



Configuration - Quality of Service Avaya Ethernet Routing Switch 5000 Series

6.3
NN47200-504, 07.01
August 2012

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

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) 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 this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: <http://www.avaya.com/support>. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) 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. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

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

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(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(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 other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: <http://www.avaya.com/support>

Contact Avaya Support

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

Contents

Chapter 1: New in this Release	9
Chapter 2: Introduction	11
ACLI command modes.....	11
Chapter 3: Policy-enabled network fundamentals	13
Summary.....	13
Port-based and role-based QoS policies.....	13
QoS overview.....	14
DiffServ concepts.....	14
QoS components.....	15
Specifying interface groups.....	16
Interface shaping.....	17
Egress queue shaping.....	18
QoS traffic profile filter sets.....	18
Traffic profile filter set metering.....	19
QoS filter limiting.....	20
The NSNA solution.....	21
User-based policies.....	21
Rules.....	21
Classifier definition.....	22
IP classifier elements.....	22
Layer 2 classifier elements.....	23
System classifier elements.....	23
Classifiers and classifier blocks.....	24
Specifying actions.....	26
Specifying interface action extensions.....	28
Specifying meters.....	29
Trusted, untrusted, untrustedv4v6, and unrestricted interfaces.....	30
QoS DSCP mutation.....	33
Specifying policies.....	34
Packet flow using QoS.....	35
QoS interface applications.....	42
ARP spoofing.....	42
DHCP snooping.....	42
DHCP spoofing.....	43
SQLSlam.....	43
Nachia.....	43
Xmas.....	44
TCP SynFinScan.....	44
TCP FtpPort.....	44
TCP DnsPort.....	44
BPDU blocker.....	44
DoS Attack Prevention Package.....	44
DAPP notification support.....	46
Automatic QoS.....	46

Precedence values.....	47
QoS errors in ACLI.....	48
Chapter 4: Configuring Quality of Service (QoS) with ACLI.....	49
Displaying QoS parameters.....	49
Displaying QoS capability and policy configuration.....	54
Configuring QoS access lists.....	54
Assigning ports to an access list.....	55
Removing an access list assignment.....	56
Creating an IP access list or Layer 2 access list.....	56
Creating an IP access list.....	57
Removing an IP access list.....	58
Creating a Layer 2 access list.....	59
Removing a Layer 2 access list.....	60
Configuring QoS security.....	61
Enabling QoS ARP spoofing.....	61
Disabling QoS ARP spoofing.....	61
Enabling QoS BPDU blocker.....	62
Disabling QoS BPDU blocker.....	62
Enabling QoS DHCP snooping and spoofing.....	62
Disabling QoS DHCP snooping and spoofing.....	63
Enabling QoS DoS applications.....	64
Disabling QoS DoS applications.....	64
QoS agent configuration.....	65
Enabling and disabling QoS agent support globally.....	65
Configuring QoS agent.....	66
Configuring QoS agent to default.....	67
Viewing QoS agent configuration information.....	68
Modifying default queue configuration.....	69
Configuring default buffering capabilities.....	69
Configuring the CoS-to-queue assignments.....	71
Configuring 802.1p priority values.....	71
Configuring QoS interface groups.....	71
Configuring ports for an interface group.....	72
Removing ports from an interface group.....	72
Creating an interface group.....	73
Removing an interface group.....	73
Configuring DSCP and 802.1p and queue associations.....	74
Configuring DSCP to 802.1p priority.....	74
Restoring egress mapping entries to default.....	75
Configuring 802.1p priority to DSCP.....	75
Restoring ingress mapping entries to default.....	76
Configuring QoS elements, classifiers, and classifier Blocks.....	76
Configuring IP classifier element entries.....	76
Viewing IP classifier entries.....	77
Removing IP classifier entries.....	78
Adding Layer 2 elements.....	78
Viewing Layer 2 elements.....	80

Removing Layer 2 elements.....	80
Linking IP and L2 classifier elements.....	80
Removing classifier entries.....	81
Combining individual classifiers.....	81
Removing classifier block entries.....	82
Configuring QoS system-element.....	83
Configuring system classifier element parameters.....	83
Viewing system classifier elements parameters.....	85
Removing system classifier element entries.....	86
Configuring QoS actions.....	86
Creating and updating QoS actions.....	86
Removing QoS actions.....	88
Configuring QoS interface action extensions.....	88
Creating interface action extension entries.....	88
Removing interface action extension entries.....	89
Configuring QoS meters.....	89
Creating QoS meter entries.....	89
Removing QoS meter entries.....	91
Configuring QoS interface shaper.....	91
Configuring interface shaping.....	91
Disabling interface shaping.....	92
Configuring a QoS interface queue shaper.....	92
Creating a QoS interface queue shaper.....	93
Deleting a QoS interface queue shaper.....	94
Viewing QoS interface queue shaper information.....	94
Configuring egress mapping.....	95
Resetting egress mapping values.....	96
Configuring QoS policies.....	96
Configuring QoS policies.....	96
Removing QoS policies.....	99
Configuring QoS traffic profile filter set.....	99
Configuring a traffic profile classifier entry.....	100
Configuring a traffic profile set.....	103
Deleting a classifier, classifier block, or an entire filter set.....	105
Viewing filter descriptions.....	105
QoS filter limiting configuration.....	106
Displaying QoS filter limiting.....	106
Disabling QoS filter limiting.....	106
Enabling QoS filter limiting.....	106
Restoring QoS filter limiting to default.....	106
Configuring QoS for the NSNA solution.....	107
Configuring QoS for NSNA filters.....	107
Deleting a classifier, classifier block, or an entire filter set.....	110
Viewing filter descriptions.....	111
Configuring user-based policies.....	111
Deleting a classifier, classifier block, or an entire filter set.....	114
Viewing filter descriptions.....	115

Maintaining the QoS agent.....	115
Removing all QoS configurations.....	115
Resetting QoS to factory default state.....	116
Changing the QoS agent to partial factory defaults.....	116
Configuring auto QoS mode.....	116
Configuring QoS UBP support.....	117
Configuring QoS statistics tracking type.....	118
Configuring NVRAM delay.....	118
Resetting NVRAM delay to default.....	119
Resetting the QoS agent.....	119
Configuring DoS Attack Prevention Package.....	119
Enabling DAPP.....	120
Configuring DAPP status tracking.....	120
Configuring DAPP minimum TCP header size.....	120
Configuring DAPP maximum IPv4 ICMP length.....	121
Configuring DAPP maximum IPv6 ICMP length.....	121
Configuring Automatic QoS.....	121
Enabling Automatic QoS.....	121
Disabling Automatic QoS.....	122
QoS statistics management.....	122
Chapter 5: Quality of Service (QoS) configuration using Enterprise Device Manager	123
Opening the QoS devices dialog box.....	123
Viewing the interface queue.....	123
Viewing interface groups.....	124
Viewing interface ID assignments.....	127
Viewing Priority Q Assign.....	128
Viewing priority mapping.....	129
Viewing DSCP mapping.....	130
Viewing meter capability.....	132
Viewing shaper capability.....	133
Opening QoS rules dialog box.....	134
Viewing the IP classifier element tab.....	134
Viewing the L2 classifier element.....	137
Viewing System Clfr Elements.....	139
Viewing classifiers.....	143
Viewing the classifier block.....	146
Opening the QoS dialog box.....	149
Viewing actions.....	149
Viewing interface action ext.....	151
Viewing the meters.....	152
Viewing policies.....	154
Viewing the interface shaper.....	158
Configuring interface queue shaper.....	159
Configuring interface apps.....	161
Viewing user-based policies.....	164
Configuring the QoS agent dialog box.....	165
Viewing the QoS configuration.....	165

Enabling and disabling QoS agent support.....	167
Enabling automatic QoS.....	167
Disabling automatic QoS.....	168
Configuring the QoS trusted processing mode.....	168
Enabling DoS Attack Prevention Package (DAPP).....	168
Configuring DAPP minimum TCP header size.....	169
Configuring DAPP maximum IPv4 ICMP length.....	169
Configuring DAPP maximum IPv6 ICMP length.....	169
Viewing policy class support.....	170
Viewing policy device identifications.....	170
Viewing the resource allocation configuration for ERS 5500.....	171
Viewing the resource allocation configuration for ERS 5600.....	172
Configuring QoS filter limiting configuration.....	174
Displaying QoS filter limiting.....	174
Disabling QoS filter limiting.....	174
Enabling QoS filter limiting.....	174
Opening the QoS NSNA/UBP/Traffic Profile dialog box.....	175
Viewing classifiers.....	175
Viewing traffic profile sets.....	179
Index.....	183

Chapter 1: New in this Release

There are no new features added to this document for Release 6.3.

New in this Release

Chapter 2: Introduction

This document provides information you need to configure Quality of Service (QoS) for the Ethernet Routing Switch 5000 Series.

ACL I command modes

ACL I provides the following command modes:

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

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

If no password is set, you can enter ACL I 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 5650TD>	No entrance command, default mode	exit or logout
Privileged EXEC 5650TD#	enable	exit or logout
Global Configuration 5650TD(config)#	configure	To return to Privileged EXEC mode, enter: end or exit

Command mode and sample prompt	Entrance commands	Exit commands
		To exit ACLI completely, enter: logout
Interface Configuration 5650TD(config-if)#	From Global Configuration mode: To configure a port, enter: interface fastethernet <port number> To configure a VLAN, enter: interface vlan <vlan number>	To return to Global Configuration mode, enter: exit To return to Privileged EXEC mode, enter: end To exit ACLI completely, enter: logout
Router Configuration 5650TD (config-router)#	From Global Configuration mode, to configure OSPF, enter: router ospf To configure RIP, enter: router rip To configure VRRP, enter: router vrrp	To return to Global Configuration mode, enter: exit To return to Privileged EXEC mode, enter: end To exit ACLI completely, enter: logout

See *Avaya Ethernet Routing Switch 5000 Series Fundamentals*, NN47200-104.

Chapter 3: Policy-enabled network fundamentals

This chapter provides an overview of the Differentiated Services (DiffServ) Quality of Service (QoS) network architecture. The Avaya Ethernet Routing Switch 5000 Series provides Avaya Command Line Interface (ACLI), SNMP, and the Enterprise Device Manager (DM) to configure QoS.

Summary

Policy-enabled networks allow system administrators to prioritize the network traffic, thereby providing better service for selected applications. Using Quality of Service (QoS), the system administrators can establish service level agreements (SLA) with customers of the network.

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

Avaya uses DiffServ to provide QoS functionality. A DiffServ architecture enables service discrimination of traffic flows by offering network resources to higher classes at the expense of lower classes of service. This architecture allows you to prioritize or to aggregate flows and provide scalable Quality of Service (QoS).

Briefly, with DiffServ, you can configure 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 how the system treats the packet as it moves through the network. The system identifies, meters and re-marks to facilitate flow prioritization. You can specify a number of policies and each policy can match one or many flows — which support complex classification scenarios.

Port-based and role-based QoS policies

The Ethernet Routing Switch 5000 Series supports both port-based and role-based Quality of Service policies. In a port-based Quality of Service environment, you apply policies directly to individual ports. In a role-based Quality of Service environment, you first assign individual ports to a role and then you assign a policy to that role.

A port-based QoS environment allows for the more direct application of Quality of Service policies and eliminates the need to group ports together when you assign policies.

You can apply port-based and role-based policies to same port; however, you are responsible for the proper division of resources across the individual policies.

QoS overview

Differentiated services (DiffServ) is a Quality of Service (QoS) network architecture that offers varied levels of service for different types of data traffic. DiffServ designates a specific level of performance on a packet-by-packet basis, instead of using the best-effort model for data delivery. 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. The QoS system also can interact with 802.1p and Layer 2 QoS.

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

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

DiffServ concepts

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

The switch implements the DiffServ basic elements within the network, which include:

- Packet classification functions
- A small set of per-hop forwarding behaviors
- Traffic metering and marking

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

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

Policies ensure that the switch treats traffic marked by the different DSCPs according to that marking, as the traffic moves within the DiffServ network.

QoS components

The Avaya Ethernet Routing Switch 5000 Series supports the following Avaya QoS classes:

- Critical and network classes have the highest priority over all other traffic.
- Premium class is an end-to-end service functioning similarly to a virtual leased line. Traffic in this service class is normally guaranteed an agreed-upon peak bandwidth. Traffic requiring this service must be shaped at the network boundary in order to undergo a negligible delay and delay variance. This service class is suitable for real-time applications, such as video and voice over IP. The recommended PHB for this service is the Expedited Forwarding (EF) PHB.
- Platinum, Gold, Silver, and Bronze classes use the Assured Forwarding (AF) PHB. These classes are 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).

[Table 1: Service Classes](#) on page 15 describes the service classes and their required treatment.

Table 1: Service Classes

Traffic category	Service class	Application type	Required treatment
Critical network control	Critical	Critical network control traffic	Highest priority over all other traffic. Guaranteed minimum bandwidth.
Standard network control	Network	Standard network control traffic	Priority over user traffic. Guaranteed minimum bandwidth.

Traffic category	Service class	Application type	Required treatment
Real time, delay intolerant, fixed bandwidth	Premium	Interhuman communications requiring interaction (such as VoIP).	Absolute bounded priority over user traffic. No packet loss for in-profile traffic. Virtual leased line with lowest amount of latency. Provisioned for peak rate.
Real time, delay tolerant, low variable bandwidth	Platinum	Interhuman communications requiring interaction with additional minimal delay (such as low-cost VoIP).	Higher-priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Real time, delay tolerant, high variable bandwidth	Gold	Single human communication with no interaction (such as web site streaming video).	High-priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Non-real time, mission critical, interactive	Silver	Transaction processing (such as Telnet, web browsing).	Medium priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Non-real time, mission critical, non-interactive	Bronze	For example, e-mail, FTP, SNMP.	Lower-priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
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.

Specifying interface groups

You use interface groups in the creation of role-based policies. Role-based policies group ports together to apply a common set of rules to them. Alternatively, port-based policies 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.

Different interfaces in a stack may not have the same capabilities. Interfaces with different capabilities can be assigned to the same role. As a result, policies and filters with certain

characteristics might not be able to reference an interface group if it contains ports that are incompatible with the policy requirements.

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

*** Note:**

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 become part of the interface group (role combination) automatically.

At factory default, the switch assigns ports to the default interface group (role combination), which is named allQoSPolicyIfcs. The switch associates each port with the default interface group, until either you associate a port with another interface group or you remove the port from all interface groups. Ports that are not associated with any interface group are disabled for QoS; they remain disabled across reboots until you assign that port to an interface group or you reset the switch to factory defaults (when it is reassigned to allQoSPolicyIfcs). Beginning in Release 6.0, QoS-disabled interfaces are associated with reserved role \$qosDisabledIfcs.

*** Note:**

You must remove all ports from an interface group before you delete it. You cannot delete an interface group when it is referenced by a policy.

*** Note:**

When QoS is reset to defaults and resources are not available to install default untrusted policies, affected ports are QoS-disabled.

Interface shaping

Interface shaping allows the system to limit the rate at which all traffic egressing through a specific interface transmits on the network. Interface shaping ensures that the limited bandwidth resources are used efficiently by the traffic generation rate upon transmission.

Shaping on a per interface basis provides full control over bandwidth consumption on your networks. Shaping, in conjunction with ingress flow metering, is a vital component of the overall bandwidth management solution.

Egress queue shaping

With egress queue shaping, you can specify the maximum and minimum egress shaping rates on an individual port and queue basis. You can configure shaping criteria for any or all egress queues associated with a switch port. The QoS agent egress queue set value determines the number of egress queues available for a port . Only Avaya Ethernet Routing Series 5600 switches (not ERS 5500 units) support egress queue shaping.

You can use QoS egress queue shaping to configure egress shaping on a per queue basis without traffic interruption. The ERS 5600 units support both port-based shaping and per-port per-egress queue shaping.

Bandwidth allocation for queues is done according to strict priority and WRR algorithms. When you configure minimum rate shaping, the system first tries to satisfy the minimum rate requests for all queues. The system allocates the remaining bandwidth according to the specified queue set servicing algorithms (strict priority and WRR), taking into account any maximum rate shaping configuration for each queue.

You can apply an interface shaper and individual queue shapers to the same egress port. In this situation, the interface shaper and any queue shaping affects egress traffic as described in the preceding paragraph.

Egress queue shaping examples

If the sum of the shape minimum rates that you configure (queue shapers) exceeds the line rate, then the system assures the minimum shape rate for queue 1 and the system distributes the remaining bandwidth to the rest of the queues using round robin (equal distribution). For ERS 5000 series switches, the system assures the minimum shape rate for queue 1 and the system distributes the remaining bandwidth to rest of queues using the WRR algorithm.

Also if queue shaper is not applied for queue 1, the rest of the queues use minimum shape rates (different than 0) for queue shaper and interface shaper is applied to the same egress port with a shape rate that is lower than any from minimum queue shaper rates, the egress traffic will be limited by interface shaper and round robin is applied to all queues except queue 1. Queue 1 traffic will not be received in this situation. For Ethernet Routing Switch 5000 series switches, queue 1 traffic is not received, egress traffic is limited by the interface shaper, and WRR is applied to all queues except queue 1.

QoS traffic profile filter sets

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

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

You can combine filter set classifier elements into a block when resources are limited. A single filter set (non-block) classifier element consumes one precedence level. Any number of filter set classifier elements combined in a block still only consume one precedence level. Therefore, when you combine compatible filter set classifier elements into blocks it can positively affect resource usage.

The switch applies policies within a set to ingress traffic in a specific order. The evaluation order dictates the order in which classifier elements associated with the same filter set name are applied. The switch applies elements with a low evaluation order before elements with a higher evaluation order. An evaluation order must be unique within a filter set. The switch determines the evaluation order for a classifier block by the lowest evaluation order of the elements that are members of the block or by indicating a block member as the "master" (the switch uses the evaluation order associated with the master block member this case).

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

- You can add or delete filter set components (filters and actions) while the filter set is associated with a port.
- You can apply multiple filter sets to a port.

Traffic profile filter set metering

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

Policy-based metering associates a unique meter with each policy that comprises the filter set. There are two types of policy-based metering:

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

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

QoS filter limiting

As part of your traffic control and management strategy you can use Filter Limiting to control the maximum number of user-defined protocol VLANs available on the switch.

Enabled by default, Filter Limiting allows you to create up to seven user-defined protocol VLANs.

If you disable Filter Limiting, you can create up to 16 user-defined protocol VLANs. However, the system generates error messages if you disable Filter Limiting in the presence of an ERS 5510 switch. For example, if you disable Filter Limiting on a stack containing ERS 5510 members the stack loses those members. If you disable Filter Limiting on a stack containing ERS 5510 members, the stack can break after reboot because the ERS 5510 has Filter Limiting enabled and the non-5510 members have Filter Limiting disabled. To restore the stack in this scenario you must enable Filter Limiting and reboot the stack.

Important:

The ERS 5510 switch supports a maximum of seven user-defined protocol VLANs. If you use an ERS 5510 as a standalone switch, or as a unit in a stack, you must enable Filter Limiting.

If you save an ASCII configuration that has Filter Limiting disabled and contains more than seven user-defined protocol VLANs, when you apply the configuration to a switch or stack that has Filter Limiting enabled, only the first seven user-defined protocol VLANs are configured. If you use ACLI, the system displays error messages and the ASCII configuration file processing continues. If you use EDM, the first error halts the ASCII file process. To prevent the Filter Limiting errors, check the Filter Limiting setting in the ASCII file to ensure that Filter Limiting is set correctly for your switch. Then boot the switch and load the ASCII file from either ACLI or EDM.

If ERS 5510 switches are present as non-base units in a stack, you can disable Filter Limiting but the system displays warning messages and the stack breaks after you reboot it.

Following are examples of Filter Limiting error messages:

- WARNING: 5510s in stack will not join stack after reboot
- WARNING: Resetting the stack will no longer allow a stack to be formed
- WARNING: Base unit may not be reachable in standalone mode

Note:

In order to reconfigure a switch or stack with decOtherEther2 protocol VLANs defined, you must set the switch/stack to default, disable filter limiting, then reboot the switch/stack before applying the ASCII configuration.

The NSNA solution

The Ethernet Routing Switch 5000 Series can be configured as a network access device for the NSNA solution.

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

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

For more information about NSNA, see *Avaya Security Configuration manual*, (NN47200-501).

User-based policies

You can configure the Ethernet Routing Switch 5000 Series to manage access with user-based policies. User-based policies revolve around the User Policy Table supporting multiple users per interface. User data is provided through interaction with EAP and is maintained in the User Policy Table. You associate a user with a specific interface, user role combination, user name string, and, optionally, user group string. You also associate each user with session information. Session data maintains state information for each user and includes a session identifier and a session start time. You also associate users with a session group identifier. The same group identifier is shared by users with the same role combination and is referenced during new user installation and the subsequent EPM policy installation to identify the policy criteria to be applied. The QoS Agent controls this session data.

User-specific roles and policy data complements the legacy interface role combinations by supporting the concept of "default" or "corporate" roles and policies, as well as user-specific roles and policies.

Rules

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

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

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

Classifier definition

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

The system automatically creates some classifiers on trusted, untrusted, and untrustedv4v6 ports. Additional classifiers are user-created.

Classifiers are not created to support trusted processing on the ERS 5600 Series platform. A hardware based DSCP table is used for this purpose. Classifier block elements now include a precedence value to facilitate evaluation ordering on ERS 5600 Series platforms.

IP classifier elements

The Avaya Ethernet Routing Switch 5000 Series classifies packets based on the following parameters in the IP header:

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

Layer 2 classifier elements

The Avaya Ethernet Routing Switch 5000 Series classifies packets based on the following parameters in the Layer 2 header:

- Source MAC address/mask
- Destination MAC address/mask
- VLAN ID number (range of)
- VLAN tag
- EtherType
- IEEE 802.1p user priority values
- Packet Type
- VLAN ID

*** Note:**

The Avaya Ethernet Routing Switch 5000 Series treats Layer 2 classifier elements with an Ethernet type of 0x0800 as an IPv4 classifier, and the ERS 5000 Series treats those with an Ethernet Type of 0x86DD as an IPv6 classifier.

System classifier elements

The system classifier element supports traffic identification based on the Layer 2 destination MAC address type.

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

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

*** Note:**

The ERS 5500 Series switch supports matching 32 bytes from the first 80 bytes of a packet. The ERS 5600 Series switch supports matching 16 bytes from the first 128 bytes of a packet.

Classifiers and classifier blocks

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

Each classifier can have a maximum of a single IP classifier element, plus a single L2 classifier element. More than one IP classifier element, or more than one L2 classifier element, cannot be put into one classifier. A classifier can contain one IP classifier element and one L2 classifier element, or one classifier element of each type, but no more. That is, the classifier can have one (and only one) of either:

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

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

As you plan classifier blocks, keep in mind that only a single IP classifier element, a single L2 classifier element, and a simple 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.

* Note:

Use blocks to combine compatible classifiers to use less resources at the policy level.

On the ERS 5500 Series switch 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 bitmask, and VLAN tag type. Block membership on the ERS 5600 Series only requires that all members match protocol fields from the same limited set. If this criterion is not met, an error message is generated when 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. On the 5500 Series switch blocks are unordered and evaluated as if simultaneously.

On the ERS 5600 Series switch, a new attribute, **eval-order**, supplies the ability to specify the block evaluation order.

You associate a classifier or classifier block through a policy with individual ports or interface groups. The switch classifies packets received from any port that is in an interface group with the same filter criteria.

You associate each classifier or classifier block with actions that the system executes when the packet matches the filter criteria in the group. A policy dictates the overall traffic treatment

(refer to [Figure 2: Flowchart of QoS Actions](#) on page 26 for an illustration of the traffic treatment) and references the filter criteria and the associated actions, metering criteria, and ports or interface groups.

You can associate classifier elements, through individual classifiers or a classifier block, with a port or interface group, action, and metering through a policy. You can apply multiple policies to a given flow. The switch determines the policy evaluation order by the policy precedence. The order of precedence is from the highest precedence value to the lowest precedence (that is, the switch evaluates a value of 8 before a value of 7).

*** Note:**

You can associate classifier blocks with a meter or action when none of the individual classifiers that comprise that block are associated with an action or meter.

[Figure 1: Relationship of classifier elements, classifiers, and classifier blocks](#) on page 25 displays the relationship between the classifier elements, classifiers, and classifier blocks.

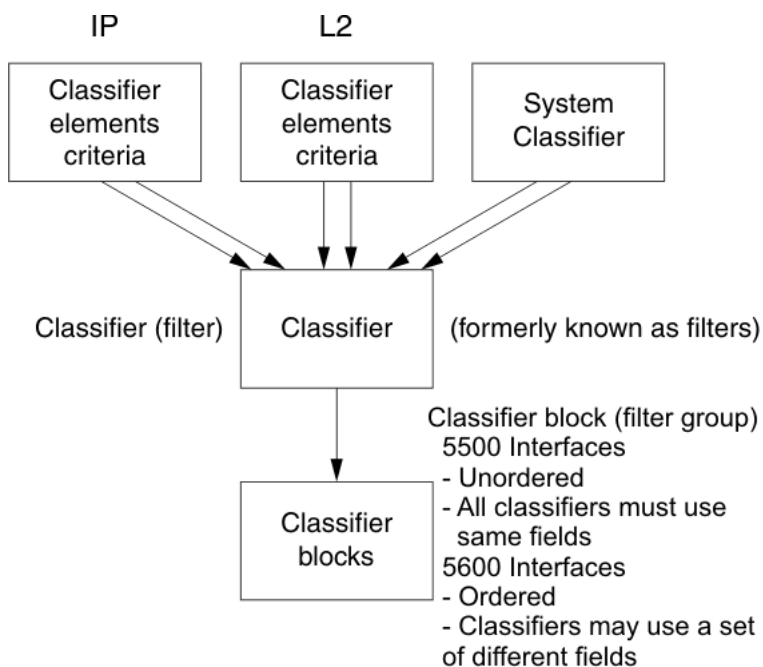


Figure 1: Relationship of classifier elements, classifiers, and classifier blocks

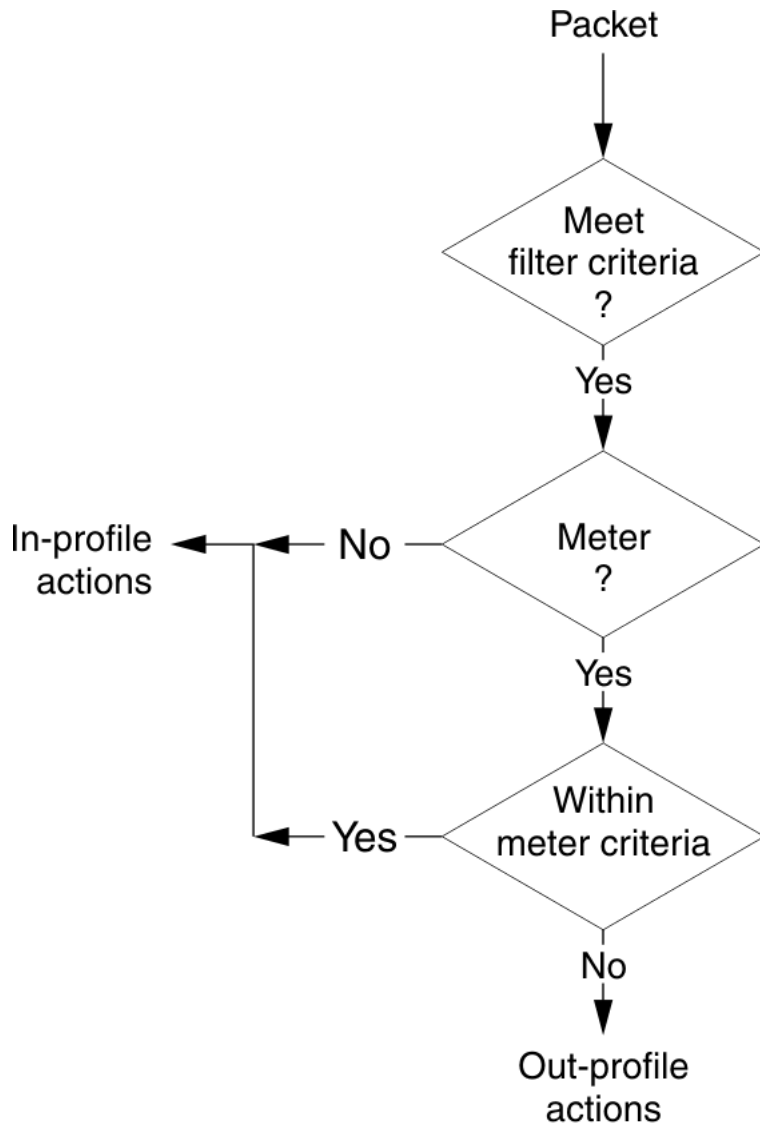
In summary, classifiers combine different classifier elements. In the case of the ERS 5500 Series switch, classifier blocks combine classifiers to form an unordered set of classification data. Unordered data means that all classifiers associated with a policy are applied as if simultaneously, with no precedence.

*** Note:**

The ERS 5600 Series switch supports creating classifier blocks using different classifiers. The switch uses evaluation order to determine which classifier block is applied first when data is matched by multiple blocks.

Specifying actions

[Figure 2: Flowchart of QoS Actions](#) on page 26 summarizes how QoS matches packets with actions.



11092EA

Figure 2: Flowchart of QoS Actions

[Table 2: Summary of Allowable Actions](#) on page 27 shows a summary of the allowable actions for different matching criteria. This information is applicable to the ERS 5500 Series switch only.

Table 2: Summary of Allowable Actions

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

*** Note:**

Native non-match action is not available on the ERS 5600 Series switch. You must define an additional wild card rule to enable native non-match support for ERS 5600 Series ports. All actions in the above table, with the exception of Non-Matching, apply to the ERS 5600 Series switch.

The Avaya Ethernet Routing Switch 5000 Series filters collectively direct the system to initiate the following actions on a packet, depending on the configuration:

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

*** Note:**

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

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

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

The actions applied to packets include those actions defined from user-defined policies and those actions defined from system default policies. The user-defined actions always carry higher precedences than the system default actions. This means that, if user-defined policies do not specify actions that overlap with the actions associated with system default policies (for example, the DSCP and 802.1p update actions installed on untrusted and untrustedv4v6

interfaces), the default policy actions will be included in the set of actions to be applied to the identified traffic.

Specifying interface action extensions

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

[Table 3: Summary of allowable interface action extensions](#) on page 28 shows a summary of the allowable interface action extensions for different matching criteria. This information is applicable to the 5500 Series switch only.

Table 3: Summary of allowable interface action extensions

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

*** Note:**

Native non-match action is not available on the ERS 5600 Series switch. You must define an additional wild card rule to enable native non-match support for ERS 5600 Series ports. All actions in the above table, with the exception of non-Matching, apply to the ERS 5600 Series switch.

*** Note:**

The Avaya Ethernet Routing Switch 5600 Series does not initiate an action extension based packet type. The user should redirect all incoming traffic, regardless of packet type (both unicast and non-unicast), towards the same port using interface action extension.

The Avaya Ethernet Routing Switch 5000 Series filters collectively direct the system to initiate the following interface action extensions on a packet, depending on your configuration:

- Set egress unicast interface — specifies redirection of normally switched known (with a previously learned destination address) unicast packets to a specific interface (port)
- Set egress non-unicast interface — specifies redirection of normally switched non-unicast (that is, broadcast, multicast, and flooding) packets to a specific interface (port)

Specifying meters

QoS metering, which operates at ingress, provides different levels of service to data streams through user-configurable parameters. A meter measures the traffic stream against a traffic profile, which you create. Meters yield 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 you can configure policies with a single meter or match action that applies to all the classifiers associated with that policy. You cannot define meters and action criteria in both the policy definition and the individual classifier block member definition.

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

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

You can use meters to configure a committed rate in Kb/s (1000 bits per second in each Kb/s). All traffic within this committed rate is In-Profile. Additionally, you can configure a maximum burst rate that specifies an allowed data burst larger than the committed rate for a brief period. After you configure this, the system offers suggestions to choose the duration for this burst. Combined, these parameters define the in-profile traffic.

*** Note:**

The range for the committed rate on the 5510 model switch is 1000 to < 1023000 Kb/s. You can configure the rate in increments of 1000 Kb/s (1 megabit) each.

*** Note:**

The range for the committed rate on the 5520, 5530, and 5600 Series models is 64 to < 10230000 Kb/s. You can configure the rate in increments of 64 Kb/s each.

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

*** Note:**

Burst rate and duration determine burst size.

The system rejects meter definitions where 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): 4096 (4K), 8192 (8K), 16384 (16K), 32768 (32K), 65536 (64K), 131072 (128K), 262144 (256K), 524288 (512K), 1048576 (1024K), 2097152 (2048K), 4194304 (4096K), 8388608 (8192K), and in the case of the 5600 Series switch, 16777216 (16384K).

*** Note:**

On 5530-24TFD, 5520-24T/48T 10/100/1000 Mbps ports and 5600 Series ports, the minimum value and granularity for the committed rate is 64 Kbps. On the 10 Gbps ports the maximum value for the committed rate is 10230000 Kbps.

Trusted, untrusted, untrustedv4v6, and unrestricted interfaces

Avaya Ethernet Routing Switch 5000 Series ports are classified into three categories:

- trusted
- untrusted
- unrestricted
- untrustedv4v6

The classifications of trusted, untrusted, untrustedv4v6, and unrestricted actually apply to groups of ports (interface groups). These three categories are also called interface classes. In your network, trusted ports usually connect to the core of the DiffServ network; untrusted and untrustedv4v6 ports typically access links that connect to end stations. Unrestricted ports can either be access links or can connect to the core network.

At factory default, all ports are untrusted. However, for interface groups you create, the default is unrestricted.

Because a port can belong to only one interface group, you can classify a port as trusted, untrusted, untrustedv4v6, or unrestricted. These types are also called interface classes.

The switch automatically associates trusted, untrusted, and untrustedv4v6 ports 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** — The switch re-marks, at the layer 2 level, IPv4 traffic it receives on trusted interfaces. The switch updates the 802.1p user priority value based on the DSCP value in the packet at ingress and the installed DSCP-to-CoS mapping data. The switch does not update the DSCP value. On the ERS 5500 series switch, remapping occurs, by default, only for standardized DSCP values (for example, EF, AFXX) and any proprietary Avaya values. On the ERS 5600 series switch, remapping occurs for all DSCP values.

The switch remaps the DSCP values and associates them with a zero 802.1p user priority value in the DCSP-to-CoS Mapping table. The ERS 5600 series switch uses a hardware based DSCP table to support trusted processing. No policies or filters are consumed by the 5600 Series.

- **Untrusted interfaces** — The switch re-marks, at the layer 3 level, the IPv4 traffic it receives on untrusted interfaces and it updates the DSCP value. How the switch determines the new DSCP value depends on whether the packet is tagged or untagged:

- **Untagged frames**

The switch uses the default port priority of the interface that receives the ingress packet to derive the DSCP value. The switch uses the default port priority to perform a lookup in the installed CoS-to-DSCP mapping table.

The 802.1p user priority value does not change. The default port priority determines this value.

(The switch uses the default port priority of the ingress interface to update the DSCP value on untagged frames on untrusted interfaces. The user sets the default port priority).

- **Tagged frames**

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

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

*** Note:**

The default processing of untrustedv4v6 interface is same as the untrusted interface, but it also applies to IPv6 traffic. It is supported on all ERS5600 and ERS5500 switches that are capable of IPv6 DSCP remarking.

[Table 4: Default QoS fields by class of interface—IPv4 only](#) on page 31 shows the default guidelines the switch uses to re-mark various fields of IPv4 traffic (and layer 2 traffic matching IPv4) based on the class of the interface. These actions occur if the user does not intervene at all; they are the default actions of the switch.

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

Type of filter	Action	Trusted	Untrusted	Unrestricted
IPv4 filter criteria or Layer 2 filter criteria matching IPv4	DSCP	Does not change	<ul style="list-style-type: none"> • Tagged—Updates to 0 (Standard) • Untagged—Updates using mapping table and port's default value 	Does not change

Type of filter	Action	Trusted	Untrusted	Unrestricted
	IEEE 802.1p	Updates based on DSCP mapping table value	<ul style="list-style-type: none"> • Tagged—Dependent on DCSP-to-COS setting. • Untagged—Priority is unchanged. 	Does not change

*** Note:**

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

The Avaya Ethernet Routing Switch 5000 Series does not trust the DSCP of IPv4 traffic received from an untrusted port; however, it does trust the DSCP of IPv4 traffic received from a trusted port.

By default, Layer 2 non-IP traffic received on either a trusted port or an untrusted port traverses the switch with no change.

The switch re-marks the 802.1p user priority value and sets the drop precedence on IPv4 traffic it receives on a trusted port. The switch does this based on the DSCP in the IP packet it receives.

If the switch receives an IPv4 packet from a trusted port, and it does not match any of the classifier elements installed by the user on this port or it does match a classifier element but may be dropped, the 5500 Series switch uses default system classifiers to change the packet IEEE 802.1p and drop precedence based on the DSCP of the packet. The 5600 Series switch uses a hardware based DSCP table for this purpose.

If the switch receives an IPV4 packet from an untrusted port and it does not match any one of the classifier elements installed by the user on the port, the Avaya Ethernet Routing Switch 5000 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 switch derives the 802.1p user priority value from the DSCP-to-CoS mapping table using the best effort DSCP, which is 0.
- If an IPv4 packet is untagged, the Avaya Ethernet Routing Switch 5000 Series uses the default classifier to change the DSCP based on the default IEEE 802.1p priority of the ingress untrusted port to index into the CoS-to-DSCP mapping table to determine the DSCP value.

[Table 5: Default mapping of DSCP to QoS class and IEEE 802.1p](#) on page 32 describes the default DSCP, QoS class, IEEE 802.1p, and egress queue assignment for packets in each traffic class.

Table 5: Default mapping of DSCP to QoS class and IEEE 802.1p

Incoming or re-marked DSCP (hex values)	QoS class	Number of queues (8)	Outgoing IEEE 802.1p user priority
CS7 (0x38)	Critical	1	7
CS6 (0x30)	Network	1	

Incoming or re-marked DSCP (hex values)	QoS class	Number of queues (8)	Outgoing IEEE 802.1p user priority
EF(0x2E), CS5(0x28)	Premium	2	6
AF41(0x22), AF42(0x24), AF43(0x26), CS4(0x20)	Platinum	3	5
AF31(0x1A), AF32(0x1C), AF33(0x1E), CS3(0x18)	Gold	4	4
AF21(0x12), AF22(0x14), AF23(0x16), CS2(0x10)	Silver	5	3
AF11(0xA), AF12(0xC), AF13(0xE), CS1(0x8)	Bronze	6	2
DE(0x0), CS0(0x0), all undefined DSCPs	Standard	7	0

As displayed in [Table 5: Default mapping of DSCP to QoS class and IEEE 802.1p](#) on page 32, the traffic service class determines the IEEE 802.1p priority that determines the egress queue of the traffic. Non-IP traffic can be in the same IP service class if the non-IP packets are assigned the same IEEE 802.1p priority.

*** Note:**

Default policies for trusted interfaces are not used on the ERS 5600 Series switch. This task is addressed by the hardware.

QoS DSCP mutation

QoS DSCP mutation supports the remarking of DSCP values in conjunction with trusted interface processing. The switch extends QoS trusted interface support by adding an egress DSCP value to the DSCP-to-COS mapping table. The switch uses this egress DSCP value to remark the trusted traffic. If the egress DSCP value is the same as the ingress DSCP value only the Class of Service (COS) is updated.

In conjunction with the QoS DSCP mutation support, you can install filters targeting all DSCP values on ERS 5000 Series switches as part of the trusted support (the ERS 5600 switches use hardware mapping tables for this purpose). Previously, filters targeting only standard DSCP values were installed on ERS 5000 Series switches in support of trusted processing. You can select partial or full trusted support through the QoS Agent configuration mechanism.

With partial mode, the switch maps trusted DSCP values to specific CoS from the egress map using only non 0 DSCP-to-CoS values, and the switch treats the rest of values as unrestricted. With full mode, the switch maps all trusted DSCP to specific CoS from the egress map.

Specifying policies

* Note:

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

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

Among policies, the switch evaluates the policy with the highest precedence first, then the policy with the next highest precedence and so on. The valid precedence range for QoS policies is 1 to 15. For example, with a precedence of 1 to 15, the system begins the evaluation with 15, moves on to 14, and so forth. This is important to remember when you configure policies.

The valid precedence range can change if you enable certain features. QoS shares resources with other switch applications such as DHCP Relay, MAC Security (5530-24TFD only), DHCP Snooping, DHCP Relay, and IP Fix. Allocations for non-QoS applications are dynamic. If you enable these features, the following list describes how it affects the precedence range:

- When you enable DHCP Relay and/or DHCP Snooping, it uses the highest available precedence value.
- When you enable MAC Security (5530-24TFD only), it uses the highest available precedence value.
- When you enable IP Fix functionality, it uses the highest available precedence value.
- When you enable IGMP, it consumes the 2 highest available precedence values.
- When you enable EAPOL, it consumes the highest available precedence value.
- When you enable EAPOL multihost (5530-24TFD only), it consumes the highest available precedence values.
- When you enable OSPF, it consumes the highest available precedence value.
- When you enable IP Source Guard, it consumes the highest available precedence value.
- When you enable ADAC, it consumes the highest available precedence value.

* Note:

You can use the CLI command `show qos diag` to see the status of mask utilization. The number of QoS policies that you can configure is 16 - ("Mask Consumed" + "Non QoS Mask Consumed").

Beginning with release 6.2, Avaya has enhanced diagnostics in for ERS 5500 switches. Diagnostics show precedence allocation on a per port basis similar to ERS 5600 switch

diagnostics and show the maximum number of filters, meters, and counters on per port basis. The diagnostics display can be slow if you use multiple QoS resources (especially if you use traffic profiles).

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

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

The policies tie together:

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

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.

*** Note:**

You can enable and disable policies. You do not have to delete policies to disable them. To modify a policy, you must first delete it and then create a new policy.

You can also track statistics for QoS. The Avaya Ethernet Routing Switch 5000 Series supports per policy and per policy, classifier, or interface statistics tracking.

*** Note:**

The ERS 5600 Series switch does not support non-match-action. You must define an additional wild card rule to enable native non-match support for ERS 5600 Series ports.

Packet flow using QoS

Using DiffServ and QoS, you can designate a specific performance level for packets. This system allows for network traffic prioritization. However, it requires some thought to configure

the prioritizations. You can specify a number of policies and each policy can match one or many flows, supporting complex classification scenarios.

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

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

The available levels of QoS classes are currently named Network, Premium, Platinum, Gold, Silver, Bronze, and Standard. The configurable DSCP and associated 802.1p value determine the level of service for each packet.

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

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

Meters, operating at ingress, keep the sorted packets within certain parameters. You can configure a committed rate of traffic, allowing for a certain amount of temporary burst traffic, as In-Profile traffic. You configure 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 switch treats traffic.

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 when the switch matches certain user-defined characteristics.

[Figure 3: QoS Policy Schematic](#) on page 37 provides a schematic overview of QoS policies.

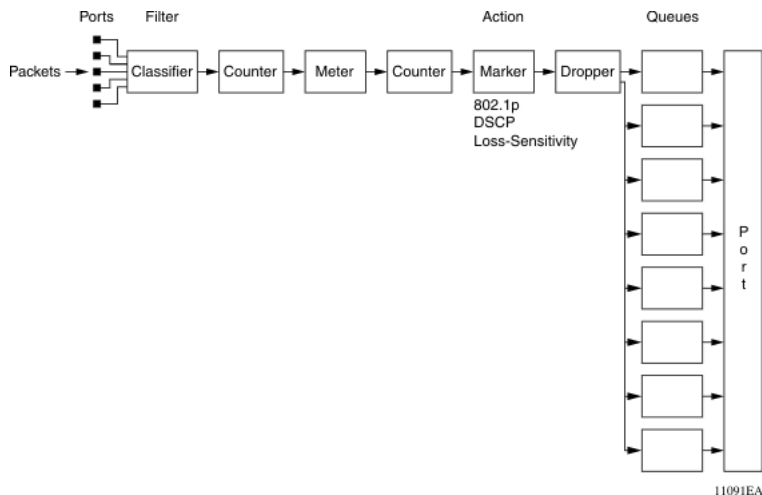


Figure 3: QoS Policy Schematic

Queue sets

A QoS queue set logically represents the queuing capabilities of an egress QoS interface. A queue set includes a number of related queuing components that dictate the queuing behavior that the queue set supports. The following list identifies the queuing components:

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

Each QoS egress port has eight queue sets that consist of anywhere from 1 to 8 queues, depending on the queue set you assign to the QoS interfaces. The IEEE 802.1p, or Class of Service (CoS), value of a packet determines which queue the packet uses. Depending on the queue set you configure, some queues use an absolute priority queuing mechanism and some queues use a Weighted Round Robin (WRR) queuing mechanism.

Beginning with software version 4.0, you can configure the queue set, and hence the number of queues per QoS interface, the buffer allocation of the queue set, and the CoS-to-queue priority for each queue within the queue set.

*** Note:**

You can configure these parameters for all QoS egress interfaces, not on a port-by-port basis. Thus, the egress queuing and buffering characteristics and the CoS-to-queue priorities are the same across all QoS ports. The Avaya Ethernet Routing Switch 5000 Series has factory default queue set and buffer allocation mode values. When you reset a system to defaults, the system has the following values:

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

Modifying queue set characteristics

You can configure the following characteristics of the queue sets:

- the number of queues per egress QoS interface, their service discipline and relative weights—you select one of the eight available predefined queue sets with the appropriate queue count, service discipline, and weights for your specific application. Eight queue sets are predefined per unit.
- the buffering resources consumed by the egress QoS interface—you select regular, large, or maximum to allocate the resources. These options determine the amount of resource sharing that can take place under certain scenarios across associated egress ports.

You cannot configure other queue characteristics, such as the service discipline or queue weights for WRR scheduler.

Although you can change the CoS-to-queue assignments for all defined queue sets, only the assignments associated with the queue set currently in use affect the traffic processing.

The queues within a queue set are referred to as CoS queues, because each queue is mapped within the queue set to a CoS priority value. The eight predefined queue sets contain a varying number of CoS queues, service disciplines, and queue weights. The relative interface bandwidth consumption percentages for WRR queues are shown as percentages.

To configure the queue set, choose one of the following eight available queue set types, which apply to all QoS egress interfaces, along with their characteristics:

- Queue set 8
 - 8 CoS queues
 - 1 queue strict priority; 7 WRR queues
 - 7 WRR queues scheduled as 41%, 19%, 13%, 11%, 8%, 5%, and 3%
- Queue set 7
 - 7 CoS queues

- 1 queue strict priority; 6 WRR queues
 - 6 WRR queues scheduled as 45%, 21%, 15%, 10%, 6%, and 3%
- Queue set 6
 - 6 CoS queues
 - 1 queue strict priority; 5 WRR queues
 - 5 WRR queues scheduled as 52%, 24%, 14%, 7%, and 3%
- Queue set 5
 - 5 CoS queues
 - 1 queue strict priority; 4 WRR queues
 - 4 WRR queues scheduled as 58%, 27%, 11%, and 4%
- Queue set 4
 - 4 CoS queues
 - 1 queue strict priority; 3 WRR queues
 - 3 WRR queues scheduled as 65%, 26%, and 9%
- Queue set 3
 - 3 CoS queues
 - 1 queue strict priority; 2 WRR queues
 - 2 WRR queues scheduled as 75% and 25%
- Queue set 2
 - 2 CoS queues
 - 2 strict priority queues
- Queue set 1
 - 1 CoS queue
 - 1 strict priority queue

You can also configure the buffer allocation (consumption) level for the configured queue set. One is chosen from among regular, large, or maximum allocations.

You can view queue set configuration information using the `show qos` command with the `if-assign` variable. The switch displays the active queue set on a stack and switch port basis as a value from 1 to 8, or a multiple of 1-8 set. For example, an active queue-set of 8 is displayed by port as 8,16,24,32,40,48,56 (depending on the ASIC).

Changing the CoS-to-queue assignment for one of the equivalent queue-sets changes the behavior of all equivalent sets.

QoS lossless buffering mode

The QoS queue set buffer allocation modes (regular, large, or maximum) determine the amount of buffer space provided for each port and priority, and provide the best possible throughput, but they are not lossless. Lossless buffering mode is critical in data center applications, where reliable data transfer is more important than enhanced throughput. With lossless mode, when a port receives traffic volume greater than port bandwidth, the port sends flow control (pause) frames to the sender. The flow control frames notify the sender to stop packet transmission for a specified amount of time. All end stations connected to the stack must be capable of symmetric flow control, and all switch ports must auto-negotiate to symmetric flow control. Flow control for 10G ports is symmetric by default when lossless buffering mode is enabled.

Lossless mode buffer settings and thresholds have been implemented for all supported QoS Queue sets (1 to 8). Avaya has only tested and only recommends Queue set 2 for this release. With Queue set 2, there are 2 CoS queues; the two queues are WRR, scheduled as 91% and 9%. Lossless oversubscription mode is supported on stacks of up to 8 ERS 5600 units.

Only ERS 5600 Series switches support QoS lossless buffering mode. You must not use QoS lossless buffering mode in a hybrid stack of ERS 5600 and ERS 5500 switches.

Individual switches that do not have QoS lossless buffering mode enabled are not allowed to join a stack that has QoS lossless buffering mode enabled.

A stack with QoS lossless buffering mode enabled, and connected as a ring stack using the redundant cable, forwards traffic in only one direction to the last unit in the stack.

Modifying CoS-to-queue priorities

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

*** Note:**

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

QoS configuration guidelines

You can install classifiers that act on traffic destined for the switch itself, such as ICMP Echo Requests (ping) and SNMP messages. If the associated action is to drop the traffic, access to the switch will be blocked for these services.

Using QoS on the Avaya Ethernet Routing Switch 5500 Series has the following limitations:

- You can configure up to 15 policies per interface (port).
- You can configure up to 63 meters per interface (port).
- You can configure up to 125 filter components per interface (port).
- When you enable tracking statistics for the policies, the switch uses one counter for each classifier for each interface (port) of the policy or a counter for each policy. You can assign up to 32 counters to an interface (port).

When using QoS on the Ethernet Routing Switch 5600 Series, resources are shared across groups of ports. The following limitations apply:

- Up to 15 policies per interface (port) can be configured
- Up to 256 filter components per precedence per hardware device group
- Up to 128 meters per precedence per hardware device group
- Up to 128 counters per precedence per hardware device group
- Up to 16 TCP/UDP port range checkers per hardware device group

Resource allocation behavior on the Ethernet Routing Switch 5600

Resource allocation on the Ethernet Routing Switch 5500 is port-based. The Content Aware Processor (CAP) of the Ethernet Routing Switch 5600 offers centralized resource allocation. The CAP utilizes 16 parallel CA lookup engines, each containing 256 rule entries.

The CAP architecture supports two levels of masking that represent both a superset and a subset of protocol fields that you can use for classification purposes. The CAP architecture supports a maximum of 16 defined policies per port.

Troubleshooting tips

If you encounter problems when you configure the queue sets, ensure that the modified queue set is associated with the QoS interfaces. You must reset the device for the changes to take effect.

Sometimes after you modify the default buffering resources, you cannot see the queue sizes in the updated queue set. Again, you must reset the device for the changes to take effect.

Finally, modified CoS-to-queue assignments affect only the active queue set; this can explain why an effect is not immediately seen after modifying the values.

QoS interface applications

The ERS 5500 Series switch supports several Quality of Service applications designed to enhance the security of the switch. These QoS security applications target several of the most common attacks launched against networks today. In contrast to the support offered by the ERS 5500 Series switch, the ERS 5600 Series switch utilizes DoS Attack Prevention Package (DAPP).

These attacks, and the QoS-based defense used to combat them, are briefly summarized in the following sections.

*** Note:**

Due to hardware limitations, the Ethernet Routing Switch 5500 Series switch supports 15 interface applications per port.

ARP spoofing

ARP spoofing is a common attack launched on network assets. ARP spoofing can be used by an attacker to spoof the IP address of a host on a LAN segment. More dangerous is the use of this mechanism to spoof the identity of a network default gateway in what is known as a man-in-the-middle attack.

The ARP Spoofing QoS application is specifically designed to prevent these man-in-the-middle attacks. The user must identify the default gateway address and which ports have ARP Spoofing support applied. This causes the switch to install a series of policies on these interfaces to perform the following operations:

1. Drop all ARP packets with a source IP address equal to the identified default gateway.
2. Pass all broadcast ARP requests.
3. Drop all non-broadcast ARP requests.
4. Drop all ARP packets with a target IP address equal to the identified default gateway.
5. Pass all ARP responses.

DHCP snooping

The DHCP Snooping QoS Application operates by classifying ports as access (untrusted) and core (trusted) and it allows only DHCP requests from the access ports. The switch discards all other types of DHCP messages received on access ports. This action prevents rogue DHCP servers from being set up by attackers on access ports and generating DHCP responses that

provide the rogue server address for the default gateway and DNS server. This action helps prevent DHCP man-in-the-middle attacks. Users must specify the interface type for the ports on which they wish to enable this support.

DHCP spoofing

Another method used to combat rogue DHCP servers is to restrict traffic destined for a client's DHCP port (UDP port 68) to that which originated from a known DHCP server IP address.

The DHCP Spoofing QoS Application requires the identification of the valid DHCP server address and the ports which have the DHCP Spoofing support applied. This action causes the switch to install two policies on these interfaces to perform the following operations:

1. Pass DHCP traffic originated by the valid DHCP server.
2. Drop DHCP traffic originated by all other hosts.

SQLSlam

The worm targeting SQL Server computers is self-propagating, malicious code that exploits a vulnerability that allows for the execution of arbitrary code on the SQL Server computer, due to a stack buffer overflow. Once the worm compromises a machine, it attempts to propagate itself by crafting packets of 376 bytes and sending them to randomly chosen IP addresses on UDP port 1434. If a vulnerable machine receives the packet, this victim machine becomes infected and also begins to propagate. Beyond the scanning activity for new hosts, the current variant of this worm has no other payload. Activity of this worm is readily identifiable on a network by the presence of 376 byte UDP packets. These packets appear to originate from seemingly random IP addresses and destined for UDP port 1434.

When enabled, the DoS SQLSlam QoS Application drops UDP traffic, whose destination port is 1434 with the byte pattern of 0x040101010101, starting at byte 47 of a tagged packet.

Nachia

The W32/Nachi variants W32/Nachi-A and W32/Nachi-B are that spread using the RPC DCOM vulnerability in a similar fashion to the W32/Blaster-A worm. Both rely upon two vulnerabilities in Microsoft software.

When enabled, the DoS Nachia QoS Application drops ICMP traffic with the byte pattern of 0xaaaaaa, starting at byte 48 of a tagged packet.

Xmas

Xmas is a DoS attack that sends TCP packets with all TCP flags set in the same packet, which is illegal. When enabled, the DoS Xmas QoS Application drops TCP traffic with the URG:PSH TCP flags set.

TCP SynFinScan

TCP SynFinScan is a DoS attack that sends both a TCP SYN and FIN in the same packet, which is illegal. When enabled, the TCP SynFinScan QoS Application drops TCP traffic with the SYN:FIN TCP flags set.

TCP FtpPort

A TCP FtpPort attack is identified by TCP packets with a source port of 20 and a destination port less than 1024, which is illegal. A legal FTP request initiates with a TCP port greater than 1024. When enabled, the TCP FtpPort QoS Application drops TCP traffic with the TCP SYN flag set and a source port of 20 with a destination port less than or equal to 1024.

TCP DnsPort

The TCP DnsPort QoS Application is similar to the TCP FtpPort application except for DNS port 53. When enabled, this application drops TCP traffic with the TCP SYN flag set and a source port of 53 with a destination port less than or equal to 1024.

BPDU blocker

There are certain scenarios in a bridged (switched) environment when the user can drop incoming BPDUs on a specific interface. When enabled, the BPDU Blocker QoS Application drops traffic with a specific multicast destination MAC address. Currently, targeted BPDU multicast destination addresses are 01:80:c2:00:00:00 and 01:00:0c:cc:cc:cd.

DoS Attack Prevention Package

The Ethernet Routing Switch 5600 Series hardware provides built-in support for detection and prevention of many common types of Denial of Service (DoS) attacks. The DoS Attack

Prevention Package (DAPP) gives network administrators the ability to enable or disable DAPP support for applicable units and to specify whether DAPP status tracking is required.

The types of common DoS attacks prevented by DAPP are:

- IP address check
 - Packet types:
 - IPv4
 - IPv6
 - Conditions detected:
 - SIP = DIP
 - LAND attack
- TCP flag checks
 - Packet types:
 - IPv6 TCP
 - IPv4 (IP not fragmented)
 - IPv4 (IP first fragment)
 - Conditions detected:
 - TCP SYN flag set and TCP source port < 1024
 - TCP control flags = 0 and TCP sequence number = 0
 - NULL scan attack
 - TCP flags FIN, URG & PSH set and TCP sequence number = 0
 - Xmas scan attack
 - TCP packets with SYN & FIN bits set
 - SynFin scan attack
- TCP fragment checks
 - Packet types:
 - IPv4 TCP
 - Conditions detected:
 - IPv4 first fragment and IP payload < MIN_TCP_HDR_SIZE (normally 20 bytes, range 0 – 255 bytes)

- IPv4 fragment and fragment offset = 1
 - Tiny Fragment (Indirect Method) attack
- ICMP checks
 - Packet types:
 - IPv4 ICMP
 - IPv6 ICMP
 - Conditions detected:
 - ICMP Echo Request and IP payload length > ICMP maximum (programmable maximum size value per packet type – maximum 1K [IPv4]/16K [IPv6])
 - ICMP packet is fragmented (IPv4 ICMP only)

When you enable DAPP, the switch monitors all attack types. Though network administrators are unable to configure the attack types to monitor, they have the ability to specify values for associated minimum TCP header size and IPv4/IPv6 ICMP maximum lengths used in detection.

*** Note:**

Avaya recommends FTP clients use passive mode when they enable DAPP.

DAPP notification support

In addition to preventing certain types of DoS attacks, DAPP gives the user the ability to configure notification and logging of such events. When you enable DAPP support with status tracking, the switch allocates a mask, filter, and counter for ports on the unit on which you enable DAPP. Through polling, the unit determines if DAPP detects a DoS attack. If the unit registers an attack, it logs an informative message and it generates a SNMP Trap (if you have configured a Trap receiver). The unit generates only one log message and trap per detection cycle (Maximum 8 per polling cycle) on each applicable unit that contains unit and port information.

Automatic QoS

Automatic QoS support provides the ability to easily identify and prioritize Avaya application traffic on Avaya data infrastructure. Automatic QoS gives users the ability to enable or disable Automatic QoS support for the whole system. The user is not able to enable and disable this feature on individual units and ports. When a user enables Automatic QoS support the switch associates additional filtering components with all of the supported interfaces classes: Untrusted/Access, untrustedv4v6/Access, Trusted/Core and Unrestricted. These additional filtering components target ingress traffic with the designated private AQ DSCP values. When

a match occurs, the switch gives traffic preferred egress queuing within the system and remarks it for appropriate downstream processing.

DSCP remarking occurs when the data infrastructure consists of AQ and non-AQ equipment. The Automatic QoS value determines whether the switch ignores AQ DSCP values, maintains them or remarks at egress.

To ensure proper treatment of AQ application traffic, the following DSCP-to-CoS mapping updates need to be made to facilitate preferred treatment for AQ application traffic:

- Set the in-use drop precedence values that the switch associates with Trusted filters and DSCP Mapping Table entries to High. This allows the AQ application traffic with a Low drop precedence value to receive preferential treatment when shared egress queues are congested.
- Mapping information loaded into hardware or enforced using filters needs to take into account the AQ application mode. If enabled, mapping information associated with private AQ DSCP values needs to take precedence over user-defined DSCP mapping data. If disabled, private AQ DSCP data is not used for initialization purposes.
- DSCP-to-COS mapping data is user configurable. When you enable the AQ application mode, the switch allows modification of entries that correspond to private AQ DSCP values but they are not installed in hardware or used to update installed filters to ensure proper Automatic QoS operation.

Automatic QoS operation may consume additional policy and filter resources depending on the platform and QoS configuration. There are scenarios where the switch rejects enabling Automatic QoS support. Avaya advises users to enable or disable the feature prior to configuring applications that share these limited resources to avoid these complications.

Certain roles and the associated default interface class processing policies are exempt from the Automatic QoS augmentation. These special purpose roles are system-owned and Avaya automatic QoS functionality is outside the current scope of usage.

*** Note:**

ASCII running config files previous to Release 6.2.0 may have auto qos configured as `qos agent nt-mode`. For this configuration to work on newer software versions, you must change `qos agent nt-mode` into `qos agent aq-mode`.

Precedence values

In some instances, precedence value allocations may interfere with QoS operations. Precedence values associated with QoS operations are static and assigned during the configuration process. The switch dynamically assigns precedence values after each reset of the device on non-QoS operations like RIP. Since both operation groups use the same pool of precedence values, conflicts can occur during a the configuration or initialization process when a QoS operation accesses a precedence value assumed by a non-QoS operation. The device

resolves these conflicts internally but the conflicts can seem to the end user to be error situations. These conflicts occur in one of the following general scenarios:

- During the configuration of a QoS operation, the device designates a precedence value that is already consumed by a non-QoS operation. The configuration command fails because the precedence value is already in use. Although this can seem to be an error situation to the end user, it is in fact a valid scenario since the precedence value is already consumed.
- After the reset of a device, the device assigns to a non-QoS operation a precedence value that was previously consumed by a QoS operation. The non-QoS operation assumes this precedence value and causes the statically assigned QoS operation to fail on start up. This appears to be an error situation to the end user but it is in fact a valid scenario since the precedence value is already consumed.

Both of these scenarios can be avoided by configuring non-QoS operations prior to the configuration of QoS operations.

! Important:

Traffic profile filter sets and User Based Policies use dynamic precedence allocation.

QoS errors in ACLI

When you apply incorrect QoS policies, apply policies to an incorrect unit, or create invalid elements, the system displays errors in EDM or ACLI. If the system cannot display the root cause of an error as a one line message, and if the error is made using ACLI, it appears as a Logs Message.

The errors can be seen for QoS, Traffic Profile, UBP, NSNA miss-configurations.

If the QoS configuration error is no more than one line and is an uncomplicated error such as, for example, deleting, enabling or disabling an invalid filter set, then the system displays it directly on the interface.

Chapter 4: Configuring Quality of Service (QoS) with ACLI

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

*** Note:**

When you use the ignore value in QoS, the system matches all values for that parameter.

QoS configurations are kept on the base unit. When a standalone unit joins a stack, the QoS configurations on the newly inserted unit are lost with the exception of interface specific settings: interface class assignment, interface applications, and interface queue shaping. The base unit must have some parameters already configured: token bucket for shaping or the settings are lost, and interface group for assignment or the port(s) is disabled.

Displaying QoS parameters

Use this procedure to display QoS parameters.

Procedure steps

1. Log on to 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 [unit] |  
egressmap [ds| status] | filter-limiting | if-action-extension  
[user | system | all | <1-65535>] | if-assign [port] | if-  
group | if-queue-shaper [port] | 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>] | l2-element [<1-65535> all | system | user]>  
| meter [user | system | all | <1-65535>] | nsna | policy  
[user | system | all | <1-65535>] | port <LINE> | queue-set |
```

```
queue-set-assignment | statistics <1-65535> | system-element
[user | system | all | <1-65535>] | ubp | user-policy}
```

Variable definitions

Variable	Value
acl-assign <1 - 65535>	Displays the specified access list assignment entry. <ul style="list-style-type: none"> • <1-65535>— displays a particular entry.
action [<1-65535> all system user]	Displays the base action entries. The applicable values are: <ul style="list-style-type: none"> • <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. The default is all.
agent <details>	Displays the global QoS parameters. details— displays the policy class support table.
arp spoofing	Displays QoS ARP spoofing prevention settings. This parameter applies only to the ERS 5500 Series.
bpdu blocker	Displays QoS BPDU settings. blocker— displays QoS BPDU blocker settings. This parameter applies only to the ERS 5500 Series.
capability [meter shaper]	Displays the current QoS meter and shaper capabilities of each interface. The applicable values are: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • <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. The default is all.
classifier-block [<1-65535> all system user]	Displays the classifier block entries. The applicable values are: <ul style="list-style-type: none"> • <1-65535>— displays a particular entry. • all— displays all user-created, default, and system entries.

Variable	Value
	<ul style="list-style-type: none"> • system— displays only system entries. • user— displays only user-created and default entries. The default is all.
dhcp [snooping spoofing]	Displays QoS DHCP settings. The applicable values are: <ul style="list-style-type: none"> • snooping— displays QoS DHCP snooping settings. • spoofing— displays QoS DHCP spoofing prevention settings. This parameter applies only to the ERS 5500 Series.
diag [unit]	Displays the diagnostics entries. unit <1-8>— displays diagnostic entries for particular unit
dos [nachia sqlslam tcp-dnsport tcp-ftpport tcp-synfinscan xmas]	Displays QoS DoS settings. The applicable values are: <ul style="list-style-type: none"> • nachia— displays QoS DoS Nachia settings. • sqlslam— displays QoS DoS SQLSlam settings. • tcp-dnsport— displays QoS DoS TCP DnsPort settings. • tcp-ftpport— displays QoS DoS TCP FtpPort settings. • tcp-synfinscan— displays QoS DoS TCP SynFinScan settings. • xmas— displays QoS DoS Xmas settings. This parameter applies only to the ERS 5500 Series.
filter-limiting	Enable (default) or disable to limit the number of user defined protocol VLANs. <ul style="list-style-type: none"> • When enabled, there can be created a maximum 7 user-defined protocol VLANs. • When disabled, there can be created a maximum 16 user-defined protocol VLANs. <p>! Important: If you disable Filter Limiting, the ERS 5510 unit cannot join the stack. The ERS 5510 supports only maximum 7 user-defined protocol VLANs.</p>
if-action-extension [<1-65535> all system user]	Displays the interface action extension entries. The applicable values are: <ul style="list-style-type: none"> • <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.

Variable	Value
	The default is 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-queue-shaper [port]	Displays the QoS interface queue shaper.
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. • <1-65535>— displays a particular 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. The default is all.
l2-acl <1 - 65535>	Displays the specified Layer 2 access list assignment entry. • <1-65535>— displays a particular 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. The default is 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. The default is all.

Variable	Value
nsna [classifier interface name]	Displays QoS NSNA entries. The applicable values are: <ul style="list-style-type: none"> • classifier— displays QoS NSNA classifier entries. • interface— displays QoS NSNA interface entries. • name— specifies the label to display a particular NSNA template entry.
policy [<1-65535> all system user]	Displays the policy entries. The applicable values are: <ul style="list-style-type: none"> • <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. The default is all.
port	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. <ul style="list-style-type: none"> • <1-65535>— displays a particular entry.
system-element [<1-65535> all system user]	Displays the system classifier element entries. The applicable values are: <ul style="list-style-type: none"> • <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.
ubp [classifier interface name]	Displays QoS UBP entries. The applicable values are: <ul style="list-style-type: none"> • classifier— displays QoS UBP classifier entries. • interface— displays QoS UBP interface entries. • name— specifies the label to display a particular UBP template entry.
user-policy	Displays QoS user policy entries.

Displaying QoS capability and policy configuration

Use this procedure to display QoS meter and shaper capabilities for system ports.

Procedure steps

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

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 detailed in this section allow for the configuration and management of QoS access lists.

You cannot meter specific traffic using access lists.

*** Note:**

QoS access list have an implicit drop-all at the end of the list. For specific L3 traffic to pass through, you must create a QoS policy to allow ARP packets on the highest available

precedence (check using `show qos diag`) before creating the access list. See the following sample configuration.

```
qos l2-element 1 ethertype 0x0806
qos classifier 1 set-id 1 element-type l2 element-id 1
qos action 10 drop-action disable
qos policy 1 port <portlist> clfr-type classifier clfr-id 1 in-profile-action 10
precedence 14
```

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 used by other applications that also utilize QoS precedences. Applications that utilize QoS precedences on the ERS 5000 include ARP, DHCP, UDP Forwarding, MAC Security, and Port Mirroring.

On the ERS 5000, by default, the device reserves four out of the 16 QoS precedences for ARP, DHCP, and two default QoS policies (UntrustedClfrs1 and UntrustedClfrs2), which leaves only 12 QoS precedences available.

You can use the `show qos diag` command to view which QoS precedences the device uses.

In the following example, the `show qos diag` output displays that ARP, DHCP, and two default QoS policies (UntrustedClfrs1 and UntrustedClfrs2) use four out of the 16 QoS precedences, which leaves only twelve QoS precedences available; therefore, you can only apply an IP or Layer 2 ACL policy with twelve IP or Layer 2 classifier elements to a port.

```
5000# show qos diag
Unit/Port      Mask Precedence Usage
-----
1/1            AR  DH                      Q  Q
AR=ARP DH=DHCP Q=QoS
```

With only 12 available QoS precedences, if you create thirteen IP or Layer 2 classifier elements in an IP or Layer 2 ACL and you attempt to apply the ACL to a port, the ERS 5000 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 Layer 2 ACL before you can apply the ACL to a port.

Use this procedure to assign ports to an access list.

Procedure steps

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

```
qos acl-assign port <port_list> acl-type {ip | l2} name
<name>
```

Variable definitions

Variable	Value
port <port_list>	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.
name <name>	Specifies the name of the access list to be used. You must configure access lists before you can assign ports to them.

Removing an access list assignment

Use this procedure to remove an access list assignment.

Procedure steps

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

```
no qos acl-assign <aclassignid>
```

Creating an IP access list or Layer 2 access list

When you create IP or Layer 2 classifier elements for IP or Layer 2 ACLs on the ERS 5000 with the command `config qos ip-acl` or `config qos l2-acl`, you may encounter the following error:

```
% Cannot modify settings
% Access element cluster count (16) exceeds limit (15)
```

This error message indicates that you have exceeded the amount of QoS precedences available for IP or Layer 2 ACLs in the ERS 5000. The system limits the number of IP and Layer 2 ACLs that you can create by the number of available QoS precedences. Although

there are 16 QoS precedences available, ARP permanently occupies the sixteenth precedence, and thus leaves only 15 valid precedences available for IP or Layer 2 classifier element creation.

Creating an IP access list

Use this procedure to create an IP access list.

Procedure steps

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

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

*** Note:**

Possible values for src-port-max and dst-port-max are based on the binary value of the respective port-min, and are obtained by replacing consecutive trailing zeros in this binary value with ones, starting at the right-most position. For example, if port-min = 200, then there are 4 possible values for port-max: 11001000 (200) 11001001 (201) 11001011 (203) 11001111 (207) The value of port-max is $\text{port-min} + 2^n - 1$, where n is the number of consecutive trailing zeros replaced. This information applies only to the ERS 5500 Series switch.

Variable definitions

Variable	Value
name <name>	Specifies the name assigned to this access list.
addr-type <addrtype>	Specifies the IP address type to use for the access list.
src-ip <source_ip>	Specifies the source IP address to use for this access list.
dst-ip <destination_ip>	Specifies the destination IP address to use for this access list.
ds-field <dscp>	Specifies the Differentiated Services Code Point (DSCP) value to use for this access list.
{protocol <protocol_type> next_header <header>}	Specifies the protocol type or IP header to use with this access list.
src-port-min <port> src-port-max <port>	Specifies the minimum and maximum source ports to use with this access list. Both values must be specified.
dst-port-min <port> dst-port-max <port>	Specifies the minimum and maximum destination ports to use with the access list. Both values must be specified.
flow-id <flowid>	Specifies the flow ID to use with this access list.
drop-action {drop pass}	Specifies the drop action to use for this access list.
update-dscp <0 - 63>	Specifies the DSCP value to update for this access list.
update-1p <0 - 7>	Specifies the 802.1p value to update for this access list.
set-drop-prec {high drop low drop}	Specifies the drop precedence to configure for this access list.
block <block_name>	Specifies the block name to associate with the access list.

Removing an IP access list

Use this procedure to remove an IP access list.

Procedure steps

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

```
no qos ip-acl <aclid>
```

Creating a Layer 2 access list

Use this procedure to create a Layer 2 access list.

Procedure steps

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

```

qos l2-acl name <name>
[src-mac <source_mac_address>]
[src-mac-mask
<source_mac_address_mask>]
[dst-mac <destination_mac_address>]
[dst-mac-mask <destination_mac_address_mask>]
[vlan-min <vid_min>
vlan-max <vid_max>]
[vlan-tag <vtag>]
[ethertype <etype>]
[priority <ieee1p_seq>]
[drop-action {drop | pass}]
[update-dscp <0-63>]
[update-lp <0-7>]
[set-drop-prec {high-drop | low-drop}]
[block <block_name>]

```

*** Note:**

Possible values for vlan-max are based on the binary value of vlan-min, and are obtained by replacing consecutive trailing zeros in this binary value with ones, starting at the right-most position. For example, if vlan-min = 200, then there are 4 possible values for vlan-max: 11001000 (200) 11001001 (201) 11001011 (203) 11001111 (207) The value of vlan-max is $\text{vlan-min} + 2^n - 1$, where n is the number of consecutive trailing zeros replaced.

Variable definitions

Variable	Value
name <name>	Specifies the name assigned to this access list.
src-mac <source_mac_address>	Specifies the source MAC address to use for this access list.

Variable	Value
src-mac-mask <source_mac_address_mask>	Specifies the source MAC address mask to use for this access list.
[dst-mac <destination_mac_addresses>]	Specifies the destination MAC address to use for this access list.
dst-mac-mask <destination_mac_address_mask>	Specifies the destination MAC address mask to use for this access list.
vlan-min <vid_min> vlan-max <vid_max>	Specifies the minimum and maximum VLANs to use with this access list. Both values must be specified.
vlan-tag <vtag>	Specifies the VLAN tag to use with this access list.
ethertype <etype>	Specifies the Ethernet protocol type to use with the access list.
priority <ieee1p_seq>	Specifies the priority value to use with this access list.
drop-action {drop pass}	Specifies the drop action to use for this access list.
update-dscp <0 - 63>	Specifies the DSCP value to update for this access list.
update-1p <0 - 7>	Specifies the 802.1p value to update for this access list.
set-drop-prec {high-drop low-drop}	Specifies the drop precedence to configure for this access list.
block <block_name>	Specifies the block name to associate with the access list.

Removing a Layer 2 access list

Use this procedure to remove a Layer 2 access list.

Procedure steps

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

```
no qos l2-acl <aclid>
```

Configuring QoS security

The ACLI commands detailed in this section allow for the configuration and management of QoS security settings. For information on displaying this information, refer to [Displaying QoS parameters](#) on page 49.

*** Note:**

Due to hardware limitations, and in a default configuration, the Ethernet Routing Switch 5500 Series model only supports 11 QoS security applications per port.

Enabling QoS ARP spoofing

Use this procedure to enable the QoS ARP spoofing application on the designated switch ports. This command applies to the ERS 5500 Series switch only.

Procedure steps

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

```
qos arp spoofing [port <port_list>] enable default-gateway
<A.B.C.D>
```

Variable definitions

Variable	Value
port <port_list>	Specifies the list of ports on which to enable the QoS ARP spoofing application.
default-gateway <A.B.C.D>	Specifies the IP address of the default gateway to use.

Disabling QoS ARP spoofing

Use this procedure to disable the QoS ARP spoofing application on the designated switch ports. This command applies to the ERS 5500 Series switch only.

Procedure steps

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

```
no qos arp spoofing port <port_list>
```

Enabling QoS BPDU blocker

Use this procedure to enable the QoS BPDU blocker application on the designated switch ports. This command applies to the ERS 5500 Series switch only.

Procedure steps

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

```
qos bpdu blocker port <port_list> enable
```

Disabling QoS BPDU blocker

Use this procedure to disable the QoS BPDU blocker application on the designated switch ports. This command applies to the ERS 5500 Series switch only.

Procedure steps

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

```
no qos bpdu blocker port <port_list>
```

Enabling QoS DHCP snooping and spoofing

Use this procedure to enable QoS DHCP snooping and spoofing applications on the designated switch ports. This command applies to the ERS 5500 Series switch only.

Procedure steps

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


```
qos dhcp snooping port <port_list> enable interface-type
{access | core}
```
3. At the command prompt, enter the following command to enable spoofing:


```
qos dhcp spoofing port <port_list> enable dhcp-server
<A.B.C.D>
```

Variable definitions

Variable	Value
port <port_list>	Specifies the ports to enable the selected QoS DHCP application on.
interface-type {access core}	Specifies the interface type to use.

Disabling QoS DHCP snooping and spoofing

Use this procedure to disable QoS DHCP snooping and spoofing applications on the designated switch ports. This command applies to the ERS 5500 Series switch only.

Procedure steps

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


```
no qos dhcp snooping port <port_list>
```
3. At the command prompt, enter the following command to disable spoofing:


```
no qos dhcp spoofing port <port_list>
```

Variable definitions

Variable	Value
port <port_list>	Specifies the ports to disable the selected QoS DHCP application on.

Enabling QoS DoS applications

Use this procedure to enable QoS DoS applications on the designated switch ports. This command applies to the ERS 5500 Series switch only.

Procedure steps

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

```
qos dos {nachia | sqlslam | tcp-dnsport | tcp-ftpport | tcp-  
synfinscan | xmas} port <port_list> enable
```

Variable definitions

Variable	Value
{nachia sqlslam tcp-dnsport tcp-ftpport tcp-synfinscan xmas}	Specifies the type of QoS DoS application to enable on the selected ports.
port <port_list>	Specifies the ports to enable the application on.

Disabling QoS DoS applications

Use this procedure to disable QoS DoS applications on the designated switch ports. This command applies to the ERS 5500 Series switch only.

Procedure steps

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

```
no qos dos {nachia | sqlslam | tcp-dnsport | tcp-ftpport |
tcp-synfinscan | xmas} port <port_list>
```

Variable definitions

Variable	Value
{nachia sqlslam tcp-dnsport tcp-ftpport tcp-synfinscan xmas}	Specifies the type of QoS DoS application to disable on the selected ports.
port <port_list>	Specifies the ports to disable the application on.

QoS agent configuration

ACLI commands detailed in this section allow for the configuration and management of the QoS agent.

Enabling and disabling QoS agent support globally

Use this procedure to globally enable or disable QoS agent support. The commands used in this procedure are available in Global Configuration mode.

Procedure steps

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command to enable QoS Agent support globally:

```
qos agent oper-mode [enable]
```

OR

```
default qos agent [oper-mode]
```

- At the command prompt, enter the following command to disable QoS agent support globally:

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

The device enables QoS agent by default. You cannot disable QoS agent support if NSNA or UBP use QoS functionality.

Variable definitions

Variable	Value
enable	Enables QoS Agent functionality for the system.
disable	Disables QoS Agent functionality for the system.

Configuring QoS agent

Use this procedure to configure QoS agent parameters.

Procedure steps

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

```
qos agent [buffer | dos-attack-prevention | aq-mode | nvram-
delay | oper-mode | queue-set | reset-default | reset-
partial-default | statistics-tracking | trusted-mode | ubp]
```

*** Note:**

If you change the QoS agent queue-set or buffer parameters, you need to perform a system reset for the new settings to be applied. If you have queue-set or buffer parameters in the ASCII running config files, you must manually change the settings and perform a reset.

Variable definitions

Variable	Value
aq-mode	Specifies the automatic QoS application traffic processing mode.

Variable	Value
buffer	Specifies the QoS resource buffer allocation.
dos-attack-prevention	Enables QoS DoS Attack Prevention. This parameter is only available on the 5600 Series switch.
nvr-am-delay	Specifies the maximum time in seconds to write configuration data to a nonvolatile storage.
oper-mode	Enables the QoS operational mode.
queue-set	Specifies the default QoS CoS queue set.
reset-default	Restores QoS to configuration default.
reset-partial-default	Restores QoS to partial configuration default.
statistics-tracking	Specifies default QoS statistics tracking.
trusted-mode	Specifies the QoS trusted processing mode. The trusted-mode parameter is available only for a mixed stack of ERS 5500 series switches.
ubp	Specifies the QoS UBP support level.

Configuring QoS agent to default

Use this procedure to configure QoS agent parameters to factory default values.

Procedure steps

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

```
default qos agent [buffer | dos-attack-prevention | aq-mode |
nvr-am-delay | oper-mode | queue-set | statistics-tracking |
trusted-mode | ubp]
```

*** Note:**

The default qos agent command has the same result as the qos agent reset-default command.

Variable definitions

Variable	Value
buffer	Restores default QoS resource buffer allocation.
dos-attack-prevention	Restores default QoS DoS attack prevention. This parameter is only available on the ERS 5600 Series switch.
aq-mode	Restores default auto QoS application traffic processing mode.
nvr-am-delay	Restores default maximum time in seconds to write configuration data to a nonvolatile storage.
oper-mode	Restores the QoS operational mode to default.
queue-set	Restores default QoS queue set.
statistics-tracking	Restores default QoS statistics tracking support.
trusted-mode	Restores the QoS trusted processing mode to default. The trusted-mode parameter is available only for a mixed stack of ERS 5500 Series switches.
ubp	Restores default QoS UBP support level.

Viewing QoS agent configuration information

Use this procedure to display the QoS agent parameter configuration.

Procedure steps

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

```
show qos agent
```

Job aid: show qos agent command output

The following displays sample `show qos agent` command output for a mixed stack of ERS 5500 series switches.

```
5530-24TFD#show qos agent
QoS Operational Mode: Enabled
QoS NVRam Commit Delay: 10 seconds
QoS Current Queue Set: 2
```

```
QoS Next Boot Queue Set: 2
QoS Current Buffering: Large
QoS Next Boot Buffering: Large
QoS UBP Support Level: Disabled
QoS Default Statistics Tracking: Aggregate
QoS DOS Attack Prevention: Disabled
  Minimum TCP Header Length: 20
  Maximum IPv4 ICMP Length: 512
  Maximum IPv6 ICMP Length: 512
Auto QoS Mode: Disabled
QoS Trusted Processing Mode: Partial
```

Modifying default queue configuration

Use this procedure to modify the default queue configuration.

Procedure steps

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

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

*** Note:**

The queue-set value sets the number of queues in a queue set for each port type. The default value is 2.

Configuring default buffering capabilities

Use this procedure to display and modify the buffer allocation mode.

Configuring default QoS resource buffer

Use this procedure to allocate the default QoS resource buffer.

Procedure steps

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

```
default qos agent buffer
```

Modifying QoS resource buffer allocation

Use this procedure to modify QoS resource buffer allocation.

Procedure steps

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

```
qos agent buffer <regular | large | maximum>
```

Variable definitions

Variable	Value
buffer	<p>Modifies the QoS resource buffer allocation. The allowed buffer allocation modes for all QoS interfaces are as follows:</p> <ul style="list-style-type: none">• regular• large• maximum <p>* Note:</p> <p>The buffer mode determines the level of resource sharing across interfaces sharing the same port hardware.</p>

Enabling lossless buffering mode

Use this procedure to enable lossless buffering mode on ERS 5600 Series switches.

Procedure steps

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

```
qos agent buffer lossless
```

Configuring the CoS-to-queue assignments

Use this procedure to display and modify the CoS-to-queue assignments.

Configuring 802.1p priority values

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

Procedure steps

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 <1-56> 1p <0-7> queue
<1-8>
```

Variable definitions

Variable	Value
queue-set <1-56>	Specifies the queue-set. The value ranges are from 1–56.
1p <0-7>	Specifies the 802.1p priority value for which the queue association is being modified. The value ranges are from 0–7.
queue <1-8>	Specifies the queue within the identified queue set to assign the 802.1p priority traffic at egress. The value ranges are from 1–8.

Configuring QoS interface groups

Use the procedures in this section to add or delete ports to or from an interface group, or add or delete the interface groups themselves.

Configuring ports for an interface group

Use this procedure to add ports to a defined interface group.

Procedure steps

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>]
```

*** Note:**

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

Variable definitions

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

Removing ports from an interface group

Use this procedure to delete ports from a defined interface group.

Procedure steps

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

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

*** Note:**

If you do not associate ports with an interface they are considered QoS disabled and you cannot apply QoS operations until you assign them to an interface group.

Creating an interface group

Use this procedure to create interface groups.

Procedure steps

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

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

Variable definitions

Variable	Value
name <WORD>	Specifies the name of the interface group; maximum is 32 US-ASCII. Name must begin with a letter a..z or A..Z.
class <trusted untrusted untrustedv4v6 unrestricted>	Defines a new interface group and specifies the class of traffic received on interfaces associated with this interface group: <ul style="list-style-type: none"> • trusted • untrusted • unrestricted • untrustedv4v6

Removing an interface group

Use this procedure to delete interface groups.

Procedure steps

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>
```

*** Note:**

If you reference an installed policy with an interface group, you cannot delete the interface group.

*** Note:**

If you associate an interface group with ports, you cannot delete the interface group.

Configuring DSCP and 802.1p and queue associations

This section contains procedures to configure DSCP, 802.1p priority and queue set associations.

Configuring DSCP to 802.1p priority

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

Procedure steps

1. 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>] [1p <0-7>] [dp <low-drop | high-drop>] [ds-new < 0-63>]
```

Variable definitions

Variable	Value
name <WORD>	Specifies the label for the egress mapping.
ds <0-63>	Specifies the DSCP value to use as a lookup key for 802.1p priority and drop precedence at egress when appropriate. The range is between 0 and 63.
1p <0-7>	Specifies the 802.1p priority value to associate with the DSCP. The range is between 0 and 7.
dp <low-drop high-drop>	Specifies the drop precedence values to associate with the DSCP:

Variable	Value
	<ul style="list-style-type: none"> • low-drop • high-drop
ds-new <0-63>	Specifies a new DSCP value to use when DSCP mutation is required. Values range from 0–63.

Restoring egress mapping entries to default

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

Procedure steps

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 this procedure to configure 802.1p priority-to-DSCP associations to assign default values at packet ingress based on the 802.1p value in the ingressing packet.

Procedure steps

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

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

Variable	Value
ds <0-63>	Specifies the DSCP value to associate with the target 802.1p priority. The range is between 0 and 63.

Restoring ingress mapping entries to default

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

Procedure steps

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

Use the ACLI commands in this section to configure elements, classifiers, and classifier blocks.

Configuring IP classifier element entries

Use this procedure to add and configure classifier entries.

Procedure steps

1. Log on 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>] [flow-id  
<flowid>] [ip-flag <ip-flags>] [ipv4-options <no-opt | with-  
opt>] [next-header <nexthead>] [session-id] [src-ip <src-  
ip-info>] [src-port-min <port>] [tcp-control <tcp-flags>]
```

Variable definitions

Variable	Value
<cid>	Specifies the element ID. The range is from 1–55000.
addr-type <addrtype>	Specifies the address type. Use the value ipv4 to indicate an IPv4 address or the value ipv6 to indicate an IPv6 address. The default value is ipv4.
ds-field <0-63>	Specifies a 6-bit DSCP value. The range is from 0–63. The default is ignore.
dst-ip <dst-ip-info>	Specifies the source IP address and mask in the form of a.b.c.d/x for IPv4, or x:x:x:x:x:x/z for IPv6. Default is 0.0.0.0.
dst-port-min <port>	Specifies the Layer 4 destination port minimum value.
flow-id <flowid>	Specifies the IPv6 flow identifier.
ip-flag <ip-flags>	Specifies the flags present in an IPv4 header.
ipv4-options <no-opt with-opt>	<p>Specifies whether the Option field is present in the packet header. Valid values are:</p> <ul style="list-style-type: none"> • no-opt— Indicates that only IPv4 packets without options will match this classifier element. • with-opt— Indicates that only IPv4 packets with options will match this classifier element. <p>IPv4 packets with ipv4-options are not matched on a ERS 5000 Series switch.</p>
next-header	Specifies the IPv6 next header classifier criteria. The range is 0–255.
src-ip <src-ip-info>	Specifies the source IP address and mask in the form of a.b.c.d/x for IPv4, or x:x:x:x:x:x/z for IPv6. The default is 0.0.0.0.
session-id	Specifies the session ID.
src-port-min <port>	Specifies the Layer 4 source port minimum value.
tcp-control <tcp-flags>	Specifies the control flags present in a TCP header.

Viewing IP classifier entries

Use this procedure to view IP classifier entries.

Procedure steps

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

```
show qos ip-element [<1-65535>] [all] [system] [user]
```

Removing IP classifier entries

Use this procedure to remove IP classifier entries.

Procedure steps

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:**

If you reference an IP element in a classifier, then you cannot delete the IP element.

Adding Layer 2 elements

Use this procedure to add Layer 2 elements.

Procedure steps

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>] [pkt-type <etherII | llc  
| snap>] [priority <ieeelp-seq>] [session-id <session-id>]  
[src-mac <src-mac>] [src-mac-mask <src-mac-mask>] [vlan-min  
<vid-min>] [vlan-max <vid-max>][vlan-tag <vtag>]
```

*** Note:**

If you reference a Layer 2 element in a classifier, you cannot delete the Layer 2 element.

Variable definitions

Variable	Value
<1-55000>	Specifies the element ID. The 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. The default is ignore.
pkt-type <etherII llc snap>	Specifies the packet frame format. <ul style="list-style-type: none"> • etherII— Indicates that only Ethernet II format frames match this classifier component. • snap— Indicates that only IEEE 802 SNAP format frames match this classifier component. • llc— Indicates that only IEEE 802 LLC format frames match this classifier component.
priority <ieee1p-seq>	Specifies the 802.1p priority values. The range is from 0–7 or all. The default is ignore.
session-id <session-id>	Specifies the session ID.
src-mac <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.
vlan-min <vid-min>	Specifies the VLAN ID minimum value element criteria. The range is 1–4094.
vlan-max <vid-max>	Specifies the VLAN ID maximum value element criteria. The range is 1–4094.
vlan-tag <format>	Specifies the packet format element criteria: <ul style="list-style-type: none"> • untagged • tagged The default is ignore.

Viewing Layer 2 elements

Use this procedure to view Layer 2 elements.

Procedure steps

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]
```

Removing Layer 2 elements

Use this procedure to delete Layer 2 element entries.

Procedure steps

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>
```

Linking IP and L2 classifier elements

Use this procedure to link IP and Layer 2 classifier elements.

Procedure steps

1. Log on to the Global Configuration mode.
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>
```

*** Note:**

If you reference a classifier in a classifier block or an installed policy, then you cannot delete the classifier.

Variable definitions

Variable	Value
classifier <1-55000>	Specifies the classifier ID. The range is 1–55000.
set-id <1-55000>	Specifies the classifier set ID. The range is 1–55000.
name <WORD>	Specifies the set label. The maximum is 16 alphanumeric characters.
element-type {ip l2 system}	Specifies the element type, which is either ip or l2, or system classifier.
element-id <1-55000>	Specifies the element ID. The range is 1–55000.

Removing classifier entries

Use this procedure to delete classifier entries.

Procedure steps

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

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

*** Note:**

Each classifier can have only a single IP classifier element plus a single Layer 2 classifier element or system classifier element. However, a classifier can be created using only one IP classifier element or only one Layer 2 classifier element or only one system classifier element.

Combining individual classifiers

Use this procedure to combine individual classifiers.

Procedure steps

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

*** Note:**

If you reference a classifier block in an installed policy, then you cannot delete the classifier block.

Variable definitions

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

Removing classifier block entries

Use this procedure to delete classifier block entries.

Procedure steps

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

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

Configuring QoS system-element

Configuring system classifier element parameters

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

Procedure steps

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

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

*** Note:**

On the ERS 5500 Series switch, when the untagged format is used the last 4 bytes (77 to 80) from data/mask pattern are reserved by the hardware and should not be configured.

On the ERS 5600 Series switch, when the untagged format is used the last 4 bytes (125-128) from data/mask pattern are reserved by the hardware and should not be configured.

Variable definitions

Variable	Value
<1-55000>	Specifies the system classifier element entry id. The range is 1–55000.
known-ip-mcast	Specifies the filter on known multicast destination address. This parameter is applicable only on ERS 5600 Series switches.
known-mcast	Specifies the filter on known multicast destination address. This parameter is applicable only on ERS 5500 Series switches.
known-non-ip-mcast	Specifies the filter on known non IP multicast destination address. This parameter is applicable only on ERS 5600 Series switches.
unknown-ip-mcast	Specifies the filter on unknown multicast destination address. This parameter is applicable only on ERS 5600 Series switches.
unknown-mcast	Specifies the filter on unknown multicast destination address. This parameter is applicable only on ERS 5500 Series switches.
unknown-ucast	Specifies the Filter on unknown unicast destination address. This parameter is applicable on both ERS 5500 and ERS 5600 Series switches.
unknown-non-ip-mcast	Specifies the filter on unknown non IP multicast destination address. This parameter is applicable only on ERS 5600 Series switches.
non-ip	Specifies the filter on non IP packets as the destination address. This parameter is applicable only on ERS 5600 Series switches.
name <WORD>	Specifies the name of the system element (1 to 16 characters in length).
pattern-format { tagged untagged }	Specifies the format of data/mask pattern. Specifies the available values are: <ul style="list-style-type: none"> • tagged— Data/mask pattern describes a tagged packet • untagged—Data/mask pattern describes an untagged packet
pattern-data <WORD>	Specifies the byte pattern data to filter on.

Variable	Value
	<p>* Note: The format of the WORD string is in the form of XX:XX:XX:.....XX.</p>
pattern-l2-format <ethernetII Ic snap>	<p>Specifies the format of the L2 pattern data and mask. Values include:</p> <ul style="list-style-type: none"> • ethernetII • Ic • snap
pattern-mask <WORD>	<p>Specifies the byte pattern mask to filter on.</p> <p>* Note: The format of the WORD string is in the form of XX:XX:XX:.....XX.</p> <p>* Note: This parameter not applicable to the ERS 5600 Series switch.</p>
pattern-ip-version	<p>Specifies the IP version of the pattern data or mask.</p> <ul style="list-style-type: none"> • ipv4—Filter IPv4 Header • ipv6—Filter IPv6 Header • non-ip—Filter non-ip packets <p>This parameter applies only to the ERS 5600 Series switch.</p>
session-id	Specifies the session ID.

Viewing system classifier elements parameters

Use this procedure to view system classifier elements parameters.

Procedure steps

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

```
show qos system-element [<1-65535>] [all] [system] [user]
```

Removing system classifier element entries

Use this procedure to remove system classifier element entries.

Procedure steps

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>
```

Configuring QoS actions

Use this section to configure QoS actions. The configuration of QoS actions directs the Avaya Ethernet Routing Switch 5000 Series to take specific action on each packet.

Creating and updating QoS actions

Use this procedure to create and update QoS actions.

Procedure steps

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-lp  
{<0-7> | use-tos-prec | use-egress}] [set-drop-prec <low-drop  
| high-drop>] [action-ext <1-55000> | action-ext-name <WORD>]
```

*** Note:**

You can restrict certain options based on the policy you associate with the specific action. You cannot delete an action that you reference in a meter or an installed policy.

Variable definitions

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. The maximum is 16 alphanumeric characters.
drop-action<enable disable deferred-pass>	<p>Specifies whether packets are dropped or not:</p> <ul style="list-style-type: none"> • enable— Drop the traffic flow • disable— Do not drop the traffic flow • deferred-pass—Traffic flow decision deferred to other installed policies <p>The default is deferred pass.</p> <p>* Note: If you omit this parameter, the default value applies.</p>
update-dscp <0-63>	<p>Specifies whether the DSCP values are updated or left unchanged; unchanged equals ignore. Enter the 6-bit DSCP value. The range is 0 to 63.</p> <p>The default is ignore.</p>
update-1p<0-7>	<p>Specifies whether 802.1p priority value are updated or left unchanged; unchanged equals ignore:</p> <ul style="list-style-type: none"> • 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. <p>The default is ignore.</p> <p>* Note: You must specify the <code>update-dscp</code> value.</p>
set-drop-prec <low-drop high-drop>	<p>Specifies the drop precedence value:</p> <ul style="list-style-type: none"> • low-drop • high-drop <p>The default is low-drop.</p>
action-ext <1-55000>	Specifies the action extension. The range is 1–55000.
action-ext-name <WORD>	Specifies a label for the action extension. The maximum is 16 alphanumeric characters.

Removing QoS actions

Use this procedure to delete QoS action entries.

Procedure steps

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

```
no qos action <10-55000>
```

*** Note:**

You cannot delete an action if you reference it with a policy, classifier block, or meter.

Configuring QoS interface action extensions

Use this procedure to configure QoS interface action extensions. QoS interface action extensions direct the Avaya Ethernet Routing Switch 5000 Series to take specific action on each packet.

Creating interface action extension entries

Use this procedure to create interface action extension entries.

Procedure steps

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>}
```

*** Note:**

If you reference an interface extension in an action entry, then you cannot delete it.

*** Note:**

The ERS 5600 Series switch requires that both egress-ucast and egress-non-ucast be specified with the same port.

Variable definitions

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. The maximum is 16 alphanumeric characters
egress-ucast <port> egress-non-ucast <port>	Specifies redirection of unicast/non-unicast to the specified port.

Removing interface action extension entries

Use this procedure to remove interface action extension entries.

Procedure steps

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>
```

Configuring QoS meters

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

Creating QoS meter entries

Use this procedure to create QoS meter entries.

Procedure steps

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>}
```

Variable definitions

Variable	Value
<1-5000>	Specifies the QoS meter. The range is 1–55000.
name <WORD>	Specifies name for meter. The maximum is 16 alphanumeric characters.
committed-rate <64-10230000>	Specifies rate that traffic must not exceed for extended periods to be considered in-profile. Enter the rate in Kb/s for in-profile traffic in increments of 1000 Kbits/sec. The range is 64 to 10230000 Kbits/sec.
burst-size <4,8,16,...,16384>	Committed burst size in Kilobytes. The value range is: 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384.
max-burst-rate <64-4294967295>	Specifies the largest burst of traffic that the device can receive in 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 the device can receive for the traffic to be considered in-profile. Used in calculating the committed burst size. Enter the burst duration in milliseconds for in-profile traffic The range is 1–4294967295 milliseconds.
in-profile-action <1-55000>	Specifies the in-profile action ID. The range is 1–55000.
in-profile-action-name <WORD>	Specifies the in-profile action name.
out-profile-action <1,9-55000>	Specifies the out-of-profile action ID. The range is 1,9 to 55000.

Variable	Value
out-profile-action-name <word>	Specifies the out of profile action name.

Removing QoS meter entries

Use this procedure to delete QoS meter entries.

Procedure steps

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

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

*** Note:**

If you reference a meter in an installed policy or classifier block you cannot delete the meter.

Configuring QoS interface shaper

Configuring interface shaping

Use this procedure to configure interface shaping.

Procedure steps

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 <burst-size> max-burst-rate
<64-4294967295> [max-burst-duration <1-4294967295>]}
```

Variable definitions

Variable	Value
burst-size <4,8,16, ..., 16384>	Specifies the committed burst size in Kilobytes. The value range is: 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384.
port <portlist>	Specifies the ports to configure shaping parameters.
name <WORD>	Specifies name for if-shape. The maximum is 16 alphanumeric characters.
shape-rate <64-10230000>	Specifies the shaping rate in kilobits/sec. The range is 64-10230000 kilobits/sec.
max-burst-rate <64-4294967295>	Specifies the largest burst of traffic that the device can receive at 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. The range is 64 to 4294967295 Kbits/sec.
max-burst-duration <1-4294967295>	Specifies the amount of time that the largest burst of traffic that the device can receive for the traffic to be considered in-profile. Used in calculating the committed burst size. Enter the burst duration in milliseconds for in-profile traffic. The range is 1–4294967295 milliseconds.

Disabling interface shaping

Use this procedure to disable interface shaping.

Procedure steps

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>]
```

Configuring a QoS interface queue shaper

Use the following procedures to configure a QoS queue shaper.

Creating a QoS interface queue shaper

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

Procedure steps

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

```
qos if-queue-shaper [port <portlist>][queue <1-8>][name
<WORD>][shape-rate <64-10230000> shape-min-rate
<64-10230000>
```

Variable definitions

Use the data in the following table to help you use the `qos if-queue-shaper port <portlist> queue <1-8> name <WORD> shape-rate <64-10230000> shape-min-rate <64-10230000>` command.

Variable	Value
name <WORD>	Specifies an alphanumeric label used to identify the QoS interface queue shaper. The value is a character string ranging from 1–16 characters in length.
port <portlist>	Specifies the port or list of ports for which to apply egress queue shaping.
queue <1-8>	Specifies the queue for the selected interface port or ports, on which traffic is shaped. The range of available values is determined by the QoS agent default queue configuration.
shape-min-rate <64-10230000>	Specifies the minimum QoS interface queue shaping rate, in kilobits per second (Kbps). Values range from 0 to 10230000 Kbps. The value must be a multiple of 64 or 1000 Kbps.
shape-rate <64-10230000>	Specifies the QoS interface queue shaping rate, in kilobits per second (Kbps). Values range from 64 to 10230000 Kbps. The value must be a multiple of 64 or 1000 Kbps.

Deleting a QoS interface queue shaper

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

Procedure steps

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


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

Variable definitions

Use the data in the following table to help you use the `no qos if-queue-shaper port <portlist> queue <1-8>` command.

Variable	Value
port <portlist>	Specifies the port or list of ports for which to apply egress queue shaping.
queue <1-8>	Specifies the queue for the selected interface port or ports, on which traffic is shaped. The range of available values is determined by the OoS agent default queue configuration.

Viewing QoS interface queue shaper information

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

Procedure steps

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


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

Variable definitions

Use the data in the following table to help you use the `show qos if-queue-shaper [port <portlist>]` command.

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

Configuring egress mapping

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

Procedure steps

1. 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> 1p <0-7> dp <low-drop|
high-drop> [ds-new <0-63>]
```

Variable definitions

Use the data in the following table to help you use the `qos egressmap name <WORD> ds <0-63> 1p <0-7> dp <low-drop|high-drop> [ds-new <0-63>]` 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. The range is between 0 and 63.
1p <0-7>	Specifies the 802.1p priority value associated with the DSCP. The values range from 0–7.

Variable	Value
dp <low-drop high-drop>	Enter the drop precedence values associated with the DSCP: <ul style="list-style-type: none">• low-drop• high-drop
ds-new <0-63>	Specifies a new DSCP value to use when DSCP mutation is required. The values range from 0–63.

Resetting egress mapping values

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

Procedure steps

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

```
default qos egressmap
```

Configuring QoS policies

Use the following ACLI commands to configure QoS policies.

 **Caution:**

When you define multiple meters that may match the same traffic, you must specify the in-profile and out-of-profile traffic as drop or pass to ensure that the traffic is processed at the prescribed rate. If you do not do this, each meter processes the traffic, and this interaction can cause traffic to be treated in unexpected ways.

Configuring QoS policies

Use this procedure to create and configure QoS policies.

Procedure steps

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

```

qos policy <1-55000>
{enable|disable
[name <WORD>]
[port <port_list> | if-group <WORD>]}
clfr-type {classifier | block}
{clfr-id <1-55000> | clfr-name <WORD>}
{{in-profile-action <1-55000> | in-profile-action-name
<WORD>}
| meter <1-55000> | meter-name <WORD>}} [non-match-action
<1-55000> | non-match-action-name <WORD>] precedence <1-15>
[track-statistics <individual | aggregate>]]

```

* Note:

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

Variable definitions

Table 6: qos policy parameters

Variable	Value
<1-55000>	Specifies the QoS policy. The range is 1–55000.
enable disable	Enables or disables the QoS policy.
name <WORD>	Specifies the name for the policy. The maximum is 16 alphanumeric characters.
port <portlist>	Specifies the ports 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 US-ASCII. 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. The range is 1–55000.
clfr-name <WORD>	Specifies the classifier name or classifier block name. The maximum is 16 alphanumeric characters.

Variable	Value
in-profile-action <1-55000>	Specifies the action ID for in-profile traffic. The range is 1–55000.
in-profile-action-name <WORD>	Specifies the action name for in-profile traffic. The maximum is 16 alphanumeric characters.
meter <1-55000>	Specifies meter ID associated with this policy. The range is 1–55000.
meter-name <WORD>	Specifies the meter name associated with this policy. The maximum of 16 alphanumeric characters.
non-match-action <1-55000>	Specifies the action ID for non-match traffic. The range is 1–55000. This parameter is not applicable to the ERS 5600 Series switches.
non-match-action-name <WORD>	Specifies the action name for non-match traffic. The maximum is 16 alphanumeric characters.
precedence <1-15>	Specifies the precedence of this policy in relation to other policies associated with the same interface group. Enter precedence number. The range is 1–15. <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">* Note:</div> <div>The device evaluates policies with a lower precedence value after policies with a higher precedence number. Evaluation goes from highest value to lowest.</div> </div>
track-statistics <individual aggregate>	Specifies statistics tracking on this policy, either: <ul style="list-style-type: none"> • individual—statistics on individual classifiers • aggregate—aggregate statistics

Job aid: Viewing QoS policies

The following is an example to view the created QoS policy.

```
5530-24TFD(config)#show qos policy 55003
```

```
Id: 55003
Policy Name: no_pc3
State: Enabled
Classifier Type: Classifier
Classifier Name: no_pc3
Classifier Id: 55003
Unit/Port: 1/8
Meter:
Meter Id:
In-Profile Action: no_pc3
```

```

In-Profile Action Id: 55003
Non-Match Action:
Non-Match Action Id:
Track Statistics: Aggregate
Precedence: 13
Session Id: 0
Storage Type: Other

5530-24TFD(config)#show qos policy 55004

Id: 55004
Policy Name: meter_pc3
State: Enabled
Classifier Type: Classifier
Classifier Name: meter_pc3
Classifier Id: 55004
Unit/Port: 1/18
Meter: meter_pc3
Meter Id: 55001
In-Profile Action:
In-Profile Action Id:
Non-Match Action:
Non-Match Action Id:
Track Statistics: Aggregate
Precedence: 13
Session Id: 0
Storage Type: Other

```

Removing QoS policies

Use this procedure to disable QoS policy entries.

Procedure steps

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

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

Configuring QoS traffic profile filter set

This section contains procedures used to configure and manipulate a traffic profile filter set.

Configuring a traffic profile classifier entry

Use this procedure to configure a traffic profile classifier entry using the following procedure.

Caution:

When you define multiple meters that may match the same traffic, you must specify the in-profile and out-of-profile traffic as drop or pass to ensure that the traffic is processed at the prescribed rate. If you do not do this, each meter processes the traffic, and this interaction can cause traffic to be treated in unexpected ways.

Procedure steps

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

```
qos traffic-profile classifier name <name>
```

Variable definitions

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

Variable	Value
name <name>	Specifies the classifier name.
addr-type <addrtype>	Specifies the type of IP address used by this classifier entry. The type is limited to IPv4 and IPv6 addresses.
block <block-name>	Specifies the label to identify access list elements that are of the same block.
committed-rate <64-10230000>	Specifies the committed rate for metering. Values range from 64-10230000 Kbps.
committed-burst-size <burst-size-options>	Specifies the committed burst size in KiloBytes.
drop-action <drop pass>	Specifies whether or not to drop nonconforming traffic.
drop-out-action	Specifies whether to drop (enable) or pass (disable) out of profile packets.
dst-field <dscp>	Specifies the value for the DiffServ Codepoint (DSCP) in a packet.

Variable	Value
dst-ip <dst-ip-info>	Specifies the IP address to match against the destination IP address of a packet.
dst-mac <dst-mac-info>	Specifies the MAC address against which the MAC destination address of incoming packets is compared.
dst-port-min <0-65535>	Specifies the minimum value for the Layer 4 destination port classifier.
dst-port-max <0-65535>	Specifies the maximum value for the Layer 4 destination port classifier.
ethertype <etype>	Specifies a value indicating the version of Ethernet protocol being used.
eval-order <0-65535>	Specifies the evaluation order for all elements with the same name.
flow-id <flowid>	Specifies the flow identifier for IPv6 packets.
ip-flags <ip-flags>	Specifies the IP fragment flag criteria.
ipv4-options <no-opt with-opt>	Specifies the IPv4 option criteria.
master	Designates the classifier as the master block member.
max-burst-rate <64-429496729>	Specifies the maximum burst rate. Values range from 64 to 4294967295 Kbps. You configure this parameter when a committed metering rate is specified.
max-burst-duration <1-4294967295>	Specifies the maximum burst duration in milliseconds (ms). Values range from 1 to 4294967295 ms. You configure this parameter when a committed metering rate is specified.
vlan-min <1-4094>	Specifies the minimum VLAN ID value for the classifier.
vlan-max <1-4094>	Specifies the maximum VLAN ID value for the classifier.
next-header <header>	Specifies the IPv6 next-header value. Values are in the range 0–255.
pkt-type <etherll llc snap>	Specifies the filter packet format ethertype encoding criteria.
priority <ieee1p-seq>	Specifies a value for the 802.1p user priority.
protocol <protocoltype>	Specifies the IPv4 protocol value.

Variable	Value
set-drop-prec <high-drop low-drop>	<p>Specifies the drop precedence for traffic matching the classifier criteria.</p> <ul style="list-style-type: none"> • high-drop—a higher probability that the packet will be dropped when traffic congestion occurs • low-drop—a lower probability that the packet will be dropped when traffic congestion occurs
set-drop-prec-out-action <high-drop low-drop>	<p>Specifies the drop precedence value associated with out of profile traffic.</p> <ul style="list-style-type: none"> • high-drop—a higher probability that the packet will be dropped when traffic congestion occurs • low-drop—a lower probability that the packet will be dropped when traffic congestion occurs
tcp-control <Urg Ack Psh Rst Syn Fin>	Specifies the TCP control criteria.
update-1p <0-7> use-egress use-tos-prec	<p>Specifies the 802.1p user priority update value:</p> <ul style="list-style-type: none"> • 0–7 — sets priority value from 0 up to 7 • use-egress — sets priority value according to egressmap by evaluating DSCP from egress traffic • use-tos-prec — sets priority value according to the first 3 bits from ingress traffic DSCP
update-dscp <0-63>	Specifies the DSCP update value.
update-dscp-out-action <0-63>	Specifies the DSCP update value in out of profile packets.
src-port-min <0-65535>	Specifies the minimum value for the Layer 4 source port number in a packet.
src-port-max <0-65535>	Specifies the maximum value for the Layer 4 source port number in a packet.
src-mac <src-mac>	Specifies the MAC source address of incoming packets.
src-ip <src-ip-info>	Specifies the IP address to match against the source IP address of a packet.

Configuring a traffic profile set

Use this procedure to configure a traffic profile set.

Procedure steps

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

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

Variable definitions

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

Variable	Value
committed-rate <64-10230000>	Specifies the committed rate in Kilobits per second.
committed-burst-size <burst-size-options>	Specifies the committed burst size in KiloBytes.
drop-out-action <enable disable>	Specifies whether to drop (enable) or pass (disable) out-of-profile packets. You configure this parameter when a metering type is selected and a committed metering rate is specified.
enable	Enables the traffic profile.
max-burst-rate <64-429496729 5>	Specifies the maximum burst rate. Values range from 64 to 4294967295 Kbps. You configure this parameter when a committed metering rate is specified.
max-burst-duration <1-4294967295>	Specifies the maximum burst duration in milliseconds (ms). Values range from 1 to 4294967295 ms. You configure this parameter when a committed metering rate is specified.
meter-mode <uniform-per-policy individual-per-policy classifier>	Specifies the metering type. <ul style="list-style-type: none"> • uniform-per-policy—a unique meter is applied to each policy that comprises the filter set with uniform rate and burst data

Variable	Value
	<p>derived from the filter set specification used for each meter</p> <ul style="list-style-type: none"> • individual-per-policy—a unique meter is applied to each policy that comprises the filter set with rate and burst data derived from the classifier data or the filter set specification • classifier—a meter is defined for each individual filter set classifier using rate and burst data associated with the classifier. If this data is not present a meter is not allocated for the classifier
name <name>	Specifies the name of the traffic profile.
port <port>	Specifies the ports for which to apply the traffic profile.
set-drop-prec-out-action <high-drop low-drop>	<p>Specifies the drop precedence value for out-of-profile traffic.</p> <ul style="list-style-type: none"> • high-drop—there is a higher probability of packets being dropped when network congestion is encountered. • low-drop—there is a lower probability of packets being dropped when network congestion is encountered. <p>You configure this parameter when a metering type is selected and a committed metering rate is specified.</p>
track-statistics <aggregate disable individual>	<p>Specifies how to track policy statistics for the traffic profile filter set.</p> <ul style="list-style-type: none"> • aggregate—all traffic profile classifiers associated with a policy share the statistics resource • disable—statistics tracking is disabled for all traffic profile classifiers • individual—each traffic profile filter set classifier has its own statistics resource
update-dscp-out-action <0-63>	Updates the DSCP value in out-of-profile IP packets. Values range from 0 to 63. You configure this parameter when a metering type is selected and a committed metering rate is specified.

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

Use this procedure to delete a filter classifier or set.

Procedure steps

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command to delete a traffic profile classifier:

```
no qos traffic-profile classifier name <classifier-name>
```
3. At the command prompt, enter the following command to delete a traffic profile set:

```
no qos traffic-profile set {name <name> | port <port>}
```

Viewing filter descriptions

Use this procedure to view filter descriptions.

Procedure steps

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

```
show qos traffic-profile classifier
```

OR

```
show qos traffic-profile classifier name <classifier name>
```
3. At the command prompt, enter the following command to view the parameters for a specific set:

```
show qos traffic-profile set <set name> port <port>
```
4. At the command prompt, enter the following command to view ports and the filter sets assigned to those ports:

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

QoS filter limiting configuration

Use the procedures in this section to disable, re-enable, and display information about QoS filter limiting, a feature that controls the maximum number of user-defined protocol VLANs.

Displaying QoS filter limiting

Use this procedure to display the filter limiting status.

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

```
show qos filter-limiting
```

Disabling QoS filter limiting

Use this procedure to disable filter limiting. Filter limiting is enabled by default.

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

```
no qos filter-limiting enable
```

3. Reset the switch to apply the change.

Enabling QoS filter limiting

If you have disabled filter limiting, use this procedure to enable filter limiting.

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

```
qos filter-limiting enable
```

3. Reset the switch to apply the change.

Restoring QoS filter limiting to default

Use this procedure to restore filter limiting to the default value, enabled.

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

```
default qos filter-limiting
```
3. Reset the switch to apply the change.

Configuring QoS for the NSNA solution

When you assign a filter set name using the `nsna vlan <vid> color <red|yellow|green> filter <name>` command (for example, `nsna vlan 110 color red filter redFilter`), the switch automatically creates all the necessary (default) QoS classifiers for the specified color with the name you assigned (in this case, `redFilter`) if that filter set does not already exist. If you had previously defined the filter set (using the `qos nsna` command), then that pre-existent filter set is used. Once you create a filter set, you can modify the filter set using the `qos nsna` command. NSNA functionality applies QoS filter sets to NSNA-enabled ports. A user defines a filter set first by defining the individual filters, followed by the overall filter set itself. The individual filters and the filter set share the same name string.

*** Note:**

When the device applies NSNA filters to a port, the device disables any existing QoS filters on that port, and applies the NSNA filters. The device re-enables the pre-existing policies when NSNA is disabled.

Configuring QoS for NSNA filters

Use this procedure to configure QoS for NSNA filters.

Procedure steps

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

```
qos nsna
```

*** Note:**

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

Variable definitions

Variable	Value
classifier name [addr-type {ipv4 ipv6}] [block] [drop-action] [ds-field] [dst-ip] [dst-mac] [dst-port-min] [ethertype] [eval-order] [flow-id] [next-header] [priority] [protocol] [set-drop-prec] [src-ip] [src-mac] [src-port-min] [update-1p] [update-dscp] [vlan-min] [vlan-tag]	Creates the QoS NSNA classifier entry. Optional parameters: <ul style="list-style-type: none"> • addr-type {ipv4 ipv6}— Specifies the type of IP address used by this classifier entry. The type is limited to IPv4 and IPv6 addresses. • block— Specifies the label to identify access list elements that are of the same block. • drop-action— Specifies whether or not to drop non-conforming traffic. • ds-field—specifies the value for the DiffServ Codepoint (DSCP) in a packet. • dst-ip— Specifies the IP address to match against the destination IP address of a packet. • dst-mac— Specifies the MAC address against which the MAC destination address of incoming packets is compared. • dst-port-min— Specifies the minimum value for the layer 4 destination port number in a packet. dst-port-max must be terminated prior to configuring this parameter. • ethertype— Specifies a value indicating the version of Ethernet protocol being used. • eval-order— Specifies the evaluation order for all elements with the same name. • flow-id— Specifies the flow identifier for IPv6 packets. • next-header— Specifies the IPv6 next-header value. Values are in the range of 0–255. • priority— Specifies a value for the 802.1p user priority. • protocol— Specifies the IPv4 protocol value. • set-drop-prec— Specifies drop precedence. • src-ip— Specifies the IP address to match against the source IP address of a packet. • src-mac— Specifies the MAC source address of incoming packets.

Variable	Value
	<ul style="list-style-type: none"> • src-port-min— Specifies the minimum value for the Layer 4 source port number in a packet. src-port-max must be terminated prior to configuring this parameter. • update-1p— Specifies an 802.1p value used to update user priority. • update-dscp— Specifies a value used to update the DSCP field in an IPv4 packet. • vlan-min— Specifies the minimum value for the VLAN ID in a packet. vlan-max must be terminated prior to configuring this parameter. • vlan-tag— Specifies the type of VLAN tagging in a packet.
<pre>set name [committed-rate] [[drop-out-action] [max-burst-rate] [max-burst-duration] [update-dscp-out-action]</pre>	<p>Creates the QoS NSNA set. Optional parameters:</p> <ul style="list-style-type: none"> • committed-rate— Specifies the committed rate in Kbps. • drop-out-action— Specifies the action to take when a packet is out-of-profile. The device only applies this action if metering is being enforced, and if the device deems the traffic to be out of profile based on the level of traffic and the metering criteria. Options are enable (packet is dropped) and disable (packet is not dropped). • max-burst-rate— Specifies the maximum number of bytes to allow in a single transmission burst. • max-burst-duration— Specifies the maximum burst duration in milliseconds. • update-dscp-out-action— Specifies an updated DSCP value for an IPv4 packet for out of profile traffic.

Job aid: Using qos nsna commands

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

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

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

*** Note:**

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

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

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

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

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

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

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

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

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

Use this procedure to delete a NSNA classifier, classifier block, or filter set.

Procedure steps

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command to delete an entire filter set:

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

3. At the command prompt, enter the following command to delete a classifier:

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

*** Note:**

You cannot reset QoS defaults if the NSNA application references a QoS NSNA filter set.

Viewing filter descriptions

Use this procedure to view filter descriptions.

Procedure steps

1. Log on to the Privileged EXEC mode in ACLI.
2. At the command prompt, enter the following command to view NSNA filter parameters:

```
show qos nsna
```
3. At the command prompt, enter the following command to view the parameters for a specific filter set:

```
show qos nsna name <filter name>
```
4. At the command prompt, enter the following command to view ports and the filter sets assigned to those ports:

```
show qos nsna interface
```
5. At the command prompt, enter the following command to view classifier entries:

```
show qos nsna classifier
```

Configuring user-based policies

Use this procedure to configure user-based policies.

Procedure steps

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

```
qos ubp
```

*** Note:**

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

Variable definitions

Variable	Value
classifier name [addr-type {ipv4 ipv6}] [block] [drop-action] [ds-field] [dst-ip] [dst-mac] [dst-port-min] [ethertype] [eval-order] [flow-id] [next-header] [priority] [protocol] [set-drop-prec] [src-ip] [src-mac] [src-port-min] [update-1p] [update-dscp] [vlan-min] [vlan-tag]	Creates the user-based policy classifier entry. Optional parameters: <ul style="list-style-type: none"> • addr-type {ipv4 ipv6} — Specifies the type of IP address used by this classifier entry. The type is limited to IPv4 and IPv6 addresses. • block — Specifies the label to identify access list elements that are of the same block. • drop-action — Specifies whether or not to drop non-conforming traffic. • ds-field — Specifies the value for the DiffServ Codepoint (DSCP) in a packet. • dst-ip — Specifies the IP address to match against the destination IP address of a packet. • dst-mac — Specifies the MAC address against which the MAC destination address of incoming packets is compared. • dst-port-min — Specifies the minimum value for the layer 4 destination port number in a packet. dst-port-max must be terminated prior to configuring this parameter. • ethertype — Specifies a value indicating the version of Ethernet protocol being used. • eval-order — Specifies the evaluation order for all elements with the same name. • flow-id — Specifies the flow identifier for IPv6 packets. • next-header — Specifies the IPv6 next-header value. Values are in the range of 0-255. • priority — Specifies a value for the 802.1p user priority. • protocol — Specifies the IPv4 protocol value. • set-drop-prec — Specifies drop precedence. • src-ip — Specifies the IP address to match against the source IP address of a packet. • src-mac — Specifies the MAC source address of incoming packets.

Variable	Value
	<ul style="list-style-type: none"> • <code>src-port-min</code> — Specifies the minimum value for the Layer 4 source port number in a packet. <code>src-port-max</code> must be terminated prior to configuring this parameter. • <code>update-1p</code> — Specifies an 802.1p value used to update user priority. • <code>update-dscp</code> — Specifies a value used to update the DSCP field in an IPv4 packet. • <code>vlan-min</code> — Specifies the minimum value for the VLAN ID in a packet. <code>vlan-max</code> must be terminated prior to configuring this parameter. • <code>vlan-tag</code> — Specifies the type of VLAN tagging in a packet.
<code>set name [committed-rate] [drop-out-action] [max-burst-rate] [max-burst-duration] [update-dscp-out-action] [set-priority]</code>	<p>Creates the user-based policy set. Optional parameters:</p> <ul style="list-style-type: none"> • <code>committed-rate</code> — Specifies the committed rate in Kbps. • <code>drop-out-action</code> — Specifies the action to take when a packet is out-of-profile. The device only applies this action if metering is being enforced, and if the device deems the traffic to be out of profile based on the level of traffic and the metering criteria. Options are enable (packet is dropped) and disable (packet is not dropped). • <code>max-burst-rate</code> — Specifies the maximum number of bytes allowed in a single transmission burst. • <code>max-burst-duration</code> — Specifies the maximum burst duration in milliseconds. • <code>update-dscp-out-action</code> — Specifies an updated DSCP value for an IPv4 packet for out of profile traffic. • <code>set-priority</code> — Specifies the priority level of this filter set.

Job aid: Using qos ubp commands

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

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

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

*** Note:**

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

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

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

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

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

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

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

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

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

Use this procedure to delete a classifier, classifier block, or filter set.

Procedure steps

1. Log on to the Global Configuration mode in ACLI.
2. At the command prompt, enter the following command to delete an entire filter set:

```
no qos ubp name <filter name>
```

*** Note:**

You cannot delete a filter set while it is in use.

3. At the command prompt, enter the following command to delete a classifier:

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

*** Note:**

You cannot reset QoS defaults if the EAP/NEAP UBP support references a QoS UBP filter set.

Viewing filter descriptions

Use this procedure to view user-based policy filter parameters, view parameters for a specific filter set, view ports and associated filter sets, and view classifier entries.

Procedure steps

1. Log on to the Privileged EXEC mode in ACLI.
2. At the command prompt, enter the following command to view user-based policy filter parameters:

```
show qos ubp
```
3. At the command prompt, enter the following command to view the parameters for a specific filter set:

```
show qos ubp name <filter name>
```
4. At the command prompt, enter the following command to view ports and the filter sets assigned to those ports:

```
show qos ubp interface
```
5. At the command prompt, enter the following command to view classifier entries:

```
show qos ubp classifier
```

Maintaining the QoS agent

Use the following ACLI commands to maintain the QoS agent.

Removing all QoS configurations

Use this command to remove all configurations except for buffering and queue-set.

Procedure steps

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

```
qos agent reset-partial-default
```

Resetting QoS to factory default state

Use this procedure to delete all user-defined entries, remove all installed policies, and reset the system to the QoS factory default values.

Procedure steps

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

```
qos agent reset-default
```

*** Note:**

You cannot reset QoS defaults if the NSNA application references a QoS NSNA filter set.

*** Note:**

You cannot reset QoS defaults if the EAP/NEAP UBP support references a QoS UBP filter set.

Changing the QoS agent to partial factory defaults

Use this procedure to change all QoS agent parameters to factory default values except resource buffer sharing and QoS CoS queue set.

Procedure steps

1. Log on to the Global Configuration Mode in ACLI.
2. Enter the following command at the command prompt:

```
qos agent reset-partial-default
```

Configuring auto QoS mode

Use this procedure to configure auto QoS mode.

Procedure steps

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

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

Variable definitions

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

Configuring QoS UBP support

Use this procedure to configure the UBP support level.

Procedure steps

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

```
qos agent ubp [disable|epm|high-security-local|low-security-local]
```

Variable definitions

Variable	Value
disable	QoS agent rejects information forwarded by other applications.
epm	QoS Agent notifications generated for EPM based on user information forwarded by other applications.

Variable	Value
high-security-local	User may be rejected if resources needed to install the UBP filter set are not available.
low-security-local	User may be accepted even if the UBP filter set could not be applied.

Configuring QoS statistics tracking type

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

Procedure steps

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

```
qos agent statistics-tracking [aggregate|disable|individual]
```

Variable definitions

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

Configuring NVRAM delay

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

Procedure steps

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

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

The default is 10 seconds.

Resetting NVRAM delay to default

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

Procedure steps

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

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

Resetting the QoS agent

Use this procedure to delete all user-defined entries, remove all installed policies, and reset the system to its QoS factory default values.

Procedure steps

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

```
default qos agent
```

Configuring DoS Attack Prevention Package

This section contains procedures used to configure the DoS Attack Prevention Package (DAPP). This feature is only applicable to the ERS 5600 Series switch.

Enabling DAPP

Use this procedure to enable DAPP.

Procedure steps

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

```
[no] qos agent dos-attack-prevention enable
```

Use the **no** form of this command to disable.

Configuring DAPP status tracking

Use this procedure to configure DAPP status tracking.

Procedure steps

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

```
qos agent dos-attack-prevention status-tracking [enable |  
max-ipv4-icmp | max-ipv6-icmp | min-tcp-header]
```

*** Note:**

If adequate resources are not available to enable this feature, the command fails.

Configuring DAPP minimum TCP header size

Use this procedure to set the minimum TCP header size used by DAPP.

Procedure steps

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


```
qos agent dos-attack-prevention min-tcp-header <0-255>
```

Configuring DAPP maximum IPv4 ICMP length

Use this procedure to set the maximum IPv4 ICMP length used by DAPP.

Procedure steps

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

```
qos agent dos-attack-prevention max-ipv4-icmp <0-1023>
```

Configuring DAPP maximum IPv6 ICMP length

Use this procedure to set the maximum IPv6 ICMP length used by DAPP.

Procedure steps

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

```
qos agent dos-attack-prevention max-ipv6-icmp <0-16383>
```

Configuring Automatic QoS

The ACLI commands detailed in this section allow for the configuration of Automatic QoS support.

Enabling Automatic QoS

Use this procedure to enable Automatic QoS support.

Procedure steps

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

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

Variable definitions

Variable	Definition
mixed	Enables AQ application traffic processing with DSCP remarking.
pure	Enables AQ application traffic processing without DSCP remarking.

Disabling Automatic QoS

Use this procedure to disable Automatic QoS support.

Procedure steps

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

```
qos agent aq-mode disable
```

QoS statistics management

Use the following command to clear all counters associated with QoS policies and installed meters.

Procedure steps

1. Log on to the Global Configuration Mode in ACLI.
2. Enter the following command at the command prompt:

```
qos agent clear-stats
```

Chapter 5: Quality of Service (QoS) configuration using Enterprise Device Manager

Use Enterprise Device Manager to manage Quality of Service (QoS) parameters on the Avaya Ethernet Routing Switch 5000 Series.

*** Note:**

In addition to the QoS configurations you create, the system creates some default classifier elements, classifiers, classifier blocks, policies, and actions. You cannot modify or delete these system default entries.

Opening the QoS devices dialog box

To open the QoS Devices dialog box:

Procedure steps

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

This section provides information about the following topics:

Viewing the interface queue

Use this procedure to display interface queues and groups:

Procedure steps

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

Variable definitions

The following table outlines the parameters of the **Interface Queue** tab.

Table 7: QoS Devices Interface Queue tab parameters

Variable	Value
SetId	Displays an integer between 1 and 65 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: <ul style="list-style-type: none"> • priorityQueuing • weightedRoundRobin
Bandwidth%	Displays relative bandwidth available to a given queue with respect to other associated queues.
AbsBandwidth	Displays absolute bandwidth available to this queue, in Kb/s.
BandwidthAllocation	Displays bandwidth allocation: relative or absolute.
ServiceOrder	Specifies the order in which a queue is serviced based on the defined discipline.
Size	Displays the size of the queue in bytes.

Viewing interface groups

Enterprise Device Manager lets you display the interface groups.

Use this procedure to display interface groups.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Devices**.
3. Select the **Interface Groups** tab.

Variable definitions

The following table outlines the parameters of the **Interface Groups** tab.

Table 8: QoS Devices Interface Groups tab parameters

Variable	Value
Id	Displays a unique identifier of an interface group.
Role	Specifies the tag (group name) used to identify interfaces with the characteristics specified by the attributes of this class

Variable	Value
	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.
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).
InterfaceClass	Specifies the type of traffic interfaces associated with the specified role combination.
StatsTrackingType	Specifies the type of statistics tracking. Options are aggregate, individual, or disabled.
StorageType	Displays storage type for this interface group: <ul style="list-style-type: none"> • Volatile • nonVolatile (default) • readOnly

This section contains information about the following topics:

- [Assigning ports to an interface group](#) on page 125
- [Deleting ports from an interface group](#) on page 126
- [Adding interface groups](#) on page 126
- [Deleting interface groups](#) on page 127

Assigning ports to an interface group

Use this procedure to assign ports to an interface group.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Devices**.
3. Select the **Interface Groups** tab.
4. Click **Interface Assignment**.
5. In the **Group Assignment screen**, click the port numbers to add to the interface group.
6. Click **OK**.

* Note:

If you add or delete many ports on a switch that is experiencing a heavy load the process can take a long time and the process can cause Enterprise Device Manager to time out.

For more information, see [Table 8: QoS Devices Interface Groups tab parameters](#) on page 124.

Deleting ports from an interface group

Use this procedure to remove ports from an interface group.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Devices**.
3. Select the **Interface Groups** tab.
4. Highlight the interface group from which to delete ports.
5. Click **Interface Assignment**.
The Group Assignment screen opens.
6. Click the port numbers to delete from the interface group.
7. Click **OK**.

For more information, see [Table 8: QoS Devices Interface Groups tab parameters](#) on page 124.

Adding interface groups

Use this procedure to add an interface group.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Devices**.
3. Select the **Interface Groups** tab.
4. Click **Insert**.
The Insert Interface Group screen opens.
5. Enter the desired ID number.
6. Enter the **Role** combination tag for this Interface Group.
7. Select the interface class desired for this interface group: **trusted**, **nonTrusted**, or **unrestricted**.
8. Click **Insert**.

For more information, see [Table 8: QoS Devices Interface Groups tab parameters](#) on page 124.

Deleting interface groups

Use this procedure to delete an interface group.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Devices**.
3. Select the **Interface Groups** tab.
4. Highlight the interface group to delete.
5. Click **Delete**.

*** Note:**

You cannot delete an interface group that a policy references. You must delete the policy first. Also, you cannot delete an interface group if you assigned ports to it.

For more information, see [Table 8: QoS Devices Interface Groups tab parameters](#) on page 124.

Viewing interface ID assignments

Use this procedure to open the **Interface ID Assignments** tab.

Procedure steps

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

Variable definitions

The following table outlines the parameters of the **Interface ID Assignments** tab.

Table 9: QoS Devices Interface ID Assignments tab parameters

Variable	Value
RoleCombination	Displays the role combination associated with the interface.
QueueSet	Displays the queue set associated with this interface.
Port	Displays the port number.
Capabilities	Displays the port capabilities.

Viewing Priority Q Assign

Use this procedure to open the **Priority Q Assign** tab.

Procedure steps

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

Variable definitions

The following table outlines the parameters of the **Priority Q Assign** tab.

Table 10: QoS Devices Priority Q Assign tab parameters

Variable	Value
Qset	Represents the queue set number. Supports the assignment of 802.1p user priority values to a queue for each specific queue set. There are 56 instances for queue set number, each instance is a multiple of one basic queue-set from 1 to 8.
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

The priority queue assignments table can be filtered to display only those records that are of interest.

Use this procedure to filter the priority queue assignments table.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Devices**.
3. Select the **Priority Q Assign** tab.
4. Click **Filter**.

The Insert Filter dialog opens.

5. Set the conditions to be used to filter the display of the **Priority Q Assign** table:

- a. Select **AND** to include all entries in the table that include all specified parameters, or select **OR** to include any of the specified parameters.
- b. Select **Ignore Case** to include all entries with the parameters being set, whether in lowercase or uppercase.
- c. Select any of the criteria from **Column** to include entries matching the criteria. **Contains** if the table is to show all entries that contain the parameters set or **Equal To** to show only those entries that are equal to the parameters being set.
- d. Select **All records** to display all the entries in the table.
- e. To display the entries in the table by queue set, select **QSet** and enter the **QSet** values to display.

6. Click **Filter**.

For more information, see [Table 10: QoS Devices Priority Q Assign tab parameters](#) on page 128.

Viewing priority mapping

Use this procedure to open the **Priority Mapping** tab.

Procedure steps

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

Variable definitions

The following table outlines the parameters of the **Priority Mapping** tab.

Table 11: QoS Devices Priority Mapping tab parameters

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

Viewing DSCP mapping

The following sections describe egress mapping. DSCP mapping configurations apply to egress for trusted QoS interfaces.

DSCP mapping tab navigation

- [Viewing egress mapping using EDM](#) on page 130
- [Configuring egress mapping using EDM](#) on page 131

Viewing egress mapping using EDM

Use this procedure to view egress mapping using EDM.

Procedure steps

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

Variable definitions

Use the data in the following table to help you understand egress mapping.

Table 12: DSCP Mapping tab parameters

Variable	Value
Dscp	Indicates the DSCP value. This is a read-only cell.
802.1pPriority	Specifies the user priority value associated with the DSCP. The values range from 0–7.
DropPrecedence	<p>Specifies the relative drop precedence value for mapping the DSCP value to a drop precedence. The values include:</p> <ul style="list-style-type: none"> • lowDropPrec • highDropPrec <p>When network congestion occurs, the system drops packets with a high drop precedence before those with a low drop precedence.</p>

Variable	Value
NewDscp	Specifies a new DSCP value to use when DSCP mutation is required. The values range from 0–63.
ServiceClass	Specifies the type of service. The value is a character string with a maximum of 16 characters.

Configuring egress mapping using EDM

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

Prerequisites

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

Procedure steps

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

Variable definitions

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

Table 13: DSCP Mapping tab parameters

Variable	Value
Dscp	Indicates the DSCP value. This is a read-only cell.
802.1pPriority	Specifies the user priority value associated with the DSCP. The values range from 0–7.
DropPrecedence	Specifies the relative drop precedence value for mapping the DSCP value to a drop precedence. The values include: <ul style="list-style-type: none"> • lowDropPrec • highDropPrec When network congestion occurs, the system drops packets with a high drop precedence before those with a low drop precedence.
NewDscp	Specifies a new DSCP value to use when DSCP mutation is required. The values range from 0–63.
ServiceClass	Specifies the type of service. The value is a character string with a maximum of 16 characters.

Viewing meter capability

Use this procedure to open the **Meter Capability** tab.

Procedure steps

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

Variable definitions

The following table outlines the parameters of the **Meter Capability** tab.

Table 14: QoS Devices Meter Capability tab parameters

Variable	Value
Port	Specifies the port to which the meter is applied.

Variable	Value
MeterSupport	Specifies the supported Token Bucket metering algorithm.
Meter Rate (Kbps)/Bucket (KBytes)/Granularity (Kbps)	Displays maximum supported Meter Rate, Meter Bucket size and Meter Granularity.

Configuring meter capability filtering

Use this procedure to configure Meter Capability filtering.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Devices**.
3. Select the **Meter Capability** tab.
4. Click the **Filter** button to set Meter Capability table view filtering criteria.
The QOSDevice, Meter Capability - Filter dialog opens.
5. Select filtering criteria and enter port, meter support, and meter rate parameters.
6. To activate your selections, click the **Filter** button on the dialog, the Meter Capability window will display entries based on the filtering criteria specified.

For more information, see [Table 14: QoS Devices Meter Capability tab parameters](#) on page 132.

Viewing shaper capability

Use this procedure to open the **Shaper Capability** tab.

Procedure steps

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

Table 15: Shaper Capability tab parameters

Variable	Value
Port	Displays the port number.
ShaperSupport	Displays the shaper support as: <ul style="list-style-type: none"> • Interface • Cos (Class of Service)

Variable	Value
Shaper Rate(Kbps)/Bucket(Kbytes)/Granularity(Kbps)	Displays the <ul style="list-style-type: none">• Shaper rate in Kilobytes per second• Bucket size in Kilobytes• Granularity in Kilobytes per second

Configuring shaper capability filtering

Use this procedure to configure Shaper Capability filtering.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Devices**.
3. Select the **Shaper Capability** tab.
4. Click the **Filter** button to set Shaper Capability table filtering.
The QOSDevice, Shaper Capability - Filter dialog opens.
5. Select filtering criteria and enter port, shaper support, and shaper rate parameters.
6. To activate your selections, click the **Filter** button on the dialog, the Shaper Capability window will display the entries based on the filtering criteria specified.

Opening QoS rules dialog box

Use this procedure to open the QoS Rules dialog box.

Procedure steps

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

This section contains information about the following topics:

Viewing the IP classifier element tab

Use this procedure to open the **IP Classifier Element** tab.

Procedure steps

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

Variable definitions

The following table outlines the parameters of the **IP Classifier Element** tab.

Table 16: QoS Rules IP Classifier Element tab parameters

Variable	Value
Id	Specifies the number of the IP classifier element.
Name	Specifies the IP classifier element name.
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 the destination IP address of packet.
DstMaskLength	Specifies the length of the destination address mask.
SrcAddr	Specifies the IP address to match against the source IP address of packet.
SrcMasklength	Specifies the length of the source address mask.
Dscp	Specifies the value for the DSCP in a packet.
Protocol/NextHeader	Specifies the IP protocol value.
DstL4Port	Specifies the value for the Layer 4 destination port number in a packet.
SrcL4Port	Specifies the value for the Layer 4 source port number in a packet.
IPv6FlowId	Specifies the flow identifier for IPv6 packets.
IpFlags	Specifies the value of flags present in an IPv4 header.
TcpCtrlFlags	Specifies the control flags present in an TCP header.
Ipv4Options	Specifies whether the Option field is present in the packet header. Valid values are <ul style="list-style-type: none"> • Present—indicates that only IPv4 packets with options match this classifier element. • Not Present—indicates that only IPv4 packets without options match this classifier element.

Variable	Value
SessionId	Specifies the session identification number.
Storage	Specifies the type of storage: <ul style="list-style-type: none">• volatile• nonVolatile (default)• readOnly

This section contains information about the following topics:

- [Adding IP classifier elements](#) on page 136
- [Deleting IP classifier elements](#) on page 136

Adding IP classifier elements

Use this procedure to add an IP classifier element.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Rules**.
3. Select the **IP Classifier Element** tab.
4. Click **Insert**.
The Insert IP Classifier Element screen opens.
5. Enter the information you want to use for this IP classifier element.
6. Click **Insert**.

Deleting IP classifier elements

Use this procedure to delete an IP classifier element.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Rules**.
3. Select the **IP Classifier Element** tab.
4. Highlight the IP classifier element to delete.
5. Click **Delete**.

*** Note:**

You cannot delete an IP classifier element if a classifier or classifier block references it. Additionally, you cannot delete an IP classifier element if the storage type is **other** or **readOnly**.

Viewing the L2 classifier element

Use this procedure to open the **L2 Classifier Element** tab.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Rules**.
3. Select the **L2 Classifier Element** tab.

Variable definitions

The following table outlines the parameters of the **L2 Classifier Element** tab.

Table 17: QoS Rules L2 Classifier Element tab parameters

Variable	Value
Id	Specifies the index that enumerates the classifier entries.
Name	Specifies the Layer 2 Classifier Element name.
DstMacAddr	Specifies the MAC address against which the MAC destination address of incoming packets are 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.
VlanId	Specifies the value for the VLAN ID in a packet.
VlanTag	Specifies the type of VLAN tagging in a packet: <ul style="list-style-type: none"> • untagged • tagged • ignore
EtherType	Specifies a value for the Ethertype.
802.1pPriority	Specifies a value for the 802.1p user priority.
PktType	Specifies the packet frame format.

Variable	Value
	<ul style="list-style-type: none"> • etherII—indicates that only Ethernet II format frames match this classifier component. • snap—indicates that only IEEE 802 SNAP format frames match this classifier component. • llc—indicates that only IEEE 802 LLC format frames match this classifier component.
Version	Specifies the version.
SessionId	Specifies the session identification number.
Storage	Specifies the type of storage.

This section contains information about the following topics:

- [Adding L2 classifier elements](#) on page 138
- [Deleting L2 classifier elements](#) on page 138

Adding L2 classifier elements

Use this procedure to add L2 classifier elements.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Rules**.
3. Select the **L2 Classifier Element** tab.
4. Click **Insert**.
The Insert L2 Classifier Element dialog opens.
5. Enter the information to use for this L2 classifier element.
6. Click **Insert**.

For more information, see [Table 17: QoS Rules L2 Classifier Element tab parameters](#) on page 137.

Deleting L2 classifier elements

Use this procedure to delete L 2 classifier elements.

Procedure steps

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

3. Select the **L2 Classifier Element** tab.
4. Highlight any table cell of the L2 classifier element to delete.
5. Click **Delete**.

Enterprise Device Manager deletes the entire L2 classifier element.

*** Note:**

You cannot delete a L2 classifier element if a classifier or classifier block references it. Additionally, you cannot delete a L2 classifier element if the storage type is **other** or **readOnly**.

For more information, see [Table 17: QoS Rules L2 Classifier Element tab parameters](#) on page 137.

Viewing System Clfr Elements

Use this procedure to open the **System Clfr Element** tab.

Procedure steps

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

Variable definitions

The following table outlines the parameters of the **System Clfr Element** tab.

Table 18: QoS Rules System Clfr Element tab parameters

Variable	Value
Id	Specifies the index that enumerates the system classifier entries.
Name	Specifies the System Classifier Element name.
UnknownUcastFrames	<p>Identifies frames with an unknown unicast destination address.</p> <ul style="list-style-type: none"> • true— Indicates frames that contain an unknown unicast destination address match this classification entry. • false— Indicates that no classification is requested based on this address type. <p>Can be applied on ERS 56xx as version 2 elements or on ERS 55xx as version 1 elements.</p>

Variable	Value
UnknownMcastFrames	<p>Identifies frames with an unknown multicast destination address.</p> <ul style="list-style-type: none"> • true— Indicates frames that contain an unknown multicast destination address match this classification entry. • false— Indicates that no classification is requested based on this address type. <p>Can be applied on ERS 55xx as version 1 elements.</p>
KnownMcastFrames	<p>Identifies frames with a known multicast destination address.</p> <ul style="list-style-type: none"> • true— Indicates frames containing a known multicast destination address match this classification entry. • false— Indicates that no classification is requested based on this address type. <p>Can be applied on ERS 55xx as version 1 elements.</p>
UnknownIpMcast	<p>Identifies IP packets with an unknown IP multicast destination address.</p> <ul style="list-style-type: none"> • true— Indicates that IP packets that contain an unknown multicast destination address match this classification entry. • false— Indicates that no classification is requested based on this address type. <p>Can be applied on ERS 56xx as version 2 elements.</p>
KnownIpMcast	<p>Identifies IP packets with a known IP multicast destination address.</p> <ul style="list-style-type: none"> • true— Indicates that IP packets that contain a known multicast destination address match this classification entry. • false— Indicates that no classification is requested based on this address type. <p>Can be applied on ERS 56xx as version 2 elements.</p>
UnknownNonIpMcast	<p>Identifies non-IP packets with an unknown MAC multicast destination address.</p> <ul style="list-style-type: none"> • true— Indicates that non-IP packets containing an unknown multicast destination address match this classification entry. • false— Indicates that no classification is requested based on this address type. <p>Can be applied on ERS 56xx as version 2 elements.</p>

Variable	Value
KnownNonIpMcast	<p>Identifies non-IP packets with a known MAC multicast destination address.</p> <ul style="list-style-type: none"> • true— Indicates that non-IP packets containing a known multicast destination address match this classification entry. • false— Indicates that no classification is requested based on this address type. <p>Can be applied on ERS 56xx as version 2 elements.</p>
NonIpPkt	<p>Supports targeting non-IP traffic.</p> <ul style="list-style-type: none"> • true— Indicates that non IP packets match this classification entry. • false— Indicates that no classification is requested based on this packet type. <p>Can be applied on ERS 56xx as version 2 elements.</p>
PatternFormat	<p>Indicates that the data link layer packet format that is used when specifying pattern match data.</p> <ul style="list-style-type: none"> • untagged— Indicates that the specified pattern match data does not include an 802.1Q tag. • tagged— Indicates that the specified pattern match data does include an 802.1Q tag. <p>The default value is tagged.</p>
PatternIPVersion	Specifies the pattern IP version.
PatternL2Format	Specifies the Layer 2 pattern format (ethernet 2, llc, or snap).
Version	Specifies the version.
SessionId	Specifies the number assigned to the session displays in this column.
Storage	<p>Specifies the storage type for this conceptual row. Conceptual rows that have the value permanent need not allow write-access to any columnar objects in the row. This object may not be modified if the associated status object is equal to active.</p>

This section contains information about the following topics:

- [Viewing the system classifier pattern](#) on page 142
- [Adding system classifier elements](#) on page 142
- [Deleting system classifier elements](#) on page 143

Viewing the system classifier pattern

Use this procedure to view the System Classifier pattern.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Rules**.
3. Select the **System Clfr Element** tab.
4. Highlight an entry in the **System Clfr Element** table.
5. Click **Pattern**.

The System Classifier Element # Pattern (Data/Position) screen opens.

Adding system classifier elements

Use this procedure to add System Classifier Elements.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Rules**.
3. Select the **System Clfr Element** tab.
4. Click **Insert**.

The Insert System Clfr Element dialog opens.

5. Select the **DestAddressType**.
6. Type the **PatternData** or **PatternPosition** information manually. Alternatively, click on the ellipses to view the Pattern screen.

The Pattern screen configures the data and position of the pattern to be used by this system classifier.

The System Classifier Element Pattern (Data/Position) screen opens.

7. Select **IPv4**, **IPv6**, or **non-IP**.
8. Select **tagged** or **untagged**.
9. Select the version, 1 or 2.

* **Note:**

You can use this setting to create system classifiers to use only on ERS 5500 Series switches (version 1) or only on ERS 5600 Series switches (version 2).

10. Select the required fields to set up a template guide so that it will be easier to configure the data and position of the pattern.

11. Type the desired **Data** and **Position** in two-digit hex number format.
12. Click **Ok**.
13. Click **Insert**.

Deleting system classifier elements

Use this procedure to delete System Classifier Elements.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Rules**.
3. Select the **System Clfr Element** tab.
4. Highlight the System Classifier Element to delete.
5. Click **Delete**.

Viewing classifiers

Use this procedure to open the **Classifier** tab.


Procedure steps

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

Variable definitions

The following table outlines the parameters of the **Classifier** tab.

Table 19: QoS Rules Classifier tab parameters

Variable	Value
Name	Specifies the name of the classifier.
SetId	Entries with the same SetId belong to the same classifier.  Note: Click heading on this column to list entries in numerical order to view which entries have the same SetId.
Specific	Describes the specific classifier element and its ID number (from the IP Classifier Element screen, the L2 Classifier)

Variable	Value
	Element screen, or System Clfr Element screen) that is included in the classifier.
SessionId	Specifies the numerical identification associated with the session.
Storage	Specifies the storage type for this conceptual row. Conceptual rows that have the value permanent need not allow write-access to any column objects in the row. This object may not be modified if the associated status object is equal to active.
Version	Specifies the version.

This section contains information about the following topics:

- [Adding classifiers](#) on page 144
- [Deleting classifiers](#) on page 145
- [Filtering classifiers](#) on page 145

Adding classifiers

Use this procedure to add classifiers.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Rules**.
3. Select the **Classifier** tab.
4. Click **Insert**.
The Insert Classifier screen opens.
5. Type the name of the classifier element.
6. Select the **IP Classifier Element**, **L2 Classifier Element**, or **System Classifier Element**.
7. Click **Insert**.

*** Note:**

You create a classifier by using the following combination:

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

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

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

Limitations on classifier creation are:

- when creating a classifier with L2 and IP elements the L2 element should contain Ethertype 0x800.
- when creating a classifier with a system element and IP element, the pattern data on the system element must contain the Ethertype value.

Deleting classifiers

Use this procedure to delete classifiers.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Rules**.
3. Select the **Classifier** tab.
4. Highlight the classifier to delete.
5. Click **Delete**.

* Note:

You cannot delete a classifier referenced in a classifier block. Additionally, you cannot delete a classifier if either the storage type **other** or **readOnly**.

Filtering classifiers

Use this procedure to filter the display of classifiers.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Rules**.
3. Select the **Classifier** tab.
4. Click **Filter**.

The Insert Filter screen opens.

5. Set the conditions to filter the display of the **Classifiers** table:
 - a. Select **AND** to include all entries in the table that include *all* specified parameters, or select **OR** to include any of the specified parameters.

- b. Select **Ignore Case** to include all entries with the parameters being set, whether in lowercase or uppercase.
 - c. Select **contains** to include in the table all entries that contain the parameters set, **does not contain** to exclude a parameter from the table, **does not equal to** to include entries that are not equal to a set parameter, or **equals to** to show only those entries that are equal to the parameters being set.
 - d. Select **All records** to display all the entries in the table.
 - e. To display the entries in the table by name, select **Name** and enter the **Name** values to display.
 - f. To display the entries in the table by setid, select **SetId** and enter the **SetId** values to display.
6. Click **Filter**.

Viewing the classifier block

Use this procedure to open the Classifier Block tab.


Procedure steps

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

Variable definitions

The following table outlines the parameters of the **Classifier Block** tab.

Table 20: QoS Rules Classifier Block tab parameters

Variable	Value
BlockNum	<p>Entries with the same BlockNum belong to the same classifier block.</p> <p> Note: Click heading on this column to list entries in numerical order to view which entries have the same BlockNum.</p>
Name	Displays the name you assigned to that classifier block.
ClassifierSetId	Displays the ID number assigned to that classifier (from the Classifier screen).
Meter	Displays the meter associated with the classifier block.

Variable	Value
Action	Displays the action followed for those flows not being metered. (For those flows being metered, this attribute is not applied.)
SessionId	Displays the numerical identification for the current session.
Storage	Specifies the storage type for this conceptual row. Conceptual rows that has the value permanent need not allow write-access to any columnar objects in the row. This object may not be modified if the associated status object is equal to active.
Version	Specifies the version.
EvalOrder	Specifies the evaluation order number.

This section contains information about the following topics:

- [Appending classifier blocks](#) on page 147
- [Adding classifier blocks](#) on page 147
- [Deleting classifier blocks](#) on page 148
- [Filtering classifier blocks](#) on page 148

Appending classifier blocks

Use this procedure to append a classifier block.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Rules**.
3. Select the **Classifier Block** tab.
4. Click **Append Classifier**.
The Insert Classifier Block dialog opens.
5. Select the Classifier to append to the Classifier Block.
6. Click **Insert**.

Adding classifier blocks

Use this procedure to add classifier blocks.

Procedure steps

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

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

*** Note:**

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

Use this procedure to delete classifier blocks.

Procedure steps

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

*** Note:**

You cannot delete the last classifier element in a classifier block if a policy references it. First delete the policy. Additionally, you cannot delete a classifier block if it is either the storage type **other** or **readOnly**.

Filtering classifier blocks

Use this procedure to filter a classifier block.

Procedure steps

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

4. Click **Filter**.
The QOSRules Classifier Block - Filter dialog opens .
5. Select the filtering condition, case, and column criteria.
6. Enter the **BlockNum** and **Name**.
7. Click **Filter**.

Opening the QoS dialog box

Use this procedure to open the QoS dialog box.

Procedure steps

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

This section has information about the following topics:

Viewing actions

Use this procedure to open the **action** tab.

This section discusses the management and use of QoS actions, interface action extensions, meters, and policies.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS**.
3. Select the **Action** tab.

Variable definitions

The following table outlines the parameters of the **Action** tab.

Table 21: QoS Action tab parameters

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.

Variable	Value
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 numerical identification for the active session.
Storage	Specifies the type of storage: <ul style="list-style-type: none"> • volatile • nonVolatile • readOnly

This section contains information about the following topics:

- [Adding QoS actions](#) on page 150
- [Deleting QoS actions](#) on page 150

Adding QoS actions

Use this procedure to add a QoS action.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS**.
3. Select the **Action** tab.
4. Click **Insert**.
The Insert Action dialog opens.
5. Enter the information and select the parameters to use for this QoS action.
6. Click **Insert**.

Deleting QoS actions

Use this procedure to delete a QoS action.

Procedure steps

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

3. Select the **Action** tab.
4. Highlight the QoS action to delete.
5. Click **Delete**.

*** Note:**

You cannot delete a QoS action that a meter, a classifier block or a policy entry reference. First delete the meter, classifier block, or policy. Additionally, you cannot delete a QoS action if it is either the storage type of **other** or **readOnly**.

Viewing interface action ext

Use this procedure to open the Interface **Action Ext** tab.

Procedure steps

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

Variable definitions

The following table outlines the parameters of the **Interface Action Ext** tab.

Table 22: QoS Interface Action Ext tab parameters

Variable	Value
Id	Specifies the number of the interface action extension.
Name	Specifies a label for 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 numerical identification for the current session.
Storage	Specifies the type of storage, either volatile or nonvolatile.

This section contains information about the following topics:

- [Adding interface action extensions](#) on page 152
- [Deleting interface action extensions](#) on page 152

Adding interface action extensions

Use this procedure to add a QoS interface action extension.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS**.
3. Select the **Interface Action Ext** tab.
4. Click **Insert**.

The Insert Interface Action Ext screen opens.

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

Deleting interface action extensions

Use this procedure to delete a QoS interface action extension.

Procedure steps

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

* **Note:**

You cannot delete a QoS interface action extension that an action entry references. First delete the action.

Viewing the meters

Use this procedure to open the **Meter** tab.

Procedure steps

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

Variable definitions

The following table outlines the parameters of the **Meter** tab.

Table 23: QoS Meter tab parameters

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 numerical identification of the current session.
Storage	Specifies the type of storage.
Version	Specifies the version.

This section contains information about the following topics:

- [Adding QoS meters](#) on page 153
- [Deleting QoS meters](#) on page 154

Adding QoS meters

Use this procedure to add a QoS meter.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS**.
3. Select the **Meter** tab.
4. Click **Insert**.
The Insert Meter dialog opens.
5. Enter the information and make the selections to use for this QoS meter.
6. Click **Insert**.

Deleting QoS meters

Use this procedure to delete QoS meters.

Procedure steps

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

 **Note:**

You cannot delete a QoS meter that a classifier block or policy references. First delete the classifier block or policy.

Viewing policies

Use this procedure to open the **Policy** tab.

 **Caution:**

When you define multiple meters that may match the same traffic, you must specify the in-profile and out-of-profile traffic as drop or pass to ensure that the traffic is processed at the prescribed rate. If you do not do this, each meter processes the traffic, and this interaction can cause traffic to be treated in unexpected ways.

Procedure steps

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

Variable definitions

The following table outlines the parameters of the **Policy** tab.

Table 24: QoS Policy tab parameters

Variable	Value
Id	Specifies the number of the QoS policy.
Status	Allows you to enable or disable the policy.

Variable	Value
Name	Displays the name for the policy.
ClassifierType	Specifies whether a classifier or a classifier block identifies traffic.
ClassifierName	Specifies the name of the classifier or classifier block associated with this policy.
InterfaceRoles	<p>Specifies the interfaces to which the policy applies.</p> <p>* Note: You must configure the role combinations before you associate it with a policy.</p>
InterfaceIndex	<p>Specifies the interface to which the policy is to be applied. A policy is associated with an interface explicitly using this attribute or implicitly using a role combination through the ntnQosPolicyInterfaceRole attribute. An interface must be identified by one and only one of these attributes. This attribute can identify an interface that does not currently exist in the system, as long as the specified interface index represents a potentially valid system interface.</p> <p>* Note: The InterfaceRoles and InterfaceIndex fields are mutually exclusive. When the InterfaceIndex field is not zero, the InterfaceRoles must be empty (select none when insert the policy). When the InterfaceRoles specifies a valid role combination, the InterfaceIndex field must be 0.</p>
Precedence	<p>Specifies the order in which multiple policies are associated with the same interface. Policies with greater precedence have higher numbers.</p> <p>* Note: Policies with higher precedence values are applied before policies with lower precedence values.</p>
Meter	<p>Specifies metering associated with this policy. Specifying a metering component causes any action criteria specified explicitly by the policy to be rejected as an error.</p> <p>* Note: You must configure meters before you associate them with a policy.</p>
InProfileAction	<p>Identifies the action to be applied to traffic with this policy. This will not be used when a meter is specified.</p> <p>* Note: You must configure actions before you associate them with a policy.</p>

Variable	Value
NonMatchAction	Identifies action taken for flows that do not match policy criteria.
StatsType	Specifies statistics tracking: <ul style="list-style-type: none"> • none—No statistics tracked for this policy. • individual—Separate counters allocated, space permitting, for each classifier referenced by the policy. • aggregate—A single counter accumulates all the statistics for all the classifiers referenced by the policy.
SessionId	Specifies the numerical identification for the current session.
Storage	Specifies the type of storage: <ul style="list-style-type: none"> • volatile • nonVolatile • readOnly
Version	Specifies the version.

This section contains information about the following topics:

- [Adding QoS policies](#) on page 156
- [Deleting QoS policies](#) on page 157
- [Viewing QoS policy stats](#) on page 157

Adding QoS policies

Use this procedure to add QoS policies.

Caution:

When you define multiple meters that may match the same traffic, you must specify the in-profile and out-of-profile traffic as drop or pass to ensure that the traffic is processed at the prescribed rate. If you do not do this, each meter processes the traffic, and this interaction can cause traffic to be treated in unexpected ways.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS**.
3. Select the **Policy** tab.
4. Click **Insert**.

The Insert QoS Policy screen opens.

5. Enter the information to use for this QoS policy.
6. Click **Insert**.

*** Note:**

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

For more information, see [Table 24: QoS Policy tab parameters](#) on page 154.

Deleting QoS policies

Use this procedure to delete QoS policies.

Procedure steps

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

For more information, see [Table 24: QoS Policy tab parameters](#) on page 154.

Viewing QoS policy stats

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

Procedure steps

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

*** Note:**

When StatsType is aggregate, the **Policy Aggregate Stats** tab is available.
When StatsType is individual, the **Policy Individual Stats** tab is available.

For more information, see [Table 24: QoS Policy tab parameters](#) on page 154.

Viewing the interface shaper

Use this procedure to open the **Interface Shaper** tab.

Procedure steps

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

Variable definitions

The following table outlines the parameters of the **Interface Shaper** tab.

Table 25: QoS Interface Shaper tab parameters

Variable	Value
Port	Specifies the port associated with interface shaping.
Name	Specifies the name applied to the interface shaping data.
ShapingRate	Specifies the token-bucket rate, in kilobits per second (kbps).
BurstSize	Specifies the maximum number of bytes in a single transmission burst.

This section contains information about the following topics:

- [Adding an interface shaper](#) on page 158
- [Deleting an interface shaper](#) on page 159

Adding an interface shaper

Use this procedure to add QoS Interface Shapers.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS**.
3. Select the **Interface Shaper** tab.
4. Click **Insert**.
The Insert Interface Shaper screen opens.
5. Click the ellipses to select the ports for the interface shaper.

The ntnQoSIfShapingPorts screen opens.

6. Select the required ports.
7. Click **Ok**.
8. Type the **Label**, **Shapingrate**, and **MaximumBurstRate**.
9. Select the **Duration** in milliseconds.
10. Click **Insert**.

Deleting an interface shaper

Use this procedure to delete an Interface Shaper.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS**.
3. Select the **Interface Shaper** tab.
4. Highlight the Interface Shaper that to delete.
5. Click **Delete**.

Configuring interface queue shaper

The following sections describe the Interface queue shaper.

Viewing QoS interface queue shaper information

Use this procedure to view QoS interface queue shaper information.

Procedure steps

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

Variable definitions

Use the data in the following table to help you understand QoS interface queue shaper information.

Table 26: Interface Queue Shaper parameters

Variable	Value
Port	Indicates the interface port number associated with a QoS interface shaper. The port number must correspond to the interface table entry with the same port number.
Queue	Indicates the queue for the selected interface port or ports, on which traffic is shaped. The range of available values is determined by the OoS agent default queue configuration.
Name	Indicates an alphanumeric label used to identify the QoS interface queue shaper.
ShapingRate	Indicates the QoS interface queue shaping rate, in kilobits per second (Kbps). Values range from 0 to 10230000 Kbps. The values must be a multiple of 64 or 1000 Kbps.
ShapingMinRate	Indicates the minimum QoS interface queue shaping rate, in kilobits per second (Kbps). Values range from 0 to 10230000 Kbps. The value must be a multiple of 64 or 1000 Kbps.

Creating a QoS interface queue shaper

Use this procedure to create a new QoS interface queue shaper.

Procedure steps

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

Variable Definitions:

Use the data in the following table to help you create a new QoS interface queue shaper.

Table 27: Interface Queue Shaper parameters

Variable	Value
Port	Specifies the interface port number associated with a QoS interface shaper. The port number must correspond to the interface table entry with the same port number.
Queue	Specifies the queue for the selected interface port or ports, on which traffic is shaped. The range of available values is determined by the OoS agent default queue configuration.
Name	Specifies an alphanumeric label used to identify the QoS interface queue shaper.
ShapingRate	Specifies the QoS interface queue shaping rate, in kilobits per second (Kbps). Values range from 64 to 10230000 Kbps. The value must be a multiple of 64 or 1000 Kbps.
ShapingMinRate	Specifies the minimum QoS interface queue shaping rate, in kilobits per second (Kbps). Values range from 0 to 10230000 Kbps. The value must be a multiple of 64 or 1000 Kbps.

Deleting a QoS interface queue shaper

Use this procedure to delete a QoS interface shaper.

Procedure steps

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

Configuring interface apps

Use this procedure to open the Interface Apps tab.

*** Note:**

Due to hardware limitations, the Ethernet Routing Switch 5500 Series switch supports only 11 interface applications per port.

! Important:

Only the ERS 5500 unit and only ERS 5500 ports have this tab available.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS**.
3. Select the **Interface Apps** tab.

Variable definitions

The following table outlines the parameters of the **Interface Apps** tab.

Table 28: QoS Interface Apps tab parameters

Variable	Value
IfIndex	Specifies the ports that this QoS application applies to.
AppEnable	Specifies the applications enabled for the interface (port) specified in IfIndex field.
DefaultGateway	Specifies the default gateway configured for the arpSpoofing application. The default gateway cannot be directly modified. To modify the default gateway for the arpSpoofing application, do the following: <ol style="list-style-type: none"> 1. Double-click the AppEnable field and de-select arpSpoofing. 2. Click Apply. 3. Double-click the AppEnable field, select arpSpoofing, and edit the DefaultGateway field. 4. Click Apply.
IfType	Specifies the interface type configured for the dhcpSnooping application.
DHCPsServer	Specifies the DHCP server configured for the dhcpSpoofing application. The DHCP server cannot be directly modified. To modify the DHCP server for the dhcpSpoofing application, do the following: <ol style="list-style-type: none"> 1. Double-click the AppEnable field and de-select dhcpSpoofing. 2. Click Apply.

Variable	Value
	<ol style="list-style-type: none"> 3. Double-click the AppEnable field, select dhcpSpoofing, and edit the DHCPServer field. 4. Click Apply.

This section contains information about the following topics:

- [Adding an interface application](#) on page 163
- [Deleting an interface application](#) on page 164

Adding an interface application

Use this procedure to add an interface application.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS**.
3. Select the **Interface Apps** tab.
4. Click **Insert**.

The Insert Interface Apps screen opens.

5. In the fields provided, enter the information for the new entry.
6. Click **Insert**.

The new Interface Application entry is displayed on the **Interface App** tab.

Variable definitions

The following table outlines the parameters of the **Insert Interface Apps** dialog box.

Table 29: QoS Insert Interface Apps dialog box parameters

Variable	Value
Ports	Click the ellipse button and select the ports to configure for the QoS application.
AppEnable	Select the applications enabled for the ports selected in the Ports field.
DefaultGateway	Specifies the default gateway to configure for the arpSpoofing application.
IfType	Specifies the interface type to configure for the dhcpSnooping application.
DHCPServer	Specifies the DHCP server to configure for the dhcpSpoofing application.

Deleting an interface application

Use this procedure to delete an interface application.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS**.
3. Select the **Interface Apps** tab.
4. Select the Interface Application to delete.
5. Click **Delete**.

Viewing user-based policies

Use this procedure to open the **User Based Policy** tab.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS**.
3. Select the **User Based Policy** tab.

Variable definitions

The following table outlines the parameters of the **User Based Policy** tab.

Table 30: QoS User Based Policy tab parameters

Variable	Value
Id	Displays the unique numerical identification for this entry.
IfIndex	Displays the interface index for this entry.
RoleCombination	Displays the role combination associated with the interface in the IfIndex field and the user identified by the UserName field. A user role combination logically identifies a physical interface to which policy rules and actions can be applied. The role combination string must unique from any other defined role combination.
UserName	Displays the name of the user associated with this entry.
UserGroup	Displays the group the user is associated with.

Variable	Value
SessionId	Displays the system-assigned session identifier used to track instances of this user policy entry.
SessionStart	Displays the system-assigned session start timestamp. The value in this field corresponds to the value of the sysUpTime, converted to seconds, at the instant this user policy entry is created or updated.
SessionGroup	Displays the system-assigned session group identifier. TIP: Multiple user sessions belong to the same group if they share the same role combination and have the same value for this field. SessionGroup is associated with installed policy criteria to identify users and interfaces to which the QoS policy is applied.
SrcMacAddr	Displays the source MAC address associated with the identified user.
SrcMacAddrMask	Specifies the bits in a source MAC address that should be considered when an 802 MAC SA comparison is performed against the address specified in the SrcMacAddr field.
Storage	Specifies the storage type for this entry.

Configuring the QoS agent dialog box

Use this procedure to open the QoS agent dialog box.

Procedure steps

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

This section contains information about the following topics:

Viewing the QoS configuration

Use this procedure to open the **Configuration** tab.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Agent**.
3. Select the **Configuration** tab.

Variable definitions

The following table outlines the parameters of the **Configuration** tab.

Table 31: QoS Agent Configuration tab parameters

Variable	Value
QosOperMode	Specifies whether the QoS Agent support is enabled or disabled.
NVRamCommitDelay	Specifies the maximum time before nonvolatile QoS data is written to NVRAM.
ResetToPartialDefaults	Resets QoS configurations to default except for queue-set and buffering type.
ResetToDefaults	Resets all policy information to factory default values.
QueueCfg	Determines the queue set that is associated with all egress interfaces by default.
BufferingCaps	Determines the method through which buffering resources are allocated to ports sharing a pool of buffers. The value of this attribute determines the level of buffer sharing or over-allocation that can take place among ports sharing a buffer pool. Higher levels of over-allocation increase the likelihood (under heavy load) of a relatively few number of ports consuming all the buffers in a pool, causing packets to be dropped on other ports due to buffer starvation.
UBPSupportLevel	Sets the level of user-based policy support.
TrackStatistics	Specifies the type of statistics tracking.
AQApplicationMode	Specifies the behavior of Auto QoS application mode.
TrustedProcessingMode	Indicates the QoS trusted processing mode status. The trusted processing mode parameter is available only for a mixed stack of ERS 5500 Series switches.
TrustedProcessingMode	Trusted processing mode: partialDscpMapping (less QoS filters used) or fullDscpMapping (64 QoS filters used).
DappEnable	DoS Attack Prevention Package for ERS 5600 switches only: disable (default), enableWithoutStatusTracking (enabled without logging messages), enableWithStatusTracking (enabled with logging messages).
DappMinTcpHdrSize	Specifies the Dapp minimum TCP header size.
Dapplpv4IcmpMaxLength	Specifies the Dapp maximum length for IPv4 ICMP packets.
Dapplpv6IcmpMaxLength	Specifies the Dapp maximum length for IPv6 ICMP packets.

This section contains information about the following topics:

- [Enabling and disabling QoS agent support](#) on page 167
- [Enabling automatic QoS](#) on page 167
- [Disabling automatic QoS](#) on page 168
- [Configuring the QoS trusted processing mode](#) on page 168
- [Enabling DoS Attack Prevention Package \(DAPP\)](#) on page 168
- [Configuring DAPP minimum TCP header size](#) on page 169
- [Configuring DAPP maximum IPv4 ICMP length](#) on page 169
- [Configuring DAPP maximum IPv6 ICMP length](#) on page 169

Enabling and disabling QoS agent support

Use this procedure to enable and disable QoS Agent support.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Agent**.
3. Select the **Configuration** tab.
4. In the **QoSOperMode**, select enable or disable.

Enabling automatic QoS

Use this procedure to enable Automatic QoS support.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Agent**.
3. Select the **Configuration** tab.
4. Select the appropriate mode in the **AQApplicationMode** section from the following:
 - **enablePureMode** - Enables Automatic QoS functionality with DSCP remarking at egress disabled.
 - **enableMixedMode** - Enables Automatic QoS functionality with DSCP remarking at egress enabled.
5. Click **Apply**.

Disabling automatic QoS

Use this procedure to disable Automatic QoS support.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Agent**.
3. Select the **Configuration** tab.
4. Select **Disable** in the **AQApplicationMode** section.
5. Click **Apply**.

Configuring the QoS trusted processing mode

Use this procedure to configure the trusted processing mode.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Agent**.
3. Select the **Configuration** tab.
4. Select the appropriate mode in the **TrustedProcessingMode** section from the following:
 - **partialDscpMapping** - Sets the QoS trusted processing mode to partial DSCP mapping.
 - **fullDscpMapping** - Sets the QoS trusted processing mode to full DSCP mapping.
5. Click **Apply**.

Enabling DoS Attack Prevention Package (DAPP)

Use this procedure to enable DAPP.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Agent**.
3. Select the **Configuration** tab.

4. Under the DoS Attack Prevention Package section, choose the **DappEnable** mode:
 - **disable** (Default) - Disables DAPP.
 - **enableWithoutStatusTracking** - Enables DAPP without enabling status tracking.
 - **enableWithStatusTracking** - Enables DAPP and enables status tracking.
5. Click **Apply**.

Configuring DAPP minimum TCP header size

Use this procedure to set the minimum TCP header size used by DAPP.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Agent**.
3. Select the **Configuration** tab.
4. Under the DoS Attack Prevention Package section, enter a value in the range 0 to 255 in the **DappMinTcpHdrSize** text box.
5. Click **Apply**.

Configuring DAPP maximum IPv4 ICMP length

Use this procedure to set the maximum IPv4 ICMP length used by DAPP.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Agent**.
3. Select the **Configuration** tab.
4. Under the DoS Attack Prevention Package section, enter a value in the range 0 to 1023 in the **DappIpv4IcmpMaxLength** text box.
5. Click **Apply**.

Configuring DAPP maximum IPv6 ICMP length

Use this procedure to set the maximum IPv6 ICMP length that DAPP uses.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Agent**.
3. Select the **Configuration** tab.
4. Under the DoS Attack Prevention Package section, enter a value in the range 0 to 16383 in the **Dapplpv6lcmpMaxLength** text box.
5. Click **Apply**.

Viewing policy class support

Use this procedure to open the **Policy Class Support** tab.

Procedure steps

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

Variable definitions

The following table outlines the parameters of the **Policy Class Support** tab.

Table 32: QoS Agent Policy Class Support tab parameters

Variable	Value
PolicyClassName	Identifies the Policy Rule Classes (PRCs) the device supports. A PRC is synonymous to a MIB table; therefore, the supported PRCs indicate which MIB tables are supported for QoS processing purposes.
CurrentInstances	Specifies the current number of Policy Rules Instances (PRIs) that are installed for a specific PRC (equates to the current number of entries in a given MIB table).
MaximumInstalledInstances	Specifies the maximum number of PRIs that a user can install and/or modify for a specific PRC (equates to the number of MIB table entries that a user can create or modify).

Viewing policy device identifications

Use this procedure to open the **Policy Device Identification** tab.


Procedure steps

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

Variable definitions

The following table outlines the parameters of the **Policy Device Identification** tab.

Table 33: QoS Agent Policy Device Identification tab parameters

Variable	Value
Descr	Describes the policy agent.  Note: The description must include the name and version identification of the policy agent hardware and software.
MaxMsg	Specifies the maximum message size in octets that the device can support.

Viewing the resource allocation configuration for ERS 5500

Use this procedure to view the resource allocation configuration for the ERS 5500 switch.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Agent**.
3. Select the **Resource Allocation (ERS5500)** tab.

Variable definitions

Variable	Value
Port	Displays the port number.
MasksConsumed	Displays the number of QoS masks (policies) in use on that interface.
FiltersConsumed	Displays the number of rules (filters) in use by policy and filter data by that interface.

Variable	Value
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.
NonQoS_masksConsumed	Displays the number of Non QoS masks (policies) in use on that interface.
NonQoS_filtersConsumed	Displays the number of rules (filters) in use by Non QoS policy and filter data by that interface.
NonQoS_metersConsumed	Displays the number of meters in use by Non QoS policy data by that interface.

Viewing the resource allocation configuration for ERS 5600

Use this procedure to view the resource allocation configuration for the ERS 5600 switch.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Agent**.
3. Select the **Resource Allocation (ERS5600)** tab.

Variable definitions

The following table outlines the parameters of the **Resource Allocation (ERS5XXX)** tab.

Table 34: QoS Agent Resource Allocation (ERS5XXX) tab parameters

Variable	Value
Precedence	Displays the applied precedence.
Port	Displays the Port number.
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.
NonQoS_filtersConsumed	Tracks the current number of filters in use, not due to installed filter data, for a given precedence level and interface.

Variable	Value
NonQosMetersConsumed	Tracks the current number of meters in use, not due to installed policy data, for a given precedence level and interface.
TotalFiltersAvail	Displays the maximum number of filters available (for each precedence and for each ASIC).
TotalMetersAvail	Displays the maximum number of meters available (for each precedence and for each ASIC).
TotalCountersAvail	Displays the maximum number of counters available (for each precedence and for each ASIC).
RangeCheckersConsumed	Displays the number of range checkers consumed by QoS.

This section contains information about the following topics:

- [Filtering the resource allocation table](#) on page 173

Filtering the resource allocation table

Use this procedure to filter the resource allocation table.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Agent**.
3. Select the **Resource Allocation (ERS5XXX)** tab.
4. Click **Filter**.
5. Set the filter conditions.
 - a. Select **AND** to include all entries in the table that include all specified parameters, or select **OR** to include any of the specified parameters.
 - b. Select **IGNORE CASE** to include all entries with the parameters being set, whether in lower case or upper case.
 - c. Define the search to return all cases in which an entry **CONTAINS, DOES NOT CONTAIN, EQUALS TO, DOES NOT EQUAL TO** the set parameters.
 - d. Select **ALL RECORDS** to display all entries in the table.
 - e. Set **Precedence** to filter by order of precedence.
 - f. Select **Port** to display the entries by port.
6. Click **Filter**.

Configuring QoS filter limiting configuration

You can use the procedures in this section to disable, re-enable, and display information about QoS Filter Limiting, a feature that controls the maximum number of user-defined protocol VLANs.

Displaying QoS filter limiting

Use this procedure to display the QoS Filter Limiting status.

1. From the navigation tree, click **QoS**.
2. From the QoS tree, click **QoS**.
3. In the working area, click the **Filter Limiting** tab.

Disabling QoS filter limiting

Use this procedure to disable QoS Filter Limiting. Filter Limiting is enabled by default.

1. From the navigation tree, click **QoS**.
2. From the QoS tree, click **QoS**.
3. In the working area, click the **Filter Limiting** tab.
4. Click the **AdminEnabled** check box to change the status.
5. On the tool bar, click **Apply**.
6. Reset the switch.

Enabling QoS filter limiting

Filter Limiting is enabled by default. If you have disabled Filter Limiting, use this procedure to enable the feature.

1. From the navigation tree, click **QoS**.
2. From the QoS tree, click **QoS**.
3. In the working area, click the **Filter Limiting** tab.
4. Click the **AdminEnabled** check box to change the status.
5. On the tool bar, click **Apply**.
6. Reset the switch.

Table 35: Filter Limiting parameters

Variable	Value
AdminEnabled	The filter limiting next-boot status,
OperEnabled	The filter limiting current status. This is a read only field.

Opening the QoS NSNA/UBP/Traffic Profile dialog box

The procedures for configuring User Based Policies and the NSNA solution are nearly identical. When you assign a filter name to a VLAN (for example, redFilter), the switch automatically creates all the necessary QoS classifiers with the name you assigned (in this case, redFilter) if that filter does not already exist.

Traffic Profile applies the QoS policy on port(s) that you specify. UBP applies the QoS policy when a user is authenticated by EAPOL or non-EAPOL.

If you had previously defined the filter, then that pre-existent filter is used. Once a filter is created (either by you or automatically by the switch), it can be modified (that is, entries can be deleted or added) on the QoS NSNA/UBP/Traffic Profile dialog box.

Caution:

When you define multiple meters that may match the same traffic, you must specify the in-profile and out-of-profile traffic as drop or pass to ensure that the traffic is processed at the prescribed rate. If you do not do this, each meter processes the traffic, and this interaction can cause traffic to be treated in unexpected ways.

Use this procedure to open the QoS NSNA/UBP/Traffic Profile dialog box.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS NSNA/UBP/Traffic Profile**.

This section contains information about the following topics:

Viewing classifiers

Use this procedure to open the **Classifier** tab.

Procedure steps

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

Variable definitions

The following table outlines the parameters of the **Classifier** tab.

Table 36: QoS NSNA/UBP/Traffic Profile Classifier tab parameters

Variable	Value
Id	Specifies the ID number of the classifier.
Type	Specifies the type of classifier. Options are NSNA, UBP, and Traffic Profile.
Name	Specifies the name of the classifier. All classifiers with the same name are part of the same filter set. That filter set has the same name as the classifiers.
Block	Specifies the block name with which the classifier is associated.
EvalPrec	Specifies the evaluation order number of the classifier in that filter set. Two classifiers in the same filter set cannot have the same evaluation order. A higher eval order means a lower precedence for the corresponding policy. You can use the save eval-order for multiple classifiers within the same block.
AddrType	Specifies the type of IP address used by this classifier entry.
DstIpAddr	Specifies the IP address to match against the destination IP address of a packet.
DstIpPrefixLength	Specifies the length of the destination address mask.
SrcIpAddr	Specifies the IP address to match against the source IP address of a packet.
SrcIpPrefixLength	Specifies the length of the source address mask.
Dscp	Specifies the value for a DiffServ Codepoint (DSCP) in a packet.
Protocol/NextHeader	Specifies the IPv4 protocol value, or the IPv6 next-header value. Values are the following: <ul style="list-style-type: none"> • 1 = ICMP-IPv4 • 2 = IGMP • 6 = TCP

Variable	Value
	<ul style="list-style-type: none"> • 17 = UDP • 46 = RSVP • 58 = ICMP-IPv6
DstL4PortMin	Specifies the minimum value for the Layer 4 destination port number in a packet.
DstL4PortMax	Specifies the maximum value for the Layer 4 destination port number in a packet.
SrcL4PortMin	Specifies the minimum value for the Layer 4 source port number in a packet.
SrcL4PortMax	Specifies the maximum value for the Layer 4 source port number in a packet.
Ipv6FlowId	Specifies the flow identifier for IPv6 packets.
Storage	Specifies the type of storage used.
DstMacAddr	Specifies the MAC address against which the MAC destination address of incoming packets is compared.
DstMacAddrMask	Specifies a mask identifying the destination MAC address.
SrcMacAddr	Specifies a 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.
VlanTag	Specifies the type of VLAN tagging in a packet: <ul style="list-style-type: none"> • untagged • tagged • ignore
EtherType	Specifies the value for the Ethertype.
UserPriority	Specifies the value for the 802.1p user priority.
ActionDrop	Specifies whether or not to drop the traffic matching filtering data.
UpdateDscp	Specifies a value used to update the DSCP field in an IPv4 packet.
UpdateUserPriority	Specifies 802.1p value used to update user priority.
ActionSetPrec	Specifies automatic drop precedence (high or low).
IpFlags	Specifies the IP flags.
TcpCtrlFlags	Specifies the TCP control flags.

Variable	Value
Ipv4Options	Specifies whether IPv4 options are present.
PktType	Specifies the Layer 2 packet type.
MasterBlockMember	Specifies whether the master classifier is within the block or not.(Traffic Profile).
Rate	Specifies the Traffic Profile classifier meter rate (Traffic Profile Per-policy-individual-metering or Per-classifier-metering).
BurstSize	Specifies the Traffic Profile burst size (Traffic Profile Per-policy-individual-metering or Per-classifier-metering).
OutActionDrop	Specifies the drop action for out-of-profile packets (Traffic Profile Per-policy-individual-metering or Per-classifier-metering).
OutActionRemarkDscp	Specifies the remark DSCP action for out-profile-packets (Traffic Profile Per-policy-individual-metering or Per-classifier-metering).
OutActionSetPrec	Specifies the set precedence for out-profile-packets (Traffic Profile Per-policy-individual-metering or Per-classifier-metering).

This section contains information about the following topics:

- [Inserting a classifier](#) on page 178
- [Deleting a classifier](#) on page 179

Inserting a classifier

Use this procedure to configure a classifier for the NSNA solution, user-base policy, or Traffic Profile.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS NSNA/UBP/Traffic Profile**.
3. Select the **Classifier** tab.
4. Click **Insert**.
The Insert Classifier dialog box opens.
5. Using the **Type** radio options, choose whether to create a classifier for the NSNA solution (**NsnaClfr**), for a User Based Policy (**UbpClfr**) or a Traffic Profile (**Traffic Profile**).
6. Enter the classifier information in the fields.

7. Change values in any fields that present default values if you want to configure specific parameters.
8. Click **Insert**.

Deleting a classifier

Use this procedure to delete a classifier.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS NSNA/UBP/Traffic Profile**.
3. Select the **Classifier** tab.
4. Select the classifier you want to delete.
5. Click **Delete**.

Filtering a classifier

Use this procedure to filter a classifier.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS NSNA/UBP/Traffic Profile**.
3. Select the **Classifier** tab.
4. Select the classifier you want to filter.
5. On the toolbar, click **Filter**.

Viewing traffic profile sets

Use this procedure to open the **Set** tab.

Procedure steps

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

Variable definitions

The following table outlines the parameters of the **Set** tab.

Table 37: QoS NSNA/UBP/Traffic Profile Set tab parameters

Variable	Value
AclType	Specifies the type of ACL (NSNA, UBP, or Traffic Profile).
Name	Specifies a name for this entry. The name must be an existing classifier name. All classifiers with this name are part of this filter set. The filter set itself has this name.
IfIndex	Specifies the logical interface index assigned to the VLAN or the physical interface.
MeteringMode	Specifies the Traffic Profile Metering Mode as: <ul style="list-style-type: none"> • noMetering • perPolicyUniformRateMetering • perPolicyIndividualRateMetring • perClassifierMetering
CommittedRate	Specifies the committed rate (in Kbps).
BurstSize	Specifies the maximum number of bytes in a single transmission burst.
OutActionDrop	Specifies the action to take when packet is out-of-profile. This action is applied only if metering is being enforced, and if the traffic is deemed out-of-profile based on the level of traffic and the metering criteria. (Metering is applied only to traffic matching the filtering data.) Options are the following: <ul style="list-style-type: none"> • drop (packet is dropped) • pass (packet is not dropped)
OutActionUpdateDscp	Specifies the action to take to update DSCP when a packet is out-of-profile. The default value is -1. The value range is between -1–63.
SetPriority	Specifies the priority in the range 1–255. You can only change this field for a User Based Policy set. .
Status	Enables or disables the Traffic Profile set policy.
Storage	Specifies the type of storage for this entry.

This section contains information about the following topics:

- [Configuring a set](#) on page 181
- [Deleting a set](#) on page 181
- [Filtering a set](#) on page 181

Configuring a set

Use this procedure to configure a set.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS NSNA/UBP/Traffic Profile**.
3. Select the **Set** tab.
4. Click **Insert**.

The Insert Set dialog box opens.

5. Enter the set information in the fields.
6. Click **Insert**.

Deleting a set

Use this procedure to delete a set.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS NSNA/UBP/Traffic Profile**.
3. Select the **Set** tab.
4. Select a set to delete.
5. Click **Delete**.

Filtering a set

Use this procedure to filter a set.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS NSNA/UBP/Traffic Profile**.
3. Select the **Set** tab.
4. Select a set to filter.
5. Click **Filter**.
6. Set the filter parameters in the dialog.
7. Click **Filter**.

Index

Numerics

802.1pPriority field[128](#), [129](#), [137](#)

A

AbsBandwidth field[123](#)

Action field[146](#)

AddressType field[135](#)

aggregate flow[14](#)

ARP spoofing[42](#)

B

Bandwidth Allocation field[123](#)

Bandwidth field[123](#)

BlockNumber field[146](#)

BurstSize field[153](#)

C

Capabilities field[124](#)

class field[73](#)

classifier blocks[24](#), [35](#)

Classifier elements[24](#), [35](#)

ClassifierName field[154](#)

classifiers[35](#)

ClassifierSetId field[146](#)

ClassifierType field[154](#)

Command Line Interface (CLI)[49](#)

CommittedRate field[153](#)

CoS priority value[38](#)

CoS queues[38](#)

CoS-to-queue[38](#), [41](#)

CurrentInstances field[170](#)

D

DCOM[43](#)

DHCP Snooping[42](#)

DHCP Spoofing[43](#)

Differentiated services (DiffServ)[14](#)

Differentiated Services (DiffServ)[13](#)

Discipline field[123](#)

Drop field[149](#)

drop precedence[30](#)

DSCP[30](#)

Dscp field[129](#), [135](#)

DstAddr field[135](#)

DstL4Port field[135](#)

DstMacAddr field[137](#)

DstMacAddrMask field[137](#)

DstMaskLength field[135](#)

E

EAP[21](#)

egress QoS interface[38](#)

end-to-end QoS[14](#)

EPM[21](#)

EtherType field[137](#)

Extension field[149](#)

G

Group Assignment dialog box[125](#)

I

ICMP Echo Requests (ping)[40](#)

Id feild[149](#)

Id field[153](#)

IEEE 802.1p priority[30](#)

in-profile-action field[90](#)

InProfileAction field[153](#), [154](#)

Insert Action dialog box[150](#)

Insert Classifier Block dialog box[147](#), [148](#)

Insert Classifier dialog box[144](#)

Insert Interface Group dialog box[126](#)

Insert IP Classifier Element dialog box[136](#)

Insert L2 Classifier Element dialog box[138](#)

Insert Meter dialog box[153](#)

Insert Policy dialog box[156](#)

Interface Action Ext dialog box[152](#)

interface action extensions[28](#)

Interface Assignment button[125](#)

Interface groups[16](#)

Interface shaping[17](#)

InterfaceClass field[124](#)

InterfaceRoles field[154](#)

interfaces[73](#)

intradomain QoS[14](#)

IPv6FlowId field[135](#)

L

Label field[151](#)

M

MaximumInstalledInstances field[170](#)

MaxMsg field[171](#)

Meter field[146](#), [154](#)

microflow[14](#)

N

Name field[149](#), [153](#)

network access device[21](#)

NonMatchAction field[154](#)

NSNA[21](#)

O

out-profile-action field[90](#)

OutOfProfileAction field[153](#)

P

Packet classifiers[21](#)

per-hop behavior (PHB)[14](#)

Platinum, Gold, Silver, and Bronze classes[15](#)

Policy-enabled networks[13](#)

PolicyClassName field[170](#)

port-based Quality of Service[13](#)

Precedence field[154](#)

precedence range[34](#)

Premium class[15](#)

Q

QoS[126](#), [147](#), [148](#), [152](#), [154](#)

meter[154](#)

role combinations[126](#)

statistics[154](#)

classifier block[148](#)

classifier blocks[147](#)

interface action extension[152](#)

interface group[126](#)

policy precedence[154](#)

policy, enabling[154](#)

ports[126](#)

QoS actions[86](#)

QoS classes[35](#)

QoS egress port[37](#)

QoS interface[37](#)

QoS interface action[88](#)

QoS interfaces[41](#)

QoS metering[29](#)

QoS queue[37](#)

QoS security settings[61](#)

Quality of Service (QoS)[13](#), [14](#)

Queue bandwidth allocation[37](#)

Queue count[37](#)

Queue field[128](#)

Queue service discipline[37](#)

Queue service order[37](#)

Queue size[37](#)

queue weights[38](#)

QueueId field[123](#)

QueueSet field[127](#)

R

role-based policies[13](#)

RoleCombination field[127](#)

Roles field[124](#)

RPC[43](#)

S

service disciplines[38](#)

ServiceOrder field[123](#)

SetDropPrecedence field[149](#)

SetEgressNonUnicastPort field[151](#)

SetEgressUnicastPort field[151](#)

SetId field[123](#), [143](#)

single policy[34](#)

SLA[14](#)

SNMP[40](#)

Specific field[143](#)

SQLSlam[43](#)

SrcAddr field[135](#)

SrcL4Port field[135](#)

SrcMacAddr field[137](#)

SrcMacAddrMask field[137](#)

SrcMaskLength field[135](#)

Standard class[15](#)

Statistics[34](#)

StatsType field[154](#)

Status field[154](#)

Storage field[135](#), [137](#), [149](#), [151](#), [153](#), [154](#)

StorageType field[124](#)

system classifier[23](#)

T

traffic stream[14](#)
troubleshooting[147](#), [148](#), [152](#), [154](#)
 QoS[147](#), [148](#), [152](#), [154](#)
trusted[30](#)

U

UDP packets[43](#)
UDP port[43](#)
unrestricted[30](#)
untrusted[30](#)
Update Dscp field[149](#)
UpdateUserPriority field[149](#)
User Policy Table[21](#)

V

video stream[14](#)
VlanId field[137](#)
VlanTag field[137](#)

W

W32/Blaster-A[43](#)
W32/Nachi[43](#)
W32/Nachi-A[43](#)
W32/Nachi-B[43](#)
worm[43](#)
worms[43](#)
WRR queues[38](#)

