Configuring Quality of Service on Avaya Ethernet Routing Switch 3500 Series

Release 5.2
NN47023-503
Issue 03.01
March 2014

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 may generally make available to users of its products and Hosted Services. 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 websites 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 Avaya hardware and software. 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 website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; 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”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link “Heritage Nortel Products”, or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, 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

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States

and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), 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, Hosted Service(s) 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. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose of this document

This document provides procedures and conceptual information to configure Quality of Service.

Related resources

Documentation

For a list of the documentation for this product, see *Documentation Roadmap Reference for Avaya Ethernet Routing Switch 3500 Series*, NN47203-101.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com.

Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to http://support.avaya.com, select the product name, and select the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Note:

Videos are not available for all products.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: New in this release

The following hardware and software features are new in Avaya Ethernet Routing Switch (ERS) 3500 Series Release 5.2:

ERS 3500 hardware

The following table lists and describes the new hardware supported in Release 5.2:

Hardware	Description
Modules	
Avaya Ethernet Routing Switch 3549GTS	48 10/100/1000 non-PoE and 2 shared SFP, plus 1 1/10 Gigabit SFP+ port, plus 2 rear dual mode/ stacking ports.
Avaya Ethernet Routing Switch 3549GTS-PWR+	48 10/100/1000 802.3at PoE+ and 2 shared SFP, plus 1 1/10 Gigabit SFP+ port, plus 2 rear dual mode/stacking ports.

ERS 3500 software features

The following software features are new for ERS 3500 Series Release 5.2:

- Avaya Energy Saver
- SLAMon enhancements
- Simple Loop Protection Protocol (SLPP) Guard
- Unified authentication
- Flash History
- Static LACP Key to Trunk ID binding

Features

There are no feature-related changes in *Avaya Ethernet Routing Switch 3500 Series Configuration - Quality of Service*, NN47203–503, for Release 5.2.

Other changes

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

Document title change

In Release 5.2, the title of this document changed from *Avaya Ethernet Routing Switch 3500 Series Configuration — Quality of Service*, NN47203-503 to *Configuring Quality of Service on Avaya Ethernet Routing Switch 3500 Series*, NN47203-503.

Chapter 3: Introduction

This document provides information you need to configure Quality of Service (QoS) for the Ethernet Routing Switch 3500 Series.

ACLI command modes

Avaya command line interface (ACLI) provides the following configuration modes:

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

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 `3526T>`	No entrance command, default mode.	Type `exit`or `logout`
Privileged EXEC `3526T#`	From User EXEC mode, type: `enable`	Type `exit` or `logout`
Global Configuration `3526T(config)#`	From Privileged EXEC mode, type: `configure`	To return to Privileged EXEC mode, type: `end` or `exit` To exit ACLI completely, type: `logout`
Interface Configuration `3526T(config-if)#`	From Global Configuration mode: To configure a port, type: `interface`	To return to Global Configuration mode, type: `exit`

Command mode and sample prompt	Entrance commands	Exit commands
	`fastethernet <port number>` To configure a VLAN, type: `interface vlan <vlan number>`	To return to Privileged EXEC mode, type: `end` To exit ACLI completely, type: `logout`

For more information about the ACLI configuration modes, see *Avaya Ethernet Routing Switch 3500 Series Fundamentals* (NN47203-102).

Chapter 4: Policy-based network fundamentals

Overview

Differentiated services (DiffServ) is a Quality of Service (QoS) network architecture that offers varied levels of service for different types of data traffic. With DiffServ you can designate a specific level of performance on a packet-by-packet basis instead of using the best-effort model for your data delivery. You can give preferential treatment (prioritization) 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 first six bits, called the DS codepoint (DSCP), are used in the DiffServ architecture. 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.

Within the DiffServ network, the marked packets are placed in a queue according to their marking, which determines the Per-Hop-Behavior (PHB) of that packet. For example, if a video stream is marked to receive the highest priority, 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. Traffic shaping can also be used to temporarily delay traffic to ensure that the flows conform to downstream bandwidth limits.

Policy-based networks and QoS

System administrators can use Policy-enabled networks to prioritize network traffic. Prioritizing network traffic provides improved service for selected applications.

System administrators can use QoS to establish service level agreements (SLA) with network customers. 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, require 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.

Differentiated Services (DiffServ) provides 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.

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

Differentiated Services concepts

Differentiated Services (DiffServ) 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 at access points. DiffServ is described in IETF RFC 2474 and 2475. 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

Within a DiffServ domain, packet treatment is regulated by classification and mapping

DiffServ designates a specific level of performance on a packet-by-packet basis, instead of using the best-effort model for data delivery. You can give preferential treatment (prioritization) 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 RFC 2474 and 2475, is marked. The DS field in the IP header is an octet, and the first six bits, called the DS codepoint (DSCP), are used in the DiffServ architecture.

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. You can configure the switch to recognize a DSCP in an ingress IP packet and prioritize the packet to one of the hardware QoS queues that are available on the switch. You can achieve DSCP recognition by mapping

the DSCP to 802.1p markings and mapping the 802.1p markings to one of hardware QoS queues.

Traffic is classified as it enters the DiffServ network and, within the DiffServ network, the marked packets are placed in a queue according to their marking, which in turn determines the per-hop behavior (PHB) of that packet. Within the IP packet, the 6 bits in the DSCP are marked to identify how the packet is treated at each subsequent network node. For example, if a video stream is marked so that it receives the highest priority; then it is placed in a highpriority 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. As the traffic moves within the DiffServ network, policies ensure that traffic, marked by the various DSCPs, is treated according to that marking.

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 system expects the traffic to be metered at the ingress point of the downstream network.

Traffic metering and shaping ensures that the traffic flow conforms to an SLA to provide certain levels of service in terms of bandwidth for different types of network traffic. Traffic shaping can also be used to temporarily delay traffic to ensure that the flows conform to downstream bandwidth limits.

Differentiated Services Code Point recognition

You can configure the Ethernet Routing Switch 3500 Series to recognize a DSCP in an ingress IP packet and prioritize the packet to one of the four hardware QoS queues that are available on the Ethernet Routing Switch 3500 Series. You can achieve DSCP recognition by mapping the DSCP to 802.1p markings and mapping the 802.1p markings to one of four hardware QoS queues.

Port-based and Role-based QoS policies

The switch supports both port-based and role-based Quality of Service (QoS) policies.

In a port-based Quality of Service environment, you apply policies directly to individual ports. A port-based Quality of Service environment provides direct application of Quality of Service policies and eliminates the need to group ports after you assign policies.

In a role-based Quality of Service environment, you must assign a role to individual ports and then assign that role to a policy.

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

Traffic Class policies and 802.1p Class of Service support

The Ethernet Routing Switch 3500 Series has four internal hardware CoS queues associated with each port for transmission of frames. The switch enables 802.1p Traffic Class by mapping the eight 802.1p priority levels into these four internal hardware CoS queues.

The internal CoS queues are labeled by priority as follows:

- Low
- Medium
- High
- Highest

The available queuing policies are as follows:

- Strict Priority
- Weighted Round Robin

Strict Priority

Strict Priority queuing operates in an interrupt fashion. Frames from the High priority queues take precedence over frames in Low priority queues. For example, if the Highest queue contains frames, all processing in the lower priority queues is stopped, and the switch transmits the Highest priority frames until that queue is empty.

When the Highest priority queue is empty, frames from the High priority queue, if any, are sent in succession, from the Highest priority queue to the Low priority queue.

One limitation with Strict Priority queuing is that it is possible for some queues to never be serviced, causing dropped packets. Therefore, Avaya does not recommend the use of Strict Priority queuing.

Weighted Round Robin

With Weighted Round Robin queuing, each queue is assigned a Q weight, which represents a relative proportion of time during which the queue can send packets.

This technique ensures each queue gets dedicated bandwidth for transmitting its packets. With Weighted Round Robin, no priority is assigned to the queues. Each queue sends frames in proportion to its Q weight.

One limitation of Weighted Round Robin queuing is that, during congestion, the actual traffic in one of the queues can rise above its allotted queue size. In this case, the excess traffic is discarded.

For more information about Weighted Round Robin (WRR) and Strict dequeuing, see Queue sets on page 36.

QoS components

The switch 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 similar 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 experience 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 used 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 a better effort treatment for packets that are in-profile (packets that do not break the service agreements between the user and the service provider).

  Following table describes the service classes and their required treatment.

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.
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,	Platinum, Gold, Silver, and Bronze	Communications requiring interaction with additional minimal delay (such	Assured Forwarding (AF)

Traffic category	Service class	Application type	Required treatment
mission-critical traffic		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.	
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.

Avaya Automatic QoS

When you enable Avaya Automatic QoS (AAQ) support through the QoS Agent, default interface class processing is enhanced. Interface class processing is based on role type, using filtering logic to identify traffic based on defined DSCP values.

AAQ improves Avaya application performance transparently, particularly in times of network congestion. Avaya application traffic consists of IP Telephony and Multimedia applications.

You enable or disable AAQ globally and you do not need to configure individual QoS components across a variety of platforms. After you enable AAQ, automatic QoS is applied end-to-end, from the application traffic to the Avaya or third party data infrastructure, and non-Avaya application traffic is unaffected.

The following table shows DSCP values that identify Avaya application traffic.

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

Avaya application traffic receives preferential treatment and is marked for downstream processing according to the AAQ Mode you select. AAQ Modes are

- disabled
- pure mode
- mixed mode

Depending on the active AAQ Mode, you can maintain or remark DSCP values using the AAQ application.

The following table describes the AAQ Modes.

Variable	Definition
disabled	Disables AAQ support for the system. This is the default mode.
mixed	Enables AQ application traffic processing on all ports with egress DSCP remapping.
pure	Enables AQ application traffic processing on all ports without egress DSCP remapping.

When AAQ Mode is pure, packets are sent with the AQ DSCP value unchanged. After AAQ Mode is mixed, the DSCP value is remarked and packets are sent with Standard DSCP.

The following table lists values for AQ DSCP, Class of Service (CoS), drop precedence, and Standard DSCP.

AQ 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)

Note:

Auto QoS mixed or pure requires a free precedence on all ports. By default, all 4 precedences are reserved, one being permanently occupied by ARP. You can free at least one precedence by moving all ports to other interface groups that do not require filters (Unrestricted, Trusted, UntrustedBasic) or removing the filters used by a non-QoS application.

Specifying interface groups

Interface groups are used to create role-based policies. Role-based policies differ from portbased policies in that role-based policies group ports to apply a common set of rules.

Port-based polices are used to apply rules to one port only. Each port can belong to only one interface group.

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). 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

Important:

You must remove all ports from an interface group before you delete the group.

You must first remove the policy to be able to remove an interface group that is referenced by a policy.

Interface shaping

Interface shaping involves limiting the rate at which all traffic leaving 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 consumption on your networks. Interface-based shaping, in conjunction with ingress flow metering, is a vital component of the overall bandwidth management solution.

Important:

You can obtain different results using a meter and/or shaper with the same parameters. This is due to the adding of VLAN encapsulation, when applicable.

Metering is applied to packets received by a port before the VLAN encapsulation is added.

Shaping is applied to packets sent on a port, after the port adds the VLAN encapsulation to the packet.

ADAC 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 3500 Series Configuration - Layer 2* (NN47203-500).

Rules

Packet classifiers identify packets according to content in the packet header, including the source address, destination address, source port number, and destination port number. Packet classifiers identify flows for additional processing.

You can use three types of classifier elements to construct a classifier:

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

Classifier definition

A classifier consists of one or more classifier elements. The classifier elements dictate the classification criteria of the classifiers. You can use only one element of each type (IP, L2, or System Classifier Element) to construct a classifier.

The figure that follows displays the relationship between the classifier elements, classifiers, and classifier blocks.

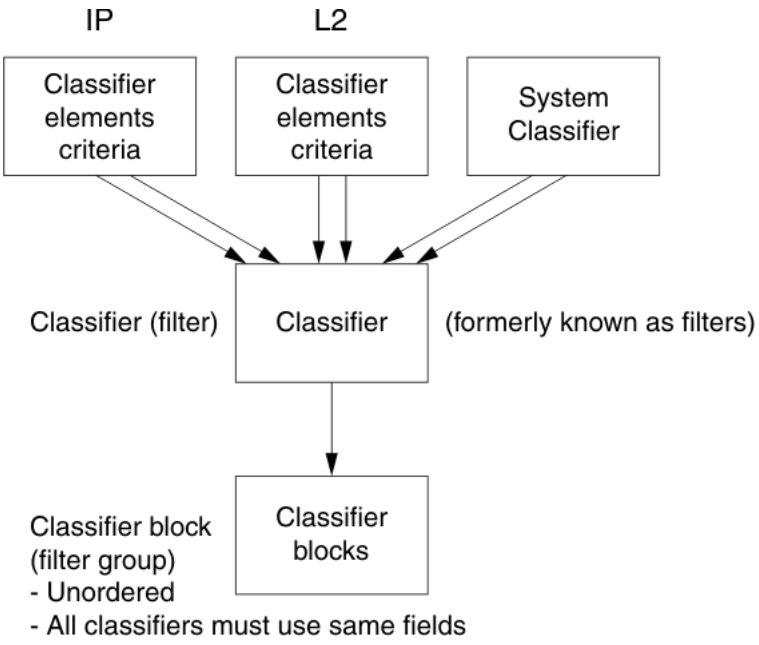

Figure 1: Relationship of classifier elements, classifiers, and classifier blocks

The system automatically creates some classifiers on untrusted ports and users create additional classifiers.

The switch supports trusted, untrusted with the variations untrustedV4V6 and untrustedBasic, and unrestricted classifications for ports.

You can apply these classifications to groups of ports (interface groups); also known 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 connected to end stations.

Unrestricted ports can be access links or connected to the core network.

The factory default setting for all ports is untrusted. However, after you create interface groups, the default setting is unrestricted.

IP classifier elements

The switch 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 or IPv6 Layer 4 source port number with TCP/UDP (range of port numbers)

Layer 2 classifier elements

The switch 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 ID numbers)
- VLAN tag
- EtherType
- IEEE 802.1p user priority values

Note:

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 when only certain protocol header fields, such as IP source address, IP protocol field, and VLAN ID for flow classification are supported.

You can create fully customized classifiers to match IP-based traffic using nontypical fields in Layers 2, 3, 4, and beyond.

The switch Content Aware Processor (CAE) lookup engine supports selection of 32 bytes within the first 80 bytes of the packet.

Classifiers and classifier blocks

You can combine classifier elements 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 (same classifier set-id) 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.

You can combine classifiers 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.

All classifiers that are part of a single classifier block (that is, with the same block number) must each filter on identically the same parameters at the packet level. This includes the same mask, range, and VLAN tag type. If this criterion is not met, an error message is generated after an attempt to create the classifier block, or to add a new member to an existing block, is made. 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 (not identical actions or meters, but also associated actions or meters).

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.

You can associate each classifier, through policies, with actions that are executed after the packet matches the filter criteria. You can associate each classifier block itself directly to an action or meter, not necessarily through a policy. 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 Specifying actions on page 27 for an illustration of the traffic treatment).

Classifier elements, through individual classifiers or a classifier block, are associated with:

- an interface group (through policies)
- action (for individual classifiers, through policies)
- metering (for individual classifiers, through policies)

You can apply multiple policies to a flow.

The policy evaluation order is determined by the policy precedence. The order of precedence appears from the highest precedence value to the lowest precedence; for example, a precedence value of 2 is evaluated before a precedence value of 1).

Important:

You can associate classifier blocks with a meter or action, but not with individual classifiers that comprise a block.

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 with no precedence.

Specifying actions

The figure that follows summarizes how QoS matches packets with actions.

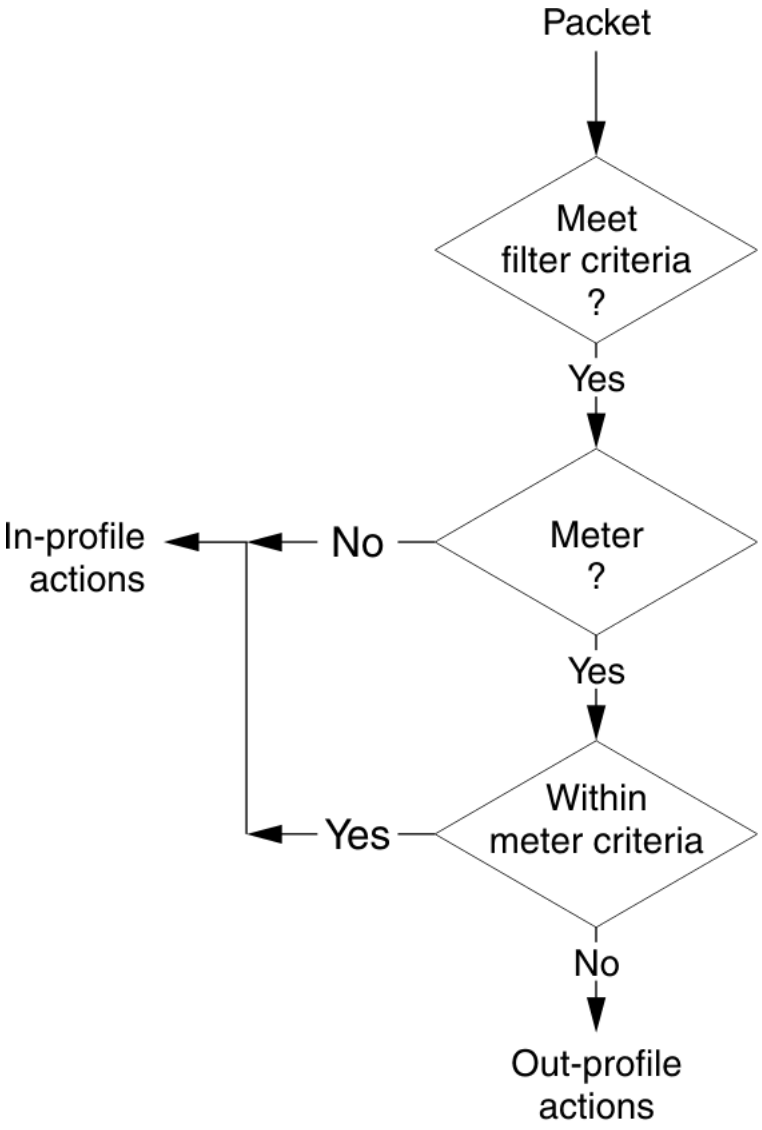

Figure 2: Flowchart of QoS Actions

Following table shows a summary of the allowable actions for different matching criteria.

Actions	In-Profile	Out-Of-Profile
Drop/transmit	X	X

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

The QoS filters direct the system to initiate the following actions on a packet collectively, 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:

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

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 interface.

The set of actions applied to the packet is a result of the policies associated with the interface, ranging from no actions to many actions.

For example, if one policy associated with the designated interface specifies a value to updating the DSCP value, while another policy associated with that same interface specifies a value to update the 802.1p user priority value, both of these actions occur. If conflicts among actions are detected—for example, if two policies on the interface request DSCP update, but specify different values—the system uses the value from the policy with the higher precedence.

The actions applied to packets include those actions from user-defined policies and those actions from system default policies.

The user-defined actions always carry higher precedences than the system default actions. That is, if user-defined policies do not specify actions that overlap with the actions associated with system default policies, the default policy actions with the lowest precedence are 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.

Following table shows a summary of the allowable interface action extensions for different matching criteria.

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 3500 Series does not initiate an action extension based packet type. So, user has to 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). And you must use the same port for both unicast and non-unicast packets redirection.

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 limit the ingress traffic stream, based on a committed-rate and burst size which you create. Thus, creating meters yields In-Profile and Out-of-Profile traffic.

You can associate different meters with different classifiers across a block of classifiers.

You can configure policies without metering, or policies 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.

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

The system applies the metering criteria to each port of the interface group (role combination) for a meter applied to a policy, and the specified bandwidth is allocated on each port, not distributed across all ports.

Using meters, you can set a Committed Rate in Kb/s (1000 b/s in each Kb/s).

The range for the committed rate is 64 Kb/s to 10 GB/s. All traffic within this Committed Rate is In-Profile.

You can also set a Maximum Burst Rate that specifies an allowed data burst larger than the Committed Rate for a specified duration.

After you set the burst rate, the system suggests burst duration rates that you can select.

For example, traffic policing limits traffic with a committed rate of 2500 Kb/s entering a port with a specific bandwidth. But, after you set a maximum burst rate to exceed the committed rate, for the specified maximum burst rate duration the system does not drop the traffic.

Combined, committed rate and maximum burst rate define the In-Profile traffic.

The system rejects meter definitions if the committed burst size is too small, based on the requested committed rate. The committed burst size can be only one of the following discrete values (in bytes): (128K), 262144 (256K), 524288 (512K).

Trusted, untrusted, and unrestricted interfaces

Ports are classified into three categories:

- trusted
- untrusted/untrustedv4v6/untrustedBasic
- 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 are either access links or are 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.

  - Untrustedv4v6 interfaces

    The same logic and re-marking as Untrusted interfaces are performed on both IPv4 and IPv6 traffic types.

  - UntrustedBasic

    The UntrustedBasic interface class behaves similarly to the Untrustedv4v6 class, with the caveat that tagged and untagged traffic are treated the same.

The following table 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 you do not intervene; they are the default actions of the switch.

Type of filter	Action	Trusted	Untrusted / Untrustedv4v6	UntrustedBasic	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	Updates to 0 (Standard), whether tagged or untagged	Does not change
	IEEE 802.1p	Updates based on DSCP mapping table value	Updates based on DSCP mapping table value	Updates based on DSCP mapping table value	Does not change

The switch 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.

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

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 switch uses default system classifiers to change the packet IEEE 802.1p and drop precedence based on the DSCP of the packet.

If a packet is received from an untrusted (IPv4) or untrustedv4v6 (both IPv4 and IPv6) port and it does not match any one of the classifier elements installed by the user on the port, the Avaya

Ethernet Routing Switch 3500 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 the packet is untagged, the switch uses the default classifier to change the DSCP based on the default IEEE 802.1p priority of the ingress untrusted port. This default priority, which is 0, can be customized. Once this priority is determined, the switch uses the DSCP-to-CoS mapping table to determine the DSCP value.

The following table lists criteria for network service classes as they pertain to DSCP, queue number, and recommended scheduler.

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

Specifying policies

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.

Important:

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

Avaya recommends that you configure all applications which assign filters (IP Source Guard, UDPForwarding) before you configure any QoS policies and QoS Access Lists.

When you configure policies, it is important to consider that the policy with the highest precedence is evaluated first, and then the policy with the next lowest precedence. The valid precedence range for QoS policies is 1 to 3.

For example, with a precedence of 1 to 3, the system begins the evaluation with 3. The valid precedence range can change if you enable certain features, such as IPSG, because QoS shares resources with these applications.

Allocations for non-QoS applications are dynamic. This means that if a certain non-QoS application is enabled at some point, it will try to set itself on the highest free precedence

available. If, for example, there is a QoS policy defined by the user on precedence 3 for port 1, and then the user enables IP Source Guard on the same port, IPSG will occupy precedence 2. However, after a reboot of the system, IPSG will transition to precedence 3, creating a conflict. Then the system automatically assigns the port to the qosDisabledIfcs interface group, and all QoS policies are no longer applied. To prevent the automatic disabling of QoS on the port in the event of a precedence conflict with a non-QoS application, it is recommended to first configure the non-QoS applications, and then the QoS settings.

Other applications that use QoS include

- EAPOL
- IP Source Guard
- UDP Forwarding

You must enable EAPOL prior to any other QoS application, because functionality can be affected.

Before you configure any QoS policies and QoS Access Lists, you must configure all QoS based applications (IP Source Guard, UDP Forwarding, and EAPOL).

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 after certain userdefined characteristics are matched. A policy action is the effect a policy has on network traffic that matches the traffic profile of the policy.

Policies combine

- Actions
- Meters
- Classifiers or classifier blocks (which contain classifier elements)
- Interface groups

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

You can assign ports 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.

Statistics can also be tracked for QoS. The switch supports statistics for each policy, classifier, or interface.

Important:

You can enable or disable policies. You do not need to delete a policy to disable it. To modify a policy, you must delete the policy first and then create a new one.

Packet flow using QoS

Using DiffServ and QoS, you can designate a specific performance level for packets. The combination allows network traffic prioritization. But, because you can create a number of policies and each policy can match one or many flows, supporting complex classification scenarios, careful planning is required.

This section contains an introduction to packet prioritization using QoS. Fundamentally, packet prioritization methods depend on the DSCP and the 802.1 priority level and drop precedence.

The QoS class directs which group of packets receives the best network throughput. The level of service for each packet is determined by the configurable DSCP. The available levels of QoS classes are Network, Premium, Platinum, Gold, Silver, Bronze, and Standard.

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

The classifiers and 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 because packets from a specific port have the same classification parameters as all others in the particular interface group (role combination).

When you configure rate limiting, you configure a percentage of port bandwidth based on the current system operating speed.

Rate limiting is implemented in the hardware based on packets per second. Based on an average packet size of 500 bytes, the system computes the packet per second rate.

For example, if you specify limiting the forwarding rate of broadcast packets to 1000 packets per second, the system discards additional broadcast packets after the broadcast packet rate exceeds the threshold value. During each second, the first 1000 broadcast packets are transmitted; then any additional broadcast packets arriving on the port, until the next second, are discarded.

Meters, operating at ingress, keep the sorted packets within certain parameters.

You can configure a committed rate of traffic, allowing a certain size for a temporary burst, as In-Profile traffic.

The system considers all other traffic 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. You can configure policies that monitor the characteristics of the traffic and perform a controlling action on the traffic after certain user-defined characteristics are matched.

The following figure provides a schematic overview of QoS policies.

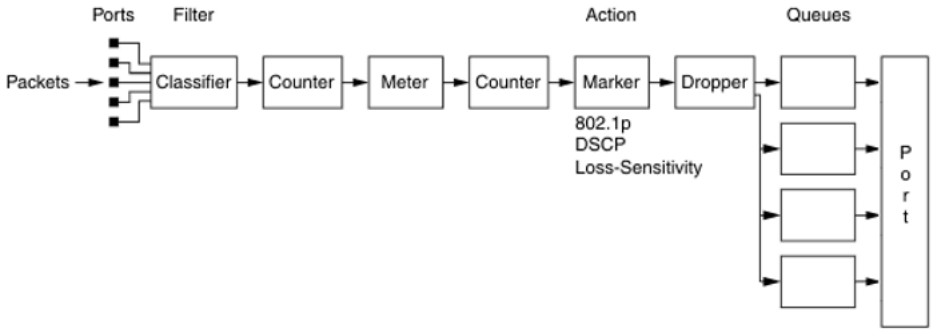

Figure 3: QoS Policy Schematic

Queue sets

A QoS queue set is used to logically represent the queuing capabilities associated with an egress QoS interface.

A queue set includes a number of related queuing components that dictate the queuing behavior supported by the set itself.

Queuing components include:

- 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. After queues are serviced using a Weighted Round Robin (WRR) 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).

Egress queuing and buffering characteristics, and the CoS-to-queue priorities, are the same across all QoS ports.

The switch factory default queue set and buffer allocation mode values are based on the following parameters:

- queue set 4 (WRR)
- buffer allocation mode: Maximum

Modifying CoS-to-queue priorities

You can modify the association of 802.1p, or CoS, values to each queue within the queue set. Within the queue you can assign a set a value of 0 to 7 to each queue in the set.

Important:

Any modification to the CoS-to-queue values takes effect immediately; do not reset the switch.

QoS configuration guidelines

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

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

The Avaya Ethernet Routing Switch 3500 supports:

- Up to 3 policies, corresponding to precedences 1–3, configurable on a per-port basis
- Up to 256 classifiers for each mask precedence
- Up to 128 meters for each mask precedence
- Up to 128 counters for each mask precedence

Using the unrestricted role for ports, the system prioritizes traffic based on 802.1p priority. The 802.1p priority allows filter configuration 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.

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

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.

For example, assign all packets marked with DSCP 46 (2E) priority, such as with VoIP, to the highest priority queue.

Example of assigning DSCP 46 (2E) priority packets to the highest priority queue

```
3526T(config)#qos if-group name "Trust_VoIP" class unrestricted
3526T(config)#no qos if-assign port 2-20
3526T(config-if)#qos if-assign port 1 name Trust_VoIP
3526T(config)#qos ip-element 1 ds-field 46
3526T(config)#qos classifier 1 set-id 1 name "Trust_VoIP" element-type ip element-
id 1
3526T(config)#qos policy 1 name "Trust_VoIP" if-group "Trust_VoIP" clfr-type
classifier clfr-id 1
in-profile-action 7 precedence 3 track-statistics
```

Chapter 5: Configuring QoS using ACLI

You can use the information in this chapter to configure Quality of Service (QoS) parameters using Avaya Command Line Interface (ACLI).

Displaying QoS parameters

You can choose which QoS parameters to display to determine the current QoS settings.

About this task

If you want to create or change QoS configuration you can use the **show qos** command, with parameters, to determine the current settings.

Procedure

1. Log on to the Privileged EXEC mode in ACLI.
2. At the command prompt, enter the following command

```
show qos {acl-assign <1-65535 | action [user | system | all |
<1-65535>] | agent <details>| capability [meter | shaper] |
classifier [user | system | all | <1-65535>] | classifier-
block [user | system | all |<1-65535> ] | diag | egressmap [ds
<0-63>]| if-action-extension [user | system | all |
<1-65535>] | if-assign [port] | if-group | if-shaper [port] |
ingressmap |ip-acl[<1-65535>]| ip-element [user | system |
all | <1-65535>] | l2-acl <1-65535> | l2-element [user |
system | all | <1-65535>] | meter [user | system | all |
<1-65535>] | policy [user | system | all | port |<1-65535>] |
port <list> | queue-set | queue-set-assignment | statistics
<1-65535> | system-element [user | system | all |<1-65535>]}
```

Variable definitions

The following table describes the parameters for the **show qos** command.

Variable	Value
acl-assign *<1-65535>*	Displays access list assignments.

Variable	Value
action *[<1-65535> | all | system | user]*	Displays the base action entries. The applicable values are: • <1-65535>—displays a particular entry. • all—displays user-created, default, and system entries. • system—displays only system entries. • user—displays only user-created and default entries. DEFAULT: all
agent *<details>*	Displays the global QoS parameters. details—displays the policy class support table.
capability *<meter | shaper>*	Displays the current QoS meter and shaper capabilities of each interface. The applicable values are: • meter—displays QoS port meter capabilities. • shaper—displays QoS port shaper capabilities.
classifier [*<1-65535>* | *all* | *system user*	Displays the classifier set entries. The applicable values are: • <1-65535>—displays a particular entry. • all—displays all user-created, default, and system entries. • system—displays only system entries. • user—displays only user-created and default entries. DEFAULT: all
classifier-block *<1-65535>* | *all* | *system* | *user*	Displays the classifier block entries. The applicable values are: • <1-65535>—displays a particular entry. • all—displays all user-created, default, and system entries. • system—displays only system entries. • user—displays only user-created and default entries. DEFAULT: all.
diag	Displays the diagnostics entries for the switch • unit, plus a value for the switch number, displays the diagnostic entries for a specific unit in a stack
egressmap *ds <0–63>*	Displays the associate between the DSCP and the 802.1p priority and drop precedence. • ds — displays mapping for specified DSCP value.
if-action-extension *<1-65535>* | *all* | *system* | *user*	Displays the interface action extension entries. The applicable values are: • <1-65535>—displays a particular entry. • all—displays all user-created, default, and system entries.

Variable	Value
	• system—displays only system entries. • user—displays only user-created and default entries. DEFAULT: all.
if-assign <*port*>	Displays the list of interface assignments. port—List of ports. Displays the configuration for particular ports
if-group	Displays the interface groups.
if-shaper <*port*>	Displays the interface shaping parameters. port—List of ports. Displays the configuration for particular ports
ingressmap	Displays the 802.1p priority to DSCP mapping.
ip-acl <*1–65535*>	Displays the specified IP access list assignment entry
ip-element <*1-65535*> | *all* | *system* | *user*	Displays the IP classifier element entries. The applicable values are: • <1-65535>—displays a particular entry. • all—displays all user-created, default, and system entries. • system—displays only system entries. • user—displays only user-created and default entries. DEFAULT: all
l2–acl <*1–65535*>	Displays the specified Layer 2 access list assignment entry.
l2-element <*1-65535*> | *all* | *system* | *user*	Displays the Layer 2 classifier element entries. The applicable values are: • <1-65535>—displays a particular entry. • all—displays all user-created, default, and system entries. • system—displays only system entries. • user—displays only user-created and default entries. DEFAULT: all
meter <*1-65535*> | *all* | *system* | *user*	Displays the meter entries. The applicable values are: • <1-65535>—displays a particular entry. • all—displays all user-created, default, and system entries. • system—displays only system entries. • user—displays only user-created and default entries. DEFAULT: all
policy <*1-65535*> | *all* | *system* | *user*	Displays the policy entries. The applicable values are:

Variable	Value
	• <1-65535>—displays a particular entry. • all—displays all user-created, default, and system entries. • port — specify list of ports • system—displays only system entries. • user—displays only user-created and default entries. DEFAULT: all
port <*list*>	Displays the QoS parameters for all ports or for specified ports.
queue-set	Displays the queue set configuration.
queue-set-assignment	Displays the association between the 802.1p priority to that of a specific queue.
statistics <*1-65535*>	Displays the policy and filter statistics values. • <1-65535>—displays a particular entry.
system-element <*1-65535*> | *all* | *system* | *user*	Displays the system classifier element entries. The applicable values are: • <1-65535>—displays a particular entry. • all—displays all user-created, default, and system entries. • system—displays only system entries. • user—displays only user-created and default entries.

Displaying QoS capability policy configuration

You can display QoS meter and shaper capabilities for system ports for your switch.

About this task

If you want to create or change QoS meter and shaper capabilities for ports, you can use the **`show qos capability`** command, with parameters, to view the current settings on your switch.

Procedure

1. Log on to the Privileged EXEC mode in ACLI.
2. At the command prompt, enter the following command

```
show qos capability {meter [port] | shaper [port]}
```

Variable definitions

The following table describes the parameters for the **show qos capability** command.

Variable	Value
meter *[port]*	Displays granularity for Committed Rate, Maximum Committed Rate, and Maximum Bucket that can be used on ports for meters. port—specifies list of ports, displays the information for particular ports
shaper *[port]*	Displays granularity for Committed Rate, Maximum Committed Rate, and Maximum Bucket that can be used on ports for shapers. port—specifies list of ports, displays the information for particular ports

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 Displaying QoS parameters on page 39.

Assigning ports to an access list

When you apply an IP or L2 ACL to a port using the `qos acl-assign port x acl-type` command, you may encounter the following error:

```
% Cannot modify settings
% Inadequate resources available for application policy criteria
```

This error message indicates that you exceeded the amount of QoS precedences available for application policies. The number of IP or L2 classifier elements you can apply to a port depends on the number of available QoS precedences that are not being utilized by other applications that also utilize QoS precedences. Applications that utilize QoS precedences on the ERS 3500 Series include ARP, DHCP, UDP Forwarding, MAC Security, and Port Mirroring.

On the ERS 3500 switches, by default, all four QoS precedences are reserved for ARP, DHCP, and two default QoS policies (UntrustedClfrs1 and UntrustedClfrs2), leaving no QoS precedences available.

You can view which QoS precedences are being utilized by using the `show qos diag` command.

In the following example, the `show qos diag` output displays that all four QoS precedences are being utilized by ARP, DHCP and two default QoS policies (UntrustedClfrs1 and UntrustedClfrs2); therefore, in order to apply an IP or L2 ACL policy, QoS precedences should be released (the fourth precedence is permanently occupied by ARP and cannot be released by the user).

```
3524T# show qos diag
Unit/Port  Mask Precedence Usage
            4   3   2   1
---------  -------------------
1/1         AR  DH  Q   Q

AR=ARP DH=DHCP Q=QoS
```

With only three available QoS precedences, if you create four IP or L2 classifier elements in an IP or L2 ACL and attempt to apply the ACL to a port, the ERS 3500 Series rejects the ACL and returns the `Inadequate resources available for application policy criteria` error message. In this scenario, to successfully apply an IP or L2 ACL to a port, you must delete one of the IP or ACL elements in the IP or L2 ACL before you can apply the ACL to a port.

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

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command

   ```
   qos acl-assign [<1-55000> enable] [port <portlist> acl-type
   <ip | l2> name <WORD>]
   ```

Variable definitions

The following table describes the parameters for the **`qos acl-assign`** command.

Variable	Value
<1–55000>	Identifies the access list assignment number
enable	Enables the access-list assignment entry
port *<portlist>*	Specifies the list of ports assigned to the specified access list
acl-type *<ip | l2>*	Specifies the type of access list used: IP or Layer 2

Variable	Value
name<*WORD*>	Specifies the name of the access list to be used. Access lists must be configured before ports can be assigned to them.
no	Removes an access list assignment

Creating an IP access list

Use this procedure to create an IP access list.

Note:

When creating IP classifier elements for an IP or L2 ACL on the ERS 3500 switch using the command **`qos ip-acl`**, you may encounter the following error:

```
% Cannot modify settings
% Access element cluster count (4) exceeds limit (3)
```

This error message indicates that you have exceeded the amount of QoS precedences available for IP or L2 ACLs in the switch. The number of IP or L2 ACLs that can be created is limited by the number of available Q0S precedences. Although there are 4 QoS precedences available, the fourth precedence is permanently occupied by ARP, thus leaving only 3 valid precedences available for IP or L2 classifier element creation.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:

```
[no] qos ip-acl name <WORD> [addr-type <ipv4> | <ipv6>]
[block <WORD>] [drop-action <disable> | <enable>] [ds-field
<0-63>] [dst-ip <A.B.C.D> | <WORD>] [dst-port-min <0-65535>
dst-port-max <0-65535>] [protocol <0-255>] [set-drop-prec
<high-drop> | <low-drop>] [src-ip <A.B.C.D> | <WORD>] [src-
port-min <0-65535> src-port-max <0-65535>] [update-1p <0-7>]
[update-dscp <0-63>]
```

Variable definitions

The following table describes the parameters for the **qos ip-acl** command.

Variable	Value
name <*WORD*>	Specifies the name used to reference the access-list element. Maximum 16 characters.
addr-type <*ipv4*> | <*ipv6*>	Specifies the IP address type as IPv4 or IPv6.
block <*WORD*>	Specifies the name to identify access-ist elements that are of the same block.
drop-action <*enable*> | <*disable*>	Specifies the drop action. Enable is drop packet. Disable is do not drop packet.
ds-field <*0–63*>	Specifies the DSCP classifier; range of 0–63.
dst-ip <*A.B.C.D*> | <*WORD*>	Specifies the destination IP address. A.B.C.D is IPv4, WORD is IPv6.
dst-port-min <*0–65535*> dst-port-max <*0–65535*>	Specifies the L4 destination port minimum and maximum value; range of 0–65535.
protocol <*0–255*>	Specifies the IPv4 protocol range; range of 0–255.
set-drop-prec <*high-drop*> | <*low-drop*>	Specifies the set drop precedence. Values include: • high-drop — higher probability of drops when congestion is encountered • low-drop — lower probability of drops when congestion is encountered.
src-ip <*A.B.C.D*> | <*WORD*>	Specifies the source IP address. A.B.C.D is iPv4, WORD is IPv6.
src-port-min <*0–65535*> src-port-max <*0–65535*>	Specifies the L4 source port minimum and maximum value; range of 0–65535.
update-1p <*0–7*>	Specifies the update user priority; range of 0–7.
update-dscp <*0–63*>	Specifies the update DSCP; range of 0–63.
[no]	Removes an access list

Creating a Layer 2 access list

Use this procedure to create a Layer 2 access list.

Note:

When creating IP classifier elements for an IP or Layer 2 ACL on the ERS 3500 switch using the command **qos ip-acl**, you may encounter the following error:

```
% Cannot modify settings
% Access element cluster count (4) exceeds limit (3)
```

This error message indicates that you have exceeded the amount of QoS precedences available for IP or Layer 2 ACLs in the switch. The number of IP or Layer 2 ACLs that can be created is limited by the number of available QoS precedences. Although there are 4 QoS precedences available, the fourth precedence is permanently occupied by ARP, thus leaving only 3 valid precedences available for IP or Layer 2 classifier element creation.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:

```
[no] qos l2-acl name <WORD> [block <WORD>] [drop-action
<disable> | <enable>] [dst-mac <dst-mac-info>] [dst-mac—mask
<dst-mac-info>] [ethertype <etype>] [priority <0-7> | <all>]
[set-drop-prec <high-drop> | <low-drop>] [src-mac <src-mac-
info>] [src-mac—mask <src-mac-info>] [update-1p <0-7>]
[update-dscp <0-63.] [vlan-min <1-4094> vlan-max <1-4094>]
[vlan-tag <tagged> | <untagged>]
```

Variable definitions

The following table describes the parameters for the **qos l2-acl** command.

Variable	Value
name <*WORD*>	Specifies the name used to reference the access-list element. Maximum 16 characters.
block <*WORD*>	Specifies the name to identify access-ist elements that are of the same block.
drop-action <*enable*> | <*disable*>	Specifies the drop action. Enable is drop packet. Disable is do not drop packet.

Variable	Value
dst-mac <*dst-mac-info*>	Specifies the destination MAC classifier.
dst-mac-mask <*dst-mac-info*>	Specifies the destination MAC mask classifier.
ethertype <*etype*>	Specifies the ethertype classifier; range of 0x0 to 0xFFFF.
priority <*0–7*> | <*all*>	Specifies the user priority classifier; range of 0–7 or all 802.1p user priority.
set-drop-prec <*high-drop*> | <*low-drop*>	Specifies the set drop precedence. Values include: • high-drop — higher probability of drops when congestion is encountered • low-drop — lower probability of drops when congestion is encountered.
src-mac <*src-mac-info*>	Specifies the source MAC classifier.
src-mac-mask <*src-mac-info*>	Specifies the source MAC mask classifier.
update-1p <*0–7*>	Specifies the update user priority; range of 0–7.
update-dscp <*0–63*>	Specifies the update DSCP; range of 0–63.
vlan-min <*0–4094*> vlan-max <*0–4094*>	Specifies the VLAN ID minimum and maximum; range of 0–4094.
vlan-tag <*tagged*> | <*untagged*>	Specifies the VLAN tag classifier. Values include: • tagged — filter on frames received as tagged • untagged — filter on frames received as untagged.
[no]	Removes a Layer 2 access list.

Configuring the QoS agent

The following sections describe configuring the QoS agent using ACLI.

Configuring QoS agent

Use this command to configure QoS agent.

About this task

You can use the following procedure to configure Avaya Automatic QoS, NVRAM delay, statistics tracking, or reset QoS to defaults.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command

```
qos agent [aq-mode <disable | mixed | pure> | nvram-delay <0-
604800> | reset-default | statistics-tracking <aggregate |
disable | individual>]
```

Variable definitions

The following table describes parameters for the **`qos agent`** command

Variable	Value
aq-mode<*disable* | *mixed* | *pure*>	Specifies the Automatic QoS configuration. Values include: • disable — Disables AQ mode. (default) • mixed — Enables AQ mode application traffic processing on all ports with egress DSCP remapping. • pure — Enables AQ mode application traffic processing on all ports without egress DSCP remapping.
nvram-delay<*0–604800*>	Specifies the maximum time in seconds to write configuration data to a nonvolatile storage.
reset-default	Restores QoS to configuration default .

Variable	Value
statistics-tracking<*aggregate* | *disable* | *individual*>	Specifies default QoS statistics tracking. Values include: • aggregate — Allocate a single statistics counter to track data for all classifier of the policy being created. • disable — No statistics tracking for QoS policy being created. • individual — Allocate individual statistics counters to track data for each classifier of the QoS policy being created.

Displaying QoS agent configuration information

Use the following procedure to display QoS agent configuration information.

Procedure

1. Log on to the Privileged EXEC mode in ACLI.
2. At the command prompt, enter the following command
   `show qos agent`

Example

The following figure shows an example output of the **`show qos agent`** command.

```
3524GT-PWR+#show qos agent
QoS Operational Mode: Enabled
QoS NVRam Commit Delay: 10 seconds
QoS Queue Set: 4
QoS Buffering: Maximum
QoS Default Statistics Tracking: Aggregate
Auto QoS Mode: Disabled
```

Restoring QoS agent to default

Use the following procedure to configure QoS agent parameters to factory default values.

About this task

The **`default qos agent`** command achieves the same result as the **`qos agent reset-default`** command.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command

   ```
   default qos agent [aq—mode | nvram-delay | statistics-tracking]
   ```

Variable definitions

The following table describes parameters for the **`default qos agent`** command.

Variable	Value
aq-mode	Restores default Auto QoS application traffic processing mode. Default is disabled.
nvram-delay	Restores default maximum time in seconds to write configuration data to nonvolatile storage.
statistics-tracking	Restores default QoS statistics tracking support.

Configuring 802.1p priority values

Use the following procedure to configure 802.1p priority values.

About this task

You can 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.

Important:

The Ethernet Routing Switch 3500 supports only one queue set, set 4.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command

   ```
   qos queue-set-assignment queue-set <4> 1p <0-7> queue <1-4>
   ```

Variable definitions

The following table describes the parameters for the **qos queue-set-assignment** command.

Variable	Value
queue-set <*4*>	Specifies the queue-set as a value. Default is 4.
1p <*0–7*>	Specifies the 802.1p priority value, as a value in a range from 0 to 7, for the queue association being modified.
queue <*1–4*>	Specifies the queue, within the identified queue set, to assign the 802.1p priority traffic to at egress. The value is expressed as an integer in a range from 1 to 4.

Configuring QoS interface groups

The following sections describe creating and configuring interface groups using ACLI.

Creating an interface group

Use the following procedure to create interface groups.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command

```
qos if-group name <WORD> class [trusted | unrestricted |
untrusted | untrustedbasic | untrustedv4v6]
```

Variable definitions

The following table describes the parameters for the **qos if-group** command.

Variable	Value
name <*WORD*>	Specifies the name of the interface group. The maximum length of the name is 32 US-ASCII characters. The name must begin with a letter a..z or A..Z.
class< *trusted* | *unrestricted* | *untrusted* | *untrustedbasic* | *untrusted v4v6*>	Specifies class of traffic received on interfaces associated with this interface group. Values include: • trusted — Traffic received on the associated interfaces are assumed to be trusted. • unrestricted — Traffic received on the associated interfaces may allow unrestricted ports to access links or connect to the core network with no default processing. • untrusted — IPv4 traffic received on the associated interfaces are assumed to be untrusted. • untrustedbasic — IPv4 and IPv6 traffic received on the associated interfaces are assumed to be untrusted (typically access links connected to end stations). Tagged and untagged traffic are treated the same for minimum resource consumption. • untrustedv4v6 — IPv4 and IPv6 traffic received on the associated interfaces are assumed to be untrusted (typically access links connected to end stations).

Removing an interface group

Use the following procedure to delete interface groups.

About this task

You cannot delete an interface group referenced by an installed policy.

You cannot delete an interface group associated with ports.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command

```
no qos if-group name <WORD>
```

Configuring ports for an interface group

Use the following procedure to add ports to a defined interface group.

About this task

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

Procedure

1. Log on to the Interface Configuration mode in ACLI.
2. At the command prompt, enter the following command

```
qos if-assign [port <portlist>] name [WORD]
```

Variable definitions

The following table describes parameters for the **`qos if-assign`** command.

Variable	Value
port <*portlist*>	Specifies the ports to add to the interface group.
name <*WORD*>	Specifies the name of the interface group in a character string from 1 to 32 characters.

Removing ports from an interface group

Use the following procedure to delete ports from a defined interface group.

About this task

Ports not associated with an interface group are considered QoS-disabled and may not have QoS operations applied until they are assigned to an interface group.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command

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

Configuring DSCP and 802.1p

The following sections describe configuring DSCP and 802.1p priority using ACLI.

Configuring DSCP to 802.1p priority

Use the following procedure to configure DSCP-to-802.1p priority and drop precedence associations.

About this task

The system assigns 802.1p and drop precedence to packets at egress, based on the DSCP in the received packet.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command
   ```
   qos egressmap [name <WORD>][ds <0-63>]
   ```

Variable definitions

The following table describes parameters for the **`qos egressmap`** command.

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; range is between 0 and 7.
dp <*low-drop* | *high-drop*>	Specifies the drop precedence values associated with the DSCP:

Variable	Value
	• low-drop • high-drop

Restoring egress mapping entries to default

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

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   default qos egressmap
   ```

Configuring 802.1p priority to DSCP

Use the following procedure to configure 802.1p priority-to-DSCP associations.

About this task

The 802.1p priority-to-DSCP associations are used to assign default values at packet ingress, based on the 802.1p value of the ingressing packet.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command
   ```
   qos ingressmap [name <WORD>] 1p <0-7> ds <0-63>
   ```

Variable definitions

The following table describes the parameters for the **`qos ingressmap`** command.

Variable	Value
name <*WORD*>	Specifies the label for the ingress mapping.
1p <*0–7*>	Specifies the 802.1p priority used as the lookup key for DSCP assignment at ingress. The range is between 0 and 7.

Variable	Value
ds <*0–63*>	Specifies the DSCP value associated with the target 802.1p priority. The range is between 0 and 63.

Restoring ingress mapping entries to default

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

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command
   ```
   default qos ingressmap
   ```

Configuring QoS elements classifiers and classifier blocks

The following sections describe configuring QoS elements, classifiers, and classifier blocks using ACLI.

Configuring IP classifier element entries

Use this procedure to add and configure classifier entries.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   qos ip-element <cid> [addr-type <addrtype>] [ds-field <dscp>]
   [dst-ip <dst-ip-info>] [dst-port-min <port> dst-port-max
   <port>] [name <WORD>] [protocol <0-255>] [session-id
   <session-id>] [src-ip <src-ip-info>] [src-port-min <port>
   src-port-max <port>]
   ```

Variable definitions

The following table describes the parameters for the **qos ip-element** command.

Variable	Value
<*cid*>	Specifies the element ID, value ranges from 1–55000.
addr-type<*addrtype*>	Specifies the address type. Use the value ipv4 to indicate an IPv4 address or, on switches that support IPv6, the value ipv6 to indicate an IPv6 address. DEFAULT: ipv4.
ds-field<*dscp*>	Specifies a 6-bit DSCP value; value ranges from 0–63. DEFAULT: ignore.
dst-ip<*dst-ip-info*>	Specifies the destination IP address and mask in the form of a.b.c.d/x for IPv4, or, on switches that support IPv6, x:x:x:x:x:x:x:x/z . DEFAULT: 0.0.0.0.
dst-port-min<*port*> dst-port-max<*port*>	Specifies the L4 destination port minimum and maximum values.
name<*WORD*>	Specifies the name of the IP element. Character string of up to 16 characters.
protocol<*0–255*>	Specifies the IPv4 protocol classifer criterial, ranges of 0–255.
session-id <session-id>	Specifies the session ID.
src-ip<*src-ip-info*>	Specifies the source IP address and mask in the form of a.b.c.d/x for IPv4, or, on switches that support IPv6, x:x:x:x:x:x:x:x/z. DEFAULT: 0.0.0.0.
src-port- min<*port*> src-port-max<*port*>	Specifies the L4 source port minimum and maximum values.
tcp-control<*tcp-flags*>	Specifies the control flags present in an TCP header.

Displaying IP classifier entries

Use this procedure to view IP classifier entries.

Procedure

1. Log on to the Privileged EXEC mode in ACLI.

2. At the command prompt, enter the following command:
   `show qos ip-element [<1-65535>] [all] [system] [user]`

Variable definitions

The following table describes the parameters for the **`show qos ip-element`** command.

Variable	Value
<1-65535>	Displays a specific entry.
all	Displays all user-created, default, and system entries.
system	Displays only system entries
user	Displays only user-created and default entries.

Removing IP classifier entries

Use this procedure to remove IP classifier entries.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   `no qos ip-element <1-55000>`

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

Variable definitions

The following table describes the parameters for the **`no qos ip-element`** command.

Variable	Value
<1-55000>	Specifies the element ID, value ranges from 1–55000.

Adding Layer 2 elements

Use this procedure to add Layer 2 elements.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:

```
qos l2-element <1-55000> [dst-mac <dst-mac>] [dst-mac-mask
<dst-mac-mask>] [ethertype <etype>] [name <WORD>] [priority
<ieee1p-seq>] [session-id <session-id>] [src-mac <src-mac>]
[src-mac-mask <src-mac-mask>] [vlan-min <vidmin> vlan-max
<vid-max>][vlan-tag <vtag>]
```

Variable definitions

The following table describes the parameters for the **`qos l2-element`** command.

Variable	Value
<1-55000>	Specifies the element ID; range is 1–55000.
dst-mac<*dst-mac*>	Specifies the destination MAC element criteria. Valid format is H.H.H.
dst-mac-mask<*dst-mac-mask*>	Specifies the destination MAC mask element criteria. Valid format is H.H.H.
ethertype<*etype*>	Specifies the Ethernet type. Valid format is 0xXXXX, for example, 0x0801. DEFAULT: ignore.
name<*WORD*>	Specifies the name of the element. Character string of up to 16 characters.
priority<*ieee1p-seq*>	Specifies the 802.1p priority values; range from 0–7 or all. DEFAULT: ignore.
session-id<*session-id*>	Specifies the session ID.
srcmac<*src-mac*>	Specifies the source MAC element criteria. Enter in the format H.H.H.
src-mac-mask<*src-mac-mask*>	Specifies the source MAC mask element criteria. Valid format is H.H.H.

Variable	Value
vlan-min<*vidmin*>vlan-max<*vid-max*>	Specifies the VLAN ID minimum and maximum value element criteria. Range is 1–4094.
vlan-tag<*vtag*>	Specifies the packet format element criteria: • untagged • tagged DEFAULT: Ignore.

Displaying Layer 2 elements

Use this procedure to view Layer 2 elements.

Procedure

1. Log on to the Privileged EXEC mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   show qos l2-element [<1-65535>] [all] [system] [user]
   ```

Variable definitions

The following table describes the parameters for the **`show qos l2-element`** command.

Variable	Value
<1-65535>	Displays a specific L2 element.
all	Displays all user-created, default, and system L2 elements.
system	Displays only system L2 elements.
user	Displays only user-created and default L2 elements.

Removing Layer 2 elements

Use this procedure to delete Layer 2 element entries.

Procedure

1. Log on to the Global Configuration mode in ACLI.

2. At the command prompt, enter the following command:
   ```
   no qos l2-element <1-55000>
   ```

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

Variable definitions

The following table describes the parameters for the **no qos l2-element** command.

Variable	Value
<1-55000>	Specifies the element ID; range is 1–55000.

Linking IP L2 and system classifier elements

Use this procedure to link IP, L2 and system classifier elements.

About this task

Each classifier can contain only one of each of the following: IP classifier element plus L2 classifier element plus system classifier element.

However, you can create a classifier that contains only one of the following: IP classifier element, L2 classifier element, system classifier element.

You cannot delete a classifier that is referenced in a classifier block or installed policy.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   qos classifier <1-55000> set-id <1-55000> [name <WORD>]
   element-type <ip | l2 | system> element-id <1-55000> |
   session-id <1-4294967295>
   ```

Variable definitions

The following table describes the parameters for the **qos classifier** command.

Variable	Value
classifier <*1-55000*>	Specifies the classifier ID RANGE: 1–55000
set-id <*1-55000*>	Specifies the classifier set ID. RANGE: 1–55000
name <*WORD*>	Specifies the set label; maximum is 16 alphanumeric characters.
element-type <*ip* | *l2* | *system*>	Specifies the element-type; either ip or l2, or system classifier.
element-id <*1-55000*>	Specifies the element ID. RANGE: 1–55000
session-id <*1-4294967295*>	Specifies the session ID. RANGE: 1–4294967295

Removing classifier entries

Use this procedure to delete classifier entries.

About this task

Important:

You cannot delete a classifier referenced in a classifier block or installed policy.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:

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

Variable definitions

The following table describes the parameters for the **no qos classifier** command.

Variable	Value
<1-55000>	Specifies the classifier ID; range is 1–55000.

Combining individual classifiers

Use this procedure to combine individual classifiers.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:

```
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 | {meter <1-55000>
| meter-name <WORD>} | session-id <1-4294967295>]
```

Variable definitions

The following table describes the parameters for the **qos classifier-block** command.

Variable	Value
classifier-block *<1-55000>*	Specifies an the classifier block ID; range is 1–55000.
block-number *<1-55000>*	Specifies the classifier block number; range is 1–55000.
name *<WORD>*	Specifies the label for the classifier block; maximum is 16 alphanumeric characters.
set-id *<1-55000>*	Specifies the classifier set to be linked to the classifier block; range is 1–55000.
set-name *<WORD>*	Specifies the classifier set name to be linked to the classifier block; maximum is 16 alphanumeric characters.
in-profile-action *<1-55000>*	Specifies the in profile action to be linked to the filter block; range is 1–55000.

Variable	Value
in-profile-action-name <*WORD*>	Specifies the in profile action name to be linked to the classifier block; maximum is 16 alphanumeric characters.
meter <*1-55000*>	Specifies the meter to be linked to the classifier block; range is 1–55000.
meter-name <*WORD*>	Specifies the meter name to be linked to the classifier block; maximum is 16 alphanumeric characters.
session-id <*1–4294967295*>	Specifies the session ID; range is 1–4294967295

Removing classifier block entries

Use this procedure to delete classifier block entries.

About this task

You cannot delete a classifier block that is references by an installed policy.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   no qos classifier-block <1-55000>
   ```

Variable definitions

The following table describes the parameters for the **`no qos classifier-block`** command.

Variable	Value
<*1-55000*>	Specifies the classifier block ID; range is 1–55000.

Configuring system classifier element parameters

Use this procedure to configure system classifier element parameters that you can use in QoS policies.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:

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

Variable definitions

The following table describes the parameters for the **`qos system-element`** command.

Variable	Value
<1-55000>	Specifies the system classifier element entry id; range is 1–55000.
known-mcast	Specifies the filter to match frames containing a known multicast destination address.
name	Specifies a unique alphanumeric identifier for the system element.
pattern-data <*WORD*>	Specifies the byte pattern data to filter on. **Note:** The format of the WORD string is in the form of XX:XX:XX:.....:XX.
pattern-format <*tagged* | *untagged*>	Specifies the format of data/mask pattern. Specifies the available values are: • tagged—Data/mask pattern describes a tagged packet • untagged—Data/mask pattern describes an untagged packet
pattern-ip-version <*ipv4* | *ipv6* | *non-ip*>	Specifies the IP version of the pattern data or mask. • ipv4—Filter IPv4 Header • ipv6—Filter IPv6 Header • non-ip—Filter non-ip packets
session-id <*session-id*>	Specifies the session ID.

Variable	Value
unknown-mcast	Specifies the filter to match frames containing an unknown multicast destination address.
unknown-ucast	Specifies the filter to match frames containing an unknown unicast destination address.

Displaying system classifier element parameters

Use this procedure to view system classifier elements parameters.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   show qos system-element [<1-65535>] [all] [system] [user]
   ```

Variable definitions

The following table describes the parameters for the **`show qos system-element`** command.

Variable	Value
<1-65535>	Displays a particular entry.
all	Displays all user-created, default, and system entries.
system	Displays only system entries.
user	Displays only user-created and default entries.

Removing system classifier element entries

Use this procedure to remove system classifier element entries.

Procedure

1. Log on to the Global Configuration mode in ACLI.

2. At the command prompt, enter the following command:
   ```
   no qos system-element <1-55000>
   ```

Variable definitions

The following table describes the parameters for the **no qos system-element** command.

Variable	Value
<1-55000>	Specifies the system classifier element entry id; range is 1–55000.

Configuring QoS actions

The following sections describe creating and configuring QoS actions using ACLI.

Creating and updating QoS actions

Use this procedure to create and update QoS actions.

About this task

The system can restrict certain options based on the policy associated with the specific action.

You cannot delete an action referenced by a meter, an installed policy or a classifier block.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   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>]
   [session-id <1-4294967295>
   ```

Variable definitions

The following table describes the parameters for the **qos action** command.

Variable	Value
<10-55000>	Specifies 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: deferred-pass. **Note:** If you omit this parameter, the default value applies.
update-dscp *<0-63>*	Specifies whether DSCP values are updated or left unchanged; unchanged equals ignore. Enter the 6-bit DSCP value; range is 0 to 63. DEFAULT: ignore.
update-1p*{<0-7>* | *use-tos-prec* | *use-egress}*	Specifies whether 802.1p priority values are updated or left unchanged: unchanged equals ignore. • ieee1p—enter the value you want; range is 0 to 7. • use-egress—uses the egress map to assign value. • use-tos-prec—uses the type of service precedence to assign value. **Note:** Requires specification of update-dscp value.

Variable	Value
set-drop-prec <*low-drop* | *high-drop*>	Specifies the drop precedence value: • low-drop • high-drop DEFAULT: low-drop.
action-ext<*1-55000*>	Specifies the action extension; range is 1–55000.
action-ext-name <*WORD*>	Specifies a label for the action extension; maximum is 16 alphanumeric characters.
session-id<*1–4294967295*>	Specify the session ID.

Removing QoS actions

Use this procedure to delete QoS action entries.

About this task

You cannot delete an action if it is referenced by a policy, classifier block, or meter.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   no qos action <10-55000>
   ```

Variable definitions

The following table describes the parameters for the **`no qos action`** command.

Variable	Value
<*10-55000*>	Specifies the QoS action; range is 10–55000.

Configuring QoS interface action extensions

The following sections describe creating and configuring interface action extensions using ACLI. QoS interface action extensions direct the switch to perform a specific action on each packet.

Creating interface action extension entries

Use this procedure to create interface action extension entries.

About this task

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

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:

```
qos if-action-extension <1-55000> [name <WORD>] {egress-ucast
<port> | egress-non-ucast <port>} [session-id <1-4294967295>]
```

Variable definitions

The following table describes the parameters for the **`qos if-action-extension`** command.

Variable	Value
<1-55000>	Specifies 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*>	Specifies redirection of unicast/non-unicast to specified port.
session-id<*1–4294967295*>	Specifies the system ID. The range is 1–4294967295.

Removing interface action extension entries

Use this procedure to remove interface action extension entries.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   no qos if-action-extension <1-55000>
   ```

Variable definitions

The following table describes the parameters for the **`no qos if-action-extension`** command.

Variable	Value
<1-55000>	Specifies the QoS action. The range is 1–55000.

Configuring QoS meters

The following sections describe creating and configuring QoS meters using ACLI.

Creating QoS meters

Use the following procedure to create a QoS meter.

About this task

You can configure the QoS meter to police the traffic by configuring the committed rate, burst rate, and burst duration.

Important:

If the committed rate is not a multiple of 64, the value is rounded down to the highest multiple of 64, smaller than the committed rate. For example, a committed rate of 1000 Kbps is automatically rounded down to 960 Kbps.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command

```
qos meter <1-5000> [name <WORD>] [committed-rate
<64-10230000>] [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>]
```

Variable definitions

The following table describes the parameters for the **`qos meter`** command.

Variable	Value
<1–5000>	Specifies the QoS meter; range is 1 to 5000.
name <*WORD*>	Specifies the name of the QoS meter. The maximum length of the name is 16 alphanumeric characters.
commited-rate<*64–10230000*>	Specifies the rate that traffic must not exceed for extended periods to be considered in-profile. Enter the rate in Kbps for in-profile traffic in increments of 64 or 1000 Kbps; range is 64 to 10230000 Kbps.
burst-size< *burst-size*>	Specifies the committed burst size in KB. The value range is; 4, 8, 16, 32, 64, 128, 256, 512.
max-burst-rate<*64–4294967295*>	Specifies the largest burst of traffic that can be received at a time for the traffic to be considered in-profile. Used in calculating the committed burst size. Enter the burst size in Kbps for in-profile traffic; range is 64 to 4294967295.
max-burst-duration<*1–4294967295*>	Specifies the amount of time the largest burst of traffic 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 to 4294967295 ms.

Variable	Value
in-profile-action<*1–55000*>	Specifies the in-profile action ID; range is 1 to 55000.
in-profile-action-name<*WORD*>	Specifies the in-profile action name.
out-profile-action-name<*WORD*>	Specifies the out-profile action name.
out-profile-action<*1,9 to 55000*>	Specifies the out-profile action ID; range is 1,9 to 55000.
session-id<*1–4294967295*>	Specifies the session ID; range is 1 to 4294967295.

Removing a QoS meter

Use the following procedure to delete a QoS meter.

About this task

You cannot delete a QoS meter referenced by an installed policy or classifier block.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command

```
no qos meter <1-5000>
```

Configuring QoS interface shapers

The following sections describe creating and configuring QoS interface shapers using ACLI.

Configuring interface shaping

Use this procedure to configure interface shaping.

Procedure

1. Log on to the Interface Configuration mode in ACLI.
2. At the command prompt, enter the following command:

```
qos if-shaper [port <portlist>] [name <WORD>] shape-rate
<64-10230000> {burst-size <4,8,16,...,512> | max-burst-rate
<64-4294967295> [max-burst-duration <1-4294967295>]}
```

Variable definitions

The following table describes the parameters for the **qos if-shaper** command.

Variable	Value
burst-size *<4,8,16, ..., 512>*	Specifies the committed burst size in Kilobytes. The value range is: 4, 8, 16, 32, 64, 128, 256, 512.
port *<portlist>*	Specifies the ports to configure shaping parameters.
name *<WORD>*	Specifies name for if-shaper; maximum is 16 alphanumeric characters.
shape-rate *<64-10230000>*	Specifies the shaping rate in kilobits/sec; range is 64-10230000 kilobits/sec.
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 to 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.

Disabling interface shaping

Use this procedure to disable interface shaping.

Procedure

1. Log on to the Interface Configuration mode in ACLI.
2. At the command prompt, enter the following command:

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

Variable definitions

The following table describes the parameters for the **no qos if-shaper** command.

Variable	Value
port <*portlist*>	Specifies a port or list of ports.

Configuring QoS policies

The following sections describe creating and configuring QoS policies using ACLI.

Creating QoS policies

Use this procedure to create and configure QoS policies.

About this task

You must define all components associated with a policy, including the interface group, element, classifier, classifier block, action, and meter, before you can reference those components in a policy.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:

```
qos policy <1-55000> [enable] [name <WORD>] {port <port> |
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 <1-3> [track-statistics <individual |
aggregate>]} [session-id <1-4294967295>]
```

Variable definitions

The following table describes the parameters for the **qos policy** command.

Variable	Value
<1-55000>	Specifies the QoS policy; range is 1–55000.
enable	Enables the QoS policy.
name<*WORD*>	Specifies the name for the policy; maximum is 16 alphanumeric characters.
port <*port*>	Specifies the port to which to directly apply this policy.
if-group<*WORD*>	Specifies the interface group name to which this policy applies; maximum number of characters is 32 USASCII. The group name must begin with a letter within the range a..z or A..Z.
clfr-type<*classifier* | *block*>	Specifies the classifier type; classifier or block.
clfr-id<*1-55000*>	Specifies the classifier ID; range is 1–55000.
clfr-name<*WORD*>	Specifies the classifier name or classifier block name; maximum is 16 alphanumeric characters.
in-profile-action<*1-55000*>	Specifies the action ID for in-profile traffic; range is 1– 55000.
in-profile-action-name<*WORD*>	Specifies the action name for in-profile traffic; maximum is 16 alphanumeric characters.
meter<*1-55000*>	Specifies meter ID associated with this policy; range is 1–55000.
meter-name<*WORD*>	Specifies the meter name associated with this policy; maximum of 16 alphanumeric characters.
precedence<*1-3*>	Specifies the precedence of this policy in relation to other policies associated with the same interface group. Enter precedence number; range is 1–3. **Note:** Policies with a lower precedence value are evaluated after policies with a higher

Variable	Value
	precedence number. Evaluation goes from highest value to lowest.
track-statistics <*individual* | *aggregate*>	Specifies statistics tracking on this policy as either: • individual — statistics on individual classifiers • aggregate — aggregate statistics
session-id <*1–4294967295*>	Specify the session ID.

Removing QoS policies

Use this procedure to remove QoS policy entries.

Procedure

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command:
   ```
   no qos policy <1-55000>
   ```

Clearing QoS statistics using ACLI

Use this procedure to clear all counters associated with QoS policies and installed meters.

Procedure

1. Log on to ACLI in Global Configuration command mode.
2. At the command prompt, enter the following command:
   ```
   qos clear-stats
   ```

Chapter 6: Configuring QoS using Enterprise Device Manager

Use the procedures in this chapter to configure and manage Quality of Service (QoS) 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.

Displaying interface queues using EDM

Use the following procedure to display interface queues.

Procedure

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

Variable definitions

The following table describes the variables associated with QoS interface Queues.

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:

Variable	Value
	• priorityQueuing • weightedRoundRobin
Bandwith %	Displays relative bandwidth available to a 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	The order in which a queue is serviced, based on the defined discipline.
Size	Displays the size of the queue in bytes.

QoS interface group management using EDM

Use the following procedures to display, add or delete QoS interface groups using EDM.

Displaying interface groups using EDM

Use the following procedure to display interface groups.

Procedure

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

Variable definitions

The following table describes the variables associated with QoS interface groups.

Variable	Value
Id	Displays a unique identifier of an interface group.

Variable	Value
Role	Specifies the tag (group name) 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. Values are: • trusted • nonTrusted • unrestricted • untrustedv4v6 • untrustedBasic
Capabilities	Specifies a 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).
StatsTracking Type	Specifies the type of statistics tracking. Options are aggregate, individual, or disabled.
StorageType	Displays the storage type for this interface group: • Volatile • nonVolatile (default) • readOnly • other

Adding interface groups

Use the following procedure to add an interface group.

Procedure

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

3. In the QoS Devices work area, click the **Interface Group** tab.
4. On the toolbar, click **Insert**.
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, unrestricted, untrustedv4v6,** or **untrustedBasic**.
8. Click **Insert**.

Deleting interface groups using EDM

Use the following procedure to delete an interface group.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Devices**.
3. In the QoS Devices work area, click the **Interface Group** tab.
4. In the Interface Group section, highlight an interface group.
5. On the toolbar, click **Delete**.

Important:

You cannot delete an interface group referenced by a policy—you must delete the policy first—and you cannot delete an interface group with assigned ports.

You can display the association between interfaces, role combinations, and queue sets. A role combination is a unique label that identifies a group of interfaces.

Assigning or deleting ports to an interface group using EDM

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

Procedure

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

2. In the QoS tree, click **QoS Devices**.
3. In the QoS Devices work area, click the **Interface Group** tab.
4. In the Interface Group section, highlight an interface group.
5. On the toolbar, click **Interface Assignment**.
6. Click the port numbers to add to the interface group.
   OR
   De-select the ports to delete.
7. Click **OK**.

Important:

If you add or delete a number of ports on a switch under heavy load, the operation can take a long time and can cause EDM to time out.

Displaying an interface ID using EDM

Use the following procedure to display the interface ID.

Procedure

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

Variable definitions

The following table describes the variables associated with QoS interface IDs

Variable	Value
Port	Displays ports numbers.
RoleCombination	Displays the role associated with the port.
QueueSet	Displays the queue set associated with this interface.
Capabilities	Displays the queuing capabilities associated with an egress QoS interface.

QoS priority queue assignment management using EDM

Use the following procedures to display and filter QoS priority queue assignments.

Displaying priority queue assignments using EDM

Use the following procedure to display priority queue assignments.

Procedure

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

Variable definitions

The following table describes the variables associated with QoS priority queue assignments.

Variable	Value
Qset	Supports the assignment of 802.1p user priority values to a queue for each specific queue set. There is one queue-set supported, queue-set 4, and 8 priority classes, 0 through 7, associated with this queue-set.
802.1pPriority	A 802.1 user priority value.
Queue	A 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.

Filtering priority queue assignments using EDM

Use the following procedure to filter QoS priority queue assignments.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Devices**.
3. In the QoS Devices work area, click the **Priority Q Assign** tab.
4. In the Priority Q Assign section, highlight a Qset..
5. On the toolbar, click **Filter**.
6. Configure the filter parameters as required.
7. Click **Filter**.

Displaying priority mapping using EDM

Use the following procedure to display priority mapping.

Procedure

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

Variable definitions

The following table describes the variables associated with QoS priority mapping.

Variable	Value
802.1pPriority	The 802.1 user priority value to map to a DSCP value at ingress.
Dscp	The DSCP value to associate with the specified 802.1 user priority value at ingress.
Name	The type of service.

Displaying DSCP mappings using EDM

Use the following procedure to display DSCP mapping.

Procedure

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

Variable definitions

The following table describes the variables associated with DSCP mapping.

Variable	Value
Dscp	Shows the DSCP value. This field is read-only.
802.1pPriority	Displays the user priority value associated with the DSCP value. RANGE: 0–7
DropPrecedence	Displays the drop precedence setting. The available settings are: • lowDropPrec • highDropPrec Traffic associated with low drop precedence is generally given priority over traffic with high drop precedence during resource allocation.
ServiceClass	Specifies the type of service associated with the DSCP value.

QoS meter capability management using EDM

Use the following procedures to display and filter QoS meter capability management.

Displaying meter capability

Use the following procedure to view QoS meter capability, the maximum rate supported, bucket sizes and granularity..

Procedure

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

Variable definitions

The following table describes the variables associated with the meter capability tab.

Variable	Value
Port	Specifies the port to which the meter is applied.
MeterSupport	Specifies the supported Token Bucket metering algorithm. The switch supports Simple Token Bucket.
Meter Rate(Kbps)/ Bucket(Kbytes)/ Granularity(Kbytes)	Displays maximum supported Meter Rate, maximum bucket size and supported granularity.

Filtering meter capability using EDM

Use the following procedure to filter QoS meter capability.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Devices**.
3. In the QoS Devices work area, click the **Meter Capability** tab.
4. In the Meter Capability section, select a port(s).
5. On the toolbar, click **Filter**.
6. Configure the filter parameters as required.

7. Click **Filter**.

QoS shaper capability management using EDM

Use the following procedures to display and filter QoS shaper capability.

Displaying Shaper Capability using EDM

Use the following procedure to display QoS interface shaper capabilities.

Procedure

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

Variable definitions

The following table describes the variables associated with the shaper capability tab.

Variable	Value
Port	The port to which the shaper is applied.
ShaperSupport	Displays the location where the shaper is applied. The switch supports shaping application for each interface.
Shaper Rate(Kbps)/Bucket (KBytes)/ Granulatiry (Kbps)	Displays the maximum supported Shaper Rate, Shaper Bucket size, and Shaper Granularity.

Filtering shaper capability using EDM

Use the following procedure to filter shaper capability.

Procedure

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

2. In the QoS tree, click **QoS Devices**.
3. In the QoS Devices work area, click the **Shaper Capability** tab.
4. Click **Filter**.
5. Configure the filter parameters as required.
6. Click **Filter**.

Managing IP classifier elements using EDM

Use the following procedures to display, add or delete IP classifier elements.

Displaying IP classifier elements using EDM

Use the following procedure to display the IP classifier elements.

Procedure

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

Variable definitions

The following table describes the variables associated with IP classifier elements.

Variable	Value
Id	Specifies the 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.

Variable	Value
DstMaskLength	Specifies the length of the destination address mask with a value from 0 to 32.
SrcAddr	Specifies the IP address to match against a packet source IP address.
SrcMaskLength	Specifies the length of the source address mask with a value from 0 to 32.
Dscp	Specifies the value for the DSCP in a packet in a range from -1 to 63 where -1 is equal to ignore, 1 is equal to ICMP-IPv4, 2 is equal to IGMP, 6 is equal to TCP, 17 is equal to UDP, 46 is equal to RSVP, and 58 is equal to ICMP-IPv6.
Protocol/NextHeader	Specifies the IPv4 protocol or IPv6 next header that the classifier element must match. Enter a value from 0 to 255 where 255 is equal to ignore.
DstL4PortMin	Specifies the minimum value for the Layer 4 destination port number in a packet. Enter a value from 0 to 65535.
DstL4PortMax	Specifies the maximum value for the Layer 4 destination port number in a packet. Enter a value from 0 to 65535. You can set PortMin to 0 and portMax to 65535 to specify ignore.
SrcL4PortMin	Specifies the minimum value for the Layer 4 source port number in a packet. Specify a value from 0 to 65535.
SrcL4PortMax	Specifies the maximum value for the Layer 4 source port number in a packet. Enter a value from 0 to 65535. You can set PortMin to 0 and portMax to 65535 to specify ignore.
Ipv6FlowId	Specifies the flow identifier for IPv6 packets in a range from -1 to 1048575 where -1 is equal to ignore.
SessionId	Specifies the session ID.
Storage	Specifies the type of storage: • volatile • nonVolatile (default) • readOnly

Adding IP classifier elements using EDM

Use the following procedure to add the IP classifier elements.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Rules**.
3. In the QoS Rules work area, click the **IP Classifier Element** tab.
4. Click **Insert**.
5. In the Insert IP classifier section, configure as required.
6. Click **Insert**.

Deleting IP classifier elements using EDM

Use the following procedure to delete IP classifier elements.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Rules**.
3. In the QoS Rules work area, click the **IP Classifier Element** tab.
4. Highlight an IP classifier element.
5. Click **Delete**.

Important:

A QoS IP Element that is referenced by a classifier, or by a block or policy cannot be deleted.

First delete the block or policy, then the classifier, and then the classifier element.

QoS layer 2 classifier element management using EDM

Use the following procedures to display, add or delete QoS layer 2 classifier elements using EDM.

Displaying L2 classifier elements using EDM

Use the following procedure to display Layer 2 classifiers.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Rules**.
3. In the QoS Rules work area, click the **L3 Classifier Element** tab.

Variable definitions

The following table describes the variables associated with L2 classifier elements.

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 will be compared.
DstMacAddrMask	Specifies a mask identifying the destination MAC address.
SrcMacAddr	Specifies the MAC source address of incoming packets.
SrcMacAddrMask	Specifies a mask identifying the source MAC address.
VlanIdMin	Specifies the minimum value for the VLAN ID in a packet.
VlanIdMax	Specifies the maximum value for the VLAN ID in a packet.

Variable	Value
VlanTag	Specifies the type of VLAN tagging in a packet: • untagged • tagged • ignore
EtherType	Specifies a value for the Ethertype.
802.1pPriority	Specifies a value for the 802.1p user priority.
SessionId	Specifies the session ID.
Storage	Specifies the type of storage.

Adding L2 classifier elements using EDM

Use the following procedure to add Layer 2 classifier elements.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Rules**.
3. In the QoS Rules work area, click the **L2 Classifier Element** tab.
4. On the toolbar, click **Insert**.
5. In the Insert Layer 2 classifier section, configure element parameters as required.
6. Click **Insert**.

Deleting L2 classifier elements using EDM

Use the following procedure to delete Layer 2 classifier elements.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Rules**.
3. In the QoS Rules work area, click the **L2 Classifier Element** tab.
4. Select a row to delete.

5. On the toolbar, click **Delete**.

Important:

A Layer 2 classifier element that is referenced by a classifier, or by a block or policy cannot be deleted. First delete the block or policy, then the classifier, and then the classifier element. A Layer 2 classifier element of the storage type **other** or **readOnly** cannot be deleted.

System classifier element management using EDM

Use the following procedures to display, add or delete QoS system classifier elements.

Displaying system classifier elements using EDM

Use the following procedure to display System Classifier Elements.

Procedure

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

Variable definitions

The following table describes the variables associated with system classifier elements.

Variable	Value
Id	The index that enumerates the system classifier entries.
Name	The name of the classifier element.
UnknownUcastFrames	If true, frames containing an unknown unicast destination address will match this classification entry. A value of false indicates that no classification is requested based on this address type.
UnknownMcastFrames	If true, frames containing an unknown multicast destination address will match this

Variable	Value
	classification entry. A value of false indicates that no classification is requested based on this address type.
KnownMcastFrames	If true, frames containing a known multicast destination address will match this classification entry. A value of false indicates that no classification is requested based on this address type.
PatternFormat	This field indicates the data link layer (L2) packet format that is used when specifying pattern match data. A value of untagged indicates that the specified pattern match data does not include an 802.1Q tag. A value of tagged indicates that the specified pattern match data includes an 802.1Q tag. DEFAULT: Tagged
PatternIpVersion	This field Indicates the IP packet format used to specify pattern match data. The only supported value is ipv4.
SessionId	Specifies the session ID.
Storage	Specifies the classifier element storage type. If the value is permanent or active you may not have write access to objects in the row.

Displaying the system classifier pattern using EDM

Use the following procedure to view the system classifier pattern.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Rules**.
3. In the QoS Rules work area, click the **System Clfr Element** tab.
4. Highlight a row in the system classifier element table.
5. Click **Pattern**.

Adding system classifier elements using EDM

Use the following procedure to add a system classifier element.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Rules**.
3. In the QoS Rules work area, click the **System Clfr Element** tab.
4. Click **Insert**.
5. In the insert system classifier section, configure as required.
6. Click **Insert**.

Deleting system classifier elements using EDM

Use the following procedure to delete System Classifier Elements.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Rules**.
3. In the QoS Rules work area, click the **System Clfr Element** tab.
4. Highlight a system classifier element row.
5. Click **Delete**.

QoS classifier management using EDM

Use the following procedures to display, add, delete, or filter classifiers using EDM.

Displaying classifiers using EDM

Use the following procedure to display classifiers.

Procedure

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

Variable definitions

The following procedure describes the variables associated with the classifier tab.

Variable	Value
Name	Specifies the name of the classifier.
SetId	Entries with the same SetId belong to the same classifier.
Specific	Describes the specific classifier element and its ID number (from the IP Classifier Element dialog box, the L2 Classifier Element dialog box, or System Clfr Element dialog box).
SessionId	Specifies the session ID.
Storage	The storage type for the classifier. If the value is other or readOnly, the system does not allow write access to objects in the row.

Adding classifiers using EDM

Use the following procedure to add classifiers.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Rules**.
3. In the QoS Rules work area, click the **Classifier** tab.
4. Click **Insert**
5. In the Insert classifier section, configure as required.
6. Click **Insert**.

Deleting classifiers using EDM

Use the following procedure to delete classifiers.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Rules**.
3. In the QoS Rules work area, click the **Classifier** tab.
4. Click the classifier row.
5. Click **Delete**.

Important:

A classifier that is referenced in a classifier block or in a policy cannot be deleted. The policy or block have to be deleted first. A classifier with a storage type of **other** or **readOnly** cannot be deleted.

Filtering classifiers using EDM

Use the following procedure to filter the display of classifiers.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Rules**.
3. In the QoS Rules work area, click the **Classifier** tab.
4. Click **Filter**.
5. In the Filter classifier section, configure filter conditions as required.
6. Click **Filter**.

QoS classifier block management using EDM

Use the following procedures to display, append, add, delete, or filter QoS classifier blocks using EDM.

Displaying classifier blocks using EDM

Use the following procedure to display classifier blocks.

Procedure

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

Variable definitions

The following table describes the variables associated with QoS classifier blocks.

Variable	Value
BlockNum	Entries with the same BlockNum belong to the same classifier block.
Name	Displays the name you assigned to that classifier block.
ClassifierSetId	Displays the ID number assigned to that classifier (from the Classifier dialog box).
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	The storage type for this classifier block. If the value is other or readOnly the objects in the row cannot be modified or deleted.

Appending classifier blocks using EDM

Use the following procedure to append a classifier block.

Procedure

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

2. In the QoS tree, click **QoS Rules**.
3. In the QoS Rules work area, click the **Classifier Block** tab.
4. Highlight a classifier from the table.
5. Click **Append Classifier**.
6. In Append Classifier section, configure as required.
7. Click **Insert**.

Adding classifier blocks using EDM

Use the following procedure to add classifier blocks.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Rules**.
3. In the QoS Rules work area, click the **Classifier Block** tab.
4. Click **Insert**.
5. In the Insert Classifier section, configure as required.
6. 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

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

3. In the QoS Rules work area, click the **Classifier Block** tab.
4. Highlight a classifier block..
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. A classifier block, if it is of the storage type **other** or **readOnly**, cannot be deleted.

Filtering classifier blocks using EDM

Use the following procedure to filter a classifier block.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Rules**.
3. In the QoS Rules work area, click the **Classifier Block** tab.
4. Highlight a classifier block.
5. Click **Filter**.
6. Select the filtering condition, case, and column.
7. Click **Filter**.

QoS action management using EDM

Use the following procedures to manage and use QoS actions.

Displaying QoS actions using EDM

Use the following procedure to display a QoS action.

Procedure

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

3. In the QoS work area, click the **Action** tab.

Variable definitions

The following table describes the variables associated with QoS actions.

Variable	Value
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: • Other • nonVolatile • readOnly

Adding QoS actions using EDM

Use the following procedure to add a QoS action.

Procedure

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

5. In the Insert action section, configure as required.
6. Click **Insert**.

Deleting QoS actions using EDM

Use the following procedure to delete a QoS action.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS**.
3. In the QoS work area, click the **Action** tab.
4. In the Action section, highlight a row to delete.
5. Click **Delete**.

QoS interface action extension management using EDM

Use the following procedures to display, add, or delete QoS interface action extensions.

Displaying Interface action extensions using EDM

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

Procedure

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

Variable definitions

The following table describes the variables associated with QoS interface action extensions.

Variable	Value
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 nonvolatile.

Adding interface action extensions using EDM

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

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **Interface Action Ext**.
3. Click **Insert**.
4. In the Insert interface action ext work area, configure as required.
5. Click **Insert**.

Deleting interface action extensions using EDM

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

Procedure

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

2. In the QoS tree, click **QoS**.
3. In the QoS work area, click the **Interface Action Ext** tab.
4. Highlight an interface action extension row.
5. Click **Delete**.

QoS meter management using EDM

Use the following procedure to display, add, or delete a QoS meter.

Displaying QoS meters using EDM

Use the following procedure to display a QoS meter.

Procedure

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

Variable definitions

The following table describes the variables associated with QoS meters.

Variable	Value
Id	Specifies the unique identifier for this entry.
Name	Specifies a name for this entry.
CommittedRate	Specifies the committed rate (in Kbps).
BurstSize	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

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS**.
3. In the QoS work area, click the **Meter** tab.
4. Click **Insert**.
5. Configure as required.
6. Click **Insert**.

Deleting QoS meters using EDM

Use the following procedure to delete a QoS meter.

Procedure

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

QoS interface shaper management using EDM

Use the following procedures to display, add, or delete QoS interface shapers.

Displaying QoS interface shapers using EDM

Use the following procedure to display QoS interface shapers.

Procedure

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

Variable definitions

The following table describes the variables associated with QoS interface shapers.

Variable	Value
Port	The port number that is associated with this instance of the shaping entry.
Name	Displays the name for the interface shaper.
ShapingRate	The bucket rate, in kilobits per second (kbps).
BurstSize	The maximum number of bytes in a single transmission burst.

Adding interface shapers using EDM

Use the following procedure to add QoS interface shapers.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS**.
3. In the QoS work area, click the **Interface Shaper** tab.
4. Click **Insert**.
5. Click the ellipses (...) to open port editor and select required ports.
6. Click **Ok**.
7. Configure the other fields as required.
8. Click **Insert**.

Deleting interface shapers using EDM

Use the following procedure to delete an interface shaper.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS**.
3. In the QoS work area, click the **Interface Shaper** tab.
4. Highlight an interface shaper row.
5. Click **Delete**.

QoS policy management using EDM

Use the following procedures to display, add, or delete QoS policies.

Displaying QoS policies using EDM

Use the following procedure to display QoS policies.

Procedure

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

Variable definitions

The following table describes the variables associated with QoS policies.

Variable	Value
Id	Indicates the number of the QoS policy.
Status	Indicates current policy status.
Name	Displays the name for the policy.

Variable	Value
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. **Important:** Configure role combinations prior to associating an interface with a policy.
InterfaceIndex	Identifies the interface the policy is associated with. **Important:** The InterfaceRoles and InterfaceIndex fields are mutually exclusive. When the InterfaceIndex field is not zero, the InterfaceRoles must be empty (select none after you 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:** The system applies policies with higher precedence values before policies with lower precedence values.
Meter	Specifies the metering associated with this policy **Important:** Meters must be configured before associating them with a policy.
InProfileAction	Identifies the action to be applied to traffic with this policy. This parameter is not be used after a meter is specified. **Important:** Actions must be configured before associating them with a policy.

Variable	Value
StatsType	Specifies statistics tracking type as one of the following: • none — no statistics tracked for this policy • individual — separate counters allocated, space permitting, for each classifier references by the policy • aggregate — a single counter accumulates all the statistics for all the classifiers referenced by a policy
SessionId	Specifies the session ID
Storage	Specifies the type of storage as one of the following: • volatile • nonVolatile • readOnly

Adding QoS policies using EDM

Use the following procedure to add a QoS policy.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS**.
3. In the QoS work area, click the **Policy** tab.
4. Click **Insert**.
5. In the Insert QoS policy section, configure as required.
6. Click **Insert**.

Deleting QoS policies using EDM

Use the following procedure to delete a QoS policy.

Procedure

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

2. In the QoS tree, click **QoS**.
3. In the QoS work area, click the **Policy** tab.
4. Highlight a QoS policy row.
5. Click **Delete**.

Displaying QoS Policy aggregate statistics using EDM

Use the following procedure to view aggregate QoS policy statistic information.

The aggregate statistical information consists 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 Meter is set to no, no out-profile packet information is available.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS**.
3. In the QoS work area, click the **Policy** tab.
4. Highlight a aggregate policy row.
5. On the toolbar, Click **Graph**.

Displaying QoS policy individual statistics using EDM

Use the following procedure to view individual QoS policy statistics information.

Individual statistical information consists of in-profile and out-profile packets. Individual statistics are provided for each policy, filter, and port. If the Policy Meter is set to none, no total out-profile packet information is available. If the Policy Meter is set to no, no out-profile packet information is available.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS**.
3. In the QoS work area, click the **Policy** tab.
4. Highlight a policy row set to individual.

5. On the toolbar, click **Graph**.

Configuring QoS agent using EDM

Use the following procedure to configure QoS agent.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Agent**.
3. In the QoS Agent work area, click the **Configuration** tab.
4. Configure fields as required.
5. On the toolbar, click **Apply**.
6. On the toolbar, you can click **Refresh** to verify the configuration.

Variable definitions

The following table describes the variables associated with configuring QoS agents.

Variable	Value
QosOperMode	Enables or disables QoS Agent.
NVRamCommitDelay	Specifies the maximum time before nonvolatile QoS data is written to NVRAM.
ResetToDefaults	Click to reset all policy information to factory default values.
DefaultQueueCfg	Specifies the default queue set number.
DefaultBufferingCaps	Specifies the method through which buffering resources are allocated to ports sharing a pool of buffers.
TrackStatistics	Specifies the type of statistics tracking to set. Options are disabled, individual, and aggregate.
AQApplicationMode	Specifies the Avaya Automatic QoS application mode. Options are disable, enablePureMode, and enableMixedMode.

Displaying policy class support using EDM

Use the following procedure to display policy class support.

Procedure

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

Variable definitions

The following table describes the variables associated with QoS policy class support.

Variable	Value
PolicyClassName	Identifies the Policy Rule Classes (PRCs) supported by the device.
CurrentInstances	The current number of Policy Rules Instances (PRIs) that are installed for a specific PRC.
MaxInstalledInstances	The maximum number of PRIs that can be installed and/or modified by a user for a specific PRC.

Displaying policy device identification using EDM

Use the following procedure to display policy device identification data.

Procedure

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

Variable definitions

The following table describes the variables associated with QoS policy device identification.

Variable	Value
Descr	A description of the policy agent. The description must include the name and version identification of the policy agent hardware and software.
MaxMsg	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.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Agent**.
3. In the QoS Agent work area, click the **Resource Allocation** tab.

Variable definitions

The following table describes the variables associated with QoS resource allocation.

Variable	Value
Port	Displays the Port number.
MasksConsumed	Displays the number of masks in use.
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.

Variable	Value
NonQosMasksConsumed	Tracks the current number of non QoS masks in use.
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.