ExtremeSwitching™

Configuring Quality of Service on Ethernet Routing Switch 4900 and 5900 Series

Release 7.6
9035396
May 2018

Notice

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

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Extreme Networks shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Extreme Networks. End User agrees to indemnify and hold harmless Extreme Networks, Extreme Networks’ 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

Extreme Networks is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Extreme Networks. Extreme Networks 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. Extreme Networks does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Extreme Networks provides a limited warranty on Extreme Networks hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Extreme Networks’ standard warranty language, as well as information regarding support for this product while under warranty is available to Extreme Networks customers and other parties through the Extreme Networks Support website: http://www.extremenetworks.com/support under the link ““Policies” or such successor site as designated by Extreme Networks. Please note that if You acquired the product(s) from an authorized Extreme Networks Channel Partner outside of the United States and Canada, the warranty is provided to You by said Extreme Networks Channel Partner and not by Extreme Networks.

“Hosted Service” means an Extreme Networks hosted service subscription that You acquire from either Extreme Networks or an authorized Extreme Networks Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Extreme Networks or Extreme Networks Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN EXTREME NETWORKS HOSTED SERVICE SUBSCRIPTION FROM EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE EXTREME NETWORKS WEBSITE, https://extremeportal.force.com OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE EXTREME NETWORKS WEBSITE, https://extremeportal.force.com OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS EXTREME NETWORKS SOFTWARE, PURCHASED FROM EXTREME NETWORKS, INC., ANY EXTREME NETWORKS AFFILIATE, OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY EXTREME NETWORKS IN WRITING, EXTREME NETWORKS DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN EXTREME NETWORKS, AN EXTREME NETWORKS AFFILIATE OR AN EXTREME NETWORKS CHANNEL PARTNER; EXTREME NETWORKS 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 EXTREME NETWORKS, INC. OR THE APPLICABLE EXTREME NETWORKS AFFILIATE (“EXTREME NETWORKS”).

Extreme Networks grants You a license within the scope of the license types described below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Extreme Networks or an Extreme Networks Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Extreme Networks in writing. Extreme Networks may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Extreme Networks through electronic means established by Extreme Networks specifically for this purpose.

Copyright

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

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Extreme Networks Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Extreme Networks’ website at:http://www.extremenetworks.com/support/policies/software-licensing or such successor site as designated by Extreme Networks. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO EXTREME NETWORKS CHANNEL PARTNER’S HOSTING OF EXTREME NETWORKS PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN EXTREME NETWORKS CHANNEL PARTNER’S HOSTING OF EXTREME NETWORKS PRODUCTS MUST BE AUTHORIZED IN WRITING BY EXTREME NETWORKS AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE EXTREME NETWORKS CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE EXTREME NETWORKS CHANNEL PARTNER’S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE EXTREME NETWORKS CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE EXTREME NETWORKS CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE EXTREME NETWORKS CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Extreme Networks product is used.

Preventing Toll Fraud

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

Security Vulnerabilities

Information about Extreme Networks’ security support policies can be found in the Global Technical Assistance Center Knowledgebase at https://gtacknowledge.extremenetworks.com/.

Downloading Documentation

For the most current versions of Documentation, see the Extreme Networks Support website: http://documentation.extremenetworks.com, or such successor site as designated by Extreme Networks.

Contact Extreme Networks Support

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

Trademarks

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

Extreme Networks is a registered trademark of Extreme Networks, Inc.

All non-Extreme Networks trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

For additional information on Extreme Networks trademarks, please see: http://www.extremenetworks.com/company/legal/

Contents

Chapter 1: Preface

Purpose

This document provides procedures and conceptual information to configure security features on the following platforms:

- Extreme Networks Ethernet Routing Switch 4900 Series
- Extreme Networks Ethernet Routing Switch 5900 Series

The security function includes tasks related to product security such as the management and protection of resources from unauthorized or detrimental access and use. This document includes information that supports the configuration and ongoing management of the following:

- communications
- data security
- user security
- access

Examples and network illustrations in this document may illustrate only one of the supported platforms. Unless otherwise noted, the concept illustrated applies to all supported platforms.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at www.extremenetworks.com/education/.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.

- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at internalinfodev@extremenetworks.com

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- GTAC (Global Technical Assistance Center) for Immediate Support
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
  - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal – Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Extreme Networks Documentation

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for previous versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing.

Subscribing to Service Notifications

Subscribe to receive an email notification for product and software release announcements, Vulnerability Notices, and Service Notifications.

About this task

You can modify your product selections at any time.

Procedure

1. In an Internet browser, go to http://www.extremenetworks.com/support/service-notification-form/ .
2. Type your first and last name.
3. Type the name of your company.
4. Type your email address.
5. Type your job title.
6. Select the industry in which your company operates.
7. Confirm your geographic information is correct.
8. Select the products for which you would like to receive notifications.
9. Click **Submit**.

Chapter 2: New in this document

There are no feature changes in this document.

Chapter 3: Policy-based Network Fundamentals

This chapter provides an overview of the Differentiated Services (DiffServ) Quality of Service (QoS) network architecture. The switch provides a Command Line Interface (CLI) and Enterprise Device Manager (EDM) to configure QoS.

Policy-based networks

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

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

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

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

Port-based and Role-based QoS policies

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

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

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

QoS overview

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

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

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

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

DiffServ concepts

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

The DiffServ basic elements are implemented within the network and include

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

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

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

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

QoS components

The switch supports the following QoS classes:

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

The following table 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, excepting the one classified as Premium.
Standard network control	Network	Standard network control traffic.	Priority over user traffic.
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.

Table continues…

Traffic category	Service class	Application type	Required treatment
Real time, delay tolerant, low variable bandwith	Platinum	Interhuman communications requiring interaction with additional minimal delay (such as low-cost VoIP).	Higher-priority scheduling. 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. Competes for additional bandwidth.
Non-real time, mission critical, interactive	Silver	Transaction processing (such as Telnet, web browsing).	Medium priority scheduling. Competes for additional bandwidth.
Non-real time, mission critical, noninteractive	Bronze	For example, e-mail, FTP, SNMP.	Lower-priority scheduling. 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.

Note:

The above prioritization of classes is a general description. You can assign different priority levels to QoS classes. For more information, see:

Packet flow using QoS on page 22

Modifying CoS-to-queue priorities on page 21

Automatic QoS

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

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

AutoQoS mode may function in pure mode or in mixed mode. Depending on active AutoQoS mode, DSCP values may be maintained or remarked by AQ application. When AutoQoS mode is pure, packets are sent with DSCP value unchanged. When AutoQoS mode is mixed, DSCP value is remarked and packets are sent with “Standard DSCP” (see the following table). The following table shows standard DSCP, CoS, and drop precedence values:

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

Automatic QoS 802.1AB MED interoperability

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

Automatic QoS and ADAC interoperability

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

Queue sets

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

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

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

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

Important:

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

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

Modifying CoS-to-queue priorities

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

❗ **Important:**

Any modification to the CoS-to-queue values takes effect immediately; the system does not have to be reset to modify these values.

Interface shaping

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

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

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

❗ **Important:**

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

Egress queue shaping

QoS shaper rate queue servicing on the switch uses a weighted round robin algorithm to shape traffic. With egress queue shaping, you can specify the maximum and minimum egress shaping rates on an individual port and queue basis. You can configure shaping criteria for any or all egress queues associated with a switch port. The number of egress queues available for a port is determined by the QoS agent egress queue set value.

You can use queue shaping in conjunction with interface shaping.

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

Packet flow using QoS

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

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

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

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

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

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

Note:

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

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

Actions determine how the traffic is treated.

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

Figure 1: QoS Policy Schematic on page 23 provides a schematic overview of QoS policies.

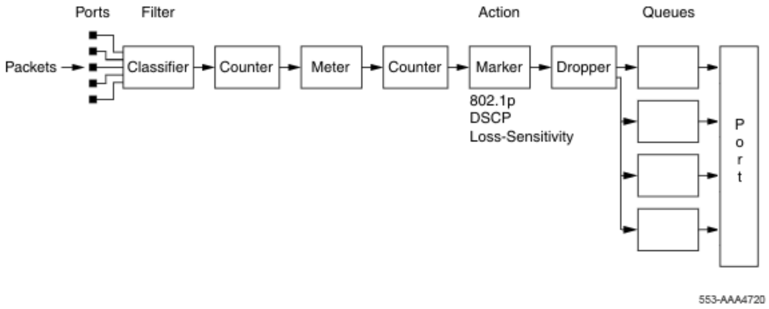

Figure 1: QoS Policy Schematic

DoS Attack Prevention Package

The switch 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:

It is recommended that 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.

User Based Policies

You can configure the switch to manage access with User Based Policies (UBP). UBP revolves around the User Policy Table supporting multiple users for each interface. User data is provided through interaction with Extensible Authentication Protocol (EAP) and is maintained in the User Policy Table. You can associate a user with a specific interface, user role combination, user name string, and optionally user group string.

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 the user-specific roles and policies.

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. When this conflict appears, the QoS is disabled on the interfaces.

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.

Specifying policies

Important:

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

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

Caution:

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

When configuring policies, it is important to consider that the policy with the highest precedence is evaluated first, and then the policy with the next lowest precedence and so on. The valid precedence range for QoS policies is 1 to 14. For example, with a precedence of 1 to 14, the system begins the evaluation with 14, moves on to 13, and so forth. Although there are 16 precedences available, the 16th and 15th precedences are permanently occupied by ARP and SPB, so, for practical purposes, 14 precedences are available.

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

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

Caution:

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

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

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

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

The policies tie together:

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

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

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

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

Important:

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

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

QoS configuration guidelines

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

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

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

Note:

Although there are 16 precedences available, the 16th and 15th precedences are permanently occupied by ARP and by ARP and SPBM only in SPBM mode, therefore for practical purposes 15 or 14 precedences are available.

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

- Up to 256 classifiers for each precedence for each ASIC.
- Up to 256 meters for each precedence for each ASIC, usable on a maximum of 8 out of the 16 available precedences.
- Up to 128 counters for each precedence for each ASIC.
- Up to 32 range checkers for each ASIC.
- Up to 14 policies per interface (port) can be configured.

The system supports 16 precedences used by QoS and non-QoS applications. Fourteen precedences can be assigned to QoS. You can configure meters on a maximum of 8 out of 16 precedences using QoS and non-QoS applications.

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

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

Model	ASIC Device 1
5928GTS	Port 1–28
5928GTS-PWR+	Port 1–28
5952GTS	Port 1–52
5952GTS-PWR+	Port 1–52
59100GTS-PWR+	Port 1-48, 97-98, second ASIC Port 49-96, 99-100
4926GTS	Port 1–26
4926GTS-PWR+	Port 1–26
4950GTS	Port 1–50
4950GTS-PWR+	Port 1–50

QoS configuration example

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

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

The following is an example of configuring QoS:

```
Switch(config)#qos if-group name "Trust_VoIP" class unrestricted
Switch(config)#no qos if-assign port 2-50
Switch(config)#qos if-assign port 1 name Trust_VoIP
Switch(config)#qos ip-element 1 ds-field 46
Switch(config)#qos classifier 1 set-id 1 name "Trust_VoIP" element-type ip element-id 1
Switch(config)#qos policy 1 name "Trust_VoIP" if-group "Trust_VoIP" clfr-type classifier
clfr-id 1 in-profile-action 7 precedence 6 track-statistics
```

QoS and traffic behavior

QoS is a Per Hop Behavior feature. This means traffic that is routed or switched by a system (is forwarded from source towards destination) is matched by QoS and is modified accordingly (drop, remark dscp, or remark priority). QoS might remark or drop traffic on ingress or egress for packets that are not forwarded, such as packets that enter or exit the CPU. OSPF, IGMP, ICMP are such examples of packets that enter or exit the CPU if these packets have the system as the destination (not forwarded by an L2 VLAN system).

The following table details QoS functionality on ingress and egress ports using routing protocols in an L3 configuration, using multicast traffic in an IGMP configuration, and showing the behavior of L2, L2 VSN, or IP Shortcuts scenario.

	Ingress filter		Egress filter	
	can drop	**can remark DSCP**	**can drop**	**can remark DSCP**
OSPF (CPU)	yes	no	yes	yes
IGMP snooping (CPU)	no	no	yes	yes
IGMP snooping proxy (CPU)	no	no	no	no
Address type IPv6 (CPU)	yes	no	yes	yes
ICMP v4 (CPU)	yes	no	yes	yes
ICMP v6 (CPU)	yes	no	yes	yes
any switched traffic in a L2 VLAN scenario	yes	yes	yes	yes
any IPv4/v6 forwarded traffic in a L3 scenario	yes	yes	yes	yes
any IPv4 forwarded traffic in an IP Shortcuts scenario	yes	yes	yes	yes
any IPv4/v6 traffic in a L2 VSN scenario	yes (on UNI ports) no (on NNI ports	yes (on UNI ports) no (on NNI ports	yes (on UNI ports) no (on NNI ports	yes (on UNI ports) no (on NNI ports
ARP (CPU)	no	n/a	n/a	n/a

Table continues…

	Ingress filter		Egress filter	
ARP pass through system (in a L2 VLAN switch scenario)	yes	n/a	n/a	n/a
LACP (CPU)	no	n/a	n/a	n/a
LLDP (CPU)	no	n/a	n/a	n/a
ADAC (CPU)	no	n/a	n/a	n/a
VLACP (CPU)	no	n/a	n/a	n/a
Autotopology (CPU)	no	n/a	n/a	n/a
DHCP (CPU)	no	n/a	n/a	n/a
STP (CPU)	no	n/a	n/a	n/a
SLPP (CPU)	no	n/a	n/a	n/a
ISIS (CPU)	no	n/a	n/a	n/a
CFM (CPU)	yes	n/a	n/a	n/a
n/a = options not available on egress for L2 packets, cannot remark DSCP on ingress for a L2 packet CPU = packets that enter or exits the system CPU (processed by the system, not forwarded)				

Traffic profile egress filters can match IPv4 and IPv6 protocols, and source and destination addresses only. The behavior described for traffic profile ingress filters is the same for the QoS, ACL or UBP policies. QoS policy, UBP and ACL can match packets on ingress basis only and can also filter on more options (L2, L3 or L4).

In an L2 VSN configuration, QoS and traffic profiles do not work on NNI ports due to double encapsulation-such policies work on UNI ports. Traffic rates configured for QoS if-shaper, QoS if-queue-shaper, and QoS meter can also issue unexpected rates for traffic passing from UNI to NNI and the reverse due to double encapsulation.

As a general rule, the egress policies can drop or remark DSCP for any traffic that exits on the CPU. On ingress, some packets for CPU can be dropped or DSCP remarked depending on specific protocols and CPU processing.

QoS traffic profile ingress, QoS policies, ACL and UBP can match traffic also on an L2, L3, and L4 basis for traffic ingress system. Using these options to drop packets can cause issues in an L2 switch scenario. For example, an ACL made on an L2 switching system to pass only a set of IP addresses has a drop implicit policy for the rest of non matched traffic. All ACLs drop the traffic that is not specified to pass. Policies to drop all non interesting traffic can be made from QoS policies, traffic profile, and UBP. In such cases, specifying to pass only some IP addresses and to drop the rest also drops APR packets. ARPs do not have IP source or destination addresses. If your policy does not pass some IP addresses towards a remote router, it is because ARP packets are dropped. To resolve this, make a QoS policy to pass ARPs on the highest available precedence before creating ACL, UBP, QoS or traffic profile policies, as shown in the following example.

```
qos if-group name unt class untrusted
qos if-assign port 1/2,2/2,3/2 name unt
qos l2-element 1 ethertype 0x806
qos classifier 1 set-id 1 element-type l2 element-id 1
qos policy 1 if-group unt clfr-type classifier clfr-id 1 in-profile-action 9 precedence
14 track-statistics individual
```

Note:

- More ports can be added or removed while the policy is applied in group named `unt`.
- Look for highest free precedence before creating ACL (show qos diag => for example, 14)

If ARPs have the L3 system as the destination (they are not forwarded by the system as in the case above), all ARPs are processed by the CPU even if a QoS, an ACL, a UBP, or a traffic profile could drop them. In this case there is no need for the QoS policy (to allow ARP) from above.

Rules

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

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

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

Classifier definition

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

Figure 2: Relationship of classifier elements, classifiers, and classifier blocks on page 32 displays the relationship between the classifier elements, classifiers, and classifier blocks.

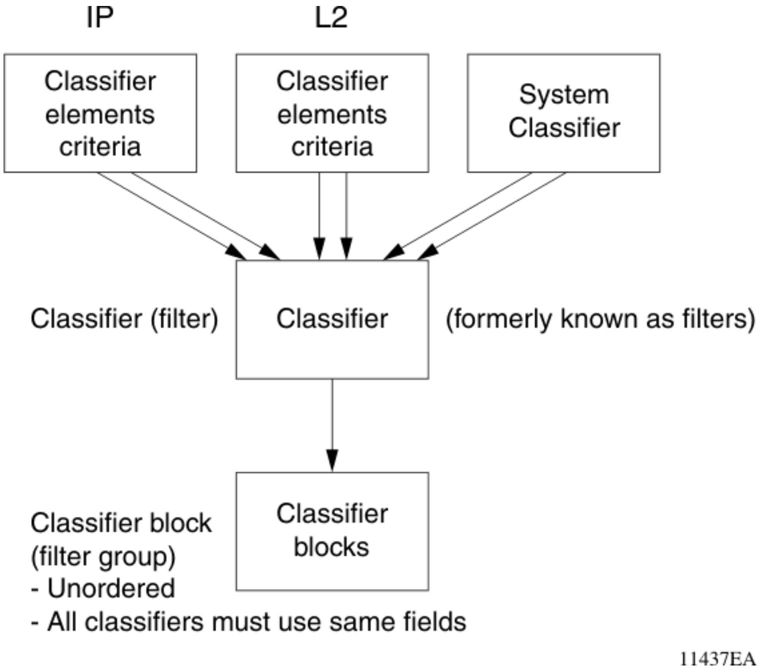
IP
L2
Classifier elements criteria
Classifier elements criteria
System Classifier
Classifier (filter)
Classifier
(formerly known as filters)
Classifier block (filter group)
- Unordered
- All classifiers must use same fields
Classifier blocks
11437EA

Figure 2: Relationship of classifier elements, classifiers, and classifier blocks

The system automatically creates some classifiers on untrusted ports and when AutoQoS is enabled, you can create additional classifiers.

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

You can apply these classifications to groups of ports (interface groups); also known as interface classes.

In your network, trusted ports are usually connected to the core of the DiffServ network and untrusted ports are typically access links connected to end stations.

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

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

IP classifier elements

The switch classifies packets based on the following parameters in the IP header:

- IPv4/IPv6 address type
- IPv6 flow identifier
- IPv4/IPv6 source address/mask
- IPv4/IPv6 destination address/mask

- IPv4 protocol type/IPv6 next-header
- IPv4/IPv6 DSCP value
- IPv4/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 switch classifies packets based on the following parameters in the Layer 2 header:

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

Important:

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

System classifier elements

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

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

The Content Aware Processor (CAE) lookup engine supports selection of 16 bytes within the first 128 bytes of the packet.

The following system classifier elements are supported:

- unknown IP multicast

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

Classifiers and classifier blocks

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

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

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

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

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

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

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

The following Classifier Elements need to be created:

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

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

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

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

Each classifier or classifier block is associated with actions that are executed when the packet matches the filter criteria in the group. The filter criteria and the associated actions, metering criteria, and interface groups are referenced by a policy, which dictates the overall traffic treatment (refer to Figure 3: Flowchart of QoS Actions on page 36 for an illustration of the traffic treatment).

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

Note:

Although there are 16 policy precedences available, the 16th and 15th precedences are permanently occupied by ARP and SPB (in SPBM mode), so, for practical purposes, 15 or 14 precedences are available.

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

Specifying actions

Figure 3: Flowchart of QoS Actions on page 36 summarizes how QoS matches packets with actions.

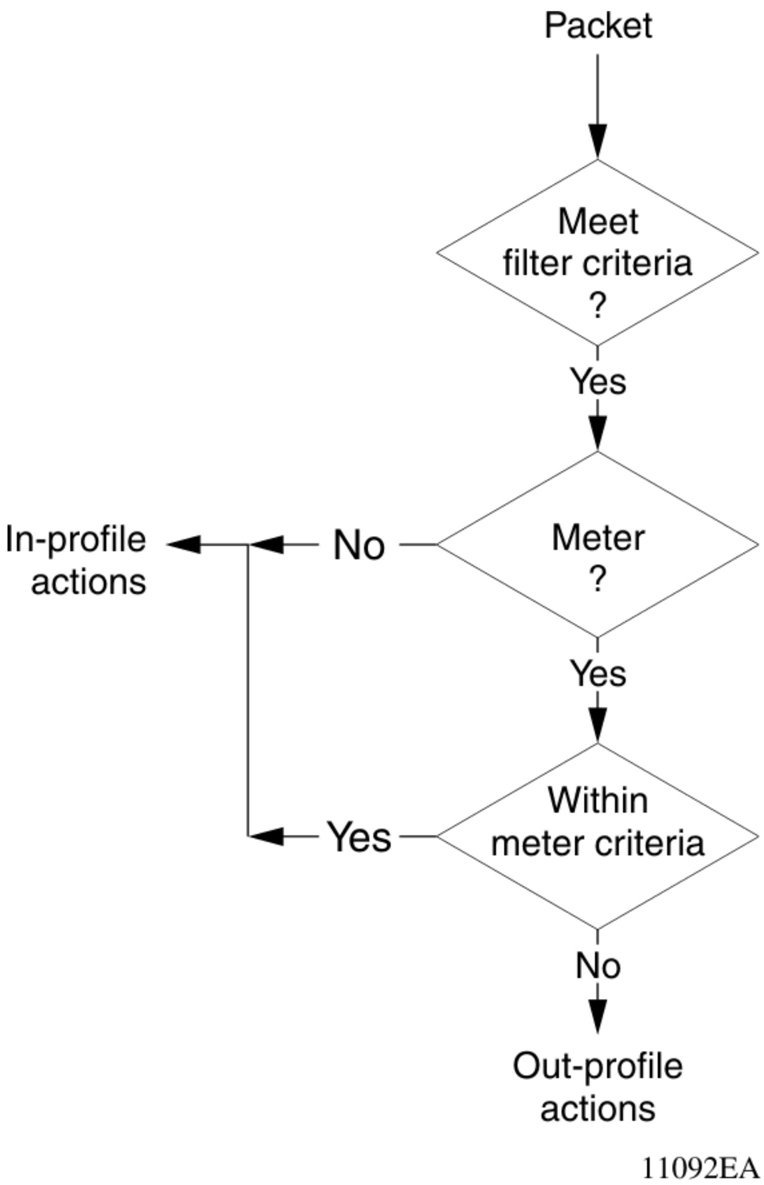

Figure 3: Flowchart of QoS Actions

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

Table 2: Summary of Allowable Actions

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

The switch filters collectively direct the system to initiate the following actions on a packet, depending on the configuration:

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

Important:

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

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

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

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

Important:

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

Specifying interface action extensions

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

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

Table 3: Summary of allowable interface action extensions

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

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

Important:

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

Specifying meters

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

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

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

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

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

Metering does not analyses or buffers the content to perform load balancing on classifiers. If a single meter is applied on a block with multiple matching elements (classifiers), load balancing between matching elements is not guaranteed. Traffic can be unevenly limited between classifiers and overall traffic can be limited to the established committed rate. In such case, uneven load balancing is seen if traffic continuously run from all classifiers. In real case scenarios, traffic does not run continuously from all classifiers at the same time, so uneven metering is rare. To avoid such scenario, individual meters for each classifier (matching elements) in a classifier block can be used.

Important:

The range for the committed rate is from 0 Kbps to 10 Gpbs using multiples of 64 Kbps or 1000 Kbps. If value 0 is selected, the specific rate is ignored.

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

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

Note:

For interface shaper, burst size can have a value from 2048 (2K) up to 8388608 (8192K).

Specifying interface groups

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

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

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

Important:

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

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

Important:

You must remove all ports from an interface group and all policies applied to that group before you delete the group.

Trusted, untrusted, and unrestricted interfaces

The switch ports are classified into three categories:

- trusted
- untrusted/untrustedv4v6/untrustedBasic
- unrestricted

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

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

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

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

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

OR

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

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

- Trusted interfaces -- IPv4 and IPv6 traffic received on trusted interfaces is re-marked at the layer 2 level, that is, the 802.1p user priority value is updated based on the DSCP value in the packet at ingress and the installed DSCP-to-CoS mapping data. The DSCP value is not updated. Remapping occurs, by default, only for standardized DSCP values (for example, EF, AFXX) and any Extreme proprietary values. The DSCP values that are remapped are associated with a non-zero 802.1p user priority value in the DSCP-to-COS Mapping Table.
- Untrusted interfaces -- IPv4 traffic received on untrusted interfaces is re-marked at the layer 3 level--that is, the DSCP value is updated. The new DSCP value is determined differently depending on whether the packet is untagged or tagged:
  - Untagged frames

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

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

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

- Tagged frames

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

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

- Untrustedv4v6 interfaces

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

- UntrustedBasic

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

The following table shows the default guidelines the switch uses to re-mark various fields of IPv4 traffic (and layer 2 traffic matching IPv4) based on the class of the interface. These actions occur if the user does not intervene at all; they are the default actions of the switch.

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

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

Important:

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

The switch does not trust the DSCP of IPv4 traffic received from an untrusted port, however, it does trust the DSCP of IPv4 traffic received from a trusted port.

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

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

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

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

If a packet is received from an untrusted (IPv4) or untrustedv4v6 (both IPv4 and IPv6) port and it does not match any one of the classifier elements installed by the user on the port, the switch uses default system classifiers to change the packet DSCP, IEEE 802.1p priority, and drop precedence as follows:

- If the packet is tagged, the 802.1p user priority value is derived from the DSCP-to-CoS mapping table using the best effort DSCP, which is 0.
- If the packet is untagged, the switch uses the default classifier to change the DSCP based on the default IEEE 802.1p priority of the ingress untrusted port. This default priority, which is 0, can be customized. Once this priority is determined, the switch uses the DSCP-to-CoS mapping table to determine the DSCP value.

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

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

QoS DSCP mutation

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

QoS traffic profile filter sets

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

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

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

For information about precedence, see Precedence values on page 25.

Policies within a set are applied to ingress traffic in a specific order. The evaluation order dictates the order in which classifier elements associated with the same filter set name are applied. Elements with a low evaluation order are applied before elements with a higher evaluation order. An evaluation order must be unique within a filter set. The 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:

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

Traffic profile filter set metering

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

Policy-based metering

Policy-based metering associates a unique meter with each policy that comprises the filter set. Each meter can independently apply to an individual classifier or block of classifiers. Meters can appear in all or some classifiers within a classifier block. The role of a master block classifier is to derive the characteristics. If multiple or no masters are detected in a classifier block, the one with the lowest evaluation order is chosen. Following are the types of policy-based metering:

- uniform metering—each meter has the same characteristics, including out-of-profile action, derived from the filter set instance definition.
- individual metering—each meter has unique characteristics, including out-of-profile action, derived from the individual classifier or master block classifier member associated with the filter set policy. If rate related characteristics are not specified in the individual or master block classifier definition, they are derived from the filter set instance.

In both uniform and individual policy-based metering, the in-profile-action is derived from the individual classifier or master block classifier.

Classifier-based metering

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.

Traffic profile filter set advantages

The following table lists the traffic profile filter set advantages over the standard QoS CLI support, as well as the deployed ACL functionality:

Feature	Traffic profile filter set advantage
Streamlined command set	Filter set definition and installation can be completed using two commands instead of using seven standard CLI QoS commands.
Combined IP and L2 options	Deployed ACL support forces you to define IP or L2 ACLs. Filter set classifier options include both IP and L2 data.
Meter availability	A filter set can be associated with metering criteria. Meters can be applied at the policy level (that is at the aggregate metering of the filters comprising a filter set policy) or to the individual classifiers within the filter set. ACL does not support metering.
No implicit drop	An ACL is terminated by an implicit drop-all prohibiting ACL layering on a port. This limitation is eliminated in the filter sets.
Addition or deletion support	Filter set classifier elements (filters or actions) can be added or deleted while the filter set is in-use (associated with a port). This type of manipulation is not supported in ACLs.
Additional filtering options	Latest IP or L2 filters options are available in conjunction with filter sets.

QoS agent disable or enable

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

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

ADAC for IP phones

For conceptual information relating to ADAC for IP phones, as well as procedures used to configure ADAC, see *Configuring VLANs, Spanning Tree, and MultiLink Trunking on Ethernet Routing Switch 4900 and 5900 Series*.

QoS queue statistics

You can use QoS queue statistics for network and configuration diagnostic. Because egress congestion is identified on a per queue basis with this feature, informed decisions are possible when configuring traffic prioritization and interface or queue shaping.

In oversubscription scenarios, dropped packets are normal. Queue packets counters indicate if the behavior is expected and acceptable or time-sensitive traffic is lost. In addition, considering that at low-level the queue resources are mostly related to buffer length, identifying the amount of actual data/bytes that is lost can help determine if a different QoS buffer allocation mechanism should be chosen.

QoS Double Wide

QoS Double Wide is an allocation mode that increases the number of possible classifier combinations. This allocation mode is also called double allocation mode.

You can use the double allocation mode to install complex classifiers that could not be installed in legacy single mode, such as classifiers based on source/destination MAC addresses used to identify EAP clients. A MAC address such as an IPv6 address is more restrictive with the other options possible in single allocation mode.

Limitations

The following restrictions apply when you use the double allocation mode:

- a precedence can have only one type of allocation mode. Double allocation mode and single allocation mode are mutually exclusive on a precedence. You cannot install a filter that requires double allocation mode on a precedence that is in single allocation mode, or vice-versa.
- the double allocation mode requires more resources per rule, resulting in less filters per precedence. The switch has 128 filters available in double allocation mode, and 256 filters available in single allocation mode.

Integration with UBP

You can use the **`alloc-mode`** parameter for the **`qos ubp classifier`** command to set the UBP allocation mode to double, single or best-effort. Blocks within a UBP filter can be forced to use only the single legacy mode or to be installed in double mode even if it is not necessary.

By default, the best-effort allocation mode is active. If you do not select an allocation mode, the system uses single mode. Only if using single allocation mode fails the system uses double mode. The decision is made per block, not per filter set. If a single classifier requires double allocation mode, then the whole block must be installed in double mode. Other blocks within the same set can be installed in single mode. This setting must be consistent across all classifiers within a block. An error message appears if there is a conflict.

The feature does not have to explicitly be enabled.

The restriction that double and legacy single allocation modes are mutually exclusive on a precedence affects the other QoS filter features and all non-QoS features that require filters to function. Using the double allocation mode increases the chance of not finding an available precedence slot that would have been possible if only single mode was used in the system. Legacy filters must skip the double precedence and try to find a single one. This could lead to situations when a filter appears in a different slot or fails to be installed even if based on legacy rules the filter should be installed. Filters that require double mode should be used as a last resort due to limited legacy compatibility and increased resource consumption.

Note:

Using double allocation mode can create a lot of restrictions. It is recommended to minimize the filter usage and balance the filter blocks involved.

Upgrading or downgrading considerations

When upgrading from a non-supported release, the allocation mode of existing UBP classifiers is set to best-effort.

Oversubscription and 2.5 Gbps support

Oversubscription occurs when traffic that needs to exit the unit on a port exceeds available bandwidth.

If oversubscription occurs on a 1 Gb port of a 5928MTS unit, pause frames will be seen on show port-statistics output in the *Received* section and *Dropped On No Resources* in the *Transmitted* section. Pause frames are not sent or received on that port and do not influence traffic behavior. They only have internal port meaning. Lossless functionality is not supported.

Oversubscription on 1 Gb or 2.5 Gb port will not equally load balance all traffic from one queue if high drop precedence is used. Not all the flows will have equally load balanced bandwidth at egress in oversubscription case. Equally load balance can be achieved using low drop precedence. For example all traffic will be considered best effort in default qos untrusted group (using default QoS and VLAN priority settings). All flows will be assigned to the same queue with high drop precedence. To set low drop precedence for best effort (untrusted qos group of ports), use the following command: **`qos egressmap ds 0 1p 0 dp low-drop`**.

Chapter 4: Configuring Quality of Service using CLI

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

Important:

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

Viewing QoS Parameters

About this task

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display QoS parameters:

   ```
   show qos [acl-assign <1 - 65535> | if-group | if-assign [port
   <portlist>]| queue-set | queue-set-assignment | queue-statistics
   [non-zero | port <LINE> | queue <1-8>] | ingressmap | egressmap ip-
   element [user | system | all | <1-65535>] | l2-element [user |
   system | all | <1-65535>] | classifier [user | system | all |
   <1-65535>] | classifier-block [user | system | all | <1-65535> ] |
   action [user | system | all] | if-action-extension [user | system |
   all | <1-65535>] | meter [user | system | all | <1-65535>] | if-
   queue-shaper [port <portlist>]| if-shaper [port <portlist>]| policy
   [user | system | all | <1-65535>] | agent | diag [unit | <cr>] | ip-
   acl <1 - 65535> | l2-acl <1 - 65535> | capability [meter | shaper]
   [port <portlist>]] system-element [user | system | all | <1-65535>]
   | statistics <1-65535> | traffic-profile [{classifier name <WORD>
   eval-order <1-255>} | interface | {set [port <LINE> name <WORD>} |
   {statistics port <LINE> name <WORD> precedence}] | port | ubp
   [interface | {classifier name <WORD>} | {statistics port <LINE> name
   ```

```
<WORD> precedence <1-7>}] | user-policy {[port <LINE>] [user
<WORD>]}
```

Variable Definitions

Use the data in the following table to use the **`show qos`** command.

Variable	Value
acl-assign <1 - 65535>	Displays the specified access list assignment entry.
if-group	Displays the interface groups.
if-assign [port <portlist>]	Displays the list of interface assignments.
queue-set	Displays the queue set configuration.
queue-set-assignment	Displays the association between the 802.1p priority to that of a specific queue.
queue-statistics [non-zero | port <LINE> | queue <1–8>]	Displays queue-statistics values. Valid values are: • non-zero- displays only queues with non-zero statistics. • port <LINE>- displays the queue statistics for the specified port. • queue <1–8>- displays the statistics on the specified queue.
ingressmap	Displays the 802.1p priority to DSCP mapping.
egressmap	Displays the association between DSCP, 802.1p priority, drop precedence, new DSCP, and the egress type of service name.
ip-element [user | system | all | <1-65535>]	Displays the IP classifier element entries. Valid values are: • user- displays only user-created and default entries. • system- displays only system entries. • all- displays user-created, default, and system entries. • <1-65535>- displays a particular entry. The default setting is all.
l2-element [user | system | all | <1-65535>]	Displays the Layer 2 element entries. Valid values are: • user- displays only user-created and default entries. • system- displays only system entries. • all- displays user-created, default, and system entries. • <1-65535>- displays a particular entry. The default setting is all.
system-element [user | system | all | <1-65535>]	Displays the system classifier element entries.

Table continues…

Variable	Value
classifier [user | system | all <1-65535>]	Displays the classifier set entries. • user- displays only user-created and default entries. • system- displays only system entries. • all- displays user-created, default, and system entries. • <1-65535>- displays a particular entry. The default setting is all.
classifier-block [user | system | all | <1-65535>]	Displays the classifier block entries. Valid values are: • user- displays only user-created and default entries. • system- displays only system entries. • all- displays user-created, default, and system entries. • <1-65535>- displays a particular entry. The default setting is all.
action [user | system | all | <1-65535>]	Displays the base action entries. Valid values are: • user- displays only user-created and default entries. • system- displays only system entries. • all- displays user-created, default, and system entries. • <1-65535>- displays a particular entry. The default setting is all.
if-action-extension [user | system | all | <1-65535>]	Displays the interface action entries. Valid values are: • user- displays only user-created and default entries. • system- displays only system entries. • all- displays user-created, default, and system entries. • <1-65535>- displays a particular entry. The default setting is all.
meter [user | system | all | <1-65535>]	Displays the meter entries. Valid values are: • user- displays user-created and default entries. • system- displays only system entries. • all - displays user-created, default, and system entries. • <1-65535>- displays a particular entry. The default setting is all.
if-queue-shaper port <portlist>	Displays the interface egress queue shaping parameters.
if-shaper port <portlist>	Displays the interface shaping parameters.

Table continues…

Variable	Value
policy [user | system | all | 1-65535>]	Displays the policy entries. Valid values are: • user- displays only user-created and default entries. • system- displays only system entries. • all- displays user-created, default, and system entries. • <1-65535>- displays a particular entry. The default setting is all.
statistics <1-65535>	Displays the policy and filter statistics values.
agent	Displays the global QoS parameters.
ip-acl <1 - 65535>	Displays the specified IP access list assignment entry.
l2-acl <1 - 65535>	Displays the specified Layer 2 access list assignment entry.
capability [meter | shaper] [port <portlist>]	Displays QoS meter or shaper port capabilities.
traffic-profile [{classifier name <WORD> eval-order <1-255>} | interface | {set [port <LINE> name <WORD>} | {statistics port <LINE> name <WORD> precedence}	Displays QoS traffic profile entries. Valid values are: • classifier- displays QoS traffic profile classifier entries. • val-order <1-255>- specifies the evaluation order to reference a specific traffic profile classifier entry. • interface- displays QoS traffic profile interface entries. • name <WORD>- specifies the label to display a specific traffic profile classifier entry. • port <LINE>- specifies the port used to reference the traffic profile entry. • precedence- specifies the precedence used to reference the traffic profile entry. • set- displays QoS traffic profile set entries. • statistics- displays QoS traffic profile statistics.
port	Displays QoS port configurations.
ubp {interface | [classifier] name <WORD> | statistics port <LINE> name <WORD> precedence <1-7>}	Displays QoS UBP entries. Valid values are: • classifier- Displays QoS UBP classifier entries. • interface- Displays QoS UBP interface entries. • name- Specifies the label to display a particular UBP template entry. • name <WORD>- Specifies the label to display a specific UBP classifier entry. • port <LINE>- Specifies a port to reference UBP entry. • precedence <1-7>- Specifies the precedence used to reference the UBP entry.

Table continues…

Variable	Value
	• statistics- Displays QoS UBP statistics.
user-policy [port <LINE>] [user <WORD>]	Displays QoS user policy entries. Valid values are: • port <LINE>- Specifies the ports used to reference the user policy entries. • user <WORD>- Specifies the user for whom the user policy must be displayed.

Displaying QoS queue statistics

Use the following procedure to display queue statistics, filtered by port, queue and/or non-zero queues.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display queue statistics:

   ```
   show qos queue-statistics [port <LINE>] [queue <1-8>] [non-zero]
   ```

Example

Note:

The **`show qos queue-statistics`** command has two output formats, depending on the switch terminal width. The following examples are based on a terminal width bigger than 105.

Display statistics on a specific port or on a specific queue:

```
Switch(config)#show qos queue-statistics port 1/14


Unit/Port  Queue     Out Packets          Out Bytes         Drop Packets         Drop
Bytes
---------  -----  ----------------  ------------------  ------------------
------------------
1/14       1      4754131           304268304           0                   0
           2      130717            8365888             4622860             314354480
           3      61119             3911616             4692458             319087144
           4      26251             1680064             4727326             321458168
           5      9009              576576              19005401            1235351064
Switch(config)#show qos queue-statistics port 1/2,1/26,2/13 queue 2

Unit/Port  Queue     Out Packets          Out Bytes         Drop Packets         Drop
Bytes
---------  -----  ----------------  ------------------  ------------------
------------------
1/2        2      33272896          2418392968          53238081            3531995776
1/26       2      32816329          2389172680          46346395            3063361080
2/13       2      32858094          2392129452          46282398            3020869800
```

Display non-zero queue statistics on the entire setup:

```
Switch(config-if)#show qos queue-statistics non-zero

Unit/Port  Queue     Out Packets          Out Bytes         Drop Packets         Drop
Bytes
---------  -----  ----------------  ------------------  ------------------
------------------
1/2        1         61                   4453              0                    0
2          2418116   154759424                              0                    0
1/3        1         61                   4453              0                    0
2          2418138   154760832                              0                    0
1/4        1         61                   4453              0                    0
2          2418158   164434724                              0                    0
1/8        1         61                   4453              0                    0
2          11811489                       803181232         562303               35987392
1/10       1         61                   4458              0                    0
2          11        704                  0                 0
1/47       1         61                   458               0                    0
2          7         448                  0                 0
```

Variable definitions

Use the data in the following table to display queues for active links using the `show qos queue-statistics` command.

Variable	Value
<port>	Displays the queue statistics for the specified port.
<queue>	Displays the statistics on the specified queue.
[non-zero]	Displays only queues with non-zero statistics.

Clearing QoS queue statistics

Use the following procedure to clear queue statistics on a specific queue or specific ports and queue.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Clear queue statistics:

```
qos clear-queue-stats [port <port_list>] [queue <queue>]
```

Example

Clearing the statistics on a specific queue or specific ports and queue:

```
Switch(config-if)#show qos queue-statistics port 1/2,1/21,2/13 non-zero

Unit/Port  Queue     Out Packets          Out Bytes         Drop Packets          Drop
Bytes
---------  -----  ----------------  ------------------  ------------------
------------------
1/2        1      91                6490                0                   0
           3      1355546           86754944            0                   0
           6      17                1088                0                   0
1/21       1      78                5552                0                   0
           2      1355546           86754944            0                   0
           6      12                768                 0                   0
2/13       2      968344            61974016            387202              24780928
           3      451929            28923456            903617              57831488
           8      91                6384                0                   0
Switch(config-if)#qos clear-queue-stats queue 3
Switch(config-if)#show qos queue-statistics non-zero


Unit/Port  Queue     Out Packets          Out Bytes         Drop Packets          Drop
Bytes
---------  -----  ----------------  ------------------  ------------------
------------------
1/2        1      98                6938                0                   0
           6      19                1216                0                   0
1/21       1      86                6176                0                   0
           2      1355546           86754944            0                   0
           6      14                896                 0                   0
2/13       2      968344            61974016            387202              24780928
           8      101               7136                0                   0
Switch(config-if)#qos clear-queue-stats port 2/13 queue  2
Switch(config-if)#show qos queue-statistics non-zero


Unit/Port  Queue     Out Packets          Out Bytes         Drop Packets          Drop
Bytes
---------  -----  ----------------  ------------------  ------------------
------------------
1/2        1      115               8137                0                   0
           6      22                1408                0                   0
1/21       1      103               7376                0                   0
           2      1355546           86754944            0                   0
           6      17                1088                0                   0
2/13       8      120               8464                0                   0
```

Variable definitions

Use the data in the following table clear statistics using the `qos clear-queue-stats` command.

Variable	Value
<port>	Clear statistics on the specified port.
<queue>	Clear statistic on the specified queue.

Configuring QoS Access Lists

The CLI commands described in this section allow for the configuration and management of QoS access lists. For information on displaying this information, refer to Viewing QoS on page 47.

Assigning ports to an access list

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

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

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

On the switch, by default, five out of the 16 QoS precedences are reserved for ARP, SPB, DHCP, and two default QoS policies (UntrustedClfrs1 and UntrustedClfrs2), leaving only 11 QoS precedences available.

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

In the following example, the `show qos diag` output displays that five out of the 16 QoS precedences are being utilized by ARP, SPB, DHCP and two default QoS policies (UntrustedClfrs1 and UntrustedClfrs2) leaving 11 QoS precedences available.Therefore, you can only apply an IP or L2 ACL policy with 11 IP or L2 classifier elements to a port.

```
Switch# show qos diag
UUnit/Port                      Mask Precedence Usage
           16  15  14  13  12  11  10   9   8   7   6   5   4   3   2   1
--------- ----------------------------------------------------------------
1/1         AR  SB  DH                                              Q   Q
AR=ARP DH=DHCP Q=QoS SB=SPB
```

With 16 available QoS precedences, if you create 12 IP or L2 classifier elements in an IP or L2 ACL and attempt to apply the ACL to a port, the switch rejects the ACL and returns the `Inadequate resources available for application policy criteria` error message. In this scenario, to successfully apply an IP or L2 ACL to a port, you must delete one of the IP or ACL elements in the IP or L2 ACL before you can apply the ACL to a port.

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. Assign ports to an access list:

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

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

Variable Definitions

Use the data in the following table to use the **qos acl-assign** command.

Variable	Value
<1 - 55000>	A unique identifier for the access list assignment.
enable	Enable the access-list assignment entry.
port <port_list>	The list of ports assigned to the specified access list.
acl-type {ip | l2}	The type of access list used; IP or Layer 2.
name <WORD>	The name of the access list to be used. Access lists must be configured before ports can be assigned to them.

Creating an IP access list

About this task

Use the following procedure to create an IP access list.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Create an IP access list:

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

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

Variable Definitions

Use the data in the following table to use the **qos ip-acl** command.

Variable	Value
name <WORD>	The name assigned to this access list.
addr-type <addrtype>	The IP address type to use for the access list; range is ipv4 or ipv6.
src-ip <source_ip>	The source IP address and mask to use for this access list, in the form of a.b.c.d/x for IPv4, or x:x:x:x:x:x:x:x/z for IPv6.
dst-ip <destination_ip>	The destination IP address to use for this access list.
ds-field <dscp>	The DSCP value to use for this access list; range is 0-63.
{protocol <protocol_type> | next_header <header>}	The protocol type or IP header to use with this access list.
src-port-min <port> src-port-max <port>	The minimum and maximum source ports to use with this access list. Both values must be specified.
dst-port-min <port> dst-port-max <port>	The minimum and maximum destination ports to use with the access list. Both values must be specified.
session-id <sessionid>	The flow ID to use with this access list.
drop-action {enable | disable}	The drop action to use for this access list. Enable specifies to drop packets and disable specifies to not drop packets.
update-dscp <0 - 63>	The DSCP value to update for this access list.
update-1p <0 - 7>	The 802.1p value to update for this access list.
set-drop-prec {high-drop | low-drop}	The drop precedence to configure for this access list.
block <block_name>	The block name to associate with the access list.

Creating a Layer 2 access list

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Create a Layer 2 access list:

   ```
   [no] qos l2-acl name <WORD> [src-mac <source_mac_address>] [src-mac-
   mask> <source_mac_address_mask>] [dst-mac <destination_mac_address>]
   [dst-mac-mask <destination_mac_address_mask> [vlan-min <vid_min>
   vlan-max <vid_max>] [vlan-tag <tagged | untagged>] [ethertype
   <etype>] [priority <ieee1p_seq>][drop-action {enable | disable}]
   [update-dscp <0 - 63>][update-1p <0 - 7>] [set-drop-prec {high-drop
   | low-drop}] [block <block_name>]
   ```

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

Variable Definitions

Use the data in the following table to use the **qos l2-acl** command.

Variable	Value
name <WORD>	The name assigned to this access list.
src-mac <source_mac_address>	The source MAC address to use for this access list.
src-mac-mask <source_mac_address_mask>	The source MAC address mask to use for this access list.
[dst-mac <destination_mac_address>]	The destination MAC address to use for this access list.
dst-mac-mask <destination_mac_address_mask>	The destination MAC address mask to use for this access list.
vlan-min <vid_min> vlan-max <vid_max>	The minimum and maximum VLANs to use with this access list. Both values must be specified.
vlan-tag <tagged | untagged>	Specify the VLAN tag classifier criteria: • untagged • tagged The default is Ignore.
ethertype <etype>	The Ethernet protocol type to use with the access list.
priority <ieee1p_seq>	The priority value to use with this access list. Valid range is 0-7 or all.
drop-action {enable | disable}	The drop action to use for this access list. Enable specifies to drop packets and disable specifies to not drop packets.
update-dscp <0 - 63>	The DSCP value to update for this access list.
update-1p <0 - 7>	The 802.1p value to update for this access list.
set-drop-prec {high-drop | low-drop}	The drop precedence to configure for this access list.
block <block_name>	The block name to associate with the access list.

Configuring CoS-to-Queue assignments

About this task

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

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Configure CoS-to-Queue assignments:

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

Example

```
Switch>enable
Switch#configure terminal
Switch(config)#qos queue-set-assignment queue-set 2 1p 4 queue 6
```

Variable Definitions

Use the data in the following table to use the **`qos queue-set-assignment queue-set`** command.

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

Configuring QoS Interface Groups

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

Adding ports to an interface group

About this task

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

Procedure

1. Enter Interface Configuration mode:

```
enable
```

```
configure terminal
```

```
interface ethernet <port number>
```

2. Add ports to an interface group:

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

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

Important:

The system automatically removes the port from an existing interface group to assign it to a new interface group. If the command is used from Global Configuration mode and port parameter is omitted, all stack ports are added in the specified interface group.

Example

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface ethernet all
Switch(config-if)#qos if-assign port 12 name NEW
```

Variable Definitions

Use the data in the following table to use the **qos if-assign** command.

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

Creating an interface group

About this task

Use the following procedure to create an interface group.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Create an interface group:

   ```
   [no] qos if-group name <WORD> class <trusted | untrusted |
   unrestricted | untrusted | untrustedbasic | untrustedv4v6>
   ```

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

   Important:

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

Variable Definitions

Use the data in the following table to use the **qos if-group** command.

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

DSCP and 802.1p and queue association configuration

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

Configuring egress mapping

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

Important:

During periods of congestion, low drop precedence traffic will be buffered, while high drop precedence traffic could be dropped due to buffer availability on the switch. Since the high drop precedence traffic may not be buffered and queued at egress, it may not be processed as per the stated WRR relative percentages. Low drop precedence traffic streams will contend for the same buffer resources, with the buffers queued and processed at egress per the WRR percentages.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Configure egress mapping:

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

Variable Definitions

Use the data in the following table to use the **`qos egressmap`** command.

Variable	Value
name <WORD>	Specifies the label for the egress mapping.
ds <0-63>	Specifies the DSCP value used as a lookup key for 802.1p priority and drop precedence at egress when appropriate; range is between 0 and 63.
1p <0–7>	Specifies the 802.1 priority associated with the target DSCP.
dp {high-drop | low-drop}	Specifies the drop precedence associated with the target DSCP.
ds-new <0–63>	Specifies the new DSCP associated with the target DSCP.

Resetting egress mapping values

About this task

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

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Reset entries:

```
default qos egressmap
```

Configuring ingress mapping values

About this task

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

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Configure ingress mapping values:

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

Variable Definitions

Use the data in the following table to use the **`qos ingressmap`** command.

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

Resetting ingress mapping values

About this task

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

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Reset the value:

```
default qos ingressmap
```

QoS IP classifier element management

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

Configuring an IP classifier element

About this task

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

Procedure

1. Enter Global Configuration mode:

```
enable

configure terminal
```

2. Configure an IP classifier element:

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

Important:

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

Variable Definitions

Use the data in the following table to use the **qos ip-element** command.

Variable	Value
<1-55000>	Specifies the IP classifier element identification number. Values range from 1–55000.
addr-type <addr_type>	Specify the address type, either ipv4 or ipv6. The default is ipv4.
ds-field <0-63>	Specifies the value for the DSCP in a packet. Values range from 0–63.
dst-ip <dst-ip-info>	Enter the source IP address and mask in the form of a.b.c.d/x or a.b.c.d x.x.x.x for IPv4, or x:x:x:x:x:x:x:x/z for IPv6. Default is 0.0.0.0.
dst-port-min <0-65535>	Specifies the minimum value permitted for the Layer 4 destination port number in a packet. Values range from 0–65535.
flow-id <0x00-0xfffff>	Specifies the flow identifier for IPv6 packets. Values range from 0–1048575 (0x00 to 0xfffff hexadecimal).
ip-flag <ip_flags>	Specifies the value of flags present in an IPv4 header.
ipv4-option <no-opt|with-opt>	Specifies whether the Option field is present in the packet header. Values include: • no-opt—indicates that only IPv4 packets without options match this classifier element. • with-opt—indicates that only IPv4 packets that include options match this classifier element.
name <WORD>	Specifies an alphanumeric label for the IP classifier element. Value is a character string from 1–16 characters in length.
next-header <0-255>	Specifies the IPv6 next header the classifier element will match. Values range from 0–255. A value of 255 indicates that the system ignores the parameter.

Table continues…

Variable	Value
protocol <0-255>	Specifies the IPv4 protocol. Values range from 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:x:x/z for IPv6. Default is 0.0.0.0.
src-port-min <0-65535>	Specifies the minimum value permitted for the Layer 4 source port number in a packet. Values range from 0–65535.
tcp-control <a|f|p|r|s|u>	Specifies the control flags present in an TCP header. Values include: • a=Ack • f=Fin • p=Psh • r=Rst • s=Syn • u=Urg

Deleting an IP classifier element

About this task

Use the following procedure to delete an IP classifier element.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Delete an IP classifier element:

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

   Important:

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

Variable Definitions

Use the data in the following table to use the **`no qos ip-element <1-55000>`** command.

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

Viewing IP classifier element information

About this task

Use the following procedure to display IP classifier configuration information.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display IP classifier element information:

   ```
   show qos ip-element
   ```

Variable Definitions

Use the data in the following table to use the **`show qos ip-element`** command.

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

QoS L2 classifier element management

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

Configuring a Layer 2 classifier element

About this task

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure Layer 2 element entries:

```
qos l2-element <1-55000> [dst-mac <dst_mac_addr>][dst-mac-mask
<dst_mac_mask>] [ethertype <0x00-0xffff>] [name <WORD>] [pkt-type
<etherII|llc|snap>] [priority <0-7|all>] [src-mac <src_mac_addr>]
[src-mac-mask <src_mac_mask>] [vlan-min <1-4094>] [vlan-tag <tagged|
untagged>]
```

Important:

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

Variable Definitions

Use the data in the following table to use the **`qos l2-element`** command.

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

Table continues…

Variable	Value
vlan-min <1-4094>	Specifies the minimum VLAN ID range for the L2 classifier element. Values range from 1–4094.
vlan-tag <tagged|untagged>	Specifies the type of VLAN tagging in a packet. Values include: • untagged • tagged

Deleting a Layer 2 classifier element

About this task

Use the following procedure to delete an L2 classifier element.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Delete a Layer 2 classifier element:

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

   Important:

   A Layer 2 element that is referenced in a classifier cannot be deleted.

Variable Definitions

Use the data in the following table to use the **`no qos l2-element <1-55000>`** command.

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

Viewing Layer 2 classifier element information

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Display Layer 2 classifier element information:

   ```
   show qos l2-element
   ```

Variable Definitions

Use the data in the following table to use the **`show qos l2-element`** command.

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

QoS system classifier element management

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

Configuring a QoS system classifier element

About this task

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

Important:

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Create and manage a QoS system classifier element:

   ```
   qos system-element <1-55000> [known-ip-mcast] [known-non-ip-mcast]
   [name <WORD>] [non-ip] [pattern-data <WORD>] [pattern-format <tagged
   | untagged>] [pattern-ip-version <ipv4|ipv6|non-ip>] [pattern-l2-
   ```

```
format <ethernetII|llc|snap>] [unknown-ip-mcast] [unknown-non-ip-
mcast] [unknown-ucast]
```

Variable Definitions

Use the data in the following table to use the **`qos system-element`** command.

Variable	Value
<1-55000>	System classifier element entry id; range is 1–55000.
known-ip-mcast	Matches frames with known IP multicast destination address.
known-non-ip-mcast	Matches frames with known non-IP multicast destination address.
name <WORD>	Specifies an alphanumeric label for the system classifier entry. Value is a character string from 1–16 characters in length.
non-ip	Matches non-IP frames.
pattern-data <WORD>	Matches frames with specific byte pattern data. The format of the WORD string is byte numbers separated by colons (XX:XX:XX:....:XX.).
pattern-format <tagged | untagged>	Specifies the format of the pattern data and mask. Values include tagged or untagged.
pattern-ip-version <ipv4|ipv6|non-ip>	Specifies the IP version of the pattern data and mask. Values include ipv4, ipv6, or non-ip.
pattern-l2-format <ethernetII|llc|snap>	Specifies the format of the L2 pattern data and mask. Values include: • ethernetII • llc • snap
unknown-ip-mcast	Matches frames with an unknown IP multicast destination address.
unknown-non-ip-mcast	Matches frames with an unknown non-IP multicast destination address.
unknown-ucast	Matches frames with an unknown unicast destination address.

Deleting a QoS system classifier element

About this task

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

Important:

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Delete a QoS system classifier element:

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

Variable Definitions

Use the data in the following table to use the **`no qos system-element`** command.

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

Viewing system classifier element information

About this task

Use this procedure to display system classifier configuration information.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Display system classifier element information:

   ```
   show qos system-element
   ```

Variable Definitions

Use the data in the following table to use the **`show qos system-element`** command.

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

QoS classifier management

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

Configuring a QoS classifier

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure classifier entries:

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

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

   Important:

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

Variable Definitions

Use the data in the following table to use the **qos classifier** command.

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

Deleting a QoS classifier

About this task

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

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Delete a QoS classifier:

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

Important:

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

Variable Definitions

Use the data in the following table to use the **`no qos classifier`** command.

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

Viewing QoS classifier information

About this task

Use the following procedure to display QoS classifier configuration information.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display QoS classifier configuration information:

```
show qos classifier
```

Variable Definitions

Use the data in the following table to use the **`show qos classifier`** command.

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

QoS classifier block management

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

Configuring classifier block entries

About this task

Use this procedure to combine individual classifiers.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure classifier block entries:

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

   Important:

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

Variable Definitions

Use the data in the following table to use the **`qos classifier-block`** command.

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

Table continues…

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

Deleting a classifier block entry

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Delete a classifier block:

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

   Important:

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

Variable Definitions

Use the data in the following table to use the **`no qos classifier-block`** command.

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

Viewing a classifier block entry

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Display a classifier block:

   ```
   show qos classifier-block
   ```

Important:

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

Variable Definitions

Use the data in the following table to use the **`show qos classifier-block`** command.

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

QoS traffic profile filter set configuration

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

When stage egress classifier is used the traffic is dropped or dscp modified for traffic egressing the port where set is applied. If stage egress is not set on classifier the traffic is dropped or dscp modified for traffic ingressing the port where set is applied.

You can use up to 75 classifier elements in a filter set.

Configuring a QoS traffic profile filter set classifier

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Create a new traffic profile filter set classifier element:

   ```
   qos traffic-profile classifier name <WORD> [addr-type <ipv4|ipv6>]
   [block <WORD>][committed-rate <64-10230000> {committed-burst-size
   <burst-size-options> drop-out-action <disable|enable>| max-burst-
   rate <64-4294967295> max-burst-duration <1-4294967295>}][drop-action
   ```

```
<disable|enable>][ds-field <0-63>] [dst-ip <dst-ip-info>][dst-mac
<dst-mac-info> dst-mac-mask <dst-mac-mask>][src-mac <src-mac> src-
mac-mask <src-mac-mask>][dst-port-min <0-65535> dst-port-max
<0-65535>][src-port-min <0-65535> src-port- max <0-65535>][ethertype
<0x0-0xFFFF>] [stage <egress>] [eval-order <1-255>][flow-id
<0x0-0xFFFF>][ip-flag <ip-flags>][ipv4-option <no-opt|with-opt>]
[master][next-header <0-255>][pkt-type <etherll|llc|snap>][priority
<0-7|all>][protocol <0-255>][set-drop-prec <high-drop|low-drop>]
[set-drop-prec-out-action <high-drop| low-drop>][src-ip <src-ip-
info>][tcp-control <Urg|Ack|Psh|Rst|Syn|Fin>][update-1p <0-7>]
[update-dscp <0-63>][update-dscp-out-action <0-63>][vlan-min
<1-4094>][vlan-max <1-4094>][vlan-tag <tagged| untagged>]
```

Variable definitions

Use the data in the following table to use the **qos traffic-profile classifier** command.

Variable	Value
name <WORD>	Specifies an alphanumeric identifier for the traffic profile. The value is a character string from 1–16 characters in length. All classifiers associated with a specific traffic-profile filter set share the same name.
addr-type <ipv4 | ipv6>	Specifies the type of IP address used by this classifier entry. The type is limited to IPv4 and IPv6 addresses.
block <WORD>	Specifies the label to identify traffic profile classifier elements that are of the same block.
committed-rate <64-10230000>	Specifies the committed rate for metering. Values range from 64-10230000 Kbps.
committed-burst-size <burst-size-options>	Specifies the committed burst size in KiloBytes.
drop-action <disable | enable>	Specifies whether to drop (enable) or pass (disable) traffic matching the classifier criteria.
drop-out-action <disable | enable>	Specifies whether to drop (enable) or pass (disable) out of profile packets.
ds-field <0-63>	Specifies the value for the DiffServ Codepoint (DSCP) in a packet.
dst-ip <dst-ip-info>	Specifies the IP address to match against the destination IP address of a packet. • IPv4 source—use the A.B.C.D/<0-32> format • IPv6 source—use the x:x:x:x:x:x:x:x/<0-128> format
dst-mac <dst-mac-info>	Specifies MAC address against which the MAC destination address of incoming packets is compared.

Table continues…

Variable	Value
`src-mac <src-mac>`	Specifies the MAC source address of incoming packets.
`dst-mac-mask <dst-mac-mask>`	Specifies the mask for the MAC address against which the MAC destination address of incoming packets is compared.
`src-mac-mask <src-mac-mask>`	Specifies the MAC source address mask of incoming packets.
`dst-port-min <0-65535>`	Specifies the minimum value for the Layer 4 destination port classifier.
`src-port-min <0-65535>`	Specifies the minimum value for the Layer 4 source port number in a packet.
`dst-port-max <0-65535>`	Specifies the maximum value for the Layer 4 destination port classifier.
`src-port-max <0-65535>`	Specifies the maximum value for the Layer 4 source port number in a packet.
`ethertype <0x0-0xFFFF>`	Specifies the type of information carried in the data portion of the frame. Values range from 0x0 to 0xFFFF hexadecimal.
`eval-order <1-255>`	Specifies the evaluation order for all elements with the same name. Values range from 1–255.
`flow-id <0x0-0xFFFF>`	Specifies the flow identifier for IPv6 packets. Values range from 0x0 to 0xFFFF hexadecimal.
`ip-flag <ip-flags>`	Specifies the IP fragment flag criteria.
`ipv4-option <no-opt | with-opt>`	Specifies the IPv4 option criteria.
`master`	Designates the classifier as the master block member.
`max-burst-rate <64-4294967295>`	Specifies the maximum burst rate. Values range from 64 to 4294967295 Kbps. You configure this parameter when a committed metering rate is specified.
`max-burst-duration <1-4294967295>`	Specifies the maximum burst duration in milliseconds (ms). Values range from 1 to 4294967295 ms. You configure this parameter when a committed metering rate is specified.
`next-header <0-255>`	Specifies the IPv6 next-header value. Values range from 0–255.
`pkt-type <etherll | llc | snap>`	Specifies the filter packet format ethertype encoding criteria.
`priority <0-7 | all>`	Specifies a 802.1p user priority value for classifier.
`protocol <0-255>`	Specifies the IPv4 protocol value. Values range from 0–255.

Table continues…

Variable	Value
`set-drop-prec <high-drop | low-drop>`	Specifies the drop precedence for traffic matching the classifier criteria. • high-drop—a higher probability that the packet will be dropped when traffic congestion occurs • low-drop—a lower probability that the packet will be dropped when traffic congestion occurs
`set-drop-prec-out-action <high-drop | low-drop>`	Specifies the drop precedence value associated with out of profile traffic. • high-drop—a higher probability that the packet will be dropped when traffic congestion occurs • low-drop—a lower probability that the packet will be dropped when traffic congestion occurs
`src-ip <src-ip-info>`	Specifies the IP address to match against the source IP address of a packet. • IPv4 source—use the A.B.C.D/<0-32> format • IPv6 source—use the x:x:x:x:x:x:x:x/<0-128> format
`stage <egress>`	Specifies the stage to apply the filter.
`tcp-control <Urg | Ack | Psh | Rst | Syn | Fin>`	Specifies the TCP control criteria.
`update-1p <0-7>`	Specifies the 802.1p user priority update value.
`update-dscp <0-63>`	Specifies the DSCP update value.
`update-dscp-out-action <0-63>`	Specifies the DSCP update value in out of profile packets.
`vlan-min <1-4094>`	Specifies the minimum VLAN ID value for the classifier.
`vlan-max <1-4094>`	Specifies the maximum VLAN ID value for the classifier.
`vlan-tag <tagged | untagged>`	Specifies whether VLAN tagged or untagged traffic is matched by the classifier.

Deleting a QoS traffic profile filter set classifier

About this task

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

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Disable or delete a QoS traffic profile filter set:

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

Variable definitions

Use the data in the following table to use the **`no qos traffic-profile classifier`** command.

Variable	Value
`name <WORD>`	Specifies an alphanumeric identifier used to target the traffic profile filter set classifier being deleted. The value is a character string from 1–16 characters in length.
`eval-order <1-255>`	Specifies the evaluation order for all elements with the same name. Values range from 1–255.

Creating a traffic profile classifier on egress stage

About this task

Use the following procedure to create a traffic profile classifier on egress stage.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   qos traffic-profile classifier <name> stage egress [addr-type
   [{<ipv4> | <ipv6>}] | dst-ip [{<ipv4> | <ipv6>}] | src-ip [{<ipv4> |
   <ipv6>}] | protocol <0-255> | drop-action [{disable | enable}] |
   block <WORD> | eval-order <1-255> | update-dscp <0-63>]
   ```

Example

The following is an example of a traffic profile egress configuration:

```
Switch (config)#qos traffic-profile classifier name class1 stage egress src-ip
192.0.2.0/24 drop-action enable

Switch (config)#qos traffic-profile set port 2/50 name class1 track-statistics individual

Switch (config)#show qos traffic-profile classifier name class1
Id: 2
Name: class1
Block:
Master: No
Eval Order: 1
Address Type: IPv4
Destination Addr/Mask: Ignore
```

```
Source Addr/Mask: 192.0.2.0/24
DSCP: Ignore
IPv4 Protocol / IPv6 Next Header: Ignore
Destination L4 Port Min: Ignore
Destination L4 Port Max: Ignore
Source L4 Port Min: Ignore
Source L4 Port Max: Ignore
IPv6 Flow Id: Ignore
IP Flags: Ignore
TCP Control Flags: Ignore
IPv4 Options: Ignore
Destination MAC Addr: Ignore
Destination MAC Mask: Ignore
Source MAC Addr: Ignore
Source MAC Mask: Ignore
VLAN: Ignore
VLAN Tag: Ignore
EtherType: Ignore
802.1p Priority: All
Packet Type: Ignore
Action Drop: Yes
Action Update DSCP: Ignore
Action Update 802.1p Priority: Ignore
Action Set Drop Precedence: Low Drop
Out-Profile Drop Action: Drop
Out-Profile Update DSCP Action: Ignore
Out-Profile Set Drop Precedence Action: Low Drop
Storage Type: NonVolatile
Stage: Egress

Switch (config)#show qos traffic-profile set name class1
Id: 2
Name: class1
Unit/Port: 2/50
State: Enabled
Meter Mode: No Metering
Statistics Type: Individual
Storage Type: NonVolatile
```

The following output provides an example of a traffic profile with multiple rules and evaluation order.

```
(config)#qos traffic-profile classifier name class2 stage egress addr-type ipv4 src-ip
192.0.2.0/24 drop-action enable eval-order 3
(config)#qos traffic-profile classifier name class2 stage egress addr-type ipv4 dst-ip
198.51.100.0/24 drop-action enable eval-order 5
(config)# qos traffic-profile classifier name class2 stage egress src-ip 1.1.1.1/32 dst-
ip 198.51.100.0/24 drop-action enable eval-order 6
qos traffic-profile classifier name class2 stage egress addr-type ipv6 src-ip
2001:DB8::/32 drop-action enable eval-order 11
qos traffic-profile set port 2/50 name class2 track-statistics individual
```

The following examples show how to configure traffic profile rules.

Drop by IPv4 addresses

```
(config)#qos traffic-profile classifier name class1 stage egress src-ip 192.0.2.0/24 drop-
action enable
(config)#qos traffic-profile classifier name class1 stage egress dst-ip 198.51.100.0/24
drop-action enable
(config)#qos traffic-profile classifier name class1 stage egress src-ip 192.0.2.0/24 dst-
ip 198.51.100.0/24 drop-action enable
```

Drop by IPv6 addresses

```
(config)#qos traffic-profile classifier name class1 stage egress addr-type ipv6 src-ip
2001:DB8::/32 drop-action enable
```

```
(config)#qos traffic-profile classifier name class1 stage egress addr-type ipv6 dst-ip
2001:DB8::/32 drop-action enable
(config)#qos traffic-profile classifier name class1 stage egress addr-type ipv6 src-ip
2001:DB8::/32 dst-ip 2001:DB8::/32 drop-action enable
```

Drop by protocol number

```
(config)#qos traffic-profile classifier name class1 stage egress protocol 6 drop-action
enable
```

Drop by IP address and protocol number

```
(config)#qos traffic-profile classifier name class1 stage egress src-ip 192.0.2.0/24 dst-
ip 198.51.100.0/24 protocol 6 drop-action enable
```

Update DSCP by IPv4 address

```
(config)#qos traffic-profile classifier name class1 stage egress src-ip 192.0.2.0/24
update-dscp 30
(config)#qos traffic-profile classifier name class1 stage egress dst-ip 198.51.100.0/24
update-dscp 30
(config)#qos traffic-profile classifier name class1 stage egress src-ip 192.0.2.0/24 dst-
ip 198.51.100.0/24 update-dscp 30
```

Update DSCP by IPv6 addresses. The TC (Traffic Class) field of the matched IPv6 packet is updated

```
(config)#qos traffic-profile classifier name class1 stage egress addr-type ipv6 src-ip
2001:DB8::/32 update-dscp 30
(config)#qos traffic-profile classifier name class1 stage egress addr-type ipv6 dst-ip
2001:DB8::/32 update-dscp 30
```

Update DSCP by protocol number

```
DUT(config)#qos traffic-profile classifier name class1 stage egress protocol 6 update-
dscp 30
```

Update DSCP by IP address

```
(config)#qos traffic-profile classifier name class1 stage egress 192.0.2.0/24 dst-ip
198.51.100.0/24 update-dscp 30
(config)#qos traffic-profile classifier name class1 stage egress addr-type ipv6 src-ip
2001:DB8::/32 update-dscp 30
(config)#qos traffic-profile classifier name class1 stage egress addr-type ipv6 dst-ip
2001:DB8::/32 update-dscp 30
```

Variable definitions

The following table describes the parameters for the **`qos traffic-profile`** command.

Variable	Definition
classifier name<*classifier_name*>	Specifies the label used to reference the Traffic Profile entry.
set	Specifies the QoS Traffic Profile set entries

Configuring a QoS traffic profile filter set

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. configure a QoS traffic profile filter set:

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

Variable definitions

Use the data in the following table to use the **`qos traffic-profile classifier set`** command.

Variable	Value
`committed-rate <64-10230000>`	Specifies the committed rate for metering. Values range from 64-10230000 Kbps.
`committed-burst-size <burst-size-options>`	Specifies the committed burst size in KiloBytes.
`drop-out-action <enable | disable>`	Specifies whether to drop (enable) or pass (disable) out-of-profile packets. You configure this parameter when a metering type is selected and a committed metering rate is specified.
`enable`	Enables the traffic profile filter set.
`name <WORD>`	Specifies the traffic profile filter set name. This name is used to identify classifier elements that are associated with the filter set.
`max-burst-rate <64-4294967295>`	Specifies the maximum burst rate. Values range from 64 to 4294967295 Kbps. You configure this parameter when a committed metering rate is specified.
`max-burst-duration <1-4294967295>`	Specifies the maximum burst duration in milliseconds (ms). Values range from 1 to 4294967295 ms. You configure this parameter when a committed metering rate is specified.
`meter-mode <uniform-per-policy | individual-per-policy | classifier>`	Specifies the metering type. • uniform-per-policy—a unique meter is applied to each policy that comprises the filter set with uniform rate and burst data derived from the filter set specification used for each meter • individual-per-policy—a unique meter is applied to each policy that comprises the filter set with rate and burst data derived from the classifier data or the filter set specification

Table continues…

Variable	Value
	• classifier—a meter is defined for each individual filter set classifier using rate and burst data associated with the classifier. If this data is not present a meter is not allocated for the classifier
`port <port>`	Specifies the ports on which the traffic profile filter set is to be applied.
`set-drop-prec-out-action <high-drop | low-drop>`	Specifies the drop precedence value for out-of-profile traffic. • high-drop—there is a higher probability of packets being dropped when network congestion is encountered. • low-drop—there is a lower probability of packets being dropped when network congestion is encountered. You configure this parameter when a metering type is selected and a committed metering rate is specified.
`track-statistics <aggregate|disable| individual>`	Specifies how to track policy statistics for the traffic profile filter set. • aggregate—all traffic profile classifiers associated with a policy share the statistics resource • disable—statistics tracking is disabled for all traffic profile classifiers • individual—each traffic profile filter set classifier has its own statistics resource
`update-dscp-out-action <0-63>`	Updates the DSCP value in out-of-profile IP packets. Values range from 0 to 63. You configure this parameter when a metering type is selected and a committed metering rate is specified.

Disabling a QoS traffic profile filter set

About this task

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

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

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Disable or delete a QoS traffic profile filter set:

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

Variable definitions

Use the data in the following table to use the **`no qos traffic-profile classifier set`** command.

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

Display QoS egress precedence information on all units

About this task

Use the following procedure to display QoS egress precedence information on all units.

Note:

There is a maximum of 4 available precedences for egress filters.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. At the command prompt, enter the following command:

   ```
   show qos diag egress
   ```

Example

The following example displays sample output for the **`show qos diag egress`** command.

```
Switch (config)#show qos diag egress
```

```
        Egress Stage
Unit/Port Mask Precedence Usage
            4   3   2   1
--------- ---------------
1/1
1/2
1/3
1/4
1/5
```

Display QoS egress precedence information on a unit

About this task

Use the following procedure to display QoS egress precedence information on a certain unit.

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. At the command prompt, enter the following command:

   `show qos diag unit <unit_no> egress`

Example

The following example displays sample output of the **`show qos diag unit`** command.

```
Switch (config)#show qos diag unit 3 egress

        Egress Stage
Unit/Port Mask Precedence Usage
            4   3   2   1
--------- ---------------
3/1
3/2
```

Viewing QoS traffic profile filter set classifier information

About this task

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

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. Display information for configured QoS traffic profile classifiers:

   `show qos traffic-profile classifier [name <WORD>][eval-order <1-255>]`

Variable definitions

Use the data in the following table to use the **show qos traffic-profile classifier** command.

Variable	Value
name <WORD>	Specifies the alphanumeric identifier of a specific traffic profile filter set for which to display classifier configuration information.
eval-order <1–255>	Specifies the evaluation order for all elements with the same name. Value ranges from 1 to 255.

Viewing QoS traffic profile filter set information

About this task

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display traffic profile filter set information for configured QoS traffic profile set instances:

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

Variable definitions

Use the data in the following table to use the **show qos traffic-profile set** command.

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

Viewing QoS traffic profile filter set interface information

About this task

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display QoS traffic profile filter set interface information:

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

Viewing QoS traffic profile filter set statistics information

About this task

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display QoS traffic profile filter set statistics:

   ```
   show qos traffic-profile statistics port <port> name <WORD>
   [precedence <1-14>]
   ```

Variable definitions

Use the data in the following table to use the **show qos traffic-profile statistics** command.

Variable	Value
name <WORD>	Specifies the alphanumeric identifier of the traffic profile filter set for which to display statistics data.
port <port>	Specifies the classifier port or ports for which to display traffic profile filter set statistics data.
precedence <1-14>	Specifies the policy precedence in relation to other policies associated with the same traffic profile. Values range from 1–14. Specifying a precedence value displays statistics data for filter set classifiers associated with the specified precedence value only. If you do not specify a precedence value, statistics data is displayed for all precedence values used by the filter set instance.

Configuring QoS actions

The configuration of QoS actions directs the switch to take specific action on each packet. Use the following procedure to create or update a QoS action.

Important:

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

Important:

You may notice unequal drop rates for two similar packet flows using similar sized fixed length packets when QOS congestion testing is performed on the switch.

Important:

During periods of congestion, low drop precedence traffic will be buffered, while high drop precedence traffic could be dropped due to buffer availability on the switch. Since the high drop precedence traffic may not be buffered and queued at egress, it may not be processed as per the stated WRR relative percentages. Low drop precedence traffic streams will contend for the same buffer resources, with the buffers queued and processed at egress per the WRR percentages.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Create or update a QoS action:

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

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

Variable Definitions

Use the data in the following table to use the **qos action** command.

Variable	Value
<10-55000>	Enter an integer to specify the QoS action; range is 10–55000.
name <WORD>	Assigns a name to a QoS action with the designated action ID. Enter the name for the action; maximum is 16 alphanumeric characters

Table continues…

Variable	Value
drop-action<enable | disable | deferred-pass>	Specifies whether packets are dropped or not: • enable--drop the traffic flow • disable--do not drop the traffic flow • deferred-pass--traffic flow decision deferred to other installed policies Default is deferred pass. **Important:** If you omit this parameter, the default value applies.
update-dscp <0-63>	Specifies whether DSCP value are updated or left unchanged; unchanged equals ignore. Enter the 6-bit DSCP value; range is 0–63. Default is ignore.
update-1p<0-7>	Specifies whether 802.1p priority value are updated or left unchanged; unchanged equals ignore: • ieee1p--enter the value you want; range is 0–7 • use-egress--uses the egress map to assign value • use-tos-prec--uses the type of service precedence to assign value. Default is ignore.
set-drop-prec <low-drop | high-drop>	Enter the loss-sensitivity value: • low-drop • high-drop Default is low-drop.
action-ext <1-55000>	Enter an integer to specify the action extension; range is 1–55000.
action-ext-name <WORD>	Specify a label for the action extension; maximum is 16 alphanumeric characters.

Configuring interface action extension entries

About this task

QoS interface action extensions direct the switch to take specific action on each packet.

Use the following procedure to create interface action extension entries.

Important:

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

Important:

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Create entries:

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

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

Variable Definitions

Use the data in the following table to use the **qos if-action-extension** command.

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

Configuring QoS meters

About this task

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

Important:

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure or create a QoS meter:

```
[no] qos meter <1-55000> [name <WORD>] [committed-rate
<64-10230000>] [burst-size <burst-size>] [max-burst-rate
<64-4294967295>] [max-burst-duration <1-4294967295>] {in-profile-
action <1-55000> | in-profile-action-name <WORD>} {out-profile-
action <1,9-55000> | out-profile-action-name <WORD>} [session-id
<1-4294967295>]
```

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

Important:

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

Variable Definitions

Use the data in the following table to use the **qos meter** command.

Variable	Value
<1-5000>	Enter an integer to specify the QoS meter; range is 1–55000.
name <WORD>	Specify name for meter; maximum is 16 alphanumeric characters.
committed-rate <64-10230000>	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; range is 64–10230000 Kbits/sec.
burst-size <burst-size>	Committed burst size in Kilobytes. The value range is: 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384.
max-burst-rate <64-4294967295>	Specifies the largest burst of traffic that can be received a given time for the traffic to be considered in-profile. Used in calculating the committed burst size. Enter the rate in Kbps for in-profile traffic in increments of 1000 Kbps or 64 Kbps. The value range is 64–10230000 Kbps.
max-burst-duration <1-4294967295>	Specifies the amount of time that the largest burst of traffic that can be received for the traffic to be considered in-profile. Used in calculating the committed burst size. Enter the burst duration in ms for in-profile traffic; range is 1–4294967295 ms.
in-profile-action <1-55000>	Specify the in-profile action ID; range is 1–55000.
in-profile-action-name <WORD>	Specify the in-profile action name.
out-profile-action-name <WORD>	Specify the out-profile action name.
out-profile-action <1,9-55000>	Specify the out-of-profile action ID; range is 1,9–55000.
session-id <1-4294967295>	Specify the session ID.

Configuring QoS Interface Shaper

About this task

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

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   interface ethernet <port number>
   ```

2. Configure parameters:

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

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

Variable Definitions

Use the data in the following table to use the **`qos if-shaper`** command.

Variable	Value
name <WORD>	Specify name for if-shaper; maximum is 16 alphanumeric characters.
port <portlist>	Specify the port or list of ports for which to apply egress shaping.
shape-rate <64-10230000>	Shaping rate in kilobits/sec; range is 64-10230000 kilobits/sec.
burst-size <burst-size>	Committeed burst size in Kilobytes. The value range is: 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192.
max-burst-rate <64-4294967295>	Maximum burst rate in kilobits/sec; range is 64-4294967295Kbits/sec.
max-burst-duration <1-4294967295>	Maximum burst duration in milliseconds; range is 1–4294967295 ms.

QoS interface queue shaper management

Use the information in this section to configure and manage a queue shaper for one or more interfaces.

Creating a QoS interface queue shaper

About this task

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

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   interface ethernet <port number>
   ```

2. Create an egress queue shaper:

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

   Important:

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

Variable Definitions

Use the data in the following table to use the **`qos if-queue-shaper`** command.

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

Deleting a QoS interface queue shaper

About this task

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

Procedure

1. Enter Interface Configuration mode:

```
enable
```

```
configure terminal
```

```
interface ethernet <port number>
```

2. Delete an egress queue shaper:

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

Variable Definitions

Use the data in the following table to use the **`no qos if-queue-shaper`** command.

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

Viewing QoS interface queue shaper information

About this task

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

Procedure

1. Enter Interface Configuration mode:

```
enable
```

```
configure terminal
```

```
interface ethernet <port number>
```

2. Display egress queue shaper information:

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

Variable Definitions

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

Configuring QoS Policies

About this task

Use the following procedure to configure QoS policies.

Important:

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure QoS policies:

   ```
   [no] qos policy <1-55000> [enable] [name <WORD>] [port <port_list>]
   if-group <WORD> clfr-type {classifier | block} {clfr-id <1-55000> |
   clfr-name <WORD>} {{in-profile-action <1-55000> | in-profile-action-
   name <WORD>} | meter <1-55000> | meter-name <WORD>} precedence
   <1-14> [track-statistics <individual | aggregate>]}
   ```

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

Variable Definitions

Use the data in the following table to use the **qos policy** command.

Variable	Value
<1-55000>	Enter an integer to specify the QoS policy; range is 1–55000.
enable	Enable (basic form) or disable (no form) the QoS policy.
name <WORD>	Enter the name for the policy; maximum is 16 alphanumeric characters.
port <port_list>	The ports to which to directly apply this policy.
if-group <WORD>	Enter the interface group name to which this policy applies; maximum number of characters is 32 US-ASCII.The group name must begin with a letter within the range a..z or A..Z.
clfr-type <classifier | block>	Specify the classifier type; classifier or block.
clfr-id <1-55000>	Specify the classifier ID; range is 1–55000.
clfr-name <WORD>	Specify the classifier name or classifier block name; maximum is 16 alphanumeric characters.

Table continues…

Variable	Value
in-profile-action <1-55000>	Enter the action ID for in-profile traffic; range is 1–55000.
in-profile-action-name <WORD>	Enter the action name for in-profile traffic; maximum is 16 alphanumeric characters.
meter <1-55000>	Enter meter ID associated with this policy; range is 1–55000.
meter-name <WORD>	Enter the meter name associated with this policy; maximum of 16 alphanumeric characters.
precedence <1-14>	Specifies the precedence of this policy in relation to other policies associated with the same interface group. Enter precedence number; range is 1–14. **Important:** Policies with a lower precedence value are evaluated after policies with a higher precedence number. Evaluation goes from highest value to lowest.
track-statistics <individual | aggregate>	Specifies statistics tracking on this policy, either: • individual--statistics on individual classifiers • aggregate--aggregate statistics

Configuring User Based Policies

Use the information in this section to configure and manage User Based Policies (UBP).

You can include up to 128 classifier elements in a UBP.

Configuring UBP using Classifier Name

About this task

Configure User Based Policies using classifier name.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enter the following command:

   ```
   qos ubp classifier name <WORD>] [addr-type {ipv4 | ipv6}] [block
   <WORD>] [drop-action{disable | enable}] [ds-field <0-63>] [dst-ip
   A.B.C.D/<0-32>] [dst-mac <H.H.H> dst-macmask <H.H.H>] [dst-port-min
   <0-65535> dst-port-max <0-65535>] [ethertype <0x0-0xFFFF>][eval-
   ```

```
order <1-255>] [master] [priority {<0-7> | all}] [protocol <0-255>]
[set-drop-prec {highdrop| low-drop}] [src-ip <A.B.C.D/<0-32>] [src-
mac <H.H.H> src-mac-mask <H.H.H>] [src-port-min <0-65535> src-port-
max <0-65535>] [update-1p {<0-7> | useegress| use-tos-prec}]
[update-dscp <0-63>] [vlan-min <1-4094> vlan-max <1-4094>] [vlantag
{tagged |untagged}]
```

Note:

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

Example

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 192.0.2.0/24 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 192.0.2.0/24 ethertype 0x0800 drop-action
disable block remedial eval-order 70
qos ubp classifier name ALPHAYELLOW dst-ip 198.51.100.0/24 ethertype 0x0800 drop-action
disable block remedial eval-order 71
qos ubp classifier name ALPHAYELLOW dst-ip 203.0.113.0/24 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
```

Variable Definitions

Use the data in the following table to use the **`qos ubp classifier name addr-type`** command.

Variable	Value
name <*1–16*>	Creates the User Based Policy classifier entry.
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 <*1–32*>	Specifies the label to identify access list elements that are of the same block.

Table continues…

Variable	Value
drop-action {enable | disable}	Specifies whether or not to drop non-conforming traffic.
ds-field <*0–63*>	Specifies the value for the DiffServ Codepoint (DSCP) in a packet.
dst-ip {<*ipv4_destination*> | <*0–32*>}	Specifies the IP address to match against the destination IP address of a packet.
dst-mac <*mac_address*>	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 number in a packet. **`dst-port-max`** must be terminated prior to configuring this parameter.
ethertype <*0x0-0xFFFF*>	Specifies a value indicating the version of Ethernet protocol being used.
eval-order <*1–255*>	Specifies the evaluation order for all elements with the same name.
master	Specifies as the master member of the block.
priority {<*0–7*> | all}	Specifies the user priority classifier criteria.
protocol <*0–255*>	Specifies the IPv4 protocol classifier criteria.
set-drop-prec {high-drop | low-drop}	Specifies the set drop precedence. Valid values are: • high-drop • low-drop
src-ip {<*A.B.C.D*> | <*0–32*>}	Specifies the source IP classifier criteria
src-mac <*mac_address*>	Specifies the source MAC classifier criteria
src-port-min <*0–65535*>	Specifies the Layer 4 source port minimum value classifier criteria.
update-1p {<*0–7*> | use-egress | use-tos-prec}	Specifies the update user priority.
update-dscp <*0–63*>	Specifies the update DSCP.
vlan-min <*1–4094*>	Specifies the VLAN ID minimum value classifier criteria.
vlan-tag {tagged | untagged}	Specifies the VLAN tag classifier criteria.

Configuring UBP using Set Name

About this task

Configure User Based Policies using set name.

Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. Enter the following command:

```
qos ubp set name [committed-rate <64-10230000> [committed-burst-size
<1024|128|16|16384|2048|256|32|4|4096|512|64|8|8192> {drop-out-
action {enable|disable}} {set-drop-prec-out-action {high-drop|low-
drop}|set-priority <1–255>|track-statistics {aggregate|disable|
individual}|update-dscp-out-action <0-63>}}]] [max-burst-rate
<64-4294967295> {[drop-out-action {disable|enable}] [max-burst-
duration <1-4294967295> ][ set-drop-prec-out-action {high-drop|low-
drop}][update-dscp-out-action <0-63>]}}] [set-priority <1-255>
[track-statistics <aggregate|disable|individual>]]
```

Note:

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

Variable Definition

Use the data in the following table to use the **`qos ubp set name`** command.

Variable	Value
set name	Creates the User Based Policy set.
committed-rate <64-10230000>	Specify the committed rate value.
committed-burst-size	Specify the burst size in KBytes.
drop-out-action {enable|disable}	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).
set-drop-prec-out-action {highdrop| low-drop}	Specify the set drop precedence out-of-profile action.
set-priority <1–255>	Specify the filter set priority.
track-statistics <aggregate|disable|individual>	Specify to track statistics on policy.
update-dscp-out-action <0-63>	Specify the remark DSCP out-of-profile action.
max-burst-rate <64-4294967295>	Specify the maximum burst rate value.
max-burst-duration <1-4294967295>	Maximum burst duration in milliseconds.
set-drop-prec-out-action {high-drop|low-drop}	Specify the set drop precedence out-of-profile action.
update-dscp-out-action <0-63>	Specify the remark DSCP out-of-profile action.
set-priority <1-255>	Specify the filter set priority.

Deleting a Classifier, Classifier Block or an Entire Filter Set

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Delete an entire filter set:

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

   ✱ **Note:**

   You cannot delete a filter set while it is in use. You can not delete a classifier if there is not a set filter for that classifier.

3. 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

About this task

Use this procedure to view User Based Policy filter parameters, specific filter set parameters, ports and associated filter sets, and classifier entries.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View user based policy filter parameters:

   ```
   show qos ubp
   ```

3. View the parameters for a specific filter set:

   ```
   show qos ubp name <filter name>
   ```

4. View ports and the filter sets assigned to those ports:

   ```
   show qos ubp interface
   ```

5. View UBP statistics:

   ```
   show qos ubp statistics port <port number> name <word>
   ```

6. View classifier entries:

   ```
   show qos ubp classifier
   ```

7. View QoS precedence usage:

   ```
   show qos diag
   ```

   ✱ **Note:**

   Use the command **`show qos diag`** to properly plan QoS precedence usage. The precedence limit for the device is 8, with 1 precedence reserved for ARP.

Maintaining the QoS agent

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

Enabling the QoS agent

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable QoS agent functionality for a switch or stack:

   ```
   qos agent oper-mode
   ```

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

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

Disabling the QoS agent

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Disable QoS agent functionality for a switch or stack:

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

   OR

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

Configuring QoS resource buffer sharing

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure QoS resource buffer sharing:

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

Variable Definitions

Use the data in the following table to use the **`qos agent buffer`** command.

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

Changing the QoS resource buffer size to default

About this task

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

❗ **Important:**

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the QoS resource buffer size to the default value:

   ```
   default qos agent buffer
   ```

Configuring Automatic QoS support

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure QoS agent AutoQoS mode:

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

Variable Definitions

Use the data in the following table to use the **`qos agent aq-mode`** command.

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

Configuring NVRAM parameters

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure NVRAM parameters:

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

Resetting NVRAM parameters

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Reset NVRAM delay time:

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

Changing the QoS CoS queue set

About this task

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

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Modify the number of active QoS CoS queue sets:

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

Variable Definitions

Use the data in the following table to use the **`qos agent queue-set`** command.

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

Changing the QoS CoS queue set to default

About this task

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

Important:

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Change the number of active QoS CoS queue sets to the switch default:

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

Changing the QoS agent to factory defaults

About this task

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

Important:

You must restart the switch for changes to QoS CoS queue set and resource buffer size to take effect.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Reset the QoS Agent to factory defaults:

   ```
   default qos agent
   ```

   OR

   ```
   qos agent reset-default
   ```

Changing the QoS agent to partial factory defaults

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Reset the QoS Agent to partial factory defaults:

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

Configuring QoS statistics tracking

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure QoS statistics tracking:

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

Variable Definitions

Use the data in the following table to use the **`qos agent statistics-tracking`** command.

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

Changing QoS statistics tracking to default

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Change the QoS statistics tracking type to the factory default:

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

Configuring DoS Attack Prevention Package

About this task

Use this procedure to configure the DoS Attack Prevention Package (DAPP).

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. To enable DAPP, enter the following command:

   ```
   qos agent dos—attack-prevention enable
   ```

3. To disable DAPP, enter the following command:

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

   OR

   ```
   default qos agent dos—attack-prevention
   ```

4. To enable DAPP status tracking, enter the following command:

   ```
   qos agent dos—attack-prevention status-tracking
   ```

   If adequate resources are not available to enable status tracking, this command fails.

5. To set the minimum TCP header size used by DAPP, enter the following command:

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

   Default value is 20.

6. To set the maximum IPv4 ICMP length used by DAPP, enter the following command:

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

Default value is 512.

7. To set the maximum IPv6 ICMP length used by DAPP, enter the following command:

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

   Default value is 512.

8. To set the DAPP parameters to their default values, enter the following command:

   ```
   default qos agent dos—attack-prevention
   ```

Viewing QoS agent configuration information

About this task

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display general switch or stack QoS agent configuration information:

   ```
   show qos agent
   ```

Viewing QoS agent configuration details

About this task

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

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display detailed switch or stack QoS agent configuration information:

   ```
   show qos agent details
   ```

Clearing QoS statistics

About this task

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

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Reset all QoS related counters:

   ```
   qos clear-stats
   ```

Configuring ADAC Auto-QoS

About this task

Use this procedure to configure ADAC Auto-QoS.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. At the prompt, enter the following command:

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

3. Verify your configuration:

   ```
   show qos agent
   ```

Example

```
Switch#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
```

Variable definitions

Use the data in the following table to use the **`qos agent aq-mode`** command.

Variable	Value
`disable`	Disables Auto QOS application traffic processing on all ports.
`mixed`	Enables Auto QOS application traffic processing with egress DSCP remapping on all ports.
`pure`	Enables Auto QOS application traffic processing without egress DSCP remapping on all ports.

Chapter 5: Configuring Quality of Service using Enterprise Device Manager

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

Important:

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

Prerequisites

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

Displaying interface queues

Displaying interface queues using EDM

Use the following procedure to display the interface queues:

Prerequisites

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

Procedure steps

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

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

Variable Definitions

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

Filtering interface queue information

About this task

You can display selected parts of the **Interface Queue** tab.

Procedure

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

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

6. Click **Filter**.

Interface group configuration using EDM

Use the information to create and manage interface groups.

Displaying interface groups using EDM

Use the following procedure to display the interface groups.

Procedure steps

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

Variable Definitions

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

Deleting ports from an interface group using EDM

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

Procedure steps

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

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

Adding interface groups using EDM

Use the following procedure to add interface groups.

Procedure steps

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

   The Insert Interface Group screen appears.
5. Enter the desired ID number.
6. Enter the **Role** combination tag for this Interface Group.
7. Select the interface class desired for this interface group: **trusted**, **nonTrusted**, **unrestricted**, **untrustedv4v6**, or **untrustedBasic**.
8. Click **Insert**.

Deleting interface groups using EDM

Use the following procedure to delete the interface groups.

Procedure steps

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

4. Highlight the interface group to delete.
5. Click **Delete**.

   ❗ **Important:**

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

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

Assigning ports to an interface group using EDM

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

Procedure steps

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

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

   ❗ **Important:**

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

Interface ID configuration using EDM

Use the following procedure to create and manage interface IDs.

Displaying an interface ID using EDM

About this task

Display the interface ID.

Procedure

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

Variable Definitions

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

Displaying priority queue assignments

Displaying priority queue assignments using EDM

Use the following procedure to view Priority Q Assignments.

Prerequisites

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

Procedure steps

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

Variable Definitions

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

Filtering priority queue assignments

About this task

You can display selected parts of the Priority Q Assignments.

Procedure

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, click **QoS Devices**.
3. In the work area, click the **Priority Q Assign** tab.
4. Click the **Filter** button on the toolbar.

   The QoS Devices, Priority Q Assign - Filter screen appears.
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. Define the display filtering criteria to return all cases in which an entry **contains**, **equals to**, **does not contain**, or **does not equal to** the set parameters.
   d. Select **All records** to display all the entries in the table.
   e. To display the entries by parameter values, enter the values to display in the appropriate fields.
6. Click **Filter**.

Displaying priority mapping using EDM

Use the following procedure to display priority mapping.

Prerequisites

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

Procedure steps

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

Variable Definitions

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.

Egress mapping configuration using EDM

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

Viewing egress mapping information using EDM

Use this procedure to display existing DSCP mapping information.

Procedure steps

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

Variable Definitions

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

Configuring egress mapping using EDM

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

Procedure steps

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

Variable Definitions

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

Variable	Value
Dscp	Indicates the DSCP value. This is a read-only cell.
802.1pPriority	Specifies the user priority value associated with the DSCP. Values range from 0–7.
DropPrecedence	Specifies the relative drop precedence value for mapping the DSCP value to a drop precedence. Values include: • lowDropPrec • highDropPrec When network congestion occurs, the system drops packets with a high drop precedence before those with a low drop precedence.
NewDscp	Specifies a new DSCP value to use when DSCP mutation is required. Values range from 0–63.
ServiceClass	Specifies the type of service. Value is a character string with a maximum of 20 characters.

Displaying Meter Capability using EDM

Use the following procedure to display QoS interface meter capabilities.

Prerequisites

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

Procedure steps

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

Variable Definitions

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

Table continues…

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

Displaying Shaper Capability using EDM

Use the following procedure to display QoS interface shaper capabilities.

Prerequisites

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

Procedure steps

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

Variable Definitions

Variable	Value
Port	Specifies the port to which the meter is applied.
ShaperSupport	Displays the location where the shaper is applied.
Shaper Rate(Kbps)/Bucket (KBytes)/ Granulatiry (Kbps	Displays the maximum supported Shaper Rate, Shaper Budket size, and Shaper Granularity.

QoS IP classifier element management using EDM

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

Viewing IP classifier element configuration using EDM

Use this procedure to display IP classifier element configuration information.

Procedure steps

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

Variable Definitions

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

Variable	Value
Id	Indicates the number of the IP classifier element.
Name	Indicates the label of the IP classifier element.
AddressType	Indicates the type of IP address used by this classifier entry. The type is limited to IPv4 and IPv6 addresses.
DstAddr	Indicates the IP address to match against a packet destination IP address.
DstMaskLength	Indicates the length of the destination address mask. Values range from 0–32. The default is 0.
SrcAddr	Indicates the IP address to match against a packet's source IP address.
SrcMasklength	Indicates the length of the source address mask. Values range from 0–32. The default is 0.
Dscp	Indicates the value for the DSCP in a packet. Values range from -1–63 (0x00 to 0x3f hexadecimal).
Protoco/Next Header	Indicates the IPv4 protocol or IPv6 next header the classifier element will match. Values range from 0–255. The following are specific value designations: • 1 = ICMP-IPv4 • 2 = IGMP • 6 = TCP • 17 = UDP • 20 = FTP Data • 21 = FTP Control • 23 = Telnet • 25 = SMTP • 46 = RSVP • 58 = ICMP-IPv6

Table continues…

Variable	Value
	• L4Port:69 = TFTP • 80 = HTTP • 443 = HTTPS
DstL4PortMin	Indicates the minimum value permitted for the Layer 4 destination port number in a packet. Values range from 0–65535.
DstL4PortMax	Indicates the maximum value permitted for the Layer 4 destination port number in a packet. Values range from 0–65535.
SrcL4PortMin	Indicates the minimum value permitted for the Layer 4 source port number in a packet. Values range from 0–65535.
SrcL4PortMax	Indicates the maximum value permitted for the Layer 4 source port number in a packet. Values range from 0–65535.
IPv6FlowId	Indicates the flow identifier for IPv6 packets. Values range from -1–1048575 (0x00 to 0xfffff hexadecimal).
IpFlags	Indicates the value of flags present in an IPv4 header. Values include: • MoreFragement • doNotFragement
TcpCtrlFlags	Indicates the control flags present in an TCP header. Values include: • Urg • Ack • Psh • Rst • Syn • Fin
Ipv4Options	Indicates whether the Option field is present in the packet header. Values include: • Present—indicates that only IPv4 packets with options match this classifier element. • Not Present—indicates that only IPv4 packets without options match this classifier element. • ignore—whether or not options are present in IPv4 packets is not considered when determining if the IPv4 packet matches this classifier
Version	Indicates the version type.
Storage	Indicates the type of storage: • volatile • nonVolatile (default) • readOnly

Creating an IP classifier element using EDM

Use this procedure to create a new IP classifier element.

Procedure steps

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

Variable definitions

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

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

Table continues…

Variable	Value
	• 2 = IGMP • 6 = TCP • 17 = UDP • 20 = FTP Data • 21 = FTP Control • 23 = Telnet • 25 = SMTP • 46 = RSVP • 58 = ICMP-IPv6 • L4Port:69 = TFTP • 80 = HTTP • 443 = HTTPS
DstL4PortMin	Specifies the minimum value permitted for the Layer 4 destination port number in a packet. Values range from 0–65535.
DstL4PortMax	Specifies the maximum value permitted for the Layer 4 destination port number in a packet. Values range from 0–65535. When you configure DstL4PortMin to 0 and DstL4PortMax to 65535, the system ignores the DstL4Port parameters.
SrcL4PortMin	Specifies the minimum value permitted for the Layer 4 source port number in a packet. Values range from 0–65535.
SrcL4PortMax	Specifies the maximum value permitted for the Layer 4 source port number in a packet. Values range from 0–65535. When you configure SrcL4PortMin to 0 and SrcL4PortMax to 65535, the system ignores the SrcL4Port parameters.
IPv6FlowId	Specifies the flow identifier for IPv6 packets. Values range from -1–1048575 (0x00 to 0xfffff hexadecimal). A value of -1 indicates that the system ignores this parameter.
IpFlags	Specifies the value of flags present in an IPv4 header. Values include: • MoreFragement • doNotFragement

Table continues…

Variable	Value
TcpCtrlFlags	Specifies the control flags present in an TCP header. Values include: • Urg • Ack • Psh • Rst • Syn • Fin
Ipv4Options	Specifies whether the Option field is present in the packet header. Values include: • 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. • ignore—whether or not options are present in IPv4 packets is not considered when determining if the IPv4 packet matches this classifier

Deleting IP classifier elements using EDM

Use this procedure to delete an IP classifier element:

Procedure steps

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

   Important:

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

QoS L2 classifier element management using EDM

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

Viewing L2 classifier element information using EDM

Use this procedure to display information about configured L2 classifiers.

Procedure steps

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

Variable Definitions

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

Variable	Value
Id	Indicates the index that enumerates the classifier entries.
Name	Indicates a label for the classifier entry.
DestMacAddr	Indicates the MAC address against which the MAC destination address of incoming packets will be compared
DstMacAddrMask	Indicates a mask identifying the destination MAC address.
SrcMacAddr	Indicates the MAC source address of incoming packets.
SrcMacAddrMask	Indicates a mask identifying the source MAC address.
VlanIdMin	Indicates the minimum value the inner VLAN ID in a double tagged packet must have to match this L2 classifier.
VlanIdMax	Indicates the minimum value the inner VLAN ID in a double tagged packet must have to match this L2 classifier.
VlanTag	Indicates the type of VLAN tagging in a packet. Values include: • untagged • tagged • ignore
EtherType	Indicates a value for the Ethernet type. Values range from 0x00 to 0xffff. If you enter a value of 0xffff, the system ignores this parameter.
802.1pPriority	Indicates a value for the 802.1p user priority. Values include: • priority0 • priority1 • priority2

Table continues…

Variable	Value
	• priority3 • priority4 • priority5 • priority6 • priority7 • ignore
PktType	Indicates the data link layer frame format that frames must have to match this L2 classifier entry. Values include: • ethernetII—only EthernetII format frames can match this classifier • snap—only IEEE 802 SNAP format frames can match this classifier • llc—only IEEE 802 LLC format frames can match this classifier • ignore—frame format is not considered in determining whether or not a frame matches this classifier
Version	Indicates the L2 classifier version.
Storage	Indicates the type of storage.

Creating an L2 classifier element using EDM

Use this procedure to create an L2 classifier element.

Procedure steps

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

Variable Definitions

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

Variable	Value
Id	Specifies the index that enumerates the classifier entries.
Name	Specifies a label for the classifier entry.

Table continues…

Variable	Value
DestMacAddr	Specifies the MAC address against which the MAC destination address of incoming packets is compared.
DstMacAddrMask	Specifies a mask identifying the destination MAC address.
SrcMacAddr	Specifies the source MAC address of incoming packets.
SrcMacAddrMask	Specifies a mask identifying the source MAC address.
VlanRange	Specifies the VLAN range for the L2 classifier element. Values range from 1–4094. When **Ignore** is selected, the system ignores the VLAN range.
VlanTag	Specifies the type of VLAN tagging in a packet. Values include: • untagged • tagged • ignore
EtherType	Specifies a value for the Ethernet type. Values range from 0x00 to 0xffff. If you enter a value of 0xffff, the system ignores this parameter.
802.1pPriority	Specifies a value for the 802.1p user priority. Values include: • priority0 • priority1 • priority2 • priority3 • priority4 • priority5 • priority6 • priority7 • ignore
PktType	Specifies the data link layer frame format that frames must have to match this L2 classifier entry. Values include: • ethernetII—only EthernetII format frames can match this classifier • snap—only IEEE 802 SNAP format frames can match this classifier • llc—only IEEE 802 LLC format frames can match this classifier • ignore—frame format is not considered in determining whether or not a frame matches this classifier

Deleting L2 classifier elements using EDM

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

Procedure steps

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

   Important:

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

QoS system classifier element management using EDM

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

Viewing QoS system classifier elements using EDM

To display System Classifier Elements:

Procedure steps

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

Variable Definitions

Variable	Value
Id	Indicates the index that enumerates the system classifier entries.
Name	Indicates the name of the system classifier element.
UnknownUcastFrames	Identifies frames with an unknown unicast destination address. • true—indicates frames containing an unknown unicast destination address match this classification entry. • false—indicates that no classification is requested based on this address type.

Table continues…

Variable	Value
UnknownIpMcast	Identifies IP packets with an unknown IP multicast destination address. • true—indicates that IP packets containing an unknown multicast destination address match this classification entry. • false—indicates that no classification is requested based on this address type.
KnownIpMcast	Identifies IP packets with a known IP multicast destination address. • true—indicates that IP packets containing a known multicast destination address match this classification entry. • false—indicates that no classification is requested based on this address type.
UnknownNonIpMcast	Identifies non-IP packets with an unknown MAC multicast destination address. • true—indicates that non-IP packets containing an unknown multicast destination address match this classification entry. • false—indicates that no classification is requested based on this address type.
KnownNonIpMcast	Identifies non-IP packets with a known MAC multicast destination address. • true—indicates that non-IP packets containing a known multicast destination address match this classification entry. • false—indicates that no classification is requested based on this address type.
NonIpPkt	Indicates that targeting non-IP traffic is supported. • true—indicates that non IP packets match this classification entry. • false—indicates that no classification is requested based on this packet type.
PatternFormat	Indicates the data link layer packet format that is used when specifying pattern match data. • untagged—indicates that the specified pattern match data does not include an 802.1Q tag. • tagged—indicates that the specified pattern match data does include an 802.1Q tag. The default value is tagged.

Table continues…

Variable	Value
PatternIpVersion	Indicates the IP packet format used to specify pattern match data. Values include: • nonIp - indicates that the specified patern match data should be applied to non-IP packets • ipv4 - indicates that the specified pattern match data should be applied to IPv4 packets • ipv6 - indicates that the specified pattern match data should be applied to IPv6 packets
PatternL2Format	Indicates the L2 packet format used to specify pattern match data. Values include: • notApplicable—specify pattern match data without indicating the target L2 packet format • ethernetII—apply the pattern match data to EthernetII format frames • snap—apply the pattern match data to IEEE 802 SNAP format frames • llc—apply the pattern match data to IEEE 802 LLC format frames
Version	Indicates the system classifier version.
Storage	Indicates the storage type for this conceptual row. Conceptual rows that has the value permanent need not allow write-access to any columnar objects in the row. This object may not be modified if the associated status object is equal to 'active'.

Viewing the QoS system classifier pattern using EDM

Use this procedure to display the QoS system classifier pattern.

Procedure steps

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

Configuring a QoS system classifier element using EDM

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

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QosRules**.
3. In the work area, click the **System Clfr Element** tab.
4. Click **Insert**.
5. In the Name dialog box, type label for the system classifier element.
6. In the **DestAddressType** section, click a radio button.
7. In the PatternData dialog box, type specific pattern data.

   OR

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

   OR

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

Variable definitions

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

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

Table continues…

Variable	Value
PatternData	Matches frames with specific byte pattern data.
PatternPosition	Matches frames at a specific position in a packet.

Deleting QoS system classifier elements using EDM

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

Procedure steps

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

QoS classifier management using EDM

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

Displaying classifiers using EDM

Use the following procedure to display classifiers.

Procedure steps

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

Variable Definitions

Variable	Value
Name	Specifies the name of the classifier.
SetId	Specifies the eEntries with the same SetId belong to the same classifier.

Table continues…

Variable	Value
	Important: Click heading on this column to list entries in numerical order to view which entries have the same SetId.
Specific	Describes the specific classifier element and its ID number (from the IP Classifier Element screen, the L2 Classifier Element screen, or System Clfr Element screen) that is included in the classifier.
Version	Indicates the version. Values include: • version1 • version2
Storage	Specifies the storage type for this conceptual row. Conceptual rows that has the value permanent need not allow write-access to any columnar objects in the row. This object may not be modified if the associated status object is equal to active.

Adding classifiers using EDM

Use the following procedure to add a classifier.

Procedure steps

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

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

   Important:

   A classifier can be created using the following classifier combinations:

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

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

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

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

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

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

Deleting classifiers using EDM

Use the following procedure to delete classifiers.

Procedure steps

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

   ❗ **Important:**

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

Filtering classifiers using EDM

Use the following procedure to filter the display of classifiers.

Procedure steps

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

   The QoS Rules, Classifier - Filter screen appears.
5. Set the conditions to filter the display of the **Classifiers** table.
   a. Select **AND** to include all entries in the table that include *all* specified parameters, or select **OR** to include any of the specified parameters.
   b. Select **Ignore Case** to include all entries with the parameters being set, whether in lowercase or uppercase.

c. Define the search to return all cases in which an entry **contains**, is **equal to**, **does not contain**, or **does not equal to** the set parameters.

d. Select **All records** to display all the entries in the table.

e. To display the entries in the table by name, select **Name** and enter the **Name** values to display.

f. To display the entries in the table by setid, select **SetId** and enter the **SetId** values to display.

6. Click **Filter**.

QoS classifier block management using EDM

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

Displaying classifier blocks using EDM

Use the following procedure to display classifier blocks.

Procedure steps

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

Variable Definitions

Variable	Value
BlockNum	Indicates the entries with the same BlockNum that belong to the same classifier block. **Important:** Click heading on this column to list entries in numerical order to view which entries have the same BlockNum.
Name	Displays the name you assigned to that classifier block.
ClassifierSetId	Displays the ID number assigned to that classifier (from the Classifier screen).
Meter	Displays the meter associated with the classifier block.
Action	Displays the action followed for those flows not being metered. (For those flows being metered, this attribute is not applied.)
EvalOrder	Specifies the evaluation order number.

Table continues…

Variable	Value
Version	Specifies the version.
Storage	Specifies the storage type for this conceptual row. Conceptual rows that has the value permanent need not allow write-access to any columnar objects in the row. This object may not be modified if the associated status object is equal to active.

Appending classifier blocks using EDM

Use the following procedure to append a classifier block.

Procedure steps

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

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

Adding classifier blocks using EDM

Use the following procedure to add classifier blocks.

Procedure steps

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

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

Important:

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

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

Deleting classifier blocks using EDM

Use the following procedure to delete classifier blocks.

Procedure steps

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

   Important:

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

Filtering classifier blocks using EDM

Use the following procedure to filter a classifier block.

Procedure steps

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

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

QoS action configuration using EDM

Use the information in this section to manage QoS actions.

Displaying QoS actions using EDM

Use the following procedure to display a QoS action.

Procedure steps

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

Variable Definitions

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

Adding QoS actions using EDM

Use the following procedure to add a QoS action.

Procedure steps

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

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

Deleting QoS actions using EDM

Use the following procedure to delete a QoS action.

Procedure steps

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

   Important:

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

QoS interface action extension configuration using EDM

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

Displaying Interface action extensions using EDM

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

Procedure steps

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

Variable Definitions

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

Adding Interface action extensions using EDM

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

Procedure steps

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

   The Insert Interface Action Ext screen appears.
5. Enter the information and make the selections to use for this Interface action extension.
6. Click **Insert**.

Deleting Interface action extensions using EDM

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

Procedure steps

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

   Important:

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

QoS meter configuration using EDM

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

Displaying QoS meters using EDM

Use the following procedure to display a QoS meter.

Procedure steps

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

Variable Definitions

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 burst size (in bytes).
InProfileAction	Specifies in profile action.
OutOfProfileAction	Specifies out of profile action.
Version	Specifies the verson.
Storage	Specifies the type of storage.

Adding QoS meters using EDM

Use the following procedure to add a QoS meter.

Procedure steps

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

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

Deleting QoS meters using EDM

Use the following procedure to delete a QoS meter.

Procedure steps

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

   Important:

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

QoS interface shaper configuration using EDM

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

Viewing QoS interface shaper information using EDM

Use this procedure to display QoS interface shaper configuration information.

Procedure steps

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

Variable Definitions

Variable	Value
Port	Indicates the interface port number associated with a QoS interface shaper. The port number must correspond to the interface table entry with the same port number.
Name	Indicates an alphanumeric label used to identify the QoS interface shaper.

Table continues…

Variable	Value
ShapingRate	Indicates the token-bucket rate, in kilobits per second (Kbps).
BurstSize	Indicates the maximum number of bytes in a single transmission burst, in kilobits per second (Kbps).

Creating a QoS interface shaper using EDM

Use this procedure to create a new QoS interface shaper.

Procedure steps

1. From the navigation tree, double-click **QoS**.
2. In the QoS tree, double-click **QoS**.
3. In the work area, click the **Interface Shaper** tab.
4. Click **Insert**.
5. Click the **Ports** ellipses.
6. Select the required ports for the interface shaper.
7. Click **Ok**.
8. In the **Name** dialog box, type a character string.
9. In the **Shaping Rate** dialog box, type a value.
10. In the **MaximumBurstRate** dialog box, type a value.
11. Double-click the **Duration** box.
12. From the list, select a value.
13. Click **Insert**.

Variable Definitions

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

Deleting a QoS interface shaper using EDM

Use this procedure to delete a QoS interface shaper.

Procedure steps

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

QoS interface queue shaper configuration using EDM

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

Viewing QoS interface queue shaper information using EDM

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

Procedure steps

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

Variable Definitions

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

Table continues…

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

Creating a QoS interface queue shaper using EDM

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

Procedure steps

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

Variable Definitions

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

Table continues…

Variable	Value
ShapingRate	Specifies the QoS interface queue shaping rate, in kilobits per second (Kbps). Values range from 64 to10230000 Kbps. The value must be a multiple of 64 or 1000 Kbps.
ShapingMinRate	Specifies the minimum QoS interface queue shaping rate, in kilobits per second (Kbps). Values range from 0 to10230000 Kbps. The value must be a multiple of 64 or 1000 Kbps.

Deleting a QoS interface queue shaper using EDM

Use this procedure to delete a QoS interface shaper.

Procedure steps

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

QoS policy configuration using EDM

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

Displaying QoS policies using EDM

Use the following procedure to display QoS policies:

Procedure steps

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

Variable Definitions

Variable	Value
Id	Specifies the number of the QoS policy.

Table continues…

Variable	Value
Status	Allows you to enable or disable the policy.
Name	Displays the name for the policy.
ClassifierType	Specifies whether a classifier or a classifier block identifies traffic.
ClassifierName	Specifies the name of the classifier or classifier block associated with this policy.
InterfaceRoles	Specifies the interfaces to which the policy applies. **Important:** You must configure the role combinations (refer to Interface ID configuration using EDM on page 115) prior to associating it with a policy.
InterfaceIndex	The ifIndex field identifies the interface to which the policy is to be applied. A policy is associated with an interface explicitly using this attribute or implicitly using a role combination through the ntnQosPolicyInterfaceRole attribute. An interface must be identified by one and only one of these attributes. This attribute can identify an interface that does not currently exist in the system, as long as the specified interface index represents a potentially valid system interface. **Important:** The InterfaceRoles and InterfaceIndex fields are mutually exclusive. When the InterfaceIndex field is not zero, the InterfaceRoles must be empty (select none when insert the policy). When the InterfaceRoles specifies a valid role combination, the InterfaceIndex field must be 0.
Precedence	Specifies the order in which multiple policies are associated with the same interface. Policies with greater precedence have higher numbers. **Important:** Policies with higher precedence values are applied before policies with lower precedence values.
Meter	Specifies metering associated with this policy. Specifying a metering component causes any action criteria specified explicitly by the policy to be rejected as an error. **Important:** You must configure meters before associating them with a policy.
InProfileAction	Identifies the action to be applied to traffic with this policy. This will not be used when a meter is specified. **Important:** You must configure actions before associating them with a policy.
StatsType	Specifies statistics tracking: • none--no statistics tracked for this policy

Table continues…

Variable	Value
	• 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
Version	Specifies the version.
Storage	Specifies the type of storage: • volatile • nonVolatile • readOnly

Adding QoS policies using EDM

Use the following procedure to add a QoS policy.

Procedure steps

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

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

   Important:

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

Deleting QoS policies using EDM

Use the following procedure to delete QoS policies.

Procedure steps

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

3. In the work area, click the **Policy** tab.
4. Highlight the QoS policy to delete.
5. Click **Delete**.

QoS Policy Stats using EDM

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

Prerequisites

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

Procedure steps

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

   Depending on the StatsType and parameters you specified for a policy, the Individual Policy Stats screen or the Policy Aggregate Stats screen can appear.

If the Policy Stats type is none, no policy statistics information appears.

If the Policy Stats type is aggregate, the following aggregate policy statistics information appears:

- total in-profile packets
- total out-profile packets

Note:

If the Policy Meter is set to none, no total out-profile packet information appears.

If the Policy Stats type is individual, individual policy statistics are provided for each policy, filter, and each port and the following individual policy statistics information appears:

- in-profile packets
- out-profile packets

Note:

If the Policy Meter is set to no, no out-profile packet information is available.

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 6: QoS User Based Pollicy 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.
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 instand 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.

QoS Traffic Profile Filter Classifier Configuration using EDM

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

Viewing Traffic Profile Filter Classifier Information Using EDM

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

Procedure Steps

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

Variable Definitions

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

Variable	Value
Type	Indicates the classifier type. Values include: • UbpClfr • TrafficProfile
Name	Indicates the name of the classifier. All classifiers with the same name are part of the same filter set. That filter set has the same name as the classifiers.
Block	Indicates the block name with which the classifier is associated.
EvalPrec	Indicates the evaluation order number of the classifier in that filter set. Two classifiers in the same filter set cannot have the same evaluation order. A higher eval order means a lower precedence for the corresponding policy. Values range from 1–255.
AddrType	Indicates the type of IP address used by this classifier entry. Values include: • N/A—the address type is non-applicable • ipv4 • ipv6
DstIpAddr	Indicates the IP address to match against the destination IP address of a packet.

Table continues…

Variable	Value
DstIpPrefixLength	Indicates the length of the destination address mask. Values range from 0–2040, with 0–32 reserved for IPv4 address masks and 0–128 reserved for IPv6 address masks.
SrcIpAddr	Indicates the IP address to match against the source IP address of a packet.
SrcIpPrefixLength	Indicates the length of the source address mask. Values range from 0–2040, with 0–32 reserved for IPv4 address masks and 0–128 reserved for IPv6 address masks.
Dscp	Indicates the value for a DiffServ Codepoint (DSCP) in a packet. Values range from -1–63 (0x00 to 0x3f hexadecimal). A value of -1 indicates that the system ignores this parameter.
Protocol/NextHeader	Indicates the IPv4 protocol value, or the IPv6 next-header value. Values range from 0–255. A value of 255 indicates that the system ignores the parameter. The following are specific value designations: • 1 = ICMP-IPv4 • 2 = IGMP • 6 = TCP • 17 = UDP • 20 = FTP Data • 21 = FTP Control • 23 = Telnet • 25 = SMTP • 46 = RSVP • 58 = ICMP-IPv6 • L4Port:69 = TFTP • 80 = HTTP • 443 = HTTPS
DstL4PortMin	Indicates the minimum value for the Layer 4 destination port number in a packet. Values range from 0–65535.
DstL4PortMax	Indicates the maximum value for the Layer 4 destination port number in a packet. Values range from 0–65535.
SrcL4PortMin	Indicates the minimum value for the Layer 4 source port number in a packet. Values range from 0–65535.
SrcL4PortMax	Indicates the maximum value for the Layer 4 source port number in a packet. Values range from 0–65535.

Table continues…

Variable	Value
Ipv6FlowId	Indicates the flow identifier for IPv6 packets. Values range from -1–1048575 (0x00 to 0xfffff hexadecimal). A value of -1 indicates that the system ignores this parameter.
IpFlags	Indicates the classifier flag to match in traffic IPv4 headers. Values include: • MoreFragement • doNotFragement
TcpCtrlFlags	Indicates the control flag to match in traffic TCP headers. Values include: • Urg • Ack • Psh • Rst • Syn • Fin
Ipv4Options	Indicates if the presence of IPv4 options in an IPv4 packet are considered when the system is searching for a match for this classifier. Values include: • ipv4OptionsPresent—only IPv4 packets with options match this classifier • ipv4OptionsNotPresent—only IPv4 packets without options match this classifier • ignore—whether or not options are present in IPv4 packets is not considered when determining if the IPv4 packet matches this classifier
Storage	Indicates the storage type for this conceptual row.
DstMacAddr	Indicates the MAC address against which the MAC destination address of incoming packets is compared.
DstMacAddrMask	Indicates a mask identifying the destination MAC address.
SrcMacAddr	Indicates a MAC source address of incoming packets.
SrcMacAddrMask	Indicates a mask identifying the source MAC address.
VlanIdMin	Indicates the minimum value for the VLAN ID in a packet. Values range from 1–4094.
VlanIdMax	Indicates the maximum value for the VLAN ID in a packet. Values range from 1–4094.
VlanTag	Indicates the type of VLAN tagging in a packet. Values include: • untagged • tagged

Table continues…

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

Table continues…

Variable	Value
	• markAsPriority4 • markAsPriority5 • markAsPriority6 • markAsPriority7 • ignore
ActionSetPrec	Indicates the automatic drop precedence. Values include: • lowDropPrec—low drop precedence • highDropPrec—high drop precedence When network traffic congestion occurs, packets with a high drop precedence are dropped before packets with a low drop precedence.
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 committed burst (in bytes).
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).
Stage	Specifies the stage for Traffic Profile classifiers. • ingressStage—ingress traffic (default option) • egressStage—egress traffic

Filtering QoS Traffic Profile Filter Classifier Information Using EDM

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

Procedure Steps

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

6. Click **Filter**.
7. Click **Apply**.

Variable Definitions

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

Variable	Value
AND	Includes all entries in the table that include all specified parameters.
OR	Includes any of the specified parameters.
Ignore Case	When selected, includes entries with the parameters being set, whether in lower case or upper case.
contains	Returns all cases in which an entry contains the set parameters.
does not contain	Returns all cases in which an entry does not contain the set parameters.
equal to	Returns all cases in which an entry is equal to the set parameters.
does not equal to	Returns all cases in which an entry is not equal to the set parameters.
All Records	When selected, displays all entries in the table.

Creating a QoS Traffic Profile Filter Classifier Using EDM

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

Procedure Steps

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

Variable Definitions

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

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

Table continues…

Variable	Value
	• 20 = FTP Data • 21 = FTP Control • 23 = Telnet • 25 = SMTP • 46 = RSVP • 58 = ICMP-IPv6 • L4Port:69 = TFTP • 80 = HTTP • 443 = HTTPS
DstL4PortMin	Specifies the minimum value for the Layer 4 destination port number in a packet. Values range from 0–65535.
DstL4PortMax	Specifies the maximum value for the Layer 4 destination port number in a packet. Values range from 0–65535.
SrcL4PortMin	Specifies the minimum value for the Layer 4 source port number in a packet. Values range from 0–65535.
SrcL4PortMax	Specifies the maximum value for the Layer 4 source port number in a packet. Values range from 0–65535.
Ipv6FlowId	Specifies the flow identifier for IPv6 packets. Values range from -1–1048575 (0x00 to 0xfffff hexadecimal). A value of -1 indicates that the system ignores this parameter.
IpFlags	Specifies the classifier flag to match in traffic IPv4 headers. Values include: • MoreFragement • doNotFragement
TcpCtrlFlags	Specifies the control flag to match in traffic TCP headers. Values include: • Urg • Ack • Psh • Rst • Syn • Fin
Ipv4Options	Specifies if the presence of IPv4 options in an IPv4 packet are considered when the system is searching for a match for this classifier. Values include: • present—only IPv4 packets with options match this classifier

Table continues…

Variable	Value
	• notPresent—only IPv4 packets without options match this classifier • ignore—whether or not options are present in IPv4 packets is not considered when determining if the IPv4 packet matches this classifier
DstMacAddr	Specifies the MAC address against which the MAC destination address of incoming packets is compared. If you leave this box empty, the system ignores this parameter.
DstMacAddrMask	Specifies a mask identifying the destination MAC address. If you leave this box empty, the system ignores this parameter.
SrcMacAddr	Specifies a MAC source address of incoming packets. If you leave this box empty, the system ignores this parameter.
SrcMacAddrMask	Specifies a mask identifying the source MAC address. If you leave this box empty, the system ignores this parameter.
VlanIdMin	Specifies the minimum value for the VLAN ID in a packet. Values range from 1–4094.
VlanIdMax	Specifies the maximum value for the VLAN ID in a packet. Values range from 1–4094. If you set VlanIdMin to 1 and VlanIdMax to 4094, the system ignores the VLAN ID parameter.
VlanTag	Specifies the type of VLAN tagging in a packet. Values include:: • untagged • tagged • ignore
EtherType	Specifies the value for the Ethernet type. Values range from 0x00 to 0xffff. If you enter a value of 0xffff, the system ignores this parameter.
UserPriority	Specifies the value for the 802.1p user priority. Values include: • matchPriority0 • matchPriority1 • matchPriority2 • matchPriority3 • matchPriority4 • matchPriority5 • matchPriority6 • matchPriority7 • matchAllPriorities

Table continues…

Variable	Value
PktType	Specifies the data link layer frame format for that can match this classifier. Values include: • ethernetII—only Ethernet II format frames can match this classifier • snap—only IEEE 802 SNAP format frames can match this classifier • llc—only IEEE 802 LLC format frames can match this classifier • ignore—frame format is not considered in determining whether or not a frame matches this classifier
ActionDrop	Specifies whether or not to drop the traffic matching filtering data. Values include: • drop • pass
UpdateDscp	Specifies a value used to update the DSCP field in an IPv4 packet. Values range from -1–63 (0x00 to 0x3f hexadecimal). A value of -1 indicates that the system ignores this parameter.
UpdateUserPriority	Specifies 802.1p value used to update user priority. Values include: • markAsPriority0 • markAsPriority1 • markAsPriority2 • markAsPriority3 • markAsPriority4 • markAsPriority5 • markAsPriority6 • markAsPriority7 • ignore
ActionSetPrec	Specifies automatic drop precedence. Values include: • lowDropPrec—low drop precedence • highDropPrec—high drop precedence When network traffic congestion occurs, packets with a high drop precedence are dropped before packets with a low drop precedence.
Stage	Specifies the stage for Traffic Profile classifiers: • ingressStage—ingress traffic (default option)

Table continues…

Variable	Value
	• egressStage—egress traffic

Deleting a QoS Traffic Profile Filter Classifier Using EDM

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

Procedure Steps

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

QoS Traffic Profile Filter Set Configuration Using EDM

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

Viewing QoS Traffic Profile Filter Set Information Using EDM

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

Procedure Steps

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

Variable Definitions

Use the data in this table to help you understand the QoS traffic profile filter set display.

Variable	Value
AclType	Indicates the type of ACL. Values include: • UbpClfr • TrafficProfile

Table continues…

Variable	Value
Name	Indicates a name for this traffic profile filter set. The name must be an existing classifier name. All classifiers with this name are part of this filter set. The filter set itself has this name.
IfIndex	Indicates the logical interface index assigned to the filter set.
MeteringMode	Specifies the Traffic Profile Metering Mode as: • noMetering • perPolicyUniformRateMetering • perPolicyIndividualRateMetring • perClassifierMetering
CommittedRate	Indicates the committed rate in kilobits per second (Kbps). Values are multiples or 64 or 1000 Kbps.
BurstSize	Indicates the size of a single transmission burst.
OutActionDrop	Specifies the action to take when packet is out-of-profile. This action is applied only if metering is being enforced, and if the traffic is deemed out-of-profile based on the level of traffic and the metering criteria. (Metering is applied only to traffic matching the filtering data.) Options are the following: • drop—the packet is dropped • pass—the packet is not dropped The default value is pass.
StatsType	Options are: • individualClfr • aggregateClfr • noStatsTracking
OutActionUpdateDscp	Indicates the action to take to update DSCP when a packet is out-of-profile. Values range from -1–63. The default value is -1.
SetPriority	Indicates the set priority. Values range from 1–255.
Status	Indicates the set status.
Storage	Indicates the type of storage.

Creating a QoS Traffic Profile Filter Set Using EDM

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

Procedure Steps

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

2. In the QoS tree, double-click **QoS UBP/Traffic Profile**.
3. In the work area, click the **Set** tab.
4. Click **Insert**.
5. Configure the parameters for the traffic profile filter set.
6. Click **Insert**.
7. Click **Apply**.

Variable Definitions

Use the data in this table to create a QoS traffic profile filter set.

Variable	Value
AclType	Specifies the type of ACL. Values include: • UbpClfr • TrafficProfile
Name	Specifies a name for this entry. The name must be an existing classifier name. All classifiers with this name are part of this filter set. The filter set itself has this name.
IfIndex	Specifies the logical interface index assigned to the filter set.
CommittedRate	Specifies the committed rate in kilobits per second (Kbps).
MaxBurstRate	Specifies the maximum rate for a single transmission burst in Kbps.
Duration	Specifies the maximum burst duration in milliseconds.
BurstSize	NOTE TO REVIEWERS: The BurstSize field is visible on the switch but was not present in this table — can you supply a definition for this value? Other tables in this section provide a definition for BurstSize — can the same definition be used here?
OutActionDrop	Specifies the action to take when packet is out-of-profile. This action is applied only if metering is being enforced, and if the traffic is deemed out-of-profile based on the level of traffic and the metering criteria. (Metering is applied only to traffic matching the filtering data.) Options are the following: • drop—packet is dropped • pass—packet is not dropped The default value is pass.
StatsType	Options are: • individualClfr • aggregateClfr

Table continues…

Variable	Value
	• noStatsTracking
OutActionUpdateDscp	Specifies the action to take to update DSCP when a packet is out-of-profile. Values range from -1–63. The default value is -1.
SetPriority	Specifies the set priority. Values range from 1–255.
Storage	NOTE TO REVIEWERS: The Storage field is visible on the switch but was not present in this table — can you supply a definition for this value? Other tables in this section provide a definition for Storage — can the same definition be used here?

Deleting a QoS Traffic Profile Filter Set Using EDM

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

Procedure Steps

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

Filtering QoS Traffic Profile Filter Set Information Using EDM

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

Procedure Steps

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

Variable Definitions

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

Variable	Value
AND	Includes all entries in the table that include all specified parameters.
OR	Includes any of the specified parameters.
Ignore Case	When selected, includes entries with the parameters being set, whether in lower case or upper case.
contains	Returns all cases in which an entry contains the set parameters.
does not contain	Returns all cases in which an entry does not contain the set parameters.
equal to	Returns all cases in which an entry is equal to the set parameters.
does not equal to	Returns all cases in which an entry is not equal to the set parameters.
All Records	When selected, displays all entries in the table.

QoS traffic profile filter set stats

Use the following procedure to view QoS traffic profile filter set statistics.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS UBP/Traffic Profile**.
3. In the work area, click the **Set** tab.
4. Select a traffic profile set from the list.
5. Click **Graph**. TrafficProfileStats appears.
6. Select a traffic profile statistics and click **Apply**.

Variable Definitions

Variable	Value
AccessAsgnId	Specifies the assigned access ID.
Precedence	Specifies the applied precedence.
EvalOrder	Specifies the evaluation order number.
InProfilePkts	Specifies the in-profile packets.
OutOfProfilePkts	Specifies the out-of-profile packets.

QoS Agent configuration using EDM

Use the information in this section to configure QoS Agent and DoS Attack Prevention Package (DAPP).

Viewing the QoS Configuration

About this task

Use the **Configuration** tab to view the QoS configuration.

Procedure

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

QoS Agent Configure Field Descriptions

Use the data in the following table to configure QoS Agent and DAPP.

Variable	Value
QosOperMode	Specifies whether the QoS Agent support is enabled or disabled. The QoS operational mode can not be disabled if QoS components are currently used by non-QoS applications. If disabled, requests related to QoS components by non-QoS applications are rejected. **Important:** Re-enabling the QoS operational mode can result in errors if you have made changes affecting available resources while QoS was temporarily disabled.
NVRamCommitDelay	Specifies the maximum time before nonvolatile QoS data is written to NVRAM. Values range from 0 to 604800 seconds.
NVRamCommitDelay	Resets QoS configurations to default except for queue-set and buffering type.
ResetToDefaults	Resets all policy information to factory default values.

Table continues…

Variable	Value
	Note: You must restart the switch for changes to ResetToDefaults to take effect.
QueueCfg	Specifies the queue set associated with all egress interfaces. Values include: • queueSetOne • queueSetTwo • queueSetThree • queueSetFour • queueSetFive • queueSetSix • queueSetSeven • queueSetEight **Note:** You must restart the switch for changes to QueueCfg to take effect.
BufferingCaps	Specifies the level of buffer sharing or over-allocation that can take place among ports sharing a buffer pool. Values include: • minimumOverAllocation—only a small amount of resource sharing is permitted • mediumOverAllocation—a medium amount of resource sharing is permitted • maximumOverAllocation—maximizes the possibility of over-allocation occurring **Note:** You must restart the switch for changes to BufferingCaps to take effect.
UBPSupportLevel	Sets the level of user based policy support. Values include: • disabled • highSecurityLocalData • lowSecurityLocalData
TrackStatistics	Specifies the type of statistics tracking. Values include: • disabled

Table continues…

Variable	Value
	• individual • aggregate
AQApplicationMode	Specifies the behavior of Auto Qos application mode. Values include: • disable • enablePureMode • enableMixedMode
DappEnable	Specifies the DoS Attack Prevention Package (DAPP). The values include: • disable—disabled by default • enableWithoutStatusTracking—enables DAPP without logging messages • enableWithStatusTracking—enables DAPP with logging messages
DappMinTcpHdrSize	Specifies the DAPP minimum TCP header size.
DappIpv4IcmpMaxLength	Specifies the DAPP maximum length for IPv4 ICMP packets.
DappIpv6IcmpMaxLength	Specifies the DAPP maximum length for IPv6 ICMP packets.

Enabling or disabling QoS agent support

About this task

Enable or disable QoS Agent support.

Procedure

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 or disabling automatic QoS

About this task

Enable or disable automatic QoS support.

Procedure

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 to enable automatic QoS:
   - enablePureMode - Enables Automatic QoS functionality with DSCP remarking at egress disabled.
   - enableMixedMode - Enables Automatic QoS functionality with DSCP remarking at egress enabled.
5. **(Optional)** Select **Disable** in the **AQApplicationMode** section to disable the automatic QoS.
6. Click **Apply**.

Configuring the QoS trusted processing mode

About this task

Configure the trusted processing mode.

Procedure

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

About this task

Enables DoS Attack Prevention Package.

Procedure

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

About this task

Sets the minimum TCP header size used by DAPP.

Procedure

1. From the navigation tree, double-click **QoS**.
2. From the QoS tree, double-click **QoS Agent**.
3. Under the **DoS Attack Prevention Package** section, enter a value in the range 0 to 255 in the **DappMinTcpHdrSize** text box.
4. Click **Apply**.

Configuring DAPP maximum IPv4 ICMP length

About this task

Sets the maximum IPv4 ICMP length used by DAPP.

Procedure

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

About this task

Sets the maximum IPv6 ICMP length that DAPP uses.

Procedure

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 **DappIpv6IcmpMaxLength** text box.
5. Click **Apply**.

Displaying policy class support using EDM

Use the following procedure to display policy class support.

Procedure steps

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

Variable Definitions

Variable	Value
PolicyClassName	Identifies the Policy Rule Classes (PRCs) supported by the device. A PRC is synonymous to a MIB table; therefore, the supported PRCs indicate which MIB tables are supported for QoS processing purposes.
CurrentInstances	Identifies the current number of Policy Rules Instances (PRIs) that are installed for a specific PRC (equates to the current number of entries in a given MIB table).
MaxInstalledInstances	Identifies the maximum number of PRIs that can be installed and/or modified by a user for a specific PRC (equates to the number of MIB table entries that can be created or modified by a user).

Displaying policy device identification using EDM

Use the following procedure to display policy device identification data.

Prerequisites

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

Procedure steps

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

Variable Definitions

Variable	Value
Descr	Specifies the description of the policy agent. **Important:** The description must include the name and version identification of the policy agent hardware and software.
MaxMsg	Specifies the maximum message size in octets that the device can support.

QoS resource allocation using EDM

Use the information in this section to filter and view resource allocation information.

Filtering the resource allocation table using EDM

Use the following procedure to filter the resource allocation table.

Procedure steps

1. From the navigation tree, double-click **Qos**.
2. In the QoS tree, double-click **QoS Agent**.
3. In the work area, click the **Resource Allocation (ERS5900)** tab.
4. Click **Filter**.

5. In QoS Agent, Resource Allocation (ERS5900)- Filter, set the filter conditions.
    a. Select **AND** to include all entries in the table that include all specified parameters, or select **OR** to include any of the specified parameters.
    b. Select **IGNORE CASE** to include all entries with the parameters being set, whether in lower case or upper case.
    c. Define the search to return all cases in which an entry **CONTAINS, DOES NOT CONTAIN, EQUALS TO, DOES NOT EQUAL TO** the set parameters.
    d. Select **ALL RECORDS** to display all entries in the table.
    e. Set **Precedence** to filter by order of precedence.
    f. Select **Port** to display the entries by port.
6. Click **Filter.**

Displaying resource allocation using EDM

Use the following procedure to display QoS resource Allocation information.

Prerequisites

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

Procedure steps

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

Variable Definitions

Variable	Value
Precedence	Displays the applied precedence (from 1–16).
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.
NonQosFiltersConsumed	Tracks the current number of filters in use, not due to installed QoS filter data, for a given precedence level and interface.

Table continues…

Variable	Value
NonQosMetersConsumed	Tracks the current number of meters in use, not due to installed QoS 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.

Viewing QoS queue statistics

Use the following procedure to display the number of bytes or packets dropped or passed on CoS queues, filtered by port, queue and/or non-zero queues.

Procedure

1. From the navigation tree, select **Qos > QoS Queue Stats**.
2. In the work area, click **Queue Statistics** to view the statistics.
3. On the toolbar, select **Filter** .

   The Filter window displays.
4. Select the Condition option.
   - AND
   - OR
5. Select the Column filter options.
   - contains
   - does not contain
   - equals to
   - does not equal to
6. Select the columns to be filtered.
7. Specify the string criteria for the selected columns.
8. **(Optional)** Clear **Ignore Case** to make the string criteria for the selected columns case sensitive.
9. Click **Filter**.

   The filtered options display in the table.

Variable definitions

Variable	Value
IfIndex	Indicates the interface index for the specified port.
Queue	Indicates the specified queue.
OutPackets	Indicates the number of packets transmitted.
OutBytes	Indicates the number of bytes transmitted.
DropPackets	Indicates the number of packets dropped.
DropBytes	Indicates the number of bytes dropped.

Glossary

Address Resolution Protocol (ARP)

Maps an IP address to a physical machine address, for example, maps an IP address to an Ethernet media access control (MAC) address.

application-specific integrated circuit (ASIC)

An application-specific integrated circuit developed to perform more quickly and efficiently than a generic processor.

Auto-Detection and Auto-Configuration (ADAC)

Provides automatic switch configuration for IP phone traffic support and prioritization. ADAC can configure the switch whether it is directly connected to the Call Server or uses a network uplink.

bandwidth

A measure of transmission capacity for a particular pathway, expressed in megabits per second (Mb/s).

class of service (CoS)

A method used to manage traffic congestion based on the CoS level assigned to the packet.

CLI

Command Line Interface (CLI) is a text-based, common command line interface used for device configuration and management across Extreme Networks products.

CLI modes

Differing command modes are available within the text-based interface, dependant on the level of user permissions determined by logon password. Each successive mode level provides access to more complex command sets, from the most restrictive—show level only, to the highest configuration levels for routing parameters, interface configuration, and security.

Differentiated Services (DiffServ)

A network architecture enabling service providers and enterprise network environments to offer varied levels of service for different traffic types.

Differentiated Services Code Point (DSCP)

The first six bits of the DS field. The DSCP uses packet marking to guarantee a fixed percentage of total bandwidth to each of several applications (guarantees quality of service).

Differentiated Services Quality of Service (DiffServ QoS)

Allows specific level of performance designation, on a packet-by-packet basis, for high performance and reliable service for voice or video over IP, or for preferential treatment of data over other traffic.

DS field

Formerly called the IPv4 Type of Service (TOS) octet or the IPv6 Traffic Class octet. The DS field provides the Differentiated Services Code Point (DSCP) that is used for packet forwarding. These fields are part of the standard IPv4 header.

Dynamic Host Configuration Protocol (DHCP)

A standard Internet protocol that dynamically configures hosts on an Internet Protocol (IP) network for either IPv4 or IPv6. DHCP extends the Bootstrap Protocol (BOOTP).

Enterprise Device Manager (EDM)

A web-based embedded management system to support single-element management. EDM provides complete configuration management functionality for the supported devices and is supplied to the customer as embedded software in the device.

Extensible Authentication Protocol over LAN (EAPoL)

A port-based network access control protocol. EAPoL provides security in that it prevents users from accessing network resources before they are authenticated.

File Transfer Protocol (FTP)

A protocol that governs transferring files between nodes, as documented in RFC 959. FTP is not secure and does not encrypt transferred data. Use FTP access only after you determine it is safe in your network.

Hypertext Transfer Protocol (HTTP)

Communications protocol for the Web.

Hypertext Transfer Protocol, Secure (HTTPS)

Communications protocol used to access a secure Web server.

Internet Control Message Protocol (ICMP)

A collection of error conditions and control messages exchanged by IP modules in both hosts and gateways.

Internet Group Management Protocol (IGMP)

IGMP is a host membership protocol used to arbitrate membership in multicast services. IP multicast routers use IGMP to learn the existence of host group members on their directly attached subnets.

Internet Protocol version 4 (IPv4)

The protocol used to format packets for the Internet and many enterprise networks. IPv4 provides packet routing and reassembly.

Internet Protocol version 6 (IPv6)

An improved version of the IP protocol, IPv6 improves the IPv4 limitations of security and user address numbers.

Layer 2

Layer 2 is the Data Link Layer of the OSI model. Examples of Layer 2 protocols are Ethernet and Frame Relay.

Layer 3

Layer 3 is the Network Layer of the OSI model. An example of a Layer 3 protocol is Internet Protocol (IP).

Logical Link Control (LLC)
A protocol used in LANs to transmit protocol data units between two end stations. This LLC layer addresses and arbitrates data exchange between two endpoints.

management information base (MIB)
The MIB defines system operations and parameters used for the Simple Network Management Protocol (SNMP).

marking
A process that uses defined rules to assign the Differentiated Services Code Point (DSCP) in a packet.

mask
A bit string that the device uses along with an IP address to indicate the number of leading bits in the address that correspond with the network part.

Media Access Control (MAC)
Arbitrates access to and from a shared medium.

microflow
A single instance of an application-to-application packet flow identified by source address, destination address, protocol ID, and source port.

MultiLink Trunking (MLT)
A method of link aggregation that uses multiple Ethernet trunks aggregated to provide a single logical trunk. A multilink trunk provides the combined bandwidth of multiple links and the physical layer protection against the failure of a single link.

NonVolatile Random Access Memory (NVRAM)
Random Access Memory that retains its contents after electrical power turns off.

policing
Ensures that a traffic stream follows the domain service-provisioning policy or service-level agreement (SLA).

policy-enabled networking
User-defined characteristics that can be set in policies used to control and monitor traffic.

port
A physical interface that transmits and receives data.

port mirroring
A feature that sends received or transmitted traffic to a second destination.

quality of service (QoS)
QoS features reserve resources in a congested network, allowing you to configure a higher priority for certain devices. For example, you can configure a higher priority for IP deskphones, which need a fixed bit rate and split the remaining bandwidth between data connections if calls in the network are more important than the file transfers.

rate limiting
Rate limiting sets the percentage of traffic that is multicast, broadcast, or both, on specified ports.

routing switch
Virtualizes the physical router interfaces to switches. A virtual router port, or interface, acts as a router port to consolidate switching and routing

functions in the broadcast domain, or between broadcast domains, and enable IP routing for higher traffic volumes.

service level agreement (SLA) A service contract that specifies the forwarding service that traffic receives.

stack Stackable Exreme Networks Ethernet Routing Switches can be connected in a stack configuration of two or more units, up to eight units maximum. A switch stack operates and is managed as a single virtual switch.

traffic profile The temporal properties of a traffic stream, such as rate.

Transmission Control Protocol (TCP) Provides flow control and sequencing for transmitted data over an end-to-end connection.

Trivial File Transfer Protocol (TFTP) A protocol that governs transferring files between nodes without protection against packet loss.

trunk A logical group of ports that behaves like a single large port.

type of service (TOS) A field in the IPv4 header that determines the Class of Service prior to the standardization of Differentiated Services.

User Datagram Protocol (UDP) In TCP/IP, a packet-level protocol built directly on the Internet Protocol layer. TCP/IP host systems use UDP for application-to-application programs.

Virtual Local Area Network (VLAN) A Virtual Local Area Network is a group of hosts that communicate as if they are attached to the same broadcast domain regardless of their physical location. VLANs are layer 2 constructs.

Voice over IP (VOIP) The technology that delivers voice information in digital form in discrete packets using the Internet Protocol (IP) rather than the traditional circuit-committed protocols of the public switched telephone network (PSTN).

weighted round robin (WRR) A mechanism that uses the packet transmission opportunity (PTO) of a queue to determine which queue to process first.