines optional parameters that you can enter with the **`show qos l2-element`** command.

Variable	Value
<1-65535>	Specifies the L2 classifier element entry for which to display configuration information. Values range from 1–65535.
<all>	Displays information for all configured L2 classifier element configuration information.
<system>	Displays information for only system related L2 classifier element configuration information.
<user>	Displays information for only user-configured L2 classifier element configuration information.

QoS system classifier element management using ACLI

Use the information in this section to configure and manage QoS system classifier elements.

Configuring a QoS system classifier element using ACLI

Use this procedure to create and manage a QoS system classifier element.

Important:

In order to be able to create a policy based on a system classifier element, you should specify a pattern-ip-version at system element creation. Otherwise, a system element with pattern

ip version – Not Applicable will be created. This element will be useful as a template for other system elements.

Procedure steps

To create and manage a QoS system classifier element, use the following command from Global Configuration mode:

```
qos system-element <1-55000> [known-ip-mcast] [known-non-ip-
mcast] [name <WORD>] [non-ip] [pattern-data <WORD>] [pattern-
format <tagged | untagged>] [pattern-ip-version <ipv4|ipv6|non-
ip>] [pattern-l2-format <ethernetII|llc|snap>] [session-id
<1-4294967295>] [unknown-ip-mcast] [unknown-non-ip-mcast]
[unknown-ucast]
```

Variable Definitions

The following table defines parameters that you enter with the **`qos system-element <1-55000> [known-ip-mcast] [known-non-ip-mcast] [name <WORD>] [non-ip] [pattern-data <WORD>] [pattern-format <tagged | untagged>] [pattern-ip-version <ipv4|ipv6|non-ip>] [pattern-l2-format <ethernetII|llc|snap>] [session-id <1-4294967295>] [unknown-ip-mcast] [unknown-non-ip-mcast] [unknown-ucast]`** command.

Variable	Value
<1-55000>	System classifier element entry id; range is 1–55000.
known-ip-mcast	Matches frames with known IP multicast destination address.
known-non-ip-mcast	Matches frames with known non-IP multicast destination address.
name <WORD>	Specifies an alphanumeric label for the system classifier entry. Value is a character string from 1–16 characters in length.
non-ip	Matches non-IP frames.
pattern-data <WORD>	Matches frames with specific byte pattern data. The format of the WORD string is byte numbers separated by colons (XX:XX:XX:.....:XX.).
pattern-format <tagged | untagged>	Specifies the format of the pattern data and mask. Values include tagged or untagged.
pattern-ip-version <ipv4|ipv6|non-ip>	Specifies the IP version of the pattern data and mask. Values include ipv4, ipv6, or non-ip.

Variable	Value
pattern-l2-format <ethernetII|llc|snap>	Specifies the format of the L2 pattern data and mask. Values include: • ethernetII • llc • snap
session-id <1-4294967295>	Specifies the session identifier.
unknown-ip-mcast	Matches frames with an unknown IP multicast destination address.
unknown-non-ip-mcast	Matches frames with an unknown non-IP multicast destination address.
unknown-ucast	Matches frames with an unknown unicast destination address.

Deleting a QoS system classifier element using ACLI

Use this procedure to delete a QoS system classifier element from your system.

Important:
In order to be able to create a policy based on a system classifier element, you should specify a pattern-ip-version at system element creation. Otherwise, a system element with pattern ip version – Not Applicable will be created. This element will be useful as a template for other system elements.

Procedure steps

To delete a QoS system classifier element, use the following command from the Global Configuration mode:

```
no qos system-element <1-55000>
```

Variable Definitions

The following table defines parameters that you enter with the **`qos system-element <1-55000>`** command.

Variable	Value
<1-55000>	Specifies the identifier for system classifier element to delete. Values range from 1–55000.

Viewing system classifier element information using ACLI

Use this procedure to display system classifier configuration information.

Procedure steps

To display system classifier element information, use the following command from the Privileged EXEC mode:

```
show qos system-element
```

Variable Definitions

The following table defines optional parameters that you can enter with the **`show qos system-element`** command.

Variable	Value
<*1-65535*>	Specifies the system classifier element entry for which to display configuration information. Values range from 1–65535.
<*all*>	Displays information for all configured system classifier element configuration information.
<*system*>	Displays information for only system related classifier element configuration information.
<*user*>	Displays information for only user-configured system classifier element configuration information.

QoS classifier management using ACLI

Use the information in this section to configure and manage QoS classifiers.

Configuring a QoS classifier using ACLI

Use the following procedure to facilitate the linking of individual IP and L2 classifier elements into a single classifier.

Procedure steps

To configure classifier entries, use the following command from Global Configuration mode:

```
qos classifier <1-55000> set-id <1-55000> [name <WORD>]
element-type {ip | l2 | system} element-id <1-55000> [session-
id <1-4294967295>]
```

Use the **no** form of this command to remove a classifier entry.

Important:
A classifier that is referenced in a classifier block or installed policy cannot be deleted.

Variable Definitions

Variable	Value
classifier <1-55000>	Enter an integer to specify the classifier ID; range is 1–55000.
set-id <1-55000>	Enter an integer to specify the classifier set ID; range is 1–55000.
name <WORD>	Specify the set label; maximum is 16 alphanumeric characters.
element-type {ip| l2 |system}	Specify the element type; either ip or l2, or system classifier.
element-id <1-55000>	Specify the element ID; range is 1–55000.
session-id <1-4294967295>	Specify the session ID.

Deleting a QoS classifier using ACLI

Use the following procedure to delete a QoS classifier from your system.

Procedure steps

To delete a QoS classifier, use the following command from Global Configuration mode:

```
no qos classifier <1-55000>
```

Important:
A classifier that is referenced in a classifier block or installed policy cannot be deleted.

Variable Definitions

The following table defines parameters that you enter with the **no qos classifier <1-55000>** command.

Variable	Value
<1-55000>	Enter an integer to specify the classifier ID; range is 1–55000.

Viewing QoS classifier information using ACLI

Use the following procedure to display QoS classifier configuration information.

Procedure steps

To display QoS classifier configuration information, use the following command from the Privileged EXEC mode:

```
show qos classifier
```

Variable Definitions

The following table defines optional parameters that you can enter with the **show qos classifier** command.

Variable	Value
<1-65535>	Specifies the classifier element entry for which to display configuration information. Values range from 1–65535.
<all>	Displays information for all configured classifier element configuration information.
<system>	Displays information for only system related classifier element configuration information.

Variable	Value
<user>	Displays information for only user-configured classifier element configuration information.

QoS classifier block management using ACLI

Use the information in this section to view and manage QoS classifier blocks.

Configuring classifier block entries using ACLI

Use this procedure to combine individual classifiers.

Procedure steps

To configure classifier block entries, use the following command from the Global Configuration mode:

```
qos classifier-block <1-55000> block-number <1-55000> [name
<WORD>]{set-id <1-55000> | set-name <WORD>} [{in-profile-action
<1-55000> | in-profile-action-name <WORD>} | {meter <1-55000> |
meter-name <WORD>}] [session-id <1-4294967295>] [eval-order]
```

Important:
A classifier block that is referenced in an installed policy cannot be deleted.

Variable Definitions

The following table defines parameters that you enter with the **`qos classifier-block <1-55000> block-number <1-55000> [name <WORD>]{set-id <1-55000> | set-name <WORD>} [{in-profile-action <1-55000> | in-profile-action-name <WORD>} | {meter <1-55000> | meter-name <WORD>}] [session-id <1-4294967295>] [eval-order <1-65535>]`** command.

Variable	Value
<1-55000>	Enter an integer to specify the classifier block ID; range is 1–55000.
block-number <1-55000>	Specify the classifier block number; range is 1–55000.

Variable	Value
[eval-order <1-65535>]	Specifies the block entry evaluation order. Values range from 1–655355.
name <WORD>	Specify the label for the classifier block; maximum is 16 alphanumeric characters.
set-id <1-55000>	Specify the classifier set to be linked to the classifier block; range is 1–55000.
set-name <WORD>	Specify the classifier set name to be linked to the classifier block; maximum is 16 alphanumeric characters.
in-profile-action <1-55000>	Specify the in profile action to be liqosked to the filter block; range is 1–55000.
in-profile-action-name <WORD>	Specify the in profile action name to be linked to the classifier block; maximum is 16 alphanumeric characters.
meter <1-55000>	Specify the meter to be linked to the classifier block; range is 1–55000.
meter-name <WORD>	Specify the meter name to be linked to the classifier block; maximum is 16 alphanumeric characters.
session-id <1-4294967295>	Specify the session ID.

Deleting a classifier block entry using ACLI

Use this procedure to delete a classifier block from your system.

Procedure steps

To delete a classifier block, use the following command from the Global Configuration mode:

```
no qos classifier-block <1-55000>
```

Important:
A classifier block that is referenced in an installed policy cannot be deleted.

Variable Definitions

The following table defines parameters that you enter with the **`no qos classifier-block <1-55000>`** command.

Variable	Value
<1-55000>	Enter an integer to specify the classifier block ID; range is 1–55000.

Viewing a classifier block entry using ACLI

Use this procedure to delete a classifier block from your system.

Procedure steps

To delete a classifier block, use the following command from the Global Configuration mode:

```
show qos classifier-block
```

Important:
A classifier block that is referenced in an installed policy cannot be deleted.

Variable Definitions

The following table defines optional parameters that you can enter with the **`show qos classifier-block`** command.

Variable	Value
<1-65535>	Specifies the classifier element entry for which to display configuration information. Values range from 1–65535.
<all>	Displays information for all configured classifier element configuration information.
<system>	Displays information for only system related classifier element configuration information.
<user>	Displays information for only user-configured classifier element configuration information.

QoS traffic profile filter set configuration using ACLI

Use the information in this section to configure QoS traffic profile filter set support.

Configuring a QoS traffic profile filter set classifier using ACLI

Use this procedure to add or delete a QoS traffic profile filter set classifier.

Procedure steps

To create a new traffic profile filter set classifier element, use the following command from the Global configuration mode:

```
qos traffic-profile classifier [name <WORD>]
```

Variable definitions

The following table defines the variables you can enter with the **`qos traffic-profile classifier [name <WORD>]`** command.

Variable	Value
`name <WORD>`	Specifies an alphanumeric identifier for the traffic profile. The value is a character string from 1–16 characters in length. All classifiers associated with a specific traffic-profile filter set share the same name.
`addr-type <ipv4 | ipv6>`	Specifies the type of IP address used by this classifier entry. The type is limited to IPv4 and IPv6 addresses.
`block <WORD>`	Specifies the label to identify traffic profile classifier elements that are of the same block.
`committed-rate <64-10230000>`	Specifies the committed rate for metering. Values range from 64-10230000 Kbps.
`committed-burst-size <burst-size-options>`	Specifies the committed burst size in KiloBytes.
`drop-action <disable | enable>`	Specifies whether to drop (enable) or pass (disable) traffic matching the classifier criteria.
`drop-out-action <disable | enable>`	Specifies whether to drop (enable) or pass (disable) out of profile packets..
`ds-field <0-63>`	Specifies the value for the DiffServ Codepoint (DSCP) in a packet.

Variable	Value
dst-ip <dst-ip-info>	Specifies the IP address to match against the destination IP address of a packet. • IPv4 source—use the A.B.C.D/<0-32> format • IPv6 source—use the x:x:x:x:x:x:x:x/<0-128> format
dst-mac <dst-mac-info>	Specifies MAC address against which the MAC destination address of incoming packets is compared.
src-mac <src-mac>	Specifies the MAC source address of incoming packets.
dst-mac-mask <dst-mac-mask>	Specifies the mask for the MAC address against which the MAC destination address of incoming packets is compared.
src-mac-mask <src-mac-mask>	Specifies the MAC source address mask of incoming packets.
dst-port-min <0-65535>	Specifies the minimum value for the Layer 4 destination port classifier.
src-port-min <0-65535>	Specifies the minimum value for the Layer 4 source port number in a packet.
dst-port-max <0-65535>	Specifies the maximum value for the Layer 4 destination port classifier.
src-port-max <0-65535>	Specifies the maximum value for the Layer 4 source port number in a packet.
ethertype <0x0-0xFFFF>	Specifies the type of information carried in the data portion of the frame. Values range from 0x0 to 0xFFFF hexadecimal.
eval-order <1-255>	Specifies the evaluation order for all elements with the same name. Values range from 1–255.
flow-id <0x0-0xFFFF>	Specifies the flow identifier for IPv6 packets. Values range from 0x0 to 0xFFFF hexadecimal.
ip-flag <ip-flags>	Specifies the IP fragment flag criteria.
ipv4-option <no-opt | with-opt>	Specifies the IPv4 option criteria.
master	Designates the classifier as the master block member.

Variable	Value
`max-burst-rate <64-4294967295>`	Specifies the maximum burst rate. Values range from 64 to 4294967295 Kbps. You configure this parameter when a committed metering rate is specified.
`max-burst-duration <1-4294967295>`	Specifies the maximum burst duration in milliseconds (ms). Values range from 1 to 4294967295 ms. You configure this parameter when a committed metering rate is specified.
`next-header <0-255>`	Specifies the IPv6 next-header value. Values range from 0–255.
`pkt-type <etherll | llc | snap>`	Specifies the filter packet format ethertype encoding criteria.
`priority <0-7 | all>`	Specifies a 802.1p user priority value for classifier.
`protocol <0-255>`	Specifies the IPv4 protocol value. Values range from 0–255.
`set-drop-prec <high-drop | low-drop>`	Specifies the drop precedence for traffic matching the classifier criteria. • high-drop—a higher probability that the packet will be dropped when traffic congestion occurs • low-drop—a lower probability that the packet will be dropped when traffic congestion occurs
`set-drop-prec-out-action <high-drop | low-drop>`	Specifies the drop precedence value associated with out of profile traffic. • high-drop—a higher probability that the packet will be dropped when traffic congestion occurs • low-drop—a lower probability that the packet will be dropped when traffic congestion occurs
`src-ip <src-ip-info>`	Specifies the IP address to match against the source IP address of a packet. • IPv4 source—use the A.B.C.D/<0-32> format • IPv6 source—use the x:x:x:x:x:x:x:x/<0-128> format

Variable	Value
`tcp-control <Urg | Ack | Psh | Rst | Syn | Fin>`	Specifies the TCP control criteria.
`update-1p <0-7>`	Specifies the 802.1p user priority update value.
`update-dscp <0-63>`	Specifies the DSCP update value.
`update-dscp-out-action <0-63>`	Specifies the DSCP update value in out of profile packets.
`vlan-min <1-4094>`	Specifies the minimum VLAN ID value for the classifier.
`vlan-max <1-4094>`	Specifies the maximum VLAN ID value for the classifier.
`vlan-tag <tagged | untagged>`	Specifies whether VLAN tagged or untagged traffic is matched by the classifier.

Deleting a QoS traffic profile filter set classifier using ACLI

Use this procedure to delete an existing QoS traffic profile filter classifier.

Procedure steps

To delete a QoS traffic profile filter classifier, use the following command from the Global configuration mode:

```
no qos traffic-profile classifier name <WORD> [eval-order <1-255>]
```

Variable definitions

The following table defines parameters that you enter with the **`no qos traffic-profile classifier name <WORD> [eval-order <1-255>]`** command.

Variable	Value
`name <WORD>`	Specifies an alphanumeric identifier used to target the traffic profile filter set classifier being deleted. The value is a character string from 1–16 characters in length.

Variable	Value
`eval-order <1-255>`	Specifies the evaluation order for all elements with the same name. Values range from 1–255.

Configuring a QoS traffic profile filter set using ACLI

Use this procedure to create a new or modify an existing traffic profile filter set.

Procedure steps

To configure a QoS traffic profile filter set, use the following command from the Global configuration mode:

```
qos traffic-profile set port <port> name <name>
```

Variable definitions

The following table defines the variables you enter with the **`qos traffic-profile set port <port>`** command.

Variable	Value
`committed-rate <64-10230000>`	Specifies the committed rate for metering. Values range from 64-10230000 Kbps.
`committed-burst-size <burst-size-options>`	Specifies the committed burst size in KiloBytes.
`drop-out-action <enable | disable>`	Specifies whether to drop (enable) or pass (disable) out-of-profile packets. You configure this parameter when a metering type is selected and a committed metering rate is specified.
`enable`	Enables the traffic profile filter set.
`name <WORD>`	Specifies the traffic profile filter set name. This name is used to identify classifier elements that are associated with the filter set.
`max-burst-rate <64-4294967295>`	Specifies the maximum burst rate. Values range from 64 to 4294967295 Kbps. You configure this parameter when a committed metering rate is specified.

Variable	Value
`max-burst-duration <1-4294967295>`	Specifies the maximum burst duration in milliseconds (ms). Values range from 1 to 4294967295 ms. You configure this parameter when a committed metering rate is specified.
`meter-mode <uniform-per-policy | individual-per-policy | classifier>`	Specifies the metering type. • uniform-per-policy—a unique meter is applied to each policy that comprises the filter set with uniform rate and burst data derived from the filter set specification used for each meter • individual-per-policy—a unique meter is applied to each policy that comprises the filter set with rate and burst data derived from the classifier data or the filter set specification • classifier—a meter is defined for each individual filter set classifier using rate and burst data associated with the classifier. If this data is not present a meter is not allocated for the classifier
`port <port>`	Specifies the ports on which the traffic profile filter set is to be applied.
`set-drop-prec-out-action <high-drop | low-drop>`	Specifies the drop precedence value for out-of-profile traffic. • high-drop—there is a higher probability of packets being dropped when network congestion is encountered. • low-drop—there is a lower probability of packets being dropped when network congestion is encountered. You configure this parameter when a metering type is selected and a committed metering rate is specified.
`track-statistics <aggregate|disable|individual>`	Specifies how to track policy statistics for the traffic profile filter set.

Variable	Value
	• aggregate—all traffic profile classifiers associated with a policy share the statistics resource • disable—statistics tracking is disabled for all traffic profile classifiers • individual—each traffic profile filter set classifier has its own statistics resource
`update-dscp-out-action <0-63>`	Updates the DSCP value in out-of-profile IP packets. Values range from 0 to 63. You configure this parameter when a metering type is selected and a committed metering rate is specified.

Disabling a QoS traffic profile filter set using ACLI

Use this procedure to delete or disable an existing traffic profile filter set.

If you have already disabled a QoS Traffic Profile set, you can re-enable it using one of the following commands:

- **`qos traffic-profile set name <WORD> enable`** to enable the QoS traffic profile filter set on all ports where it was initially applied
- **`qos traffic-profile set port <port> name <WORD> enable`** to enable the QoS traffic profile filter set on specified ports only

Procedure steps

To disable or delete a QoS traffic profile filter set, use the following command from the Global configuration mode:

```
no qos traffic-profile set port [port <port>] name <WORD>
enable
```

Variable definitions

The following table defines parameters that you enter with the **`no qos traffic-profile set port <port> name <WORD> enable`** command.

Variable	Value
`port <port>`	Specifies the port or ports on which to disable or delete the traffic profile filter set.

Variable	Value
`name <WORD>`	Specifies the traffic profile filter set name to disable or delete.
`enable`	Disables the traffic profile filter set. **Important:** If you do not include *enable* with the command, the filter set instance is deleted.

Viewing QoS traffic profile filter set classifier information using ACLI

Use this procedure to display QoS traffic profile filter set classifier configuration information.

Procedure steps

To display information for configured QoS traffic profile classifiers, use the following command from the Privileged EXEC configuration mode:

```
show qos traffic-profile classifier [name <WORD>]
```

Variable definitions

The following table defines parameters that you enter with the **`show qos traffic-profile classifier [name <WORD>]`** command.

Variable	Value
`name <WORD>`	Specifies the alphanumeric identifier of a specific traffic profile filter set for which to display classifier configuration information.

Viewing QoS traffic profile filter set information using ACLI

Use this procedure to display QoS traffic profile filter set configuration information for a traffic profile filter set instance.

Procedure steps

To display traffic profile filter set information for configured QoS traffic profile set instances, use the following command from the Privileged EXEC configuration mode:

```
show qos traffic-profile set [port <port>] name <WORD>
```

Variable definitions

The following table defines parameters that you enter with the **`show qos traffic-profile set [port <port>] [name <WORD>]`** command.

Variable	Value
`name <WORD>`	Specifies the alphanumeric identifier of the traffic profile filter set for which to display configuration information.
`port <port>`	Specifies the classifier port or ports for which to display traffic profile filter set configuration information.

Viewing QoS traffic profile filter set interface information using ACLI

Use this procedure to display QoS traffic profile filter set configuration information for switch or stack interfaces.

Procedure steps

To display QoS traffic profile filter set interface information, use the following command from the Privileged EXEC configuration mode:

```
show qos traffic-profile interface
```

Viewing QoS traffic profile filter set statistics information using ACLI

Use this procedure to display QoS traffic profile filter set statistics for a specific port and traffic profile filter classifier.

Procedure steps

To display QoS traffic profile filter set statistics, use the following command from the Privileged EXEC configuration mode:

```
show qos traffic-profile statistics port <port> name <WORD>
[precedence <1-7>]
```

Variable definitions

The following table defines parameters that you enter with the **`show qos traffic-profile statistics port <port> name <WORD> [precedence <1-7>]`** command.

Variable	Value
`name <WORD>`	Specifies the alphanumeric identifier of the traffic profile filter set for which to display statistics data.
`port <port>`	Specifies the classifier port or ports for which to display traffic profile filter set statistics data.
`precedence <1-7>`	Specifies the policy precedence in relation to other policies associated with the same traffic profile. Values range from 1–7. Specifying a precedence value displays statistics data for filter set classifiers associated with the specified precedence value only. If you do not specify a precedence value, statistics data is displayed for all precedence values used by the filter set instance.

Configuring QoS actions

The configuration of QoS actions directs the Avaya Ethernet Routing Switch 4500 Series to take specific action on each packet. Use the following procedure to create or update a QoS action.

Important:

Certain options can be restricted based on the policy associated with the specific action. An action that is referenced in a meter or an installed policy cannot be deleted.

Important:

You may notice unequal drop rates for two similar packet flows using similar sized fixed length packets when QOS congestion testing is performed on Avaya Ethernet Routing Switch 4500.

Procedure steps

To create or update a QoS action, use the following command from Global Configuration mode:

```
[no] qos action <10-55000> [name <WORD>] [drop-action <enable | disable | deferred-pass>] [update-dscp <0-63>] [update-1p {<0-7> | use-tos-prec | use-egress}] [set-drop-prec <low-drop | high-drop>] [action-ext <1-55000> | action-ext-name <WORD>]
```

Use the **no** form of this command to delete a QoS action.

Variable Definitions

Variable	Value
<10-55000>	Enter an integer to specify the QoS action; range is 10–55000.
name <WORD>	Assigns a name to a QoS action with the designated action ID. Enter the name for the action; maximum is 16 alphanumeric characters
drop-action<enable | disable | deferred-pass>	Specifies whether packets are dropped or not: • enable--drop the traffic flow • disable--do not drop the traffic flow • deferred-pass--traffic flow decision deferred to other installed policies Default is deferred pass. **Important:** If you omit this parameter, the default value applies.
update-dscp <0-63>	Specifies whether DSCP value are updated or left unchanged; unchanged equals ignore. Enter the 6-bit DSCP value; range is 0–63. Default is ignore.

Variable	Value
update-1p<0-7>	Specifies whether 802.1p priority value are updated or left unchanged; unchanged equals ignore: • ieee1p--enter the value you want; range is 0–7 • use-egress--uses the egress map to assign value • use-tos-prec--uses the type of service precedence to assign value. Default is ignore.
set-drop-prec <low-drop | high-drop>	Enter the loss-sensitivity value: • low-drop • high-drop Default is low-drop.
action-ext <1-55000>	Enter an integer to specify the action extension; range is 1–55000.
action-ext-name <WORD>	Specify a label for the action extension; maximum is 16 alphanumeric characters.

Configuring interface action extension entries

QoS interface action extensions direct the Avaya Ethernet Routing Switch 4500 Series to take specific action on each packet.

Use the following procedure to create interface action extension entries.

Important:
An interface extension that is referenced in an action entry cannot be deleted.

Important:
All traffic (both unicast and non-unicast) should be redirected to the same port.

Procedure steps

To create entries, use the following command from Global Configuration mode:

```
[no] qos if-action-extension <1-55000> [name <WORD>] {egress-ucast <port> | egress-non-ucast <port> } [sesson-id]
```

Use the **no** form of this command to delete entries.

Variable Definitions

Variable	Value
<1-55000>	Enter an integer to specify the QoS action. The range is 1–55000
name <WORD>	Assigns a name to a QoS action with the designated action ID. Enter the name for the action; maximum is 16 alphanumeric characters
egress-ucast <port> | egress-non-ucast <port>	Specify redirection of unicast/non-unicast to specified port.
session-id	Specify the session ID.

Configuring QoS meters

Use the following procedure to set the meters, if you want to meter or police the traffic, configure the committed rate, burst rate, and burst duration.

Important:

In case committed rate is not a multiple of 64, this value is rounded down to the highest multiple of 64, smaller than committed rate. For example, a committed rate of 1000 kbps is automatically rounded down to 960 kbps.

Procedure steps

To configure or create a QoS meter, use the following command from Global Configuration mode:

```
[no] qos meter <1-55000> [name <WORD>] [committed-rate
<64-32000000>] [burst-size <burst-size>] [max-burst-rate
<64-4294967295>] [max-burst-duration <1-4294967295>] {in-
profile-action <1-55000> | in-profile-action-name <WORD>} {out-
profile-action <1,9-55000> | out-profile-action-name <WORD>}
[session-id <1-4294967295>]
```

Use the **no** form of this command to delete a QoS meter entry.

Important:
A meter that is referenced in an installed policy cannot be deleted.

Variable Definitions

Variable	Value
<1-55000>	Enter an integer to specify the QoS meter; range is 1–55000.
name <WORD>	Specify name for meter; maximum is 16 alphanumeric characters.
committed-rate <64-32000000>	Specifies rate that traffic must not exceed for extended periods to be considered in-profile. Enter the rate in Kb/s for in-profile traffic in increments of 1000 Kbits/sec; range is 64–32000000 Kbits/sec.
burst-size <burst-size>	Committed burst size in Kilobytes. The value range is: 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384.
max-burst-rate <64-4294967295>	Specifies the largest burst of traffic that can be received a given time for the traffic to be considered in-profile. Used in calculating the committed burst size. Enter the burst size in Kb/s for in-profile traffic; range is 64–4294967295 Kbits/sec
max-burst-duration <1-4294967295>	Specifies the amount of time that the largest burst of traffic that can be received for the traffic to be considered in-profile. Used in calculating the committed burst size. Enter the burst duration in ms for in-profile traffic; range is 1–4294967295 ms.
in-profile-action <1-55000>	Specify the in-profile action ID; range is 1–55000.
in-profile-action-name <WORD>	Specify the in-profile action name.
out-profile-action-name <WORD>	Specify the out-profile action name.
out-profile-action <1,9-55000>	Specify the out-of-profile action ID; range is 1,9–55000.
session-id <1-4294967295>	Specify the session ID.

Configuring QoS Interface Shaper

Use the following procedure to configure the interface shaping parameters for a set of ports.

Procedure steps

To configure parameters, use the following command from Interface Configuration mode:

```
[no] qos if-shaper [name <WORD>] [shape-rate <64-10230000>]
[burst-size <burst-size>] [max-burst-rate <64-4294967295>]
[max-burst-duration <1-4294967295>]
```

Use the **no** form of this command to disable interface shaping for a set of ports.

Variable Definitions

Variable	Value
<WORD>	Specify name for if-shaper; maximum is 16 alphanumeric characters.
shape-rate <64-10230000>	Shaping rate in kilobits/sec; range is 64-10230000 kilobits/sec.
burst-size <burst-size>	Committeed burst size in Kilobytes. The value range is: 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384.
max-burst-rate <64-4294967295>	Maximum burst rate in kilobits/sec; range is 64-4294967295Kbits/sec.
max-burst-duration <1-4294967295>	Maximum burst duration in milliseconds; range is 1–4294967295 ms.

Creating a QoS interface queue shaper using ACLI

Use the following procedure to create an egress queue shaper for one or more interfaces.

Procedure steps

To create an egress queue shaper, use the following command from the Interface Configuration mode:

```
qos if-queue-shaper [port <portlist>] [queue <1-8>] [name
<WORD>] shape-rate <0-10230000> shape-min-rate <0-10230000>
```

Important:

If you configure the shape rate to 0 for a specific queue or port, shaping is not performed on that queue or port.

Variable Definitions

Variable	Value
name <WORD>	Specifies an alphanumeric label used to identify the QoS interface queue shaper. Value is a character string ranging from 1–16 characters in length.
port <portlist>	Specifies the port or list of ports for which to apply egress queue shaping.
queue <1-8>	Specifies the queue for the selected interface port or ports, on which traffic is shaped. The range of available values is determined by the OoS agent default queue configuration.
shape-min-rate <0-10230000>	Specifies the minimum QoS interface queue shaping rate, in kilobits per second (Kbps). Values range from 0 to10230000 Kbps.
shape-rate <0-10230000>	Specifies the QoS interface queue shaping rate, in kilobits per second (Kbps). Values range from 0 to10230000 Kbps.

Deleting a QoS interface queue shaper using ACLI

Use the following procedure to delete an egress queue shaper for one or more interfaces.

Procedure steps

To delete an egress queue shaper, use the following command from the Interface Configuration mode:

```
no qos if-queue-shaper [port <portlist>] [queue <1-8>]
```

Variable Definitions

Variable	Value
name <WORD>	Specifies an alphanumeric label used to identify the QoS interface queue shaper. Value is a character string ranging from 1–16 characters in length.
port <portlist>	Specifies the port or list of ports for which to delete egress queue shaping.
queue <1-8>	Specifies the queue for the selected interface port or ports, on which traffic is shaped. The range of available values is determined by the OoS agent default queue configuration.

Viewing QoS interface queue shaper information using ACLI

Use the following procedure to display egress queue shaper information for one or more interfaces.

Procedure steps

To display egress queue shaper information, use the following command from the Interface Configuration mode:

```
show qos if-queue-shaper [port <portlist>]
```

Variable Definitions

Variable	Value
port <portlist>	Specifies the port or list of ports for which to display egress queue shaping.

Configuring QoS Policies

Use the following procedure to configure QoS policies.

Important:

All components associated with a policy, including the interface group, element, classifier, classifier block, action, and meter, must be defined before referencing those components in a policy.

Related topics:

[Procedure steps](#) on page 92
[Variable Definitions](#) on page 92

Procedure steps

To configure QoS policies, use the following command from Global Configuration mode:

```
[no] qos policy <1-55000> [enable | disable] [name <WORD>]
[port <port_list>] if-group <WORD> clfr-type {classifier |
block} {clfr-id <1-55000> | clfr-name <WORD>} {{in-profile-
action <1-55000> | in-profile-action-name <WORD>} | meter
<1-55000> | meter-name <WORD>} precedence <1-8> [track-
statistics <individual | aggregate>]} [session-id
<1-4294967295>]
```

Use the **no** form of this command to delete QoS policy entries.

Variable Definitions

Variable	Value
<1-55000>	Enter an integer to specify the QoS policy; range is 1–55000.
[enable | disable]	Enable or disable the QoS policy. Default is disable.
name <WORD>	Enter the name for the policy; maximum is 16 alphanumeric characters.
port <port_list>	The ports to which to directly apply this policy.

Variable	Value
if-group <WORD>	Enter the interface group name to which this policy applies; maximum number of characters is 32 US-ASCII.The group name must begin with a letter within the range a..z or A..Z.
clfr-type <classifier | block>	Specify the classifier type; classifier or block.
clfr-id <1-55000>	Specify the classifier ID; range is 1–55000.
clfr-name <WORD>	Specify the classifier name or classifier block name; maximum is 16 alphanumeric characters.
in-profile-action <1-55000>	Enter the action ID for in-profile traffic; range is 1–55000.
in-profile-action-name <WORD>	Enter the action name for in-profile traffic; maximum is 16 alphanumeric characters.
meter <1-55000>	Enter meter ID associated with this policy; range is 1–55000.
meter-name <WORD>	Enter the meter name associated with this policy; maximum of 16 alphanumeric characters.
precedence <1-7>	Specifies the precedence of this policy in relation to other policies associated with the same interface group. Enter precedence number; range is 1–7. **Important:** Policies with a lower precedence value are evaluated after policies with a higher precedence number. Evaluation goes from highest value to lowest.
track-statistics <individual | aggregate>	Specifies statistics tracking on this policy, either: • individual--statistics on individual classifiers • aggregate--aggregate statistics
session-id <1-4294967295>	Specify the session ID.

Maintaining the QoS agent using ACLI

The following procedures allow for the maintenance of the QoS agent.

Enabling the QoS agent using ACLI

Use this procedure to enable QoS agent functionality for a switch or stack.

Procedure steps

To enable QoS agent functionality for a switch or stack, use either of the following commands from Global configuration mode:

```
qos agent oper-mode enable
```

```
default qos agent oper-mode
```

Disabling the QoS agent using ACLI

Use this procedure to disable QoS agent functionality for a switch or stack.

Procedure steps

To disable QoS agent functionality for a switch or stack, use either of the following commands from Global configuration mode:

```
no qos agent oper-mode enable
```

```
no qos agent oper-mode
```

Configuring QoS resource buffer sharing using ACLI

Use this procedure to configure how the QoS buffer resources are shared across ports.

Procedure steps

To configure QoS resource buffer sharing, use the following command from Global configuration mode:

```
qos agent buffer [regular|large|maximum]
```

Variable Definitions

Use the data in this table to configure the QoS resource buffer sharing.

Variable	Value
`regular`	Specifies the minimum amount of resource sharing.
`large`	Specifies the medium amount of resource sharing.
`maximum`	Specifies the maximum amount of resource sharing.

Changing the QoS resource buffer size to default using ACLI

Use this procedure to change the QoS resource buffer size to the default value (large).

Important:
Changes to the QoS buffer size are initiated only after the next switch restart.

Procedure steps

To configure the QoS resource buffer size to the default value, use the following command from Global configuration mode:

```
default qos agent buffer
```

Configuring Automatic QoS support using ACLI

This procedure describes how to configure the QoS agent AutoQoS mode.

Procedure steps

To configure QoS agent AutoQoS mode, use the following command from Global configuration mode:

```
qos agent aq-mode [disable|mixed|pure]
```

Variable Definitions

Variable	Value
disable	Specially marked application traffic processing is disabled on all ports.
mixed	Avaya application traffic processing is enabled on all port with egress DSCP mapping.
pure	Avaya application traffic processing is enabled on all ports without egress DSCP mapping.

Configuring NVRAM parameters using ACLI

Use the following procedure to specify the maximum amount of time, in seconds, before non-volatile QoS configuration is written to non-volatile storage. Delaying NVRAM access can be used to minimize file input and output. This can aid QoS agent efficiency if a large amount of QoS data is being configured.

Procedure steps

To configure NVRAM parameters, use the following command from Global Configuration mode:

```
qos agent nvram-delay <0-604800>
```

Resetting NVRAM parameters using ACLI

Use the following procedure to reset the NVRAM delay time to factory default.

Procedure steps

To reset NVRAM delay time, use the following procedure from Global Configuration mode:

```
default qos agent nvram-delay
```

Changing the QoS CoS queue set using ACLI

Use this procedure to modify the number of active QoS CoS queue sets.

Important:
Changes to the QoS CoS queue set are initiated only after the next switch restart.

Procedure steps

To modify the number of active QoS CoS queue sets, use the following command from Global configuration mode:

```
qos agent queue-set <1-8>
```

Variable Definitions

Use the data in this table to modify the number of active QoS CoS queue sets.

Variable	Value
<1-8>	Specifies the number of active QoS CoS queue sets. Values range from 1–8.

Changing the QoS CoS queue set to default using ACLI

Use this procedure to change the number of active QoS CoS queue sets to the switch default.

Important:
Changes to the QoS CoS queue set are initiated only after the next switch restart.

Procedure steps

To change the number of active QoS CoS queue sets to the switch default, use the following command from Global configuration mode:

```
default qos agent queue-set
```

Changing the QoS agent to factory defaults using ACLI

Use this procedure to change all QoS agent parameters to factory default values.

Procedure steps

To reset the QoS Agent to factory defaults, use the either of the following commands from Global Configuration mode:

```
default qos agent
```

```
qos agent reset-default
```

Configuring QoS statistics tracking using ACLI

Use this procedure to configure the type of statistics tracking to use with QoS.

Procedure steps

To configure QoS statistics tracking , use the following command from Global Configuration mode:

```
qos agent statistics-tracking [aggregate|disable|ind ividual]
```

Variable Definitions

Use the data in this table to configure QoS statistics tracking.

Variable	Value
`aggregate`	Allocates a single statistics counter to track data for all classifiers contained in the QoS policy being created.
`disable`	Disables statistics tracking.
`individual`	Allocates individual statistics counters to track data for each classifier contained in the QoS policy being created.

Changing QoS statistics tracking to default using ACLI

Use this procedure to change the QoS statistics tracking type to the factory default.

Procedure steps

To change the QoS statistics tracking type to the factory default, use the following command from Global Configuration mode:

```
default qos agent statistics-tracking
```

Viewing QoS agent configuration information using ACLI

Use this procedure to display general switch or stack QoS agent configuration information.

Procedure steps

To display general switch or stack QoS agent configuration information, use the following command from Privileged EXEC configuration mode:

```
show qos agent
```

Viewing QoS agent configuration details using ACLI

Use this procedure to display detailed switch or stack QoS agent configuration information.

Procedure steps

To display detailed switch or stack QoS agent configuration information, use the following command from Privileged EXEC configuration mode:

```
show qos agent details
```

Chapter 5: Configuring Quality of Service using Enterprise Device Manager

This chapter discusses how to configure DiffServ and Quality of Service (QoS) parameters for policy-enabled networks using Enterprise Device Manager (EDM).

Important:
In addition to the QoS configurations created, the system creates some default classifier elements, classifiers, classifier blocks, policies, and actions. These system default entries cannot be modified or deleted.

Prerequisites

- Open one of the supported browsers.
- Enter the IP address of the switch to open an EDM session.

Displaying interface queues using EDM

Use the following procedure to display the interface queues:

Prerequisites

- Open one of the supported browsers.
- Enter the IP address of the switch to open an EDM session.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Devices**.
3. In the work area, click the **Interface Queue** tab to view the interface queues.

Variable Definitions

Variable	Value
SetId	Displays an integer between 1 and 65535 that identifies the specific queue set.
QueueId	Displays an integer that uniquely identifies a specific queue within a set of queues.
Discipline	Displays the paradigm used to empty the queue: • priorityQueuing • weightedRoundRobin
Bandwidth %	Displays relative bandwidth available to a given queue with respect to other associated queues.
AbsBandwidth	Displays absolute bandwidth available to this queue, in Kb/s.
BandwidthAllocation	Displays bandwidth allocation: relative or absolute.
ServiceOrder	Specifies the order in which a queue is serviced based on the defined discipline.
Size	Displays the size of the queue in bytes.

Interface group configuration using EDM

Use the information to create and manage interface groups.

Interface group configuration using EDM navigation

- Displaying interface groups using EDM on page 103
- Assigning ports to an interface group using EDM on page 105
- Deleting ports from an interface group using EDM on page 104
- Adding interface groups using EDM on page 104
- Deleting interface groups using EDM on page 105

Displaying interface groups using EDM

Use the following procedure to display the interface groups.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Devices**.
3. In the work area, click the **Interface Group** tab to view the interface group information.

Variable Definitions

Variable	Value
Id	Displays a unique identifier of an interface group.
Role	Specifies the tag used to identify interfaces with the characteristics specified by the attributes of this class instance. These identifiers can be used within a number of classes to identify a physical set of interfaces to which policy rules and actions can apply.
InterfaceClass	Specifies the type of traffic interfaces associated with the specified role combination.
Capabilities	Specifies the list of the interface capabilities used by the PDP or network manager to select the policies and configurations that can be pushed to the Policy Enforcement Point (PEP).

Variable	Value
StatsTrackingType	Specifies the type of statistics tracking used.
StorageType	Displays storage type for this interface group: • Volatile • nonVolatile (default) • readOnly • other

Deleting ports from an interface group using EDM

Use the following procedure to remove ports from an interface group.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Devices**.
3. In the work area, click the **Interface Group** tab.
4. Highlight the interface group from which you want to delete ports.
5. Click **Interface Assignment** button on the toolbar. .

   The Port Editor: undefined screen appears
6. De-select the port numbers to delete them from the interface group.
7. Click **OK**.

Adding interface groups using EDM

Use the following procedure to add interface groups.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Devices**.
3. In the work area, click the **Interface Group** tab.
4. Click **Insert**.

The Insert Interface Group screen appears.

5. Enter the desired ID number.
6. Enter the **Role** combination tag for this Interface Group.
7. Select the interface class desired for this interface group: **trusted**, **nonTrusted**, or **unrestricted**.
8. Click **Insert**.

Deleting interface groups using EDM

Use the following procedure to delete the interface groups.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Devices**.
3. In the work area, click the **Interface Group** tab.
4. Highlight the interface group to delete.
5. Click **Delete**.

Important:
An interface group that is referenced by a policy cannot be deleted. The policy must first be deleted. Also, an interface group that has ports assigned to it cannot be deleted.

The association between interfaces, role combinations, and queue sets can be displayed. A role combination is a unique label that identifies a group of interfaces.

Assigning ports to an interface group using EDM

Use the following procedure to assign ports to an interface group.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Devices**.

3. In the work area, click the **Interface Group** tab.
4. Highlight the interface group for which you want to add parts.
5. Click the **Interface Assignment** button on the toolbar.

   ThePort Editor: undefined screen appears.
6. Select the port numbers to add to the interface group.
7. Click **OK**.

Important:
Adding or deleting a number of ports on a switch experiencing a heavy load can take a long time and can cause the EDM to time out.

Interface ID configuration using EDM

Use the following procedure to create and manage interface IDs.

Interface ID configuration using EDM navigation

- Displaying an interface ID using EDM on page 106
- Filtering Interface ID Assignments table using EDM on page 107

Displaying an interface ID using EDM

Use the following procedure to display the interface ID.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Devices**.
3. In the work area, click the **Interface ID Assignments** tab to view the interface id information.

Variable Definitions

Field	Description
Port	Displays ports numbers.
RoleCombination	Displays the role combination associated with the interface.
QueueSet	Displays the queue set associated with this interface.
Capabilities	Displays the capabilities.

Filtering Interface ID Assignments table using EDM

Use the following procedure to display the selected parts of the Interface ID Assignments tab.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Devices**.
3. In the work area, click the **Interface ID Assignments** tab.
4. Click the **Filter** button on the toolbar.

   The Qos Devices, Interface ID Asignments - Filter screen appears.
5. Set the conditions to be used to filter the display of the **Interface ID Assignments** table.
   a. Select **AND** to include all entries in the table that include *all* specified parameters, or select **OR** to include *any* of the specified parameters.
   b. Select **Ignore Case** to include all entries with the parameters being set, whether in lowercase or uppercase.
   c. Define the display filtering criteria to return all cases in which an entry **contains**, **equals to**, **does not contain**, or **does not equal to** the set parameters.
   d. Select **All records** to display all the entries in the table.
   e. To display the entries in the table by interface, select **Port** and enter the **Port** string to display.

f. To display the entries in the table by role combinations, select **RoleCombination** and enter the **RoleCombination** values to display.

g. To display the entries in the table by queue set, select **QueueSet** and enter the **QueueSet** values to display.

6. Click **Filter**.

Displaying priority queue assignments using EDM

Use the following procedure to view Priority Q Assignments.

Prerequisites

- Open one of the supported browsers.
- Enter the IP address of the switch to open an EDM session.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Devices**.
3. In the work area, click the **Priority Q Assign** tab to view the priority queue.

Variable Definitions

Field	Description
Qset	Supports the assignment of 802.1p user priority values to a queue for each specific queue set. There are four queue sets and there are 8 priority classes, 0 through 7, for each supported queue set.
802.1pPriority	Specifies the 802.1 user priority value.
Queue	Specifies the queue in a specified queue set that is assigned a priority value. To change a Queue assignment, click in the cell and type a new value.

Displaying priority mapping using EDM

Use the following procedure to display priority mapping.

Prerequisites

- Open one of the supported browsers.
- Enter the IP address of the switch to open an EDM session.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Devices**.
3. In the work area, click the **Priority Mapping** tab to view the priority mapping.

Variable Definitions

Field	Description
802.1pPriority	Specifies the 802.1 user priority value to map to a DSCP value at ingress.
Dscp	Specifies the DSCP value to associate with the specified 802.1 user priority value at ingress. To change a DSCP assignment, double-click in a Dscp cell and edit the value.
Name	Specifies the type of service.

Egress mapping configuration using EDM

You can use the information in this section to view and modify DSCP to COS mapping configurations.

Egress mapping configuration using EDM navigation

- Viewing egress mapping information using EDM on page 110
- Configuring egress mapping using EDM on page 111

Viewing egress mapping information using EDM

Use this procedure to display existing DSCP mapping information.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QoS Devices**.
3. In the work area, click the **DSCP Mapping** tab.

Variable Definitions

Variable	Value
Dscp	Indicates the DSCP value.
802.1pPriority	Indicates the user priority value associated with the DSCP. Values range from 0–7.
DropPrecedence	Indicates the relative drop precedence value for mapping the DSCP value to a drop precedence. Values include: • lowDropPrec • highDropPrec When network congestion occurs, the system drops packets with a high drop precedence before those with a low drop precedence.
NewDscp	Indicates a new DSCP value to use when DSCP mutation is required.
ServiceClass	Specifies the type of service.

Configuring egress mapping using EDM

Use the following procedure to configure DSCP-to-802.1p priority and drop precedence associations that are used for assigning these values at packet egress, based on the DSCP in the received packet.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QoS Devices**.
3. In the work area, click the **DSCP Mapping** tab.
4. To select a DSCP map to edit, click a**Dscp** row.
5. In the Dscp row, double-click the cell in the **802.1pPriority** column.
6. From the list, select a value.
7. In the Dscp row, double-click the cell in the **DropPrecedence** column.
8. From the list, select a value.
9. In the Dscp row, double-click the cell in the **NewDscp** column.
10. In the dialog box, type a value.
11. In the Dscp row, double-click the cell in the **ServiceClass** column.
12. In the dialog box, type a character string.

Variable Definitions

Use the data in the following table to configure egress mapping.

Variable	Value
Dscp	Indicates the DSCP value. This is a read-only cell.
802.1pPriority	Specifies the user priority value associated with the DSCP. Values range from 0–7.
DropPrecedence	Specifies the relative drop precedence value for mapping the DSCP value to a drop precedence. Values include: • lowDropPrec • highDropPrec

Variable	Value
	When network congestion occurs, the system drops packets with a high drop precedence before those with a low drop precedence.
NewDscp	Specifies a new DSCP value to use when DSCP mutation is required. Values range from 0–63.
ServiceClass	Specifies the type of service. Value is a character string with a maximum of 20 characters.

Displaying Meter Capability using EDM

Use the following procedure to display QoS interface meter capabilities.

Prerequisites

- Open one of the supported browsers.
- Enter the IP address of the switch to open an EDM session.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Devices**.
3. In the work area, click the **Mater Capability** tab to view the meter capability information.

Variable Definitions

Field	Description
Port	Specifies the port to which the meter is applied.
MeterSupport	Specifies the supported Token Bucket metering algorithm. Release 5.0 supports Simple Token Bucket.
Meter Rate(Kbps)/Bucket(KBytes)/ Granularity (Kbps)	Displays maximum suppported Meter Rate.

Displaying Shaper Capability using EDM

Use the following procedure to display QoS interface shaper capabilities.

Prerequisites

- Open one of the supported browsers.
- Enter the IP address of the switch to open an EDM session.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Devices**.
3. In the work area, click the **Shaper Capability** tab to view the information.

Variable Definitions

Field	Description
Port	Specifies the port to which the meter is applied.
ShaperSupport	Displays the location where the shaper is applied. Release 5.0 supports shaping application for each interface.
Shaper Rate(Kbps)/Bucket (KBytes)/Granulatiry (Kbps	Displays the maximum supported Shaper Rate, Shaper Budket size, and Shaper Granularity.

QoS IP classifier element management using EDM

Use the information in this section to configure and manage QoS IP classifier elements.

QoS IP classifier element management using EDM navigation

- Viewing IP classifier element configuration using EDM on page 114
- Creating an IP classifier element using EDM on page 116
- Deleting IP classifier elements using EDM on page 119

Viewing IP classifier element configuration using EDM

Use this procedure to display IP classifier element configuration information.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QosRules**.
3. In the work area, click the **IP Classifier Element** tab.

Variable Definitions

Use the data in the following table to view IP classifier element configuration.

Variable	Value
Id	Indicates the number of the IP classifier element.
Name	Indicates the label of the IP classifier element.
AddressType	Indicates the type of IP address used by this classifier entry. The type is limited to IPv4 and IPv6 addresses.
DstAddr	Indicates the IP address to match against a packet destination IP address.
DstMaskLength	Indicates the length of the destination address mask. Values range from 0–32. The default is 0.
SrcAddr	Indicates the IP address to match against a packet's source IP address.
SrcMasklength	Indicates the length of the source address mask. Values range from 0–32. The default is 0.
Dscp	Indicates the value for the DSCP in a packet. Values range from -1–63 (0x00 to 0x3f hexadecimal).

Variable	Value
Protoco/Next Header	Indicates the IPv4 protocol or IPv6 next header the classifier element will match. Values range from 0–255. The following are specific value designations: • 1 = ICMP-IPv4 • 2 = IGMP • 6 = TCP • 17 = UDP • 20 = FTP Data • 21 = FTP Control • 23 = Telnet • 25 = SMTP • 46 = RSVP • 58 = ICMP-IPv6 • L4Port:69 = TFTP • 80 = HTTP • 443 = HTTPS
DstL4PortMin	Indicates the minimum value permitted for the Layer 4 destination port number in a packet. Values range from 0–65535.
DstL4PortMax	Indicates the maximum value permitted for the Layer 4 destination port number in a packet. Values range from 0–65535.
SrcL4PortMin	Indicates the minimum value permitted for the Layer 4 source port number in a packet. Values range from 0–65535.
SrcL4PortMax	Indicates the maximum value permitted for the Layer 4 source port number in a packet. Values range from 0–65535.
IPv6FlowId	Indicates the flow identifier for IPv6 packets. Values range from -1–1048575 (0x00 to 0xfffff hexadecimal).
IpFlags	Indicates the value of flags present in an IPv4 header. Values include: • MoreFragement • doNotFragement
TcpCtrlFlags	Indicates the control flags present in an TCP header. Values include:

Variable	Value
	• Urg • Ack • Psh
	• Rst • Syn • Fin
Ipv4Options	Indicates whether the Option field is present in the packet header. Values include: • Present—indicates that only IPv4 packets without options match this classifier element. • Not Present—indicates that only IPv4 packets that include options match this classifier element. • ignore—whether or not options are present in IPv4 packets is not considered when determining if the IPv4 packet matches this classifier
Version	Indicates
SessionId	Indicates the session identification number.
Storage	Indicates the type of storage: • volatile • nonVolatile (default) • readOnly

Creating an IP classifier element using EDM

Use this procedure to create a new IP classifier element.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QosRules**.
3. In the work area, click the **IP Classifier Element** tab.
4. Click **Insert**.

5. Configure the parameters for the IP classifier element.
6. Click **Insert**.

Variable definitions

Use the data in this table to create an IP classifier element.

Variable	Value
Id	Specifies the identification number of the IP classifier element.
Name	Specifies the label of the IP classifier element.
AddressType	Specifies the type of IP address used by this classifier entry. The type is limited to IPv4 and IPv6 addresses.
DstAddr	Specifies the IP address to match against a packet destination IP address.
DstMaskLength	Specifies the length of the destination address mask. Values range from 0–32. The default is 0.
SrcAddr	Specifies the IP address to match against a packet source IP address.
SrcMasklength	Specifies the length of the source address mask. Values range from 0–32. The default is 0.
Dscp	Specifies the value for the DSCP in a packet. Values range from -1–63 (0x00 to 0x3f hexadecimal). A value of -1 indicates that the system ignores this parameter.
Protoco/Next Header	Specifies the IPv4 protocol or IPv6 next header the classifier element will match. Values range from 0–255. A value of 255 indicates that the system ignores the parameter. The following are specific value designations: • 1 = ICMP-IPv4 • 2 = IGMP • 6 = TCP • 17 = UDP • 20 = FTP Data • 21 = FTP Control

Variable	Value
	• 23 = Telnet • 25 = SMTP • 46 = RSVP • 58 = ICMP-IPv6 • L4Port:69 = TFTP • 80 = HTTP • 443 = HTTPS
DstL4PortMin	Specifies the minimum value permitted for the Layer 4 destination port number in a packet. Values range from 0–65535.
DstL4PortMax	Specifies the maximum value permitted for the Layer 4 destination port number in a packet. Values range from 0–65535. When you configure DstL4PortMin to 0 and DstL4PortMax to 65535, the system ignores the DstL4Port parameters.
SrcL4PortMin	Specifies the minimum value permitted for the Layer 4 source port number in a packet. Values range from 0–65535.
SrcL4PortMax	Specifies the maximum value permitted for the Layer 4 source port number in a packet. Values range from 0–65535. When you configure SrcL4PortMin to 0 and SrcL4PortMax to 65535, the system ignores the SrcL4Port parameters.
IPv6FlowId	Specifies the flow identifier for IPv6 packets. Values range from -1–1048575 (0x00 to 0xfffff hexadecimal). A value of -1 indicates that the system ignores this parameter.
IpFlags	Specifies the value of flags present in an IPv4 header. Values include: • MoreFragement • doNotFragement
TcpCtrlFlags	Specifies the control flags present in an TCP header. Values include: • Urg • Ack • Psh

Variable	Value
	• Rst • Syn • Fin
Ipv4Options	Specifies whether the Option field is present in the packet header. Values include: Present—indicates that only IPv4 packets without options match this classifier element. • Not Present—indicates that only IPv4 packets that include options match this classifier element. • ignore—whether or not options are present in IPv4 packets is not considered when determining if the IPv4 packet matches this classifier

Deleting IP classifier elements using EDM

Use this procedure to delete an IP classifier element:

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QosRules**.
3. In the work area, click the **IP Classifier Element** tab.
4. To select an IP classifier element to delete, click the element row.
5. Highlight the IP classifier element to delete.
6. Click **Delete**.

Important:
You cannot delete an IP classifier element if it is referenced by a classifier or classifier block. Additionally, an IP classifier element cannot be deleted if it is of the storage type of other or readOnly.

QoS L2 classifier element management using EDM

Use the information in this section to configure and manage QoS L2 classifier elements.

QoS L2 classifier element management using EDM navigation

- Viewing L2 classifier element information using EDM on page 120
- Creating an L2 classifier element using EDM on page 122
- Deleting L2 classifier elements using EDM on page 123

Viewing L2 classifier element information using EDM

Use this procedure to display information about configured L2 classifiers.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QosRules**.
3. In the work area, click the **L2 Classifier Element** tab.

Variable Definitions

Use the data in this table to help you understand the L2 classifier element information display.

Variable	Value
Id	Indicates the index that enumerates the classifier entries.
Name	Indicates a label for the classifier entry.
DestMacAddr	Indicates the MAC address against which the MAC destination address of incoming packets will be compared
DstMacAddrMask	Indicates a mask identifying the destination MAC address.
SrcMacAddr	Indicates the MAC source address of incoming packets.
SrcMacAddrMask	Indicates a mask identifying the source MAC address.

Variable	Value
VlanIdMin	Indicates the minimum value the inner VLAN ID in a double tagged packet must have to match this L2 classifier.
VlanIdMax	Indicates the minimum value the inner VLAN ID in a double tagged packet must have to match this L2 classifier.
VlanTag	Indicates the type of VLAN tagging in a packet. Values include: • untagged • tagged • ignore
EtherType	Indicates a value for the Ethernet type. Values range from 0x00 to 0xffff. If you enter a value of 0xffff, the system ignores this parameter.
802.1pPriority	Indicates a value for the 802.1p user priority. Values include: • priority0 • priority1 • priority2 • priority3 • priority4 • priority5 • priority6 • priority7 • ignore
PktType	Indicates the data link layer frame format that frames must have to match this L2 classifier entry. Values include: • ethernetII—only EthernetII format frames can match this classifier • snap—only IEEE 802 SNAP format frames can match this classifier • llc—only IEEE 802 LLC format frames can match this classifier • ignore—frame format is not considered in determining whether or not a frame matches this classifier
Version	Indicates the L2 classifier version.
SessionId	Indicates the session identifier.
Storage	Indicates the type of storage.

Creating an L2 classifier element using EDM

Use this procedure to create an L2 classifier element.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QosRules**.
3. In the work area, click the **L2 Classifier Element** tab.
4. Click **Insert**.
5. Configure parameters for the L2 classifier element.
6. Click **Insert**.

Variable Definitions

Use the data in this table to create an L2 classifier element.

Variable	Value
Id	Specifies the index that enumerates the classifier entries.
Name	Specifies a label for the classifier entry.
DestMacAddr	Specifies the MAC address against which the MAC destination address of incoming packets is compared.
DstMacAddrMask	Specifies a mask identifying the destination MAC address.
SrcMacAddr	Specifies the source MAC address of incoming packets.
SrcMacAddrMask	Specifies a mask identifying the source MAC address.
VlanRange	Specifies the VLAN range for the L2 classifier element. Values range from 1–4094. When **Ignore** is selected, the system ignores the VLAN range.
VlanTag	Specifies the type of VLAN tagging in a packet. Values include: • untagged • tagged • ignore
EtherType	Specifies a value for the Ethernet type. Values range from 0x00 to 0xffff. If you enter a value of 0xffff, the system ignores this parameter.

Variable	Value
802.1pPriority	Specifies a value for the 802.1p user priority. Values include: • priority0 • priority1 • priority2 • priority3 • priority4 • priority5 • priority6 • priority7 • ignore
PktType	Specifies the data link layer frame format that frames must have to match this L2 classifier entry. Values include: • ethernetII—only EthernetII format frames can match this classifier • snap—only IEEE 802 SNAP format frames can match this classifier • llc—only IEEE 802 LLC format frames can match this classifier • ignore—frame format is not considered in determining whether or not a frame matches this classifier

Deleting L2 classifier elements using EDM

Use this procedure to delete L2 classifier elements from the table.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QosRules**.
3. In the work area, click the **L2 Classifier Element** tab.
4. To select an L2 classifier element to delete, click the element row.
5. Click **Delete**.

Important:
A L2 classifier element cannot be deleted if it is referenced by a classifier or classifier block. Additionally, a L2 classifier element cannot be deleted if it is of the storage type of other or readOnly.

QoS system classifier element management using EDM

Use the information in this section to configure and manage QoS system classifier elements.

QoS system classifier element management using EDM navigation

- Viewing QoS system classifier elements using EDM on page 124
- Viewing the QoS system classifier pattern using EDM on page 127
- Configuring a QoS system classifier element using EDM on page 127
- Deleting QoS system classifier elements using EDM on page 129

Viewing QoS system classifier elements using EDM

To display System Classifier Elements:

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QosRules**.
3. In the work area, click the **System Clfr Element** tab.

Variable Definitions

Field	Description
Id	Indicates the index that enumerates the system classifier entries.
Name	Indicates the name of the system classifier element.

Field	Description
UnknownUcastFrames	Identifies frames with an unknown unicast destination address. • true—indicates frames containing an unknown unicast destination address match this classification entry. • false—indicates that no classification is requested based on this address type.
UnknownMcastFrames	Identifies frames with an unknown multicast destination address. • true—indicates frames containing an unknown multicast destination address match this classification entry. • false—indicates that no classification is requested based on this address type.
KnownMcastFrames	Identifies frames with a known multicast destination address. • true—indicates frames containing a known multicast destination address match this classification entry. • false—indicates that no classification is requested based on this address type.
UnknownIpMcast	Identifies IP packets with an unknown IP multicast destination address. • true—indicates that IP packets containing an unknown multicast destination address match this classification entry. • false—indicates that no classification is requested based on this address type.
KnownIpMcast	Identifies IP packets with a known IP multicast destination address. • true—indicates that IP packets containing a known multicast destination address match this classification entry. • false—indicates that no classification is requested based on this address type.
UnknownNonIpMcast	Identifies non-IP packets with an unknown MAC multicast destination address.

Field	Description
	• true—indicates that non-IP packets containing an unknown multicast destination address match this classification entry. • false—indicates that no classification is requested based on this address type.
KnownNonIpMcast	Identifies non-IP packets with a known MAC multicast destination address. • true—indicates that non-IP packets containing a known multicast destination address match this classification entry. • false—indicates that no classification is requested based on this address type.
NonIpPkt	Indicates that targeting non-IP traffic is supported. • true—indicates that non IP packets match this classification entry. • false—indicates that no classification is requested based on this packet type.
PatternFormat	Indicates the data link layer packet format that is used when specifying pattern match data. • untagged—indicates that the specified pattern match data does not include an 802.1Q tag. • tagged—indicates that the specified pattern match data does include an 802.1Q tag. The default value is tagged.
PatternIpVersion	Indicates the IP packet format used to specify pattern match data. Values include: • nonIp - indicates that the specified patern match data should be applied to non-IP packets • ipv4 - indicates that the specified pattern match data should be applied to IPv4 packets • ipv6 - indicates that the specified pattern match data should be applied to IPv6 packets
Version	Indicates the system classifier version.
SessionId	Indicates the system classifier session identifier.
PatternL2Format	Indicates the L2 packet format used to specify pattern match data. Values include:

Field	Description
	• notApplicable—specify pattern match data without indicating the target L2 packet format • ethernetII—apply the pattern match data to EthernetII format frames • snap—apply the pattern match data to IEEE 802 SNAP format frames • llc—apply the pattern match data to IEEE 802 LLC format frames
Storage	Indicates the storage type for this conceptual row. Conceptual rows that has the value permanent need not allow write-access to any columnar objects in the row. This object may not be modified if the associated status object is equal to 'active'.

Viewing the QoS system classifier pattern using EDM

Use this procedure to display the QoS system classifier pattern.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QosRules**.
3. In the work area, click the **System Clfr Element** tab.
4. Click **Pattern**.

Configuring a QoS system classifier element using EDM

Use this procedure to create and manage a QoS system classifier element.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QosRules**.
3. In the work area, click the **System Clfr Element** tab.
4. Click **Insert**.

5. In the Name dialog box, type label for the system classifier element.
6. In the **DestAddressType** section, click a radio button.
7. In the PatternData dialog box, type specific pattern data.

   OR

   Click the **PatternData** ellipsis to select specific pattern data.
8. In the PatternPosition dialog box, type specific pattern position data.

   OR

   Click the **PatternPosition** ellipsis to select specific pattern position data.
9. Click **Insert**.
10. Click **Apply**.

Variable definitions

Use the data in this table to configure a QoS system classifier element.

Variable	Value
Name	Specifies an alphanumeric label for the system classifier entry. Value is a character string from 1–16 characters in length.
DestAddressType	Specifies the address type for matching destination frames. • none—destination frames are not matched • unknownUcast—matches frames with an unknown unicast destination address • unknownMcast—matches frames with an unknown multicast destination address • knownMcast—matches frames with an known multicast destination address • UnknownIpMcast—matches frames with an unknown IP multicast destination address • KnownIpMcast—matches frames with known IP multicast destination address • UnknownNonIpMcast—matches frames with an unknown non-IP multicast destination address

Variable	Value
	• KnownNonIpMcast—matches frames with known non-IP multicast destination address • NonIpPkt—matches non-IP frames
PatternData	Matches frames with specific byte pattern data.
PatternPosition	Matches frames at a specific position in a packet.

Deleting QoS system classifier elements using EDM

Use this procedure to delete QoS system classifier elements from the table.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QosRules**.
3. In the work area, click the **System Clfr Element** tab.
4. To select an system classifier element to delete, click the element row.
5. Click **Delete**.

QoS classifier management using EDM

Use the information in this section to configure and manage QoS classifiers.

QoS classifier management using EDM navigation

- Displaying classifiers using EDM on page 130
- Adding classifiers using EDM on page 130
- Deleting classifiers using EDM on page 131
- Filtering classifiers using EDM on page 132

Displaying classifiers using EDM

Use the following procedure to display classifiers.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Rules**.
3. In the work area, click the **Classifier** tab to view the classifiers.

Variable Definitions

Field	Description
Name	Specifies the name of the classifier.
SetId	Specifies the eEntries with the same SetId belong to the same classifier. **Important:** Click heading on this column to list entries in numerical order to view which entries have the same SetId.
Specific	Describes the specific classifier element and its ID number (from the IP Classifier Element screen, the L2 Classifier Element screen, or System Clfr Element screen) that is included in the classifier.
SessionId	Specifies the session ID.
Storage	Specifies the storage type for this conceptual row. Conceptual rows that has the value permanent need not allow write-access to any columnar objects in the row. This object may not be modified if the associated status object is equal to active.

Adding classifiers using EDM

Use the following procedure to add a classifier.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Rules**.
3. In the work area, click the **Classifier** tab.
4. Click **Insert**.

   The Insert Classifier screen appears.
5. Type the name of the classifier element.
6. Select the **IP Classifier Element, L2 Classifier Element,** or **System Classifier Element**.
7. Click **Insert**.

Important:

A classifier can be created using the following classifier combinations:

- one IP classifier element
- one L2 classifier element
- one IP classifier element plus one L2 classifier elements

A classifier can also be created by using the following combination:

- one system classifier element
- one IP classifier, one system classifier
- one L2 classifier, one system classifier
- one IP, one L2, plus one system classifier

A classifier can be created by using any combination of classifier elements.

Entries with the same **SetId** belong to the same classifier. Click on the **SetId** column header to sort the table by **SetId** value; this makes it very easy to see which entries have the same **SetId** value.

Deleting classifiers using EDM

Use the following procedure to delete classifiers.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Rules**.

3. In the work area, click the **Classifier** tab.
4. Highlight the classifier to delete.
5. Click **Delete**.

Important:
A classifier that is referenced in a classifier block cannot be deleted. Additionally, a classifier cannot be deleted if it is of the storage type of **other** or **readOnly**.

Filtering classifiers using EDM

Use the following procedure to filter the display of classifiers.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Rules**.
3. In the work area, click the **Classifier** tab.
4. Click **Filter** button on the toolbar.

   The QoS Rules, Classifier - Filter screen appears.
5. Set the conditions to filter the display of the **Classifiers** table.
   a. Select **AND** to include all entries in the table that include *all* specified parameters, or select **OR** to include any of the specified parameters.
   b. Select **Ignore Case** to include all entries with the parameters being set, whether in lowercase or uppercase.
   c. Define the search to return all cases in which an entry **contains**, is **equal to**, **does not contain**, or **does not equal to** the set parameters.
   d. Select **All records** to display all the entries in the table.
   e. To display the entries in the table by name, select **Name** and enter the **Name** values to display.
   f. To display the entries in the table by setid, select **SetId** and enter the **SetId** values to display.
6. Click **Filter**.

QoS classifier block management using EDM

Use the information in this section to view and manage QoS classifier blocks.

QoS classifier block management using EDM navigation

- Displaying classifier blocks using EDM on page 133
- Appending classifier blocks using EDM on page 134
- Adding classifier blocks using EDM on page 134
- Deleting classifier blocks using EDM on page 135
- Filtering classifier blocks using EDM on page 136

Displaying classifier blocks using EDM

Use the following procedure to display classifier blocks.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Rules**.
3. In the work area, click the **Classifier Block** tab to view the blocks.

Variable Definitions

Field	Description
BlockNum	Indicates the entries with the same BlockNum that belong to the same classifier block. **Important:** Click heading on this column to list entries in numerical order to view which entries have the same BlockNum.
Name	Displays the name you assigned to that classifier block.

Field	Description
ClassifierSetId	Displays the ID number assigned to that classifier (from the Classifier screen).
Meter	Displays the meter associated with the classifier block.
Action	Displays the action followed for those flows not being metered. (For those flows being metered, this attribute is not applied.)
SessionId	Specifies the session ID.
Storage	Specifies the storage type for this conceptual row. Conceptual rows that has the value permanent need not allow write-access to any columnar objects in the row. This object may not be modified if the associated status object is equal to active.

Appending classifier blocks using EDM

Use the following procedure to append a classifier block.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Rules**.
3. In the work area, click the **Classifier Block** tab.
4. Click **Append Classifier** button on the toolbar.

   The Insert Classifier Block screen appears.
5. Select the Classifier to append to the Classifier Block.
6. Click **Insert**.

Adding classifier blocks using EDM

Use the following procedure to add classifier blocks.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Rules**.
3. In the work area, click the **Classifier Block** tab.
4. Click **Insert**.

   The Insert Classifier Block screen appears.
5. Enter the name of the classifier block.
6. Select the **Classifier, Meter**, and **Action**.
7. Click **Insert.**

Important:

If one of the classifiers in a classifier block has associated actions or meters, then all classifier elements of that classifier block must also have associated actions or meters (not identical values for the actions or meters, but also associated actions or meters).

Entries with the same **BlockNum** belong to the same classifier block. Click on the **BlockNum** column header to sort the table by **Block Number** value.

Deleting classifier blocks using EDM

Use the following procedure to delete classifier blocks.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Rules**.
3. In the work area, click the **Classifier Block** tab.
4. Highlight the classifier block to delete.
5. Click **Delete**.

Important:

The last classifier element in a classifier block cannot be deleted if it is referenced by a policy. First delete the policy. Additionally, a classifier block cannot be deleted if it is of the storage type of **other** or **readOnly**.

Filtering classifier blocks using EDM

Use the following procedure to filter a classifier block.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Rules**.
3. In the work area, click the **Classifier Block** tab.
4. Click **Filter**.

   The **QoSRules, Classifier Block - Filter** dialog box appears.
5. Select the filtering condition, case, and column.
6. Type the **BlockNum** and **Name**.
7. Click **Filter**.

QoS action configuration using EDM

Use the information in this section to manage QoS actions.

QoS action configuration using EDM navigation

- Displaying QoS actions using EDM on page 136
- Adding QoS actions using EDM on page 137
- Deleting QoS actions using EDM on page 138

Displaying QoS actions using EDM

Use the following procedure to display a QoS action.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS**.
3. In the work area, click the **Action** tab.

Variable Definitions

Field	Description
Id	Specifies the identifier for the action.
Name	Specifies a name for the action.
Drop	Specifies whether a packet is dropped, not dropped, or whether the decision is deferred.
UpdateDscp	Specifies a value used to update the DSCP field in an IPv4 packet.
SetDropPrecedence	Specifies automatic drop precedence.
UpdateUserPriority	Specifies a value for the 802.1p user priority.
Extension	Specifies linking additional actions. (These are defined on the Interface Action Ext Table.)
SessionId	Specifies the session ID.
Storage	Specifies the type of storage: • volatile • nonVolatile • readOnly

Adding QoS actions using EDM

Use the following procedure to add a QoS action.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS**.

3. Click the **Action** tab.
4. Click **Insert**.
5. Enter the information and make the selections to use for this QoS action.
6. Click **Insert**.

Deleting QoS actions using EDM

Use the following procedure to delete a QoS action.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS**.
3. Click the **Action** tab.
4. Highlight the QoS action to delete.
5. Click **Delete**.

Important:
A QoS action that is referenced by a meter, classifier block, or policy entry cannot be deleted. First delete the meter, classifier block, or policy. Additionally, a QoS action cannot be deleted it is of the storage type of **other** or **readOnly**.

QoS interface action extension configuration using EDM

Use the information in this section to create and manage QoS interface action extensions.

QoS interface action extension configuration using EDM navigation

- Displaying Interface action extensions using EDM on page 139
- Adding Interface action extensions using EDM on page 139
- Deleting Interface action extensions using EDM on page 140

Displaying Interface action extensions using EDM

Use the following procedure to display a QoS interface action extension.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS**.
3. In the work area, click the **Interface Action Ext** tab.

Variable Definitions

Field	Description
Id	Specifies the number of the interface action extension.
Name	Specifies the label of the interface action extension.
SetEgressUnicastPort	Specifies redirection of normally-switched unicast packets to a specified interface.
SetEgressNonUnicastPort	Specifies redirection of normally-switched non-unicast packets (broadcast and multicast traffic) to a specified interface.
SessionId	Specifies the session ID.
Storage	Specifies the type of storage, either volatile or non-volatile.

Adding Interface action extensions using EDM

Use the following procedure to add a QoS interface action extension.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS**.
3. In the work area, click the **Interface Action Ext** tab.

4. Click **Insert**.

   The Insert Interface Action Ext screen appears.

5. Enter the information and make the selections to use for this Interface action extension.
6. Click **Insert**.

Deleting Interface action extensions using EDM

Use the following procedure to delete a QoS interface action extension.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS**.
3. In the work area, click the **Interface Action Ext** tab.
4. Highlight the interface action extension to delete.
5. Click **Delete**.

Important:
A QoS interface action extension that is referenced by an action entry cannot be deleted. First delete the action.

QoS meter configuration using EDM

Use the information in this section to create and manage QoS meters.

QoS meter configuration using EDM navigation

- Displaying QoS meters using EDM on page 141
- Adding QoS meters using EDM on page 141
- Deleting QoS meters using EDM on page 142

Displaying QoS meters using EDM

Use the following procedure to display a QoS meter.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS**.
3. In the work area, click the **Meter** tab.

Variable Definitions

Field	Description
id	Specifies the unique identifier for this entry.
Name	Specifies a name for this entry.
CommittedRate	Specifies the committed rate (in Kbps).
CommittedBurstSize	Specifies the committed burst (in bytes).
InProfileAction	Specifies in profile action.
OutOfProfileAction	Specifies out of profile action.
SessionId	Specifies the session ID.
Storage	Specifies the type of storage.

Adding QoS meters using EDM

Use the following procedure to add a QoS meter.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS**.
3. In the work area, click the **Meter** tab.
4. Click **Insert**.

The Insert Meter screen appears.

5. Enter the information and make the selections to use for this QoS meter.
6. Click **Insert**.

Deleting QoS meters using EDM

Use the following procedure to delete a QoS meter.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS**.
3. In the work area, click the **Meter** tab.
4. Highlight the QoS meter to delete.
5. Click **Delete**.

Important:
A QoS meter that is referenced by a classifier block or policy cannot be deleted. First delete the classifier block or policy.

QoS interface shaper configuration using EDM

Use the information in this section to create or delete a QoS interface shaper, or to view QoS interface shaper configuration information.

QoS interface shaper configuration using EDM navigation

- Viewing QoS interface shaper information using EDM on page 142
- Creating a QoS interface shaper using EDM on page 143
- Deleting a QoS interface shaper using EDM on page 144

Viewing QoS interface shaper information using EDM

Use this procedure to display QoS interface shaper configuration information.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QoS**.
3. In the work area, click the **Interface Shaper** tab.

Variable Definitions

Variable	Value
Port	Indicates the interface port number associated with a QoS interface shaper. The port number must correspond to the interface table entry with the same port number.
Name	Indicates an alphanumeric label used to identify the QoS interface shaper.
ShapingRate	Indicates the token-bucket rate, in kilobits per second (Kbps).
BurstSize	Indicates the maximum number of bytes in a single transmission burst, in kilobits per second (Kbps).

Creating a QoS interface shaper using EDM

Use this procedure to create a new QoS interface shaper.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QoS**.
3. In the work area, click the **Interface Shaper** tab.
4. Click **Insert**.
5. Click the **Ports** ellipses.
6. Select the required ports for the interface shaper.
7. Click **Ok**.
8. In the **Name** dialog box, type a character string.

9. In the **Shaping Rate** dialog box, type a value.
10. In the **MaximumBurstRate** dialog box, type a value.
11. Double-click the **Duration** box.
12. From the list, select a value.
13. Click **Insert**.

Variable Definitions

Variable	Value
Port	Specifies the interface port number associated with a QoS interface shaper. The port number must correspond to the interface table entry with the same port number.
Name	Specifies an alphanumeric label used to identify the QoS interface shaper.
ShapingRate	Specifies the token-bucket rate, in kilobits per second (Kbps). Value must be a multiple of 64 or 1000 Kbps.
BurstSize	Specifies the maximum number of bytes in a single transmission burst, in kilobits per second (Kbps).
Duration	Specifies the burst duration in milliseconds.

Deleting a QoS interface shaper using EDM

Use this procedure to delete a QoS interface shaper.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QoS**.
3. In the work area, click the **Interface Shaper** tab.
4. To select a shaper to delete, click the shaper row.
5. Click **Delete**.

QoS interface queue shaper configuration using EDM

Use the information in this section to create or delete a QoS interface queue shaper, or to view QoS interface queue shaper configuration information.

QoS interface queue shaper configuration using EDM navigation

- Viewing QoS interface queue shaper information using EDM on page 145
- Creating a QoS interface queue shaper using EDM on page 146
- Deleting a QoS interface queue shaper using EDM on page 147

Viewing QoS interface queue shaper information using EDM

Use the following procedure to display QoS interface queue shaper configuration information.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QoS**.
3. In the work area, click the **Interface Queue Shaper** tab.

Variable Definitions

Variable	Value
Port	Indicates the interface port number associated with a QoS interface shaper. The port number must correspond to the interface table entry with the same port number.
Queue	Indicates the queue for the selected interface port or ports, on which traffic is shaped. The range of available values is determined by the OoS agent default queue configuration.

Variable	Value
Name	Indicates an alphanumeric label used to identify the QoS interface queue shaper.
ShapingRate	Indicates the QoS interface queue shaping rate, in kilobits per second (Kbps). Values range from 64 to10230000 Kbps. The value must be a multiple of 64 or 1000 Kbps.
ShapingMinRate	Indicates the minimum QoS interface queue shaping rate, in kilobits per second (Kbps). Values range from 0 to10230000 Kbps. The value must be a multiple of 64 or 1000 Kbps.

Creating a QoS interface queue shaper using EDM

Use the following procedure to create a new QoS interface queue shaper.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QoS**.
3. In the work area, click the **Interface Queue Shaper** tab.
4. Click **Insert**.
5. Click the **Ports** ellipses.
6. Select the required ports for the interface queue.
7. Click **Ok**.
8. In the **Queue** dialog box, type a value.
9. In the **Name** dialog box, type a character string.
10. In the **ShapingRate** dialog box, type a value.
11. In the **ShapingMinRate** dialog box, type a value.
12. Click **Insert**.

Variable Definitions

Variable	Value
Port	Specifies the interface port number associated with a QoS interface shaper. The port number must correspond to the interface table entry with the same port number.
Queue	Specifies the queue for the selected interface port or ports, on which traffic is shaped. The range of available values is determined by the OoS agent default queue configuration.
Name	Specifies an alphanumeric label used to identify the QoS interface queue shaper.
ShapingRate	Specifies the QoS interface queue shaping rate, in kilobits per second (Kbps). Values range from 64 to10230000 Kbps. The value must be a multiple of 64 or 1000 Kbps.
ShapingMinRate	Specifies the minimum QoS interface queue shaping rate, in kilobits per second (Kbps). Values range from 0 to10230000 Kbps. The value must be a multiple of 64 or 1000 Kbps.

Deleting a QoS interface queue shaper using EDM

Use this procedure to delete a QoS interface shaper.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QoS**.
3. In the work area, click the **Interface Queue Shaper** tab.
4. To select a queue shaper to delete, click the queue shaper row.
5. Click **Delete**.

QoS policy configuration using EDM

Use the information in this section to create and manage QoS policies.

QoS policy configuration using EDM navigation

- Displaying QoS policies using EDM on page 148
- Adding QoS policies using EDM on page 150
- Deleting QoS policies using EDM on page 150

Displaying QoS policies using EDM

Use the following procedure to display QoS policies:

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS**.
3. In the work area, click the **Policy** tab.

Variable Definitions

Field	Description
Id	Specifies the number of the QoS policy.
Status	Allows you to enable or disable the policy.
Name	Displays the name for the policy.
ClassifierType	Specifies whether a classifier or a classifier block identifies traffic.
ClassifierName	Specifies the name of the classifier or classifier block associated with this policy.
InterfaceRoles	Specifies the interfaces to which the policy applies.

Field	Description
	Important: You must configure the role combinations (refer to Interface ID configuration using EDM on page 106) prior to associating it with a policy.
InterfaceIndex	The ifIndex field identifies the interface to which the policy is to be applied. A policy is associated with an interface explicitly using this attribute or implicitly using a role combination through the ntnQosPolicyInterfaceRole attribute. An interface must be identified by one and only one of these attributes. This attribute can identify an interface that does not currently exist in the system, as long as the specified interface index represents a potentially valid system interface. **Important:** The InterfaceRoles and InterfaceIndex fields are mutually exclusive. When the InterfaceIndex field is not zero, the InterfaceRoles must be empty (select none when insert the policy). When the InterfaceRoles specifies a valid role combination, the InterfaceIndex field must be 0.
Precedence	Specifies the order in which multiple policies are associated with the same interface. Policies with greater precedence have higher numbers. **Important:** Policies with higher precedence values are applied before policies with lower precedence values.
Meter	Specifies metering associated with this policy. Specifying a metering component causes any action criteria specified explicitly by the policy to be rejected as an error. **Important:** You must configure meters before associating them with a policy.
InProfileAction	Identifies the action to be applied to traffic with this policy. This will not be used when a meter is specified. **Important:** You must configure actions before associating them with a policy.
StatsType	Specifies statistics tracking:

Field	Description
	• none--no statistics tracked for this policy • individual--separate counters allocated, space permitting, for each classifier referenced by the policy • aggregate--a single counter accumulates all the statistics for all the classifiers referenced by the policy
SessionId	Specifies the session ID.
Storage	Specifies the type of storage: • volatile • nonVolatile • readOnly

Adding QoS policies using EDM

Use the following procedure to add a QoS policy.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS**.
3. In the work area, click the **Policy** tab.
4. Click **Insert**.

   The Insert QoS Policy screen appears.
5. Enter the information to use for this QoS policy.
6. Click **Insert**.

Important:

The **InterfaceRoles** and **InterfaceIndex** fields are mutually exclusive. When the **InterfaceIndex** field is not zero, the **InterfaceRoles** must be empty (select **none** when inserting the policy). When the **InterfaceRoles** specifies a valid role combination, the **InterfaceIndex** field must be 0.

Deleting QoS policies using EDM

Use the following procedure to delete QoS policies.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS**.
3. In the work area, click the **Policy** tab.
4. Highlight the QoS policy to delete.
5. Click **Delete**.

QoS Policy Stats using EDM

Use the following procedure to view QoS Policy Stats information for a policy.

Prerequisites

- Open one of the supported browsers.
- Enter the IP address of the switch to open an EDM session.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS**.
3. In the work area, click the **Policy** tab.
4. Select a policy from the list.
5. Click **Graph**.

   The Policy Aggregate Stats screen appears.

If the Policy Stats type is set to none, no stats information appears.

If the Policy Stats type is set to aggregate, the aggregate stats information appears. The aggregate stats consist of total in-profile packets and total out-profile packets. If the Policy Meter is set to none, no total out-profile packet information is available.

If the Policy Stats type is set to individual, the individual stats, consisting of in-profile and out-profile packets, appears. If policy meter is set to no, no out-profile packet information is available. Individual stats are provided for each policy, for each filter, for each port.

QoS traffic profile filter classifier configuration using EDM

Use the information in this section to view and manage QoS traffic profile filter classifier configurations.

QoS traffic profile filter classifier configuration using EDM navigation

- Viewing QoS traffic profile filter classifier information using EDM on page 152
- Filtering QoS traffic profile filter classifier information using EDM on page 157
- Creating a QoS traffic profile filter classifier using EDM on page 158
- Deleting a QoS traffic profile filter classifier using EDM on page 163

Viewing QoS traffic profile filter classifier information using EDM

Use this procedure to display existing QoS traffic profile filter classifier configuration information.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QoS NSNA/Traffic Profile**.
3. In the work area, click the **Classifier** tab.

Variable Definitions

Use the data in the following table to help you understand the QoS traffic profile filter classifier display.

Variable	Value
Id	Indicates the ID number of the classifier.
Type	Indicates the classifier type. Values include:

Variable	Value
	• NsnaClfr • TrafficProfile
Name	Indicates the name of the classifier. All classifiers with the same name are part of the same filter set. That filter set has the same name as the classifiers.
Block	Indicates the block name with which the classifier is associated.
EvalPrec	Indicates the evaluation order number of the classifier in that filter set. Two classifiers in the same filter set cannot have the same evaluation order. A higher eval order means a lower precedence for the corresponding policy. Values range from 1–255.
AddrType	Indicates the type of IP address used by this classifier entry. Values include: • N/A—the address type is non-applicable • ipv4 • ipv6
DstIpAddr	Indicates the IP address to match against the destination IP address of a packet.
DstIpPrefixLength	Indicates the length of the destination address mask. Values range from 0–2040, with 0–32 reserved for IPv4 address masks and 0–128 reserved for IPv6 address masks.
SrcIpAddr	Indicates the IP address to match against the source IP address of a packet.
SrcIpPrefixLength	Indicates the length of the source address mask. Values range from 0–2040, with 0–32 reserved for IPv4 address masks and 0–128 reserved for IPv6 address masks.
Dscp	Indicates the value for a DiffServ Codepoint (DSCP) in a packet. Values range from -1–63 (0x00 to 0x3f hexadecimal). A value of -1 indicates that the system ignores this parameter.
Protocol/NextHeader	Indicates the IPv4 protocol value, or the IPv6 next-header value. Values range from 0–255. A value of 255 indicates that the system ignores the parameter. The following are specific value designations: • 1 = ICMP-IPv4 • 2 = IGMP • 6 = TCP

Variable	Value
	• 17 = UDP • 20 = FTP Data • 21 = FTP Control • 23 = Telnet • 25 = SMTP • 46 = RSVP • 58 = ICMP-IPv6 • L4Port:69 = TFTP • 80 = HTTP • 443 = HTTPS
DstL4PortMin	Indicates the minimum value for the Layer 4 destination port number in a packet. Values range from 0–65535.
DstL4PortMax	Indicates the maximum value for the Layer 4 destination port number in a packet. Values range from 0–65535.
SrcL4PortMin	Indicates the minimum value for the Layer 4 source port number in a packet. Values range from 0–65535.
SrcL4PortMax	Indicates the maximum value for the Layer 4 source port number in a packet. Values range from 0–65535.
Ipv6FlowId	Indicates the flow identifier for IPv6 packets. Values range from -1–1048575 (0x00 to 0xfffff hexadecimal). A value of -1 indicates that the system ignores this parameter.
IpFlags	Indicates the classifier flag to match in traffic IPv4 headers. Values include: • MoreFragement • doNotFragement
TcpCtrlFlags	Indicates the control flag to match in traffic TCP headers. Values include: • Urg • Ack • Psh • Rst

Variable	Value
	• Syn • Fin
Ipv4Options	Indicates if the presence of IPv4 options in an IPv4 packet are considered when the system is searching for a match for this classifier. Values include: • ipv4OptionsPresent—only IPv4 packets with options match this classifier • ipv4OptionsNotPresent—only IPv4 packets without options match this classifier • ignore—whether or not options are present in IPv4 packets is not considered when determining if the IPv4 packet matches this classifier
Storage	Indicates the storage type for this conceptual row.
DstMacAddr	Indicates the MAC address against which the MAC destination address of incoming packets is compared.
DstMacAddrMask	Indicates a mask identifying the destination MAC address.
SrcMacAddr	Indicates a MAC source address of incoming packets.
SrcMacAddrMask	Indicates a mask identifying the source MAC address.
VlanIdMin	Indicates the minimum value for the VLAN ID in a packet. Values range from 1–4094.
VlanIdMax	Indicates the maximum value for the VLAN ID in a packet. Values range from 1–4094.
VlanTag	Indicates the type of VLAN tagging in a packet. Values include: • untagged • tagged • ignore
EtherType	Indicates the value for the Ethernet type. Values range from 0x00 to 0xffff. If you enter a value of 0xffff, the system ignores this parameter.
UserPriority	Indicates the value for the 802.1p user priority. Values include: • matchPriority0 • matchPriority1

Variable	Value
	• matchPriority2 • matchPriority3 • matchPriority4 • matchPriority5 • matchPriority6 • matchPriority7 • matchAllPriorities
PktType	Indicates the data link layer frame format for that can match this classifier. Values include: • ethernetII—only Ethernet II format frames can match this classifier • snap—only IEEE 802 SNAP format frames can match this classifier • llc—only IEEE 802 LLC format frames can match this classifier • ignore—frame format is not considered in determining whether or not a frame matches this classifier
ActionDrop	Indicates whether or not to drop the traffic matching filtering data. Values include: • drop • pass
UpdateDscp	Indicates a value used to update the DSCP field in an IPv4 packet. Values range from -1–63 (0x00 to 0x3f hexadecimal). A value of -1 indicates that the system ignores this parameter.
UpdateUserPriority	Indicates 802.1p value used to update user priority. Values include: • markAsPriority0 • markAsPriority1 • markAsPriority2 • markAsPriority3 • markAsPriority4 • markAsPriority5 • markAsPriority6

Variable	Value
	• markAsPriority7 • ignore
ActionSetPrec	Indicates the automatic drop precedence. Values include: • lowDropPrec—low drop precedence • highDropPrec—high drop precedence When network traffic congestion occurs, packets with a high drop precedence are dropped before packets with a low drop precedence.

Filtering QoS traffic profile filter classifier information using EDM

Use this procedure to display selected parts of the QoS traffic profile filter classifier.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QoS NSNA/Traffic Profile**.
3. In the work area, click the **Classifier** tab.
4. To select a traffic profile filter classifier to filter, click a traffic profile filter classifier row.
5. Configure the filter parameters for the traffic profile filter set.
6. Click **Filter**.
7. Click **Apply**.

Variable Definitions

Use the data in the following table to filter QoS traffic profile filter classifier information.

Variable	Value
AND	Includes all entries in the table that include all specified parameters.
OR	Includes any of the specified parameters.
Ignore Case	When selected, includes entries with the parameters being set, whether in lower case or upper case.

Variable	Value
contains	Returns all cases in which an entry contains the set parameters.
does not contain	Returns all cases in which an entry does not contain the set parameters.
equal to	Returns all cases in which an entry is equal to the set parameters.
does not equal to	Returns all cases in which an entry is not equal to the set parameters.
All Records	When selected, displays all entries in the table.

Creating a QoS traffic profile filter classifier using EDM

Use this procedure to create a new QoS traffic profile filter classifier.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QoS NSNA/Traffic Profile**.
3. In the work area, click the **Classifier** tab.
4. Click **Insert**.
5. Configure the parameters to classify traffic on your network.
6. Click **Insert**.
7. Click **Apply**.

Variable Definitions

Use the data in the following table to create a QoS traffic profile filter classifier.

Variable	Value
Type	Specifies the classifier type. Values include: • NsnaClfr • TrafficProfile
Name	Specifies the name of the classifier. All classifiers with the same name are part of the same filter set. That filter set has the same name as the classifiers.

Variable	Value
Block	Specifies the block name with which the classifier is associated.
EvalPrec	Specifies the evaluation order number of the classifier in that filter set. Two classifiers in the same filter set cannot have the same evaluation order. A higher eval order means a lower precedence for the corresponding policy. Values range from 1–255.
AddrType	Specifies the type of IP address used by this classifier entry. Values include: • N/A—the address type is non-applicable • ipv4 • ipv6
DstIpAddr	Specifies the IP address to match against the destination IP address of a packet. If you leave this box empty, the system ignores this parameter.
DstIpPrefixLength	Specifies the length of the destination address mask. Values range from 0–2040, with 0–32 reserved for IPv4 address masks and 0–128 reserved for IPv6 address masks.
SrcIpAddr	Specifies the IP address to match against the source IP address of a packet. If you leave this box empty, the system ignores this parameter.
SrcIpPrefixLength	Specifies the length of the source address mask. Values range from 0–2040, with 0–32 reserved for IPv4 address masks and 0–128 reserved for IPv6 address masks.
Dscp	Specifies the value for a DiffServ Codepoint (DSCP) in a packet. Values range from -1–63 (0x00 to 0x3f hexadecimal). A value of -1 indicates that the system ignores this parameter.
Protocol/NextHeader	Specifies the IPv4 protocol value, or the IPv6 next-header value. Values range from 0–255. A value of 255 indicates that the system ignores the parameter. The following are specific value designations: • 1 = ICMP-IPv4 • 2 = IGMP • 6 = TCP • 17 = UDP • 20 = FTP Data • 21 = FTP Control

Variable	Value
	• 23 = Telnet • 25 = SMTP • 46 = RSVP • 58 = ICMP-IPv6 • L4Port:69 = TFTP • 80 = HTTP • 443 = HTTPS
DstL4PortMin	Specifies the minimum value for the Layer 4 destination port number in a packet. Values range from 0–65535.
DstL4PortMax	Specifies the maximum value for the Layer 4 destination port number in a packet. Values range from 0–65535.
SrcL4PortMin	Specifies the minimum value for the Layer 4 source port number in a packet. Values range from 0–65535.
SrcL4PortMax	Specifies the maximum value for the Layer 4 source port number in a packet. Values range from 0–65535.
Ipv6FlowId	Specifies the flow identifier for IPv6 packets. Values range from -1–1048575 (0x00 to 0xfffff hexadecimal). A value of -1 indicates that the system ignores this parameter.
IpFlags	Specifies the classifier flag to match in traffic IPv4 headers. Values include: • MoreFragement • doNotFragement
TcpCtrlFlags	Specifies the control flag to match in traffic TCP headers. Values include: • Urg • Ack • Psh • Rst • Syn • Fin

Variable	Value
Ipv4Options	Specifies if the presence of IPv4 options in an IPv4 packet are considered when the system is searching for a match for this classifier. Values include: • present—only IPv4 packets with options match this classifier • notPresent—only IPv4 packets without options match this classifier • ignore—whether or not options are present in IPv4 packets is not considered when determining if the IPv4 packet matches this classifier
DstMacAddr	Specifies the MAC address against which the MAC destination address of incoming packets is compared. If you leave this box empty, the system ignores this parameter.
DstMacAddrMask	Specifies a mask identifying the destination MAC address. If you leave this box empty, the system ignores this parameter.
SrcMacAddr	Specifies a MAC source address of incoming packets. If you leave this box empty, the system ignores this parameter.
SrcMacAddrMask	Specifies a mask identifying the source MAC address. If you leave this box empty, the system ignores this parameter.
VlanIdMin	Specifies the minimum value for the VLAN ID in a packet. Values range from 1–4094.
VlanIdMax	Specifies the maximum value for the VLAN ID in a packet. Values range from 1–4094. If you set VlanIdMin to 1 and VlanIdMax to 4094, the system ignores the VLAN ID parameter.
VlanTag	Specifies the type of VLAN tagging in a packet. Values include:: • untagged • tagged • ignore
EtherType	Specifies the value for the Ethernet type. Values range from 0x00 to 0xffff. If you enter a value of 0xffff, the system ignores this parameter.
UserPriority	Specifies the value for the 802.1p user priority. Values include:

Variable	Value
	• matchPriority0 • matchPriority1 • matchPriority2 • matchPriority3 • matchPriority4 • matchPriority5 • matchPriority6 • matchPriority7 • matchAllPriorities
PktType	Specifies the data link layer frame format for that can match this classifier. Values include: • ethernetII—only Ethernet II format frames can match this classifier • snap—only IEEE 802 SNAP format frames can match this classifier • llc—only IEEE 802 LLC format frames can match this classifier • ignore—frame format is not considered in determining whether or not a frame matches this classifier
ActionDrop	Specifies whether or not to drop the traffic matching filtering data. Values include: • drop • pass
UpdateDscp	Specifies a value used to update the DSCP field in an IPv4 packet. Values range from -1–63 (0x00 to 0x3f hexadecimal). A value of -1 indicates that the system ignores this parameter.
UpdateUserPriority	Specifies 802.1p value used to update user priority. Values include: • markAsPriority0 • markAsPriority1 • markAsPriority2 • markAsPriority3 • markAsPriority4 • markAsPriority5

Variable	Value
	• markAsPriority6 • markAsPriority7 • ignore
ActionSetPrec	Specifies automatic drop precedence. Values include: • lowDropPrec—low drop precedence • highDropPrec—high drop precedence When network traffic congestion occurs, packets with a high drop precedence are dropped before packets with a low drop precedence.

Deleting a QoS traffic profile filter classifier using EDM

Use the following procedure to delete an existing QoS traffic profile filter classifier.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QoS NSNA/Traffic Profile**.
3. In the work area, click the **Classifier** tab.
4. To select a classifier to delete, click the classifier Id.
5. Click **Delete**.

QoS traffic profile filter set configuration using EDM

Use the information in this section to create and manage QoS generic filter sets.

QoS traffic profile filter set configuration using EDM navigation

- Viewing QoS traffic profile filter set information using EDM on page 164
- Filtering QoS traffic profile filter set information using EDM on page 167
- Creating a QoS traffic profile filter set using EDM on page 165
- Deleting a QoS traffic profile filter set using EDM on page 166

Viewing QoS traffic profile filter set information using EDM

Use this procedure to display existing QoS traffic profile filter set configuration information.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QoS NSNA/Traffic Profile**.
3. In the work area, click the **Set** tab.

Variable Definitions

Use the data in this table to help you understand the QoS traffic profile filter set display.

Variable	Value
AclType	Indicates the type of ACL. Values include: • NsnaClfr • TrafficProfile
Name	Indicates a name for this traffic profile filter set. The name must be an existing classifier name. All classifiers with this name are part of this filter set. The filter set itself has this name.
IfIndex	Indicates the logical interface index assigned to the VLAN.
CommittedRate	Indicates the committed rate in kilobits per second (Kbps). Values are multiples or 64 or 1000 Kbps.
BurstSize	Indicates the size of a single transmission burst.
OutActionDrop	Specifies the action to take when packet is out-of-profile. This action is applied only if metering is being enforced, and if the traffic is deemed out-of-profile based on the level of traffic and the metering criteria. (Metering is applied only to traffic matching the filtering data.) Options are the following: • drop—the packet is dropped • pass—the packet is not dropped The default value is pass.

Variable	Value
OutActionUpdateDscp	Indicates the action to take to update DSCP when a packet is out-of-profile. Values range from -1–63. The default value is -1.
SetPriority	Indicates the set priority. Values range from 1–255.
Status	Indicates the set status.
Storage	Indicates the type of storage.

Creating a QoS traffic profile filter set using EDM

Use this procedure to create a new QoS traffic profile filter set.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QoS NSNA/Traffic Profile**.
3. In the work area, click the **Set** tab.
4. Click **Insert**.
5. Configure the parameters for the traffic profile filter set.
6. Click **Insert**.
7. Click **Apply**.

Variable Definitions

Use the data in this table to create a QoS traffic profile filter set.

Variable	Value
AclType	Specifies the type of ACL. Values include: • NsnaClfr • TrafficProfile
Name	Specifies a name for this entry. The name must be an existing classifier name. All classifiers with this name are part of this filter set. The filter set itself has this name.
IfIndex	Specifies the logical interface index assigned to the VLAN.

Variable	Value
CommittedRate	Specifies the committed rate in kilobits per second (Kbps).
MaxBurstRate	Specifies the maximum rate for a single transmission burst in Kbps.
Duration	Specifies the maximum burst duration in milliseconds.
OutActionDrop	Specifies the action to take when packet is out-of-profile. This action is applied only if metering is being enforced, and if the traffic is deemed out-of-profile based on the level of traffic and the metering criteria. (Metering is applied only to traffic matching the filtering data.) Options are the following: • drop—packet is dropped • pass—packet is not dropped The default value is pass.
OutActionUpdateDscp	Specifies the action to take to update DSCP when a packet is out-of-profile. Values range from -1–63. The default value is -1.
SetPriority	Specifies the set priority. Values range from 1–255.

Deleting a QoS traffic profile filter set using EDM

Use this procedure to delete a QoS traffic profile filter set.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QoS NSNA/Traffic Profile**.
3. In the work area, click the **Set** tab.
4. Click **Delete**.

Filtering QoS traffic profile filter set information using EDM

Use this procedure to display selected parts of the QoS traffic profile filter set.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QoS NSNA/Traffic Profile**.
3. In the work area, click the **Set** tab.
4. To select a traffic profile filter set to filter, click a traffic profile row.
5. Configure the filter parameters for the traffic profile filter set.
6. Click **Filter**.
7. Click **Apply**.

Variable Definitions

Use the data in the following table to filter QoS traffic profile filter set information.

Variable	Value
AND	Includes all entries in the table that include all specified parameters.
OR	Includes any of the specified parameters.
Ignore Case	When selected, includes entries with the parameters being set, whether in lower case or upper case.
contains	Returns all cases in which an entry contains the set parameters.
does not contain	Returns all cases in which an entry does not contain the set parameters.
equal to	Returns all cases in which an entry is equal to the set parameters.
does not equal to	Returns all cases in which an entry is not equal to the set parameters.
All Records	When selected, displays all entries in the table.

Configuring the QoS agent using EDM

Use this procedure to configure the QoS agent.

Prerequisites

- Open one of the supported browsers.
- Enter the IP address of the switch to open an EDM session.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QoS Agent**.
3. In the work area, click the **Configuration** tab.
4. In the **QosOperMode** section , click a radio button.
5. Double-click the **NVRamCommitDelay** dialog box.
6. Type a value.
7. To partially reset installed QoS policy state information to the switch default, select the **ResetToPartialDefaults** checkbox.
8. To reset installed QoS policy state information to the switch default, select the **ResetToDefaults** checkbox.
9. In the **DefaultQueueCfg** section , click a radio button.
10. In the **DefaultBufferingCaps** section , click a radio button.
11. In the **TrackStatistics** section , click a radio button.
12. In the **NtApplicationMode** section , click a radio button.

Variable Definitions

Variable	Value
QosOperMode	Controls overall QoS processing for the system.

Variable	Value
	• enable—all QoS functionality is enabled • disable—installed QoS components are temporarily removed until the operational mode is re-enabled The QoS operational mode can not be disabled if QoS components are currently being used by non-QoS applications. If disabled, requests related to QoS components by non-QoS applications will be rejected. **Important:** Re-enabling the QoS operational mode can result in errors if you have made changes affecting available resources while QoS was temporarily disabled.
NVRamCommitDelay	Specifies the maximum time before non-volatile QoS data is written to NVRAM. Values range from 0–604800 seconds.
ResetToPartialDefaults	When selected, resets all QoS agent values to default, except DefaultQueueCfg and DefaultBufferingCaps.
ResetToDefaults	When selected, resets all QoS agent values to default. **Important:** You must restart the switch for changes to ResetToDefaults to take effect.
DefaultQueueCfg	Specifies the default queue set associated with all egress interfaces. Values include: • queueSetOne • queueSetTwo • queueSetThree • queueSetFour • queueSetFive • queueSetSix • queueSetSeven • queueSetEight **Important:** You must restart the switch for changes to DefaultQueueCfg to take effect.

Variable	Value
DefaultBufferingCaps	Specifies the level of buffer sharing or over-allocation that can take place among ports sharing a buffer pool. Values include: • minimumOverAllocation—only a small amount of resource sharing is permitted • mediumOverAllocation—a medium amount of resource sharing is permitted • maximumOverAllocation—maximizes the possibility of over-allocation occurring **Important:** You must restart the switch for changes to DefaultBufferingCaps to take effect.
TrackStatistics	Specifies the type of statistics tracking. Values include: • disabled • individual • aggregate
NtApplicationMode	Specifies the Avaya Automatic QoS application mode. Values include: • disable • enablePureMode • enableMixedMode

QoS policy class support management using EDM

Use the information in this section to display and filter resource allocation table information.

QoS policy class support management using EDM navigation

- Displaying policy class support using EDM on page 171
- Filtering the resource allocation table using EDM on page 171

Displaying policy class support using EDM

Use the following procedure to display policy class support.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Agent**.
3. In the work area, click the **Policy Class Support** tab.

Variable Definitions

Field	Description
PolicyClassName	Identifies the Policy Rule Classes (PRCs) supported by the device. A PRC is synonymous to a MIB table; therefore, the supported PRCs indicate which MIB tables are supported for QoS processing purposes.
CurrentInstances	Identifies the current number of Policy Rules Instances (PRIs) that are installed for a specific PRC (equates to the current number of entries in a given MIB table).
MaxInstalledInstances	Identifies the maximum number of PRIs that can be installed and/or modified by a user for a specific PRC (equates to the number of MIB table entries that can be created or modified by a user).

Filtering the resource allocation table using EDM

Use the following procedure to filter the resource allocation table.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Agent**.
3. In the work area, click the **Policy Class Support** tab.

4. Click **Filter**.
5. In QoS Agent, Resource Allocation - Filter, set the filter conditions.
    a. Select **AND** to include all entries in the table that include all specified parameters, or select **OR** to include any of the specified parameters.
    b. Select **IGNORE CASE** to include all entries with the parameters being set, whether in lower case or upper case.
    c. Define the search to return all cases in which an entry **CONTAINS, DOES NOT CONTAIN, EQUALS TO, DOES NOT EQUAL TO** the set parameters.
    d. Select **ALL RECORDS** to display all entries in the table.
    e. Set **Precedence** to filter by order of precedence.
    f. Select **Port** to display the entries by port.
6. Click **Filter.**

Displaying policy device identification using EDM

Use the following procedure to display policy device identification data.

Prerequisites

- Open one of the supported browsers.
- Enter the IP address of the switch to open an EDM session.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Agent**.
3. In the work area, click the **Policy Device Identification** tab to view the data.

Variable Definitions

Field	Description
Descr	Specifies the description of the policy agent. **Important:** The description must include the name and version identification of the policy agent hardware and software.
MaxMsg	Specifies the maximum message size in octets that the device can support.

Displaying resource allocation using EDM

Use the following procedure to display QoS resource Allocation information.

Prerequisites

- Open one of the supported browsers.
- Enter the IP address of the switch to open an EDM session.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Agent**.
3. In the work area, click the **Resource Allocation** tab.

Variable Definitions

Field	Description
Precedence	Displays the applied precedence (from 1–8).
Port	Displays the Port number.

Field	Description
FiltersConsumed	Displays the number of rules (filters) in use by policy and filter data by that interface.
MetersConsumed	Displays the number of meters in use by policy data by that interface.
CountersConsumed	Displays the number of counters in use by that interface.
NonQosFiltersConsumed	Tracks the current number of filters in use, not due to installed filter data, for a given precedence level and interface.
NonQosMetersConsumed	Tracks the current number of meters in use, not due to installed policy data, for a given precedence level and interface.
TotalFiltersAvail	Displays the maximum number of filters available (for each precedence and for each ASIC).
TotalMetersAvail	Displays the maximum number of meters available (for each precedence and for each ASIC).
TotalCountersAvail	Displays the maximum number of counters available (for each precedence and for each ASIC).
RangeCheckersConsumed	Displays the number of range checkers consumed by QoS.