NORTEL

Nortel Ethernet Routing Switch 5000 Series

Configuration - Quality of Service

Release: 6.2
Document Revision: 06.01

www.nortel.com

NN47200-504

Nortel Ethernet Routing Switch 5000 Series
Release: 6.2
Publication: NN47200-504
Document release date: 28 June 2010

Contents

New in this Release

The following sections detail what's new in *Nortel Ethernet Routing Switch 5000 Configuration — Quality of Service* (NN47200-504) for Release 6.2.

Features

See the following sections for information about feature changes:

Enhanced Quality of Service engine

The produce uses an enhanced Quality of Service (QoS) engine to provide more efficient resource use.

Filter Limiting

Enabled by default, Filter Limiting limits the maximum number of user-defined protocol VLANs to 7 . When you disable Filter Limiting, you can create a maximum of 16 user-defined protocol VLANs. The ERS 5510 switch supports a maximum of 7 user-defined protocol VLANs and cannot join a stack if you disable Filter Limiting.

Automatic QoS and ADAC interoperability

Automatic QoS and, Autodetection and Autoconfiguration (ADAC) interoperability enhances automatic QoS implementation on the switch so you can use Automatic QoS and ADAC simultaneously. With Release 6.2 you can enable ADAC and configure Automatic QoS on the port so that ADAC can use the Automatic QoS DiffServe Code Point (DSCP) markings.

Automatic QoS 802.1AB Media Endpoint Device interoperability

Automatic QoS 802.1AB Media Endpoint Device (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.

QoS Egress Queue Shaping

You can use QoS Egress Queue Shaping to configure egress shaping on a port by port and queue by queue basis.Both port-based shaping and per-port per-egress queue shaping are supported in this release. The enhancement allows the traffic flow to be shaped at a CoS level and you can implement the egress queue shaping to provide control on a per queue by queue basis. For more information, see:

- "Egress queue shaping" (page 22)

- "Configuring a QoS interface queue shaper" (page 97)

- "Interface queue shaper configuration" (page 178)

QoS DSCP Mutation

QoS DSCP mutation extends Quality of Service trusted interface support by using the mapping tables, rather than filters, to permit the recolor of DSCP values on egress. The enhancement adds an egress DSCP value the DSCP-to-COS mapping table; the switch uses the egress DSCP value to set the Class of Service (COS) and recolor the DSCP value on egress. In the current QoS implementation of Trusted interface class, the IPv4 traffic received on trusted interfaces is remarked 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 remarked CoS value is used for queuing at egress and possibly for downstream packet processing in a tagged VLAN environment. In some cases, you may need to remark the packet DSCP value at egress as well based on the incoming DSCP value. This DSCP mutation operation can be used by defining individual filters to match and remark targeted DSCP values. The DSCP-to-COS Mapping Table can be easily extended to specify DSCP mutation values and to apply these automatically on Trusted interfaces.

For more information, see:

- "QoS DSCP mutation" (page 39)
- "Configuring egress mapping using the NNCLI" (page 100)
- "Resetting egress mapping values using the NNCLI" (page 100)
- "Displaying QoS Parameters" (page 55)
- "Viewing DSCP mapping" (page 138)

QoS lossless buffering mode for data center applications

QoS lossless buffering mode is critical in data center applications, where reliable data transfer is more important than enhanced throughput. With lossless buffering mode, when a port receives volumes of traffic greater than port bandwidth, the port sends flow control (pause) frames to the sender. QoS lossless buffering is applicable for ERS 5600 series switches only.

Other changes

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

Enterprise Device Manager

Enterprise Device Manager (EDM) replaces both the Java-based Device Manager and Web-based management user interfaces. EDM is an embedded element management and configuration application for Ethernet Routing Switch 5000 Series switches. EDM provides a Web-based graphical user interface through a standard web browser for the convenience of full configuration and management on the switch, and retains the look and feel of Device Manager. For more information, see:

- "Configuring Quality of Service (QoS) using Enterprise Device Manager" (page 129)

Multiple Port Configuration

Among the many functions available in EDM, you can configure port-specific features for a single port, a group of ports, or all ports. Multiple Port Configuration appears as a pane in the work area wherever this function is available. By default the pane appears and you can close and open it with a click of the task bar. For more information about EDM, see *Ethernet Routing Switch 5000 Series Fundamentals* (NN47200-104).

Introduction

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

NNCLI command modes

NNCLI provides the following command modes:

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

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

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

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

Command mode and sample prompt	Entrance commands	Exit commands
User EXEC 5650TD>	No entrance command, default mode	**exit** or **logout**
Privileged EXEC 5650TD#	**enable**	**exit** or **logout**

Command mode and sample prompt	Entrance commands	Exit commands
Global Configuration `5650TD(config)#`	`configure`	To return to Privileged EXEC mode, enter: **end** or **exit** To exit NNCLI completely, enter: **logout**

Interface Configuration
 	
`5650TD(config-if)#`
	From Global Configuration mode:
	To configure a port, enter:
	
	`interface fastethernet <port number>`
	
	To configure a VLAN, enter:
	
	`interface vlan <vlan number>`
		To return to Global Configuration mode, enter:
		
		exit
		
		To return to Privileged EXEC mode, enter:
		
		end
		
		To exit NNCLI completely, enter:
		
		logout

Router Configuration
 	
`5650TD (config-router)#`
	From Global Configuration mode, to configure OSPF, enter:
	
	`router ospf`
	
	To configure RIP, enter:
	
	`router rip`
	
	To configure VRRP, enter:
	
	`router vrrp`
		To return to Global Configuration mode, enter:
		
		exit
		
		To return to Privileged EXEC mode, enter:
		
		end
		
		To exit NNCLI completely, enter:
		
		logout

See *Nortel Ethernet Routing Switch 5000 Series Fundamentals* NN47200-104

Navigation

This document contains the following chapters:

-
-
-

Policy-Enabled Network Fundamentals

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

Summary

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

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

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

Briefly, with DiffServ, policies can be used to identify traffic to forward or drop, meter, re-mark, and assign to certain interfaces. The system marks the DiffServ (DS) field of IP packets to define how the packet is treated as it moves through the network. Flow prioritization is facilitated by identifying, metering, and re-marking. A number of policies can be specified and each policy can match one or many flows—supporting complex classification scenarios.

Port-based and Role-based QoS Policies

The Ethernet Routing Switch 5000 Series supports both port-based and role-based Quality of Service policies. In a port-based Quality of Service environment, policies are applied 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 QoS environment allows for the more direct application of Quality of Service policies and eliminates the need to group ports together when assigning policies.

Port-based and role-based policies can be applied to same port; however the switch administrator is responsible for the proper division of resources across the individual policies.

QoS overview

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

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

Within the DiffServ network, the marked packets are placed in a queue according to their marking, which in turn determines the per-hop behavior (PHB) of that packet. For example, if a video stream is marked so that it receives the highest 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). 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 different DSCPs, is treated according to that marking.

QoS components

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

- Critical and Network classes have the highest priority over all other traffic.

- Premium class is an end-to-end service functioning similarly to a virtual leased line. Traffic in this service class is normally guaranteed an agreed-upon peak bandwidth. Traffic requiring this service must be shaped at the network boundary in order to undergo a negligible delay and delay variance. This service class is suitable for real-time applications, such as video and voice over IP. The recommended PHB for this service is the Expedited Forwarding (EF) PHB.

- Platinum, Gold, Silver, and Bronze classes use the Assured Forwarding (AF) PHB. These classes are used for real-time, delay-tolerant traffic and non-real-time, mission-critical traffic.

- Standard class is the best-effort IP service with an additional, optional use of traffic classification that is used at the network boundary to

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

Table 1 "Service Classes" (page 20) describes the service classes and their required treatment.

Table 1
Service Classes

Traffic category	Service class	Application type	Required treatment
Critical network control	Critical	Critical network control traffic	Highest priority over all other traffic. Guaranteed minimum bandwidth.
Standard network control	Network	Standard network control traffic	Priority over user traffic. Guaranteed minimum bandwidth.
Real time, delay intol erant, fixed bandwidth	Premium	Interhuman communicati ons requiring interaction (such as VoIP).	Absolute bounded priority over user traffic. No packet loss for in-profile traffic. Virtual leased line with lowest amount of latency. Provisioned for peak rate.
Real time, delay tole rant, low variable bandwidth	Platinum	Interhuman communicati ons requiring interaction with additional minimal delay (such as low-cost VoIP).	Higher-priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Real time, delay tole rant, high variable bandwidth	Gold	Single human communication with no interaction (such as web site streaming video).	High-priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Non-real time, missi on critical, interactive	Silver	Transaction processing (such as Telnet, web browsing).	Medium priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.

**Table 1
Service Classes (cont'd.)**

Traffic category	Service class	Application type	Required treatment
Non-real time, mission critical, non-interactive	Bronze	For example, e-mail, FTP, SNMP.	Lower-priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Non-real time, non-mission critical	Standard	Bulk transfer (such as large FTP transfers, after-hours tape backup).	Best-effort delivery. Uses remaining available bandwidth.

Specifying interface groups

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

Each port can belong to only one interface group. One policy references only one interface group; however, you can configure several policies to reference the same interface group.

Different interfaces in a stack may not have the same capabilities. Interfaces with different capabilities can be assigned to the same role. As a result, policies and filters with certain characteristics might not be able to reference an interface group if it contains ports that are incompatible with the policy requirements.

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

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

At factory default, 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 not associated with any 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). Beginning in Release 6.0, QoS-disabled interfaces are associated with reserved role $qosDisabledIfcs.

> *Note 1:* All ports must be removed from an interface group before it is deleted. An interface group cannot be deleted when it is referenced by a policy.
>
> *Note 2:* When QoS is reset to defaults and resources are not available to install default untrusted policies, affected ports are QoS-disabled.

Interface shaping

Interface shaping 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 upon transmission.

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

Egress queue shaping

With egress queue shaping, you can specify the maximum and minimum egress shaping rates on an individual port and queue basis. You can configure shaping criteria for any or all egress queues associated with a switch port. The number of egress queues available for a port is determined by the QoS agent egress queue set value.

You can use QoS Egress Queue Shaping to configure egress shaping on a per queue basis without traffic interruption. Both port-based shaping and per-port per-egress queue shaping are supported.

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

An interface shaper and individual queue shapers can be applied to the same egress port. In this situation, egress traffic will be impacted by the interface shaper and any queue shaping being performed as described in the preceding paragraph.

Egress queue shaping examples

In case the sum of shape minimum rates configured (queue shapers) exceeds the line rate, the minimum shape rate is assured for queue 1 and the remaining bandwidth is distributed to rest of queues using Round Robin (equal distribution). For ERSwitch 4500 serires switches, minimum shape rate is assured for queue 1 and the remaining bandwidth is distributed to rest of queues using the WRR algorithm.

Also if queue shaper is not applied for queue 1, the rest of queues use minimum shape rates (different than 0) for queue shaper and interface shaper is applied to the same egress port with a shape rate that is lower than any from minimum queue shaper rates, the egress traffic will be limited by interface shaper and Round Robin is applied to all queues except queue 1. Queue 1 traffic will not be received in this situation. For Ethernet Routing Switch 4500 serires switches, queue 1 traffic is not received, egress traffic is limited by the interface shaper, and WRR is applied to all queues except queue 1.

QoS traffic profile filter sets

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

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

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

Policies within a set are applied to ingress traffic in a specific order. The evaluation order dictates the order in which classifier elements associated with the same filter set name are applied. Elements with a low evaluation order are applied before elements with a higher evaluation order. An evaluation order must be unique within a filter set. The evaluation order for a classifier block is determined by the lowest evaluation order of the elements that are members of the block or by indicating a block member as the "master" (the evaluation order associated with the master block member is used in 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 associates a unique meter with each policy that comprises the filter set. There are two types of policy-based metering:

- uniform metering—each meter has the same characteristics derived from the filter set instance definition.

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

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

QoS Filter Limiting

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

Enabled by default, Filter Limiting allows you to create up to 7 user-defined protocol VLANs.

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

> **ATTENTION**
> The ERS 5510 switch supports a maximum of 7 user-defined protocol VLANs. If
> you use an ERS 5510 as a standalone switch, or as a unit in a stack, you must
> enable Filter Limiting.

If you save an ASCII configuration that has Filter Limiting disabled and
contains more than 7 user-defined protocol VLANs, when you apply the
configuration to a switch or stack that has Filter Limiting enabled, only
the first 7 user-defined protocol VLANs are configured. If you are using
NNCLI, the system displays error messages and the ASCII configuration
file processing continues. If you are using EDM, the first error halts the
ASCII file process. To prevent the Filter Limiting errors, check the Filter
Limiting setting in the ASCII file to ensure that Filter Limiting is set correctly
for your switch. Then boot the switch and load the ASCII file from either
NNCLI or EDM.

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

Following are examples of Filter Limiting error messages:

- `WARNING: 5510s in stack will not join stack after reboot`

- `WARNING: Resetting the stack will no longer allow a stack to be formed`

- `WARNING: Base unit may not be reachable in standalone mode`

The Nortel SNA solution

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

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

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

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

User based policies

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

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

Rules

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

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

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

Classifier definition

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.

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

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

IP classifier elements

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

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

Layer 2 classifier elements

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

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

Note: 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

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

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

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

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

Classifiers and classifier blocks

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

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

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

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

As classifier blocks are planned, keep in mind that only a single IP classifier element, a single L2 classifier element, and a simple system classifier element can appear in each classifier. For example, to group five

IP classifier elements create five separate classifiers, each with a unique IP classifier element, and then create a classifier block referencing those five classifiers.

> *Note:* Using blocks to combine compatible classifiers uses less resources at the policy level.

On the 5500 Series switch all classifiers that are part of a single classifier block (that is, with the same block number) must each filter on identically the same parameters at the packet level. This includes the same mask, range bitmask, and VLAN tag type. Block membership on the 5600 Series only requires that all members match protocol fields from the same limited set. If this criterion is not met, an error message is generated when an attempt to create the classifier block, or to add a new member to an existing block, is made. Also, if one of the classifier elements in a classifier block has associated actions or meters, then all classifier elements of that classifier block must also have associated actions or meters. On the 5500 Series switch blocks are unordered and evaluated as if simultaneously.

On the 5600 Series switch, a new attribute, `eval-order`, has been added to supply the ability to specify the block evaluation order.

A classifier or classifier block is associated through a policy with individual ports or 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 ports or interface groups are referenced by a policy, which dictates the overall traffic treatment (refer to Figure 2 "Flowchart of QoS Actions" (page 31) for an illustration of the traffic treatment).

Classifier elements, through individual classifiers or a classifier block, are associated with a port or 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 8 is evaluated before a value of 7).

> *Note:* Classifier blocks can be also associated with a meter or action when none of the individual classifiers that comprise that block have associated an action or meter.

Figure 1 "Relationship of classifier elements, classifiers, and classifier blocks" (page 30) displays the relationship between the classifier elements, classifiers, and classifier blocks.

Figure 1
Relationship of classifier elements, classifiers, and classifier blocks
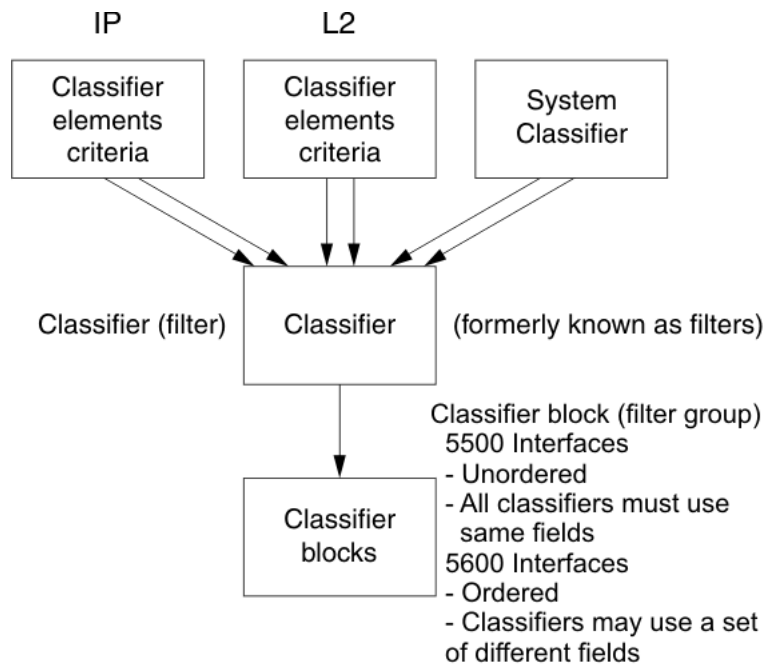
In summary, classifiers combine different classifier elements. In the case of the 5500 Series switch, classifier blocks combine classifiers to form an unordered set of classification data. Unordered data means that all classifiers associated with a policy are applied as if simultaneously, with no precedence.

> *Note:* The 5600 Series switch supports creating classifier blocks using different classifiers. Evaluation order is used to determine which classifier block is applied first when data is matched by multiple blocks.

Specifying actions

summarizes how QoS matches packets with actions.

Figure 2
Flowchart of QoS Actions

Packet

Meet
filter criteria
?

Yes

In-profile ← No — Meter
actions   ?

Yes

Within
← Yes — meter criteria

No

Out-profile
actions
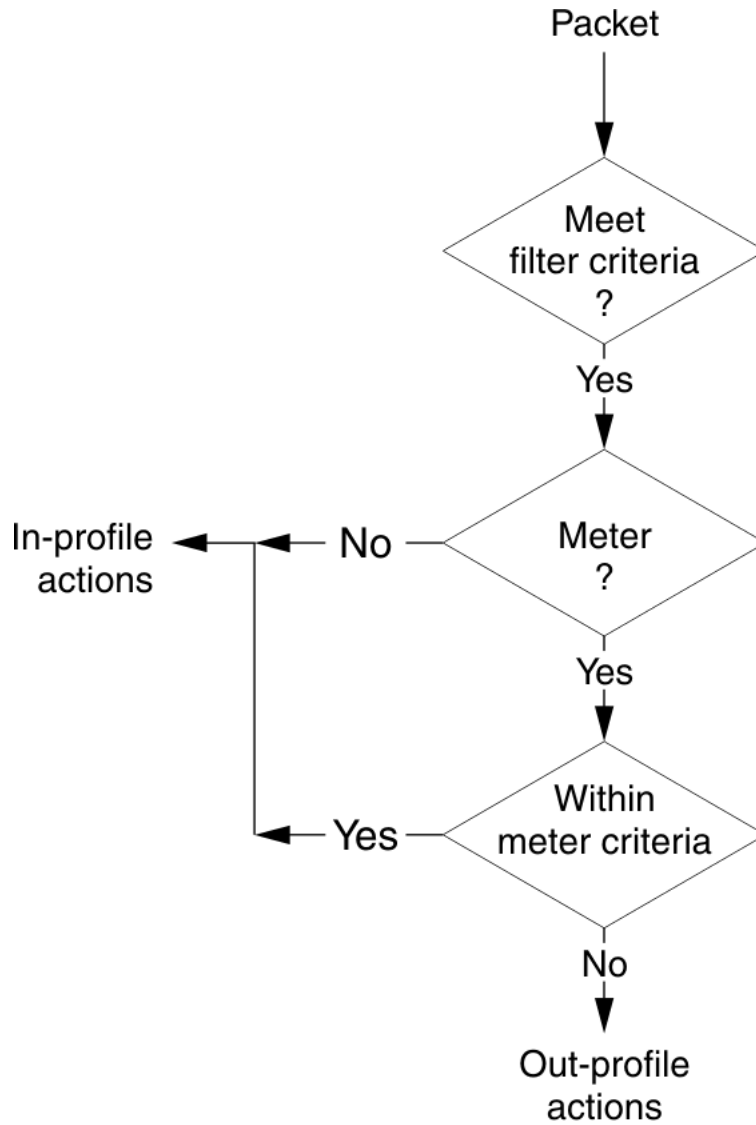
11092EA

Table 2 "Summary of Allowable Actions" (page 31) shows a summary of
the allowable actions for different matching criteria. This information is
applicable to the 5500 Series switch only.

Table 2
Summary of Allowable Actions

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

Table 2
Summary of Allowable Actions (cont'd.)

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

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

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

- Drop

- Re-mark the packet

    — Re-mark a new DiffServ Codepoint (DSCP)

    — Re-mark the 802.1p field

    — Assign a drop precedence

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

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

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

The actions applied to packets include those actions defined from user-defined policies and those actions defined from system default policies. The user-defined actions always carry higher precedences than

the system default actions. This means that, if user-defined policies do not specify actions that overlap with the actions associated with system default policies (for example, the DSCP and 802.1p update actions installed on untrusted interfaces), the default policy actions will be included in the set of actions to be applied to the identified traffic.

Specifying interface action extensions

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

Table 3 "Summary of allowable interface action extensions" (page 33) shows a summary of the allowable interface action extensions for different matching criteria. This information is applicable to the 5500 Series switch only.

Table 3
Summary of allowable interface action extensions

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

Note 1: Native non-match action is not available on the 5600 Series switch. You must define an additional wild card rule to enable native non-match support for 5600 Series ports. All actions in the above table, with the exception of Non-Matching, apply to the 5600 Series switch.

Note 2: The Nortel Ethernet Routing Switch 5600 Series does not initiate an action extension based packet type. The user should redirect all incoming traffic, regardless of packet type (both unicast and non-unicast), towards the same port using interface action extension.

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

* Set egress unicast interface — specifies redirection of normally switched known (with a previously learned destination address) unicast packets to a specific interface (port)

* Set egress non-unicast interface — specifies redirection of normally switched non-unicast (that is, broadcast, multicast, and flooding) packets to a specific interface (port)

Specifying meters

QoS metering, which operates at ingress, provides different levels of service to data streams through user-configurable parameters. A meter 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 block member definition.

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

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

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

> *Note 1:* The range for the committed rate on the 5510 model switch is 1000 to < 1023000 Kb/s. The rate is set in increments of 1000 Kb/s (1 megabit) each.

> *Note 2:* The range for the committed rate on the 5520, 5530, and 5600 Series models is 64 to < 10230000 Kb/s. The rate is set in increments of 64 Kb/s each.

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

> *Note:* Burst rate and duration are used to determine burst size.

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), 2097152 (2048K), 4194304 (4096K), 8388608 (8192K), and in the case of the 5600 Series switch, 16777216 (16384K).

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

Trusted, untrusted, and unrestricted interfaces

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

- trusted

- untrusted

- unrestricted

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

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

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

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

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

OR

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

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

- Trusted interfaces — IPv4 traffic received on trusted interfaces is re-marked at the layer 2 level, that is, the 802.1p user priority value is updated based on the DSCP value in the packet at ingress and the installed DSCP-to-CoS mapping data. The DSCP value is not

updated. On the 5500 Series switch, remapping occurs, by default, only for standardized DSCP values (for example, EF, AFXX) and any proprietary Nortel values. On the 5600 Series switch, remapping occurs for all DSCP values. The DSCP values that are remapped are associated with a zero 802.1p user priority value in the DSCP-to-COS Mapping Table. The 5600 Series switch uses a hardware based DSCP table to support Trusted processing. No policies or filters are consumed by the 5600 Series.

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

  — Untagged frames

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

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

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

  — Tagged frames

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

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

Table 4 "Default QoS fields by class of interface—IPv4 only" (page 37) 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	• Tagged—Dependent on DCSP-to-COS setting. • Untagged—Priority is unchanged.	Does not change

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

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

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

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

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

If an IPv4 packet is received from an untrusted port and it does not match any one of the classifier elements installed by the user on the port, the Nortel Ethernet Routing Switch 5000 Series uses default system classifiers to change the packet DSCP, IEEE 802.1p priority, and drop precedence as follows:

- If the packet is tagged, the 802.1p user priority value is derived from the DSCP-to-CoS mapping table using the best effort DSCP, which is 0.

- If an IPv4 packet is untagged, the Nortel Ethernet Routing Switch 5000 Series uses the default classifier to change the DSCP based on the default IEEE 802.1p priority of the ingress untrusted port to index into the CoS-to-DSCP mapping table to determine the DSCP value.

Table 5 "Default mapping of DSCP to QoS class and IEEE 802.1p" (page 38) describes the default DSCP, QoS class, IEEE 802.1p, and egress queue assignment for packets in each traffic class.

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

Incoming or re-marked DSCP (hex values)	QoS class	Number of queues (8)	Outgoing IEEE 802.1p user priority
CS7 (0x38)	Critical	1	7
CS6 (0x30)	Network	1	
EF(0x2E), CS5(0x28)	Premium	2	6
AF41(0x22), AF42(0x24), AF43(0x26), CS4(0x20)	Platinum	3	5
AF31(0x1A), AF32(0x1C), AF33(0x1E), CS3(0x18)	Gold	4	4
AF21(0x12), AF22(0x14), AF23(0x16), CS2(0x10)	Silver	5	3
AF11(0xA), AF12(0xC), AF13(0xE), CS1(0x8)	Bronze	6	2
DE(0x0), CS0(0x0), all undefined DSCPs	Standard	7	0

As displayed in Table 5 "Default mapping of DSCP to QoS class and IEEE 802.1p" (page 38), the traffic service class determines the IEEE 802.1p priority that determines the egress queue of the traffic. Non-IP traffic can be in the same IP service class if the non-IP packets are assigned the same IEEE 802.1p priority.

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

QoS DSCP mutation

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

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

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

Specifying policies

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

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

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

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

- When **DHCP Relay** and/or **DHCP Snooping** is enabled, it uses the highest available precedence value.

- When **MAC Security (5530-24TFD only)** is enabled, it uses the highest available precedence value.

- When **IP Fix** functionality is enabled, it uses the highest available precedence value.

- When **IGMP** is enabled, it consumes the 2 highest available precedence values.

- When **EAPOL** is enabled, it consumes the highest available precedence value.

- When **EAPOL multihost (5530-24TFD only)** is enabled, it consumes the highest available precedence values.

- When **OSPF** is enabled, it consumes the highest available precedence value.

- When **IP Source Guard** is enabled, it consumes the highest available precedence value.

- When **ADAC** is enabled, it consumes the highest available precedence value.

    Note: The status of mask utilization per port can be seen using "show qos diag" NNCLI command. The number of QoS policies that can be configured is 16 - ("Mask Consumed" +"Non QoS Mask Consumed"). Beginning with release 6.2, diagnostics have been enhanced in for ERS 5500 switches. Diagnostics show precedence allocation on a per port basis similar to ERS 5600 switch diagnostics and show the maximum number of filters, meters, and counters on per port basis. The diagnostics display can be slow if multiple QoS resources are used (especially if traffic profiles are used).

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 or individual ports

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.

> *Note:* 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 Nortel Ethernet Routing Switch 5000 Series supports per policy and per policy, classifier, or interface statistics tracking.

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

Packet flow using QoS

Using DiffServ and QoS, a specific performance level for packets can be designated. This system allows for network traffic prioritization. However, it requires some thought to configure the prioritizations. 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 which group of packets receives the best network throughput, which group of packets receives the next best throughput, and so on. The level of service for each packet is determined by the configurable DSCP.

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

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

The classifiers/classifier blocks are associated with policies, and policies are organized into a hierarchy. The 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).

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

Actions determine how the traffic is treated.

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

Figure 3 "QoS Policy Schematic" (page 43) provides a schematic overview of QoS policies.

Figure 3
QoS Policy Schematic
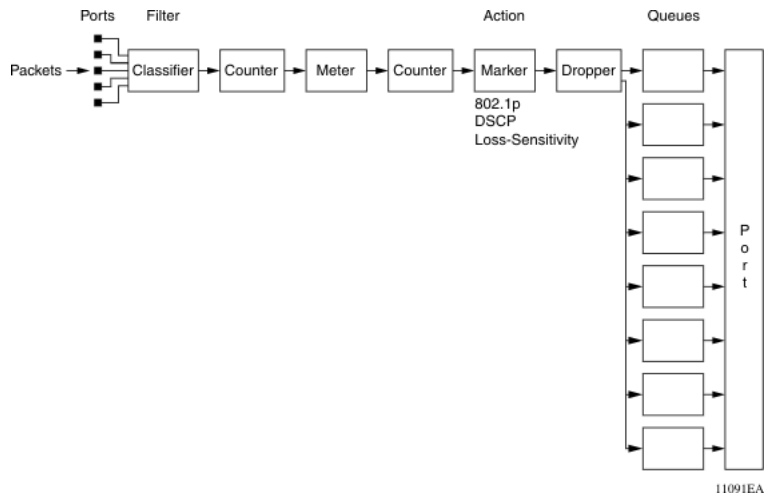
Queue sets

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

- Queue count—the number of different CoS queues in the set.

- Queue service discipline—indicates the means through which queues (competing for limited transmission bandwidth) and the packets held in the queues are scheduled for transmission.

- Queue bandwidth allocation—indicates the absolute or relative amount of bandwidth that can be consumed by the queues in the set. When queues are serviced using a Weighted Round Robin (WRR) or Weighted Fair Queuing (WFQ) discipline, these values represent the weights associated with the queues.

- Queue service order—when multiple service disciplines are in use, the service order indicates service precedence assigned to individual queues (strict priority) or clusters of queues (WRR).

- Queue size—indicates the maximum buffering resources that can be consumed by the individual queue.

Each QoS egress port has eight queue sets consisting of anywhere from 1 to 8 queues, depending on the queue set you assign to the QoS interfaces. Packets are assigned to a queue based on the IEEE 802.1p, or Class of Service (CoS), value associated with that packet. Depending

on the queue set you configure, some queues are serviced in an absolute priority fashion and some queues can be serviced in a Weighted Round Robin (WRR) fashion.

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

> *Note:* These parameters can be configured for all QoS egress interfaces, not on a port-by-port basis. Thus, the egress queuing and buffering characteristics and the CoS-to-queue priorities are the same across all QoS ports. The Nortel Ethernet Routing Switch 5000 Series has factory default queue set and buffer allocation mode values. When a system is reset to defaults, the system has the following values:
>
> - *factory default queue set: queue set 2*
> - *buffer allocation mode: Large*

Modifying queue set characteristics

The following characteristics of the queue sets can be configured:

- 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. 8 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.

Other queue characteristics, such as the service discipline or queue weights for WRR scheduler, cannot be configured.

Although the CoS-to-queue assignments can be changed 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 will 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

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

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

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

QoS lossless buffering mode

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

Lossless mode buffer settings and thresholds have been implemented for all supported QoS Queue sets (1 to 8). Only Queue set 2 has been tested and recommended for this release. With Queue set 2, there are 2 CoS queues; the two queues are WRR, scheduled as 91% and 9%.. Oversubscription ratios of 10 ingress ports to 1 egress port are supported on stacks of up to 5 ERS5600 units, in this release

QoS lossless buffering mode is supported on ERS 5600 series switches only. You must not use QoS lossless buffering mode in a hybrid stack of ERS 5600 and ERS 5500 switches.

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

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

Modifying CoS-to-queue priorities

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

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

QoS configuration guidelines

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

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

- Up to 15 policies per interface (port) can be configured.

- Up to 63 meters per interface (port) can be configured.

- Up to 125 filter components per interface (port) can be configured.

- When tracking statistics is enabled for the policies, the switch uses one counter for each classifier for each interface (port) of the policy or a counter for each policy. Up to 32 counters can be assigned to an interface (port).

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

- Up to 15 policies per interface (port) can be configured

- Up to 256 filter components per precedence per hardware device group

- Up to 128 meters per precedence per hardware device group

- Up to 128 counters per precedence per hardware device group

- Up to 16 TCP/UDP port range checkers per hardware device group

Resource allocation behavior on the Ethernet Routing Switch 5600

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

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

Troubleshooting tips

If problems are encountered configuring the queue sets, ensure that the modified queue set is associated with the QoS interfaces. It is important to note that the device must be reset for the changes to take effect.

Sometimes after modifying the default buffering resources, the queue sizes cannot be seen in the updated queue set. Again, the device must be reset for the changes to take effect.

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

QoS Interface Applications

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

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

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

ARP Spoofing

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

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

1. Drop all ARP packets with a source IP address equal to the identified default gateway.

2. Pass all broadcast ARP requests.

3. Drop all non-broadcast ARP requests.

4. Drop all ARP packets with a target IP address equal to the identified default gateway.

5. Pass all ARP responses.

DHCP Snooping

The DHCP Snooping QoS Application operates by classifying ports as access (untrusted) and core (trusted) and allowing only DHCP requests from the access ports. All other types of DHCP messages received on access ports are discarded. This action prevents rogue DHCP servers from being set up by attackers on access ports and generating DHCP responses that provide the rogue server address for the default gateway and DNS server. This action helps prevent DHCP man-in-the-middle attacks. Users must specify the interface type for the ports on which they wish to enable this support.

DHCP Spoofing

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

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

1. Pass DHCP traffic originated by the valid DHCP server.

2. Drop DHCP traffic originated by all other hosts.

SQLSlam

The worm targeting SQL Server computers is self-propagating, malicious code that exploits a vulnerability that allows for the execution of arbitrary code on the SQL Server computer, due to a stack buffer overflow. Once the worm compromises a machine, it attempts to propagate itself by crafting packets of 376 bytes and sending them to randomly chosen

IP addresses on UDP port 1434. If the packet is sent to a vulnerable machine, this victim machine becomes infected and also begins to propagate. Beyond the scanning activity for new hosts, the current variant of this worm has no other payload. Activity of this worm is readily identifiable on a network by the presence of 376 byte UDP packets. These packets appear to originate from seemingly random IP addresses and destined for UDP port 1434.

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

Nachia

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

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

Xmas

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

TCP SynFinScan

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

TCP FtpPort

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

TCP DnsPort

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

BPDU Blocker

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

DoS Attack Prevention Package

The Ethernet Routing Switch 5600 Series hardware provides built-in support for detection and prevention of many common types of Denial of Service (DoS) attacks. The DoS Attack Prevention Package (DAPP) gives network administrators the ability to enable or disable DAPP support for applicable units and to specify whether DAPP status tracking is required.

The types of common DoS attacks prevented by DAPP are:

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

– IPv4 TCP

— Conditions detected:

– IPv4 first fragment and IP payload < MIN_TCP_HDR_SIZE (normally 20 bytes, range 0 – 255 bytes)

– IPv4 fragment and fragment offset = 1

– Tiny Fragment (Indirect Method) attack

- ICMP checks

— Packet types:

– IPv4 ICMP

– IPv6 ICMP

— Conditions detected:

– ICMP Echo Request and IP payload length > ICMP maximum (programmable maximum size value per packet type – maximum 1K [IPv4]/16K [IPv6])

– ICMP packet is fragmented (IPv4 ICMP only)

When DAPP is enabled, all attack types are monitored. 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: FTP clients are recommended to utilize passive mode when DAPP is enabled.

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 a user enables DAPP support with status tracking, a mask, filter, and counter is allocated for ports on the unit on which DAPP is enabled. Through polling, the unit determines if DAPP has detected a DoS attack. Should an attack be registered, an informative message is logged and a SNMP Trap is generated (if a Trap receiver has been configured). Only one log message and trap is generated per detection cycle (Maximum 8 per polling cycle) on each applicable unit that contains unit and port information.

Automatic QoS

Automatic QoS support provides the ability to easily identify and prioritize Nortel application traffic on Nortel data infrastructure. Automatic QoS gives users the ability to enable or disable Automatic QoS support for the whole system. The user is not able to enable and disable this feature on individual units and ports. When a user enables Automatic QoS support

additional filtering components are associated with all of the supported interfaces classes: Untrusted/Access, Trusted/Core and Unrestricted. These additional filtering components target ingress traffic with the designated private NT DSCP values. When a match occurs, the traffic is given prefered egress queuing within the system and is remarked for appropriate downstream processing.

DSCP remarking occurs when the data infrastructure consists of NT and non-NT equipment. The Automatic QoS value determines whether NT DSCP values are ignored, maintained or remarked at egress.

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

- Set the in-use drop precedence values that are associated with Trusted filters and DSCP Mapping Table entries to High. This allows the NT application traffic with a Low drop precedence value to receive preferential treatment when shared egress queues are congested.

- Mapping information loaded into hardware or enforced using filters will need to take into account the NT application mode. If enabled, mapping information associated with private NT DSCP values will need to take precedence over user-defined DSCP mapping data. If disabled, private NT DSCP data will not be used for initialization purposes.

- DSCP-to-COS mapping data is user configurable. When the NT application mode is enabled, modification of entries that correspond to private NT DSCP values will be allowed but will not be installed in hardware or used to update installed filters to ensure proper Automatic QoS operation.

Automatic QoS operation may consume additional policy and filter resources depending on the platform and QoS configuration. There will be scenarios where enabling Automatic QoS support will be rejected. Users are advised to enable or disable the feature prior to configuring applications that share these limited resources to avoid these complications.

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

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. Non-QoS

operations like RIP are dynamically assigned precedence values after each reset of the device. Since both operation groups use the same pool of precedence values, conflicts can occur when a precedence value assumed by a non-QoS operation is accessed by a QoS operation during the configuration or initialization process. These conflicts are resolved internally by the device but 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, a precedence value is designated that is already consumed by a non-QoS operation. The configuration command will fail 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, a non-QoS operation is assigned 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 will appear to be an error situation to the end user but it is in fact a valid scenario since the precedence value is already consumed.

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

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

QoS errors in NNCLI

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

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

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

Configuring Quality of Service (QoS) with the NNCLI

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

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

Displaying QoS Parameters

Use the following procedure to display QoS parameters.

Procedure steps

Step	Action
1	Display QoS parameters by using the following command from Privileged EXEC mode.

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

--End--

Variable definitions

Variable	Value
acl-assign <1 - 65535>	Displays the specified access list assignment entry. • <1-65535>—Displays a particular entry.

Variable	Value
action [<1-65535> | all | system | user]	Displays the base action entries. The applicable values are: • <1-65535>—displays a particular entry. • all—displays user-created, default, and system entries. • system—displays only system entries. • user—displays only user-created and default entries. Default is all.
agent <details>	Displays the global QoS parameters. details—displays the policy class support table.
arp spoofing	Displays QoS ARP spoofing prevention settings. This parameter applies only to the 5500 Series..
bpdu blocker	Displays QoS BPDU settings. blocker—displays QoS BPDU blocker settings. This parameter applies only to the 5500 Series.
capability [meter | shaper]	Displays the current QoS meter and shaper capabilities of each interface. The applicable values are: • meter—displays QoS port meter capabilities. • shaper—displays QoS port shaper capabilities.
classifier [<1-65535> | all | system user]	Displays the classifier set entries. The applicable values are: • <1-65535>—displays a particular entry. • all—displays all user-created, default, and system entries. • system—displays only system entries. • user—displays only user-created and default entries. Default is all.

Variable	Value
classifier-block [<1-65535> | all | system | user]	Displays the classifier block entries. The applicable values are: • <1-65535>—displays a particular entry. • all—displays all user-created, default, and system entries. • system—displays only system entries. • user—displays only user-created and default entries. Default is all.
dhcp [snooping | spoofing]	Displays QoS DHCP settings. The applicable values are: • snooping—displays QoS DHCP snooping settings. • spoofing—displays QoS DHCP spoofing prevention settings. This parameter applies only to the 5500 Series.
diag [unit]	Displays the diagnostics entries. unit <1-8>—displays diagnostic entries for particular unit
dos [nachia | sqlslam | tcp-dnsport | tcp-ftpport | tcp-synfinscan | xmas]	Displays QoS DoS settings. The applicable values are: • nachia—displays QoS DoS Nachia settings. • sqlslam—displays QoS DoS SQLSlam settings. • tcp-dnsport—displays QoS DoS TCP DnsPort settings. • tcp-ftpport—displays QoS DoS TCP FtpPort settings. • tcp-synfinscan—displays QoS DoS TCP SynFinScan settings. • xmas—displays QoS DoS Xmas settings. This parameter applies only to the 5500 Series.

Variable	Value
filter-limiting	Enable (default) or disable to limit the number of user defined protocol VLANS. • When enabled, there can be created a maximum 7 user-defined protocol VLANs. • When disabled, there can be created a maximum 16 user-defined protocol VLANs **ATTENTION** The ERS 5510 unit cannot join the stack if Filter Limiting is disabled. The ERS 5510 supports only maximum 7 user-defined protocol VLANs.
if-action-extension [<1-65535> | all | system | user]	Displays the interface action extension entries. The applicable values are: • <1-65535>—displays a particular entry. • all—displays all user-created, default, and system entries. • system—displays only system entries. • user—displays only user-created and default entries. Default is all.
if-assign [port]	Displays the list of interface assignments. port—List of ports. Displays the configuration for particular ports
if-group	Displays the interface groups.
if-queue-shaper [port]	Displays the QoS interface queue shaper.
if-shaper [port]	Displays the interface shaping parameters. port—List of ports. Displays the configuration for particular ports
ingressmap	Displays the 802.1p priority to DSCP mapping.
ip-acl <1 - 65535>	Displays the specified IP access list assignment entry. • <1-65535>—displays a particular entry.

Variable	Value
ip-element [<1-65535> | all | system | user]	Displays the IP classifier element entries. The applicable values are: • <1-65535>—displays a particular entry. • all—displays all user-created, default, and system entries. • system—displays only system entries. • user—displays only user-created and default entries. Default is all.
l2-acl <1 - 65535>	Displays the specified Layer 2 access list assignment entry. • <1-65535>—displays a particular entry.
l2-element [<1-65535> | all | system | user]	Displays the Layer 2 classifier element entries. The applicable values are: • <1-65535>—displays a particular entry. • all—displays all user-created, default, and system entries. • system—displays only system entries. • user—displays only user-created and default entries. Default is all.
meter [<1-65535> | all | system | user]	Displays the meter entries. The applicable values are: • <1-65535>—displays a particular entry. • all—displays all user-created, default, and system entries. • system—displays only system entries. • user—displays only user-created and default entries. Default is all.
nsna [classifier | interface | name]	Displays QoS NSNA entries. The applicable values are: • classifier—displays QoS NSNA classifier entries. • interface—displays QoS NSNA interface entries. • name—specifies the label to display a particular NSNA template entry.

Variable	Value
policy [<1-65535>	all	system	user]	Displays the policy entries. The applicable values are: • <1-65535>—displays a particular entry. • all—displays all user-created, default, and system entries. • system—displays only system entries. • user—displays only user-created and default entries. Default is all.
port	Displays the QoS parameters for all ports or for specified ports.
queue-set	Displays the queue set configuration.
queue-set-assignment	Displays the association between the 802.1p priority to that of a specific queue.
statistics <1-65535>	Displays the policy and filter statistics values. • <1-65535>—displays a particular entry.
system-element [<1-65535>	all	system	user]	Displays the system classifier element entries. The applicable values are: • <1-65535>—displays a particular entry. • all—displays all user-created, default, and system entries. • system—displays only system entries. • user—displays only user-created and default entries.
ubp [classifier	interface	name]	Displays QoS UBP entries. The applicable 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.
user-policy	Displays QoS User Policy entries.

Displaying QoS capability policy configuration

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

Procedure steps

Step	Action
1	Display QoS capability policy configuration by using the following command from Privileged EXEC mode: **show qos capability {meter [port] | shaper [port]}**
	--End--

Variable definitions

Variable	Value
meter [port]	Displays granularity for committed rate, maximum committed rate and maximum bucket that can be used on ports for meters. port—specifies list of ports. Displays the information for particular ports
shaper [port]	Displays granularity for committed rate, maximum committed rate and maximum bucket that can be used on ports for shapers. port—specifies list of ports. Displays the information for particular ports

Configuring QoS Access Lists

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

Assigning ports to an access list

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

Procedure steps

Step	Action
1	Assign ports to an access list by using the following command in Global Configuration mode. **qos acl-assign** **port <port_list>** **acl-type {ip | l2}** **name <name>**
	--End--

Variable definitions

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

Removing an access list assignment

Use the following procedure to remove an access list assignment .

Procedure steps

Step	Action

1   Remove an access list assignment by using the following command from Global Configuration mode.

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

--End--

Creating an IP access list

Use the following procedure to create an IP access list.

Procedure steps

Step	Action

1   Create an access list by using the following procedure from Global Configuration mode.

```
qos ip-acl name <name>
[addr-type <addrtype>]
[src-ip <source_ip>]
[dst-ip <destination_ip>]
[ds-field <dscp>]
[{protocol <protocol_type> | next_header
<header>}]
[src-port-min <port>
src-port-max <port>]
[dst-port-min <port>
dst-port-max <port>]
[flow-id <flowid>]
[drop-action {drop | pass}]
[update-dscp <0 - 63>]
[update-1p <0 - 7>]
[set-drop-prec {high drop | low drop}]
[block <block_name>]
```

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

--End--

Variable definitions

Variable	Value
name <name>	Specifies the name assigned to this access list.
addr-type <addrtype>	Specifies the IP address type to use for the access list.
src-ip <source_ip>	Specifies the source IP address to use for this access list.
dst-ip <destination_ip >	Specifies the destination IP address to use for this access list.
ds-field <dscp>	Specifies the DSCP value to use for this access list.

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

Removing an IP access list

Use the following procedure to remove an IP access list.

Procedure steps

Step	Action
1	Remove an access list by using the following command from Global Configuration mode.

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

--End--

Creating a Layer 2 access list

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

Procedure steps

Step	Action
1	Create an access list by using the following command from Global Configuration mode.

```
qos l2-acl name <name>
[src-mac <source_mac_address>]
[src-mac-mask
<source_mac_address_mask>]
[dst-mac <destination_mac_address>]
[dst-mac-mask
<destination_mac_address_mask>]
[vlan-min <vid_min>
vlan-max <vid_max>]
[vlan-tag <vtag>]
[ethertype <etype>]
[priority <ieee1p_seq>]
[drop-action {drop | pass}]
[update-dscp <0 - 63>]
[update-1p <0 - 7>]
[set-drop-prec {high-drop | low-drop}]
[block <block_name>]
```

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

--End--

Variable definitions

Variable	Value
name <name>	Specifies the name assigned to this access list.
src-mac <source_mac_address>	Specifies the source MAC address to use for this access list.
src-mac-mask <source_mac_address_mask>	Specifies the source MAC address mask to use for this access list.
[dst-mac <destination_mac_address>]	Specifies the destination MAC address to use for this access list.

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

Removing a Layer 2 access list

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

Procedure steps

Step	Action
1	Remove an access list by using the following command from Global Configuration mode. `no qos l2-acl <aclid>`

--End--

Configuring QoS security

The NNCLI commands detailed in this section allow for the configuration and management of QoS security settings. For information on displaying this information, refer to .

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

Enabling QoS ARP spoofing

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

Procedure steps

Step	Action
1	Enable the QoS ARP spoofing application by using the following command from Interface Configuration mode. `qos arp spoofing [port <port_list>] enable default-ga teway <A.B.C.D>`
	--End--

Variable definitions

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

Disabling QoS ARP spoofing

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

Procedure steps

Step	Action
1	Disable the QoS ARP spoofing application by using the following command from Interface Configuration mode. `no qos arp spoofing port <port_list>`
	--End--

Enabling QoS BPDU blocker

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

Procedure steps

Step	Action
1	Enable the BPDU blocker application by using the following command from Interface Configuration mode. `qos bpdu blocker port <port_list> enable`

--End--

Disabling QoS BPDU blocker

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

Procedure steps

Step	Action
1	Disable the BPDU blocker application by using the following command from Interface Configuration mode. `no qos bpdu blocker port <port_list>`

--End--

Enabling QoS DHCP snooping and spoofing

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

Procedure steps

Step	Action
1	Enable snooping by using the following command from Interface Configuration mode. `qos dhcp snooping port <port_list> enable interface-type {access	core}`
2	Enable spoofing by using the following command from Interface Configuration mode.

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

--End--

Variable definitions

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

Disabling QoS DHCP snooping and spoofing

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

Procedure steps

Step	Action
1	Disable snooping by using the following command from Interface Configuration mode. `no qos dhcp snooping port <port_list>`
2	Disable spoofing by using the following command from Interface Configuration mode. `no qos dhcp spoofing port <port_list>`

--End--

Variable definitions

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

Enabling QoS DoS applications

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

Procedure steps

Step	Action
1	Enable QoS DoS applications by using the following command from Interface Configuration mode.

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

--End--

Variable definitions

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

Disabling QoS DoS applications

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

Procedure steps

Step	Action
1	Disable QoS DoS applications by using the following command from Interface Configuration mode.

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

--End--

Variable definitions

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

QoS Agent configuration

The NNCLI commands detailed in this section allow for the configuration and management of the QoS Agent.

Globally enabling and disabling QoS Agent support

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

Procedure steps

Step	Action
1	Globally enable QoS Agent support using the following command: **`qos agent oper-mode [enable]`** **OR** **`default qos agent [oper-mode]`**
2	Globally disable QoS Agent support using the following command: **`no qos agent oper-mode [enable]`**

--End--

QoS Agent support is enabled by default. QoS Agent support cannot be disabled if QoS functionality is currently used by NSNA or UBP.

Variable definitions

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

Configuring QoS agent

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

Procedure steps

Step	Action
1	Configure QoS agent by using the following command from Global Configuration mode.

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

--End--

Variable definitions

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

Configuring QoS agent to default

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

Procedure steps

Step	Action
1	Configure QoS agent parameters to factory default values by using the following command from Global Configuration mode.

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

--End--

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

Variable definitions

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

Viewing QoS agent configuration information
Use the following procedure to display the QoS agent parameter configuration.

Procedure steps

Step	Action
1	Display the QoS agent parameter configuration by using the following command from Privileged EXEC Configuration mode. `show qos agent`

--End--

Job aid: `show qos agent` **command output**

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

```
5530-24TFD#show qos agent
QoS Operational Mode:  Enabled
QoS NVRam Commit Delay:  10 seconds
QoS Queue Set:  2
QoS Buffering:  Large
QoS UBP Support Level:  Low Security Local Data
QoS Default Statistics Tracking:  Aggregate
QoS DOS Attack Prevention:  Disabled
Minimum TCP Header Length:  20
Maximum IPv4 ICMP Length:  512
Maximum IPv6 ICMP Length:  512
Auto QoS mode:  Disabled
QoS Trusted Processing Mode:  Partial
```

Modifying default queue configuration

Use the following procedure to modify the default queue configuration.

Procedure steps

Step	Action
1	Modify the configuration by using the following command from Global Configuration mode. `qos agent queue-set <1-8>`
	--End--

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

Configuring Default Buffering Capabilities

Use the following NNCLI commands to display and modify the buffer allocation mode.

Configuring default QoS resource buffer

Use the following procedure to allocate the default QoS resource buffer.

Procedure steps

Step	Action
1	Restore the default the resource buffer by using the following command from Global Configuration mode.

```
default qos agent buffer
```

--End--

Modifying QoS resource buffer allocation

Use the following procedure to modify QoS resource buffer allocation.

Procedure steps

Step	Action
1	Modify resource buffer allocation by using the following command from Global Configuration mode. `qos agent buffer <regular ∣ large ∣ maximum>`

--End--

Variable definitions

Variable	Value
buffer	Modifies the QoS resource buffer allocation. The allowed buffer allocation modes for all QoS interfaces are as follows: • regular • large • maximum *Note:* The buffer mode determines the level of resource sharing across interfaces sharing the same port hardware.

Enabling lossless buffering mode

Use the following procedure to enable lossless buffering mode on ERS 5600 series switches.

Procedure steps

Step	Action
1	To enable lossless buffering mode on ERS 5600 series switches, use the following command from Global Configuration mode: `qos agent buffer lossless`

--End--

Configuring the CoS-to-Queue assignments

Use the following NNCLI commands to display and modify CoS-to-queue assignments.

Configuring 802.1p priority values

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

Procedure steps

Step	Action
1	Configure priority values by using the following command from Global Configuration mode. `qos queue-set-assignment queue-set <1-56> 1p <0-7> queue <1-8>`
	--End--

Variable definitions

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

Configuring QoS interface groups

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

Configuring ports for an interface group

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

Procedure steps

Step	Action
1	Add ports by using the following command from Interface Configuration mode.

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

--End--

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

Variable definitions

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

Removing ports from an interface group

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

Procedure steps

Step	Action

1   Delete ports by using the following command from Interface Configuration mode.

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

--End--

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

Creating an interface group

Use the following procedure to create interface groups.

Procedure steps

Step	Action

1   Create interface groups by using the following command from Global Configuration mode.

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

--End--

Variable definitions

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

Removing an interface group

Use the following procedure to delete interface groups.

Procedure steps

Step	Action
1	Delete interface groups by using the following command from Global Configuration mode. `no qos if-group name <WORD>`

<div align="center">--End--</div>

Note 1: An interface group referenced by an installed policy cannot be deleted.

Note 2: An interface group associated with ports cannot be deleted.

Configuring DSCP and 802.1p and queue associations

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

Configuring DSCP to 802.1p priority

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

Step	Action
1	Configure priority by using the following command from Global Configuration mode. `qos egressmap [name <WORD>] [ds <0-63>] [1p <0-7>] [dp <low-drop │ high-drop>] [ds-new < 0-63>]`

--End--

Variable definitions

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

Restoring egress mapping entries to default

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

Procedure steps

Step	Action
1	Reset the entries by using the following command from Global Configuration mode. `default qos egressmap`

--End--

Configuring 802.1p priority to DSCP

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

Procedure steps

Step	Action
1	Configure priority by using the following command from Global Configuration mode. `qos ingressmap [name <WORD>] 1p <0-7> ds <0-63>`

--End--

Variable definitions

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

Restoring ingress mapping entries to default

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

Procedure steps

Step	Action
1	Reset the entries by using the following command from Global Configuration mode. `default qos ingressmap`

--End--

Configuring QoS Elements, Classifiers, and Classifier Blocks

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

Configuring IP classifier element entries

Use the following procedure to add and configure classifier entries.

Procedure steps

Step	Action
1	Add and configure classifier entries by using the following command from Global Configuration mode.

```
qos ip-element <cid> [addr-type <addrtype>] [ds-field
<dscp>] [dst-ip <dst-ip-info>] [dst-port-min <port>]
[flow-id <flowid>] [ip-flag <ip-flags>] [ipv4-options
<no-opt | with-opt>] [next-header <nextheader>]
[session-id] [src-ip <src-ip-info>] [src-port-min
<port>] [tcp-control <tcp-flags>]
```

<div align="center">**--End--**</div>

Variable definitions

Variable	Value
<cid>	Specifies the element ID, value ranges from 1–55000.
addr-type <addrtype>	Specifies the address type. Use the value ipv4 to indicate an IPv4 address or the value ipv6 to indicate an IPv6 address. The default value is ipv4.
ds-field <0-63>	Specifies a 6-bit DSCP value; value ranges from 0–63. Default is ignore.
dst-ip <dst-ip-info>	Specifies the source IP address and mask in the form of a.b.c.d/x for IPv4, or x:x:x:x:x:x:x:x/z for IPv6. Default is 0.0.0.0.
dst-port-min <port>	Specifies the L4 destination port minimum value.
flow-id <flowid>	Specifies the IPv6 flow identifier.
ip-flag <ip-flags>	Specifies the flags present in an IPv4 header.

Variable	Value
ipv4-options <no-opt | with-opt>	Specifies whether the Option field is present in the packet header. Valid values are: • no-opt—indicates that only IPv4 packets without options will match this classifier element. • with-opt—indicates that only IPv4 packets with options will match this classifier element. IPv4 packets with ipv4-options are not matched on a ERS 5000 series switch.
next-header	Specifies the IPv6 next header classifier criteria; range is 0–255.
src-ip <src-ip-info>	Specifies the source IP address and mask in the form of a.b.c.d/x for IPv4, or x:x:x:x:x:x:x:x/z for IPv6. Default is 0.0.0.0.
session-id	Specifies the session ID.
src-port-min <port>	Specifies the L4 source port minimum value.
tcp-control <tcp-flags>	Specifies the control flags present in an TCP header.

Viewing IP classifier entries

Use the following procedure to view IP classifier entries.

Procedure steps

Step	Action
1	View IP classifier element entries by using the following commands from the Privileged EXEC Configuration mode. `show qos ip-element [<1-65535>] [all] [system] [user]`

--End--

Removing IP classifier entries

Use the following procedure to remove IP classifier entries.

Procedure steps

Step	Action
1	Remove IP classifier entries by using the following command from Global Configuration mode.

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

--End--

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

Adding Layer 2 elements

Use the following procedure to add Layer 2 elements.

Procedure steps

Step	Action
1	Add Layer 2 elements by using the following command from the Global Configuration mode.

```
qos l2-element <1-55000> [dst-mac <dst-mac>]
[dst-mac-mask <dst-mac-mask>] [ethertype <etype>]
[pkt-type <etherII | llc | snap>] [priority
<ieee1p-seq>] [session-id <session-id>] [src-mac
<src-mac>] [src-mac-mask <src-mac-mask>] [vlan-min
<vid-min>] [vlan-max <vid-max>][vlan-tag <vtag>]
```

--End--

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

Variable definitions

Variable	Value
<1-55000>	Specifies the element ID; range is 1–55000.
dst-mac <dst-mac>	Specifies the destination MAC element criteria. Valid format is H.H.H.
dst-mac-mask <dst-mac-mask>	Specifies the destination MAC mask element criteria. Valid format is H.H.H.
ethertype <etype>	Specifies the Ethernet type. Valid format is 0xXXXX, for example, 0x0801. Default is ignore.

Variable	Value
pkt-type <etherII | llc | snap>	Specifies the packet frame format. • etherII—indicates that only Ethernet II format frames match this classifier component. • snap—indicates that only EEE 802 SNAP format frames match this classifier component. • llc—indicates that only IEEE 802 LLC format frames match this classifier component.
priority <ieee1p-seq>	Specifies the 802.1p priority values; range from 0–7 or all. Default is ignore.
session-id <session-id>	Specifies the session ID.
src-mac <src-mac>	Specifies the source MAC element criteria. Enter in the format H.H.H.
src-mac-mask <src-mac-mask>	Specifies the source MAC mask element criteria. Valid format is H.H.H.
vlan-min <vid-min>	Specifies the VLAN ID minimum value element criteria. Range is 1–4094.
vlan-max <vid-max>	Specifies the VLAN ID maximum value element criteria. Range is 1–4094.
vlan-tag <format>	Specifies the packet format element criteria: • untagged • tagged The default is Ignore.

Viewing Layer 2 elements

Use the following procedure to view Layer 2 elements.

Procedure steps

Step	Action
1	View Layer 2 element entries by using the following commands from the Privileged EXEC Configuration mode. `show qos l2-element [<1-65535>] [all] [system] [user]`

--End--

Removing Layer 2 elements

Use the following procedure to delete Layer 2 element entries.

Procedure steps

Step	Action
1	Delete element entries by using the following command from Global Configuration mode. `no qos l2-element <1-55000>`

--End--

Linking IP and L2 classifier elements

Use the following procedure to link IP and L2 classifier elements.

Procedure steps

Step	Action
1	Link elements by using the following command from Global Configuration mode. `qos classifier <1-55000> set-id <1-55000> [name <WORD>]` `element-type {ip	l2	system} element-id <1-55000>`

--End--

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

Variable definitions

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

Removing classifier entries

Use the following procedure to delete classifier entries.

Procedure steps

Step	Action
1	Delete classifier entries by using the following command from Global Configuration mode. `no qos classifier <1-55000>`

--End--

Note: Each classifier can have only a single IP classifier element plus a single L2 classifier element or system classifier element. However, a classifier can be created using only one IP classifier element or only one L2 classifier element or only one system classifier element.

Combining individual classifiers

Use the following procedure to combine individual classifiers.

Procedure steps

Step	Action

1	Combine individual classifiers by using the following command from Global Configuration mode.
	
	`qos classifier-block <1-55000> block-number <1-55000>`
	`[name <WORD>]{set-id <1-55000> | set-name <WORD>}`
	`[{in-profile-action <1-55000> | in-profile-action-name`
	`<WORD>} | {meter <1-55000> | meter-name <WORD>}]`

--End--

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

Variable definitions

Variable	Value
classifier-block<1-55000>	Specifies an the classifier block ID; range is 1–55000.
block-number <1-55000>	Specifies the classifier block number; range is 1–55000.
name <WORD>	Specifies the label for the classifier block; maximum is 16 alphanumeric characters.

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

Removing classifier block entries

Use the following procedure to delete classifier block entries.

Procedure steps

Step	Action
1	Delete classifier block entries by using the following command from Global Configuration mode.

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

--End--

Configuring QoS system-element

Configuring system classifier element parameters

Use the following procedure to configure system classifier element parameters that may be used in QoS policies.

Procedure steps

Step	Action
1	Configure system classifier element parameters by using the following command from Global Configuration mode.

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

--End--

Note: On the 5500 Series switch, when untagged format is used the last 4 bytes (77 to 80) from data/mask pattern are reserved by the hardware and should not be configured.On the 5600 Series switch, when untagged format is used the last 4 bytes (125-128) from data/mask pattern are reserved by the hardware and should not be configured.

Variable definitions

Variable	Value
<1-55000>	Specifies the system classifier element entry id; range is 1–55000.
known-ip-mcast	Specifies the filter on known multicast destination address. This parameter is applicable only on ERS 5600 series switches.
known-non-ip-mcast	Specifies the filter on known non IP multicast destination address. This parameter is applicable only on ERS 5600 series switches.
unknown-ip-mcast	Specifies the filter on unknown multicast destination address. This parameter is applicable only on ERS 5600 series switches.
unknown-ucast	Specifies the Filter on unknown unicast destination address. This parameter is applicable on both ERS 5600 series switches.
unknown-non-ip-mcast	Specifies the filter on unknown non IP multicast destination address. This parameter is applicable only on ERS 5500 and 5600 series switches.
non-ip	Specifies the filter on non IP packets as the destination address. This parameter is applicable only on ERS 5600 series switches.

Variable	Value
pattern-format { tagged | untagged }	Specifies the format of data/mask pattern. Specifies the available values are: • tagged— Data/mask pattern describes a tagged packet • untagged—Data/mask pattern describes an untagged packet
pattern-data <WORD>	Specifies the byte pattern data to filter on. *Note:* The format of the WORD string is in the form of XX:XX:XX:....:XX.
pattern-l2-format <ethernetII|llc|snap>	Specifies the format of the L2 pattern data and mask. Values include: • ethernetII • llc • snap
pattern-mask <WORD>	Specifies the byte pattern mask to filter on. *Note 1:* The format of the WORD string is in the form of XX:XX:XX:....:XX. *Note 2:* This parameter not applicable to the 5600 Series switch.
pattern-ip-version	Specifies the IP version of the pattern data or mask. • ipv4—Filter IPv4 Header • ipv6—Filter IPv6 Header • non-ip—Filter non-ip packets This parameter applies only to the 5600 Series switch.
session-id	Specifies the session ID.

Viewing system classifier elements parameters

Use the following procedure to view system classifier elements parameters.

Procedure steps

Step	Action
1	View system classifier elements parameters by using the following commands from the Privileged EXEC Configuration mode.

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

--End--

Removing system classifier element entries

Use the following procedure to remove system classifier element entries.

Procedure steps

Step	Action
1	Remove system classifier element entries by using the following command from Global Configuration mode.

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

--End--

Configuring QoS actions

The configuration of QoS actions directs the Nortel Ethernet Routing Switch 5000 Series to take specific action on each packet. This section covers the following NNCLI commands.

Creating and updating QoS actions

Use the following procedure to create and update QoS actions.

Procedure steps

Step	Action
1	Create or update QoS actions by using the following command from Global Configuration mode.

```
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>]
```

--End--

Note: 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.

Variable definitions

Variable	Value
<10-55000>	Specifies the QoS action; range is 10–55000.
name <WORD>	Assigns a name to a QoS action with the designated action ID. Enter the name for the action; maximum is 16 alphanumeric characters
drop-action<enable | disable | deferred-pass>	Specifies whether packets are dropped or not: • enable—drop the traffic flow • disable—do not drop the traffic flow • deferred-pass—traffic flow decision deferred to other installed policies Default is deferred pass. *Note:* 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 to 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 to 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. *Note:* Requires specification of **update-dscp** value.
set-drop-prec <low-drop | high-drop>	Specifies the drop precedence value: • low-drop • high-drop Default is low-drop.

Variable	Value
action-ext <1-55000>	Specifies the action extension; range is 1–55000.
action-ext-name <WORD>	Specifies a label for the action extension; maximum is 16 alphanumeric characters.

Removing QoS actions

Use the following procedure to delete QoS action entries.

Procedure steps

Step	Action
1	Delete QoS action entries by using the following command from Global Configuration mode.

no qos action <10-55000>

--End--

Note: An action cannot be deleted if referenced by a policy, classifier block, or meter.

Configuring QoS iInterface action extensions

QoS interface action extensions direct the Nortel Ethernet Routing Switch 5000 Series to take specific action on each packet. This section covers the following NNCLI commands.

Creating interface action extension entries

Use the following procedure to create interface action extension entries.

Procedure steps

Step	Action
1	Create interface action extension entries by using the following command from Global Configuration mode.

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

--End--

Note 1: An interface extension that is referenced in an action entry cannot be deleted.

Note 2: The 5600 Series switch requires that both egress-ucast and egress-non-ucast be specified with the same port.

Variable definitions

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

Removing interface action extension entries

Use the following procedure to remove interface action extension entries.

Procedure steps

Step	Action
1	Remove interface action extension entries by using the following command from Global Configuration mode.

```
no qos if-action-extension <1-55000>
```

--End--

Configuring QoS meters

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

Creating QoS meter entries

Use the following procedure to create QoS meter entries.

Procedure steps

Step	Action
1	Create QoS meter entries by using the following command from Global Configuration mode.

```
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>}
```

--End--

Variable definitions

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

Removing QoS meter entries

Use the following procedure to delete QoS meter entries.

Procedure steps

Step	Action
1	Remove QoS meter entries by using the following command from Global Configuration mode. `no qos meter <1-55000>`

<p align="center">--End--</p>

Note: A meter that is referenced in an installed policy or classifier block cannot be deleted.

Configuring QoS interface shaper

Configuring interface shaping

Use the following procedure to configure interface shaping.

Procedure steps

Step	Action
1	Configure interface shaping by using the following command from Interface Configuration mode. `qos if-shaper [port <portlist>] [name <WORD>] shape-rate <64-10230000> {burst-size <burst-size> max-burst-rate <64-4294967295> [max-burst-duration <1-4294967295>]}`

<p align="center">--End--</p>

Variable definitions

Variable	Value
burst-size <4,8,16, ..., 16384>	Specifies the committed burst size in Kilobytes. The value range is: 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384.
port <portlist>	Specifies the ports to configure shaping parameters.
name <WORD>	Specifies name for if-shaper; maximum is 16 alphanumeric characters.
shape-rate <64-10230000>	Specifies the shaping rate in kilobits/sec; range is 64-10230000 kilobits/sec.

Variable	Value
max-burst-rate <64-4294967295>	Specifies the largest burst of traffic that can be received a given time for the traffic to be considered in-profile. Used in calculating the committed burst size. Enter the burst size in Kb/s for in-profile traffic; range is 64 to 4294967295 Kbits/sec.
max-burst-duration <1-4294967295>	Specifies the amount of time that the largest burst of traffic that can be received for the traffic to be considered in-profile. Used in calculating the committed burst size. Enter the burst duration in ms for in-profile traffic; range is 1–4294967295 ms.

Disabling interface shaping

Use the following procedure to disable interface shaping.

Procedure steps

Step	Action
1	Disable interface shaping by using the following command from Interface Configuration mode. `no qos if-shaper [port <portlist>]`

<div align="center">**--End--**</div>

Configuring a QoS interface queue shaper

Use the following procedures to configure a QoS queue shaper.

Configuring a QoS interface queue shaper navigation

- "Creating a QoS interface queue shaper using the NNCLI" (page 97)

- "Deleting a QoS interface queue shaper using the NNCLI" (page 98)

- "Viewing QoS interface queue shaper information using the NNCLI" (page 99)

Creating a QoS interface queue shaper using the NNCLI

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

Procedure steps

Step	Action
1	Create an egress queue shaper by using the following command from the Interface Configuration mode: `qos if-queue-shaper [port <portlist>][queue <1-8>][name <WORD>][shape-rate <64-10230000> shape-min-rate <64-10230000>`

<div align="center">

--End--

</div>

Variable definitions

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

Variable	Value
`name <WORD>`	Specifies an alphanumeric label used to identify the QoS interface queue shaper. 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 <64-10230000>`	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.
`shape-rate <64-10230000>`	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.

Deleting a QoS interface queue shaper using the NNCLI

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

Procedure steps

Step	Action
1	Delete an egress queue shaper by using the following command from the Interface Configuration mode: `no qos if-queue-shaper port <portlist> queue <1-8>`

--End--

Variable definitions

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

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

Viewing QoS interface queue shaper information using the NNCLI

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

Procedure steps

Step	Action
1	Display egress queue shaper information by using the following command from the Interface Configuration mode: `show qos if-queue-shaper [port <portlist>]`

--End--

Variable definitions

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

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

Configuring egress mapping using the NNCLI

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

Step	Action

1	To configure egress mapping, use the following command from Global Configuration mode:
	
	`qos egressmap name <WORD> ds <0-63> 1p <0-7> dp`
	`<low-drop│high-drop> [ds-new <0-63>]`

--End--

Variable definitions

Use the data in the following table to help you use the `qos egressmap name <WORD> ds <0-63> 1p <0-7> dp <low-drop│high-drop> [ds-new <0-63>]` command.

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

Resetting egress mapping values using the NNCLI

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

Procedure steps

Step	Action
1	To reset the entries, use the following command from the Global Configuration mode: `default qos egressmap`

--End--

Configuring QoS policies

Use the following NNCLI commands to configure QoS policies.

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

Configuring QoS policies

Use the following procedure to create and configure QoS policies.

Procedure steps

Step	Action
1	Create a QoS policy by using the following command from Global Configuration mode.

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

--End--

Note: 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.

Variable definitions

Table 6
qos policy parameters

Variable	Value
<1-55000>	Specifies the QoS policy; range is 1–55000.
enable|disable	Enables or disables the QoS policy.
name <WORD>	Specifies the name for the policy; maximum is 16 alphanumeric characters.
port <portlist>	Specifies the ports to which to directly apply this policy.
if-group <WORD>	Specifies the interface group name to which this policy applies; maximum number of characters is 32 US-ASCII. The group name must begin with a letter within the range a..z or A..Z.
clfr-type <classifier	block>	Specifies the classifier type; classifier or block.
clfr-id <1-55000>	Specifies the classifier ID; range is 1–55000.
clfr-name <WORD>	Specifies the classifier name or classifier block name; maximum is 16 alphanumeric characters.
in-profile-action <1-55000>	Specifies the action ID for in-profile traffic; range is 1–55000.
in-profile-action-name <WORD>	Specifies the action name for in-profile traffic; maximum is 16 alphanumeric characters.

Table 6
qos policy parameters (cont'd.)

Variable	Value
meter <1-55000>	Specifies meter ID associated with this policy; range is 1–55000.
meter-name <WORD>	Specifies the meter name associated with this policy; maximum of 16 alphanumeric characters.
non-match-action <1-55000>	Specifies the action ID for non-match traffic; range is 1–55000. This parameter is not applicable to 5600 Series switches.
non-match-action-name <WORD>	Specifies the action name for non-match traffic; maximum is 16 alphanumeric characters.
precedence <1-15>	Specifies the precedence of this policy in relation to other policies associated with the same interface group. Enter precedence number; range is 1–15. *Note:* 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

Job aid: Viewing QoS policies

The following is an example to view the created `qos policy`

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

Id:  55003
Policy Name:  no_pc3
State:  Enabled
Classifier Type:  Classifier
Classifier Name:  no_pc3
Classifier Id:  55003
Unit/Port:  1/8
Meter:
Meter Id:
In-Profile Action:  no_pc3
In-Profile Action Id:  55003
Non-Match Action:
Non-Match Action Id:
Track Statistics:  Aggregate
Precedence:  13
Session Id:  0
Storage Type:  Other
5530-24TFD(config)#show qos policy 55004

Id:  55004
Policy Name:  meter_pc3
State:  Enabled
Classifier Type:  Classifier
Classifier Name:  meter_pc3
Classifier Id:  55004
Unit/Port:  1/18
Meter:  meter_pc3
Meter Id:  55001
In-Profile Action:
In-Profile Action Id:
Non-Match Action:
Non-Match Action Id:
Track Statistics:  Aggregate
Precedence:  13
Session Id:  0
Storage Type:  Other
5530-24TFD(config)#
```

Removing QoS policies

Use the following procedure to disable QoS policy entries. Policies can be enabled using the `qos policy <policynum> enable` command.

Procedure steps

Step	Action
1	Remove QoS policy entries by using the following command from Global Configuration mode.

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

--End--

QoS traffic profile filter set configuration

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

Configuring a traffic profile classifier entry

Configure a traffic profile classifier entry using the following procedure.

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

Procedure steps

Step	Action
1	To create a new traffic profile filter set classifier element, use the following command from the Global configuration mode: `qos traffic-profile classifier name <name>`

--End--

Variable definitions

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

Variable	Value
name <name>	Specifies the classifier name.
addr-type <addrtype>	Specifies the type of IP address used by this classifier entry. The type is limited to IPv4 and IPv6 addresses.
block <block-name>	Specifies the label to identify access list elements that are of the same block.

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-action <drop | pass>	Specifies whether or not to drop nonconforming traffic.
drop-out-action	Specifies whether to drop (enable) or pass (disable) out of profile packets.
dst-field <dscp>	Specifies the value for the DiffServ Codepoint (DSCP) in a packet.
dst-ip <dst-ip-info>	Specifies the IP address to match against the destination IP address of a packet.
dst-mac <dst-mac-info>	Specifies the MAC address against which the MAC destination address of incoming packets is compared.
dst-port-min <0-65535>	Specifies the minimum value for the Layer 4 destination port classifier.
dst-port-max <0-65535>	Specifies the maximum value for the Layer 4 destination port classifier.
ethertype <etype>	Specifies a value indicating the version of Ethernet protocol being used.
eval-order <0-65535>	Specifies the evaluation order for all elements with the same name.
flow-id <flowid>	Specifies the flow identifier for IPv6 packets.
ip-flags <ip-flags>	Specifies the IP fragment flag criteria.
ipv4-options <no-opt | with-opt>	Specifies the IPv4 option criteria.
master	Designates the classifier as the master block member.
max-burst-rate <64-429496729>	Specifies the maximum burst rate. Values range from 64 to 4294967295 Kbps. You configure this parameter when a committed metering rate is specified.

Variable	Value
max-burst-duration <1-4294967295>	Specifies the maximum burst duration in milliseconds (ms). Values range from 1 to 4294967295 ms. You configure this parameter when a committed metering rate is specified.
vlan-min <1-4094>	Specifies the minimum VLAN ID value for the classifier.
vlan-max <1-4094>	Specifies the maximum VLAN ID value for the classifier.
next-header <header>	Specifies the IPv6 next-header value. Values are in the range 0–255.
pkt-type <etherll | llc | snap>	Specifies the filter packet format ethertype encoding criteria.
priority <ieee1p-seq>	Specifies a value for the 802.1p user priority.
protocol <protocoltype>	Specifies the IPv4 protocol value.
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
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.

Variable	Value
src-port-min <0-65535>	Specifies the minimum value for the Layer 4 source port number in a packet.
src-port-max <0-65535>	Specifies the maximum value for the Layer 4 source port number in a packet.
src-mac <src-mac>	Specifies the MAC source address of incoming packets.
src-ip <src-ip-info>	Specifies the IP address to match against the source IP address of a packet.

Configuring a traffic profile set

Use the following procedure to configure a traffic profile set.

Procedure steps

Step	Action
1	To configure a QoS traffic profile filter set entry, use the following command from the Global configuration mode: `qos traffic-profile set port <port>`

--End--

Variable definitions

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

Variable	Value
commited-rate <64-10230000>	Specifies the committed rate in Kilobits per second.
committed-burst-size <burst-size-options>	Specifies the committed burst size in KiloBytes.
drop-out-action <enable | disable>	Specifies whether to drop (enable) or pass (disable) out-of-profile packets. You configure this parameter when a metering type is selected and a committed metering rate is specified.
enable	Enables the traffic profile.

Variable	Value
max-burst-rate <64-429496729 5>	Specifies the maximum burst rate. Values range from 64 to 4294967295 Kbps. You configure this parameter when a committed metering rate is specified.
max-burst-duration <1-4294967295>	Specifies the maximum burst duration in milliseconds (ms). Values range from 1 to 4294967295 ms. You configure this parameter when a committed metering rate is specified.
meter-mode <uniform-per-policy | individual-per-policy | classifier>	Specifies the metering type. • uniform-per-policy—a unique meter is applied to each policy that comprises the filter set with uniform rate and burst data derived from the filter set specification used for each meter • individual-per-policy—a unique meter is applied to each policy that comprises the filter set with rate and burst data derived from the classifier data or the filter set specification • classifier—a meter is defined for each individual filter set classifier using rate and burst data associated with the classifier. If this data is not present a meter is not allocated for the classifier
name <name>	Specifies the name of the traffic profile.
port <port>	Specifies the ports to apply the traffic profile to.
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.

Variable	Value
	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.

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

Use the following procedure to delete a filter classifier or set.

Procedure steps

Step	Action
1	Delete a Traffic Profile classifier by using the following command from the Global Configuration mode. `no qos traffic-profile classifier name <classifier-na me>`
2	Delete a Traffic Profile set by using the following command from the Global Configuration mode. `no qos traffic-profile set {name <name>	port <port>}`

--End--

Viewing filter descriptions

Use the following procedure to view filter descriptions .

Procedure steps

Step	Action

1	View classifier entries by using the following commands from the Privileged EXEC Configuration mode.
	
	`show qos traffic-profile classifier`
	
	OR
	
	`show qos traffic-profile classifier name <classifier name>`

2	View the parameters for a specific set by using the following command from the Privileged EXEC Configuration mode. `show qos traffic-profile set <set name> port <port>`
3	View ports and the filter sets assigned to those ports by using the following command from the Privileged EXEC Configuration mode. `show qos traffic-profile interface`

--End--

QoS Filter Limiting configuration using NNCLI

You can use the procedures in this section to disable, re-enable, and display information about QoS Filter Limiting, a feature that controls the maximum number of user-defined protocol VLANs

Displaying QoS Filter Limiting using NNCLI

Use this procedure to display the Filter Limiting status.

Step	Action
1	From the Global Configuration mode prompt, enter the following NNCLI command. `show qos filter-limiting`

--End--

Disabling QoS Filter Limiting

Use this procedure to disable Filter Limiting. Filter Limiting is enabled by default.

Step	Action
1	From the Global Configuration mode prompt, enter the following NNCLI command:
	`no qos filter-limiting enable`
2	Reset the switch to apply the change.

--End--

Enabling QoS Filter Limiting

If you have disabled Filter Limiting, use this procedure to enable Filter Limiting.

Step	Action
1	From the Global Configuration mode prompt, enter the following NNCLI command:
	`qos filter-limiting enable`
2	Reset the switch to apply the change.

--End--

Restoring QoS Filter Limiting to default

Use the following procedure to restore Filter Limiting to the default value, enabled.

Step	Action
1	From the Global Configuration mode prompt, enter the following NNCLI command:
	`qos default filter-limiting`
2	Reset the switch to apply the change.

--End--

Configuring QoS for the Nortel SNA solution

When you assign a filter set name using the `nsna vlan <vid> color <red|yellow|green> filter <name>` command (for example, `nsna vlan 110 color red filter redFilter`), the switch automatically creates all the necessary (default) QoS classifiers for the specified color

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

> *Note:* When the Nortel SNA filters are applied to a port, any existing QoS filters on that port are disabled, and the Nortel SNA filters are applied. Pre-existing policies are re-enabled when Nortel SNA is disabled.

Configuring QoS for SNA filters

Use the following procedure to configure QoS for SNA filters.

Procedure steps

Step	Action
1	Configure QoS for Nortel SNA filters by using the following command from the Global configuration mode. `qos nsna` > *Note:* To modify an entry in a filter set, you must delete the entry and add a new entry with the desired modifications.

<div align="center">

--End--

</div>

Variable definitions

Variable	Value
classifier name [addr-type {ipv4|ipv6}] [block] [drop-action] [ds-field] [dst-ip] [dst-mac] [dst-port-min] [ethertype] [eval-order] [flow-id] [next-header] [priority] [protocol] [set-drop-prec] [src-ip] [src-mac] [src-port-min] [update-1p] [update-dscp] [vlan-min] [vlan-tag]	Creates the QoS Nortel SNA classifier entry. Optional parameters: • addr-type {ipv4|ipv6}—specifies the type of IP address used by this classifier entry. The type is limited to IPv4 and IPv6 addresses. • block—specifies the label to identify access list elements that are of the same block. • drop-action—specifies whether or not to drop non-conforming traffic.

Variable	Value
	• ds-field—specifies the value for the DiffServ Codepoint (DSCP) in a packet.
	• dst-ip—specifies the IP address to match against the destination IP address of a packet.
	• dst-mac—specifies the MAC address against which the MAC destination address of incoming packets is compared.
	• dst-port-min—specifies the minimum value for the layer 4 destination port number in a packet. **dst-port-max** must be terminated prior to configuring this parameter.
	• ethertype—specifies a value indicating the version of Ethernet protocol being used.
	• eval-order—specifies the evaluation order for all elements with the same name.
	• flow-id—specifies the flow identifier for IPv6 packets.
	• next-header—specifies the IPv6 next-header value. Values are in the range 0–255.
	• priority—specifies a value for the 802.1p user priority.
	• protocol—specifies the IPv4 protocol value.
	• set-drop-prec—specifies drop precedence
	• src-ip—specifies the IP address to match against the source IP address of a packet.
	• src-mac—specifies the MAC source address of incoming packets.
	• src-port-min—specifies the minimum value for the Layer 4 source port number in a packet. **src-port-max** must be terminated prior to configuring this parameter.
	• update-1p—specifies an 802.1p value used to update user priority.
	• update-dscp—specifies a value used to update the DSCP field in an IPv4 packet.
	• vlan-min— specifies the minimum value for the VLAN ID in a packet. **vlan-max** must be terminated prior to configuring this parameter.
	• vlan-tag—specifies the type of VLAN tagging in a packet.
set name [commited-rate] [[drop-out-action] [max-burst-rate]	Creates the QoS Nortel SNA set.

Variable	Value
[max-burst-duration] [update-dscp-out-action]	Optional parameters: • commited-rate—specifies the commited rate in Kbps. • drop-out-action—specifies the action to take when a packet is out-of-profile. This action is only applied if metering is being enforced, and if the traffic is deemed out of profile based on the level of traffic and the metering criteria. Options are **enable** (packet is dropped) and **disable** (packet is not dropped). • max-burst-rate—specifies the maximum number of bytes allowed in a single transmission burst. • max-burst-duration—specifies the maximum burst duration in milliseconds. • update-dscp-out-action—specifies an updated DSCP value for an IPv4 packet for out of profile traffic.

Job aid: Using qos nsna commands

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

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

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

> *Note:* To consume only one precedence level, group classifiers in a classifier block.

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

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

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

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

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

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

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

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

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

Procedure steps

Step	Action
1	Delete an entire filter set by using the following command from the Global configuration mode.
	`no qos nsna name <filter name>`
2	Delete a classifier by using the following command from the Global configuration mode.
	`no qos nsna name <filter name> eval-order <value>`

<div align="center">**--End--**</div>

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

Viewing filter descriptions

Use the following procedure to view filter descriptions.

Procedure steps

Step	Action
1	View Nortel SNA filter parameters by using the following command from the Privileged EXEC configuration mode.
	`show qos nsna`
2	View the parameters for a specific filter set by using , the following command from the Privileged EXEC configuration mode.
	`show qos nsna name <filter name>`

3   View ports and the filter sets assigned to those ports by using
the following command from the Privileged EXEC configuration
mode.

```
show qos nsna interface
```

4   View classifier entries by using the following command from the
Privileged EXEC configuration mode.

```
show qos nsna classifier
```

--End--

Configuring User Based Policies

Use the following procedure to configure User Based Policies.

Procedure steps

Step	Action
1	Configure User Based Policies by using the following command from the Global configuration mode. ```qos ubp``` *Note:* To modify an entry in a filter set, you must delete the entry and add a new entry with the desired modifications.

--End--

Variable definitions

Variable	Value
classifier name [addr-type {ipv4|ipv6}] [block] [drop-action] [ds-field] [dst-ip] [dst-mac] [dst-port-min] [ethertype] [eval-order] [flow-id] [next-header] [priority] [protocol] [set-drop-prec] [src-ip] [src-mac] [src-port-min] [update-1p] [update-dscp] [vlan-min] [vlan-tag]	Creates the User Based Policy classifier entry. Optional parameters: • addr-type {ipv4|ipv6} specifies the type of IP address used by this classifier entry. The type is limited to IPv4 and IPv6 addresses. • block specifies the label to identify access list elements that are of the same block. • drop-action specifies whether or not to drop non-conforming traffic. • ds-field specifies the value for the DiffServ Codepoint (DSCP) in a packet.

Variable	Value
	• dst-ip specifies the IP address to match against the destination IP address of a packet.
	• dst-mac specifies the MAC address against which the MAC destination address of incoming packets is compared.
	• dst-port-min specifies the minimum value for the layer 4 destination port number in a packet. `dst-port-max` must be terminated prior to configuring this parameter.
	• ethertype specifies a value indicating the version of Ethernet protocol being used.
	• eval-order specifies the evaluation order for all elements with the same name.
	• flow-id specifies the flow identifier for IPv6 packets.
	• next-header specifies the IPv6 next-header value. Values are in the range 0-255.
	• priority specifies a value for the 802.1p user priority.
	• protocol specifies the IPv4 protocol value.
	• set-drop-prec specifies drop precendence
	• src-ip specifies the IP address to match against the source IP address of a packet.
	• src-mac specifies the MAC source address of incoming packets.
	• src-port-min specifies the minimum value for the Layer 4 source port number in a packet. `src-port-max` must be terminated prior to configuring this parameter.
	• update-1p specifies an 802.1p value used to update user priority.
	• update-dscp specifies a value used to update the DSCP field in an IPv4 packet.
	• vlan-min specifies the minimum value for the VLAN ID in a packet. `vlan-max` must be terminated prior to configuring this parameter.
	• vlan-tag specifies the type of VLAN tagging in a packet.
set name [commited-rate] [drop-out-action] [max-burst-rate]	Creates the User Based Policy set.

Variable	Value
[max-burst-duration] [update-dscp-out -action] [set-priority]	Optional parameters: • commited-rate specifies the commited rate in Kbps. • drop-out-action specifies the action to take when a packet is out-of-profile. This action is only applied if metering is being enforced, and if the traffic is deemed out of profile based on the level of traffic and the metering criteria. Options are **enable** (packet is dropped) and **disable** (packet is not dropped). • max-burst-rate specifies the maximum number of bytes allowed in a single transmission burst. • max-burst-duration specifies the maximum burst duration in milliseconds. • update-dscp-out-action specifies an updated DSCP value for an IPv4 packet for out of profile traffic.. • set-priority specifies the priority level of this filter set.

Job aid: Using qos ubp commands

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

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

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

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

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

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

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

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

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

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

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

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

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

Procedure steps

Step	Action
1	Delete an entire filter set by using the following command from the Global configuration mode.

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

> *Note:* You cannot delete a filter set while it is in use.

Step	Action
2	Delete a classifier by using the following command from the Global configuration mode.

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

--End--

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

Viewing filter descriptions

Use the following procedure to view User-based Policy filter parameters, view parameters for a specific filter set, view ports and associated filter sets, and view classifier entries.

Procedure steps

Step	Action
1	View User Based Policy filter parameters by using the following command from the Privileged EXEC configuration mode.

```
show qos ubp
```

2   View the parameters for a specific filter set by using the following command from the Privileged EXEC configuration mode.

`show qos ubp name <filter name>`

3   View ports and the filter sets assigned to those ports by using the following command from the Privileged EXEC configuration mode.

`show qos ubp interface`

4   View classifier entries by using the following command from the Privileged EXEC configuration mode.

`show qos ubp classifier`

--End--

Maintaining the QoS Agent

Use the following NNCLI commands to maintain the QoS agent.

Removing all QoS configurations

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

`qos agent reset-partial-default`

Resetting QoS to factory default state

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

Procedure steps

Step	Action
1	Reset QoS to factory defaults by using the following command from Global Configuration mode. `qos agent reset-default`

--End--

Note 1: You cannot reset QoS defaults if the NSNA application references a QoS NSNA filter set.

Note 2: You cannot reset QoS defaults if the EAP/NEAP UBP support references a QoS UBP filter set.

Configuring QOS NT mode

Use the following procedure to configure the QoS Agent NT mode.

Procedure steps

Step	Action
1	Configure QoS NT mode by using the following command from Global Configuration mode. `qos agent nt-mode [pure|mixed|disabled]`
	--End--

Variable definitions

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

Configuring QoS UBP support

Use the following procedure to configure the UBP support level.

Procedure steps

Step	Action
1	Configure the UBP support level by using the following command from Global Configuration mode. `qos agent ubp [disable|epm|high-security-local|low-security-local]`
	--End--

Variable definitions

Variable	Value
disable	QoS agent rejects information forwarded by other applications.
epm	QoS Agent notifications generated for EPM based on user information forwarded by other applications.
high-security-local	User may be rejected if resources needed to install the UBP filter set are not available.
low-security-local	User may be accepted even if the UBP filter set could not be applied.

Configuring QoS statistics tracking type

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

Procedure steps

Step	Action
1	Configure the QoS statistics tracking type by using the following command from Global Configuration mode. `qos agent statistics-tracking [aggregate|disable|ind ividual]`
	--End--

Variable definitions

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

Configuring NVRAM delay

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

Procedure steps

Step	Action
1	Configure NVRAM delay by using the following command from Global Configuration mode. `qos agent nvram-delay <0-604800>` Default is 10 seconds.
	--End--

Resetting NVRAM delay to default

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

Procedure steps

Step	Action
1	Reset NVRAM delay to default by using the following command from Global Configuration mode. `default qos agent nvram-delay`

--End--

Resetting the QoS agent

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

Procedure steps

Step	Action
1	Reset the QoS agent by using the following command from Global Configuration mode. `default qos agent`

--End--

Configuring DoS Attack Prevention Package

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

Enabling DAPP

Use the following procedure to enable DAPP.

Procedure steps

Step	Action
1	Enable DAPP by using the following command from Global Configuration mode: `[no] qos agent dos-attack-prevention enable`

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

--End--

Configuring DAPP status tracking

Use the following procedure to configure DAPP status tracking.

Procedure steps

Step	Action
1	Enable DAPP status tracking by using the following command from Global Configuration mode:

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

--End--

Note: If adequate resources are not available to enable this feature the command will fail.

Configuring DAPP minimum TCP header size

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

Procedure steps

Step	Action
1	Set the minimum TCP header size by using the following command from Global Configuration mode:

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

--End--

Configuring DAPP maximum IPv4 ICMP length

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

Procedure steps

Step	Action
1	Set the maximum IPv4 ICMP length by using the following command from Global Configuration mode: `qos agent dos-attack-prevention max-ipv4-icmp <0-1023>`

<div align="center">**--End--**</div>

Configuring DAPP maximum IPv6 ICMP length

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

Procedure steps

Step	Action
1	Set the maximum IPv6 ICMP length by using the following command from Global Configuration mode: `qos agent dos-attack-prevention max-ipv6-icmp <0-16383>`

<div align="center">**--End--**</div>

Configuring Automatic QoS

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

Enabling Automatic QoS

Use the following procedure to enable Automatic QoS support.

Procedure steps

Step	Action
1	Enable Automatic QoS support by using the following command from Privileged Executive mode. `qos agent nt-mode [mixed│pure]`

<div align="center">**--End--**</div>

Variable definitions

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

Disabling Automatic QoS

Use the following procedure to disable Automatic QoS support.

Procedure steps

Step	Action

1   Disable Automatic QoS support by using the following command from Privileged Executive mode.

```
qos agent nt-mode disable
```

--End--

Configuring Quality of Service (QoS) using Enterprise Device Manager

This chapter describes using the Enterprise Device Manager to manage Quality of Service (QoS) parameters on the Nortel Ethernet Routing Switch 5000 Series .

Note: 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.

This section contains information about the following topics:

QoS Devices dialog box
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

To open the QoS Devices dialog box:

Procedure steps

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

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

--End--

This section provides information about the following topics:

Viewing the Interface Queue
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

To display interface queues and groups:

Procedure steps

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

--End--

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

Table 7
Qos Devices Interface Queue tab parameters

Variable	Value
SetId	Displays an integer between 1 and 65 that identifies the specific queue set.

Table 7
Qos Devices Interface Queue tab parameters (cont'd.)

Variable	Value
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 a queue is serviced based on the defined discipline.
Size	Displays the size of the queue in bytes.

Viewing Interface Groups

Enterprise Device Manager lets you display the interface groups.

Prerequisites

• Open one of the supported Web browsers.

• Access the switch.

• Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to display interface groups.

Procedure steps

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

--End--

Variable definitions

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

Table 8
QoS Devices Interface Groups tab parameters

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

This section contains information about the following topics:

Assigning ports to an interface group
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

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

Procedure steps

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

> *Note:* Adding or deleting a number of ports on a switch experiencing a heavy load can take a long time and can cause the Enterprise Device Manager to time out.

--End--

For more information, see Table 8 "QoS Devices Interface Groups tab parameters" (page 132).

Deleting ports from an interface group
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

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

Procedure steps

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

8   Click **OK**.

--End--

For more information, see Table 8 "QoS Devices Interface Groups tab parameters" (page 132).

Adding interface groups
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to add an interface group.

Procedure steps

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

--End--

For more information, see Table 8 "QoS Devices Interface Groups tab parameters" (page 132).

Deleting interface groups
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to delete an interface group.

Procedure steps

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

> *Note:* 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.

--End--

For more information, see .

Viewing Interface ID Assignments
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Interface ID Assignments tab.

Procedure steps

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

--End--

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

Table 9
QoS Devices Interface ID Assignments tab parameters

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

Viewing Priority Q Assign
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Priority Q Assign tab.

Procedure steps

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

<div align="center">**--End--**</div>

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

Table 10
QoS Devices Priority Q Assign tab parameters

Variable	Value
Qset	Represents the queue set number. Supports the assignment of 802.1p user priority values to a queue for each specific queue set. There are 56 instances for queue set number, each instance is a multiple of one basic queue-set from 1 to 8.
802.1pPriority	A 802.1 user priority value.
Queue	A queue in a specified queue set that is assigned a priority value. To change a Queue assignment, click in the cell and type a new value.

Filtering priority queue assignments

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

Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to filter the priority queue assignments table.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS Devices**.
3	Select the **Priority Q Assign** tab.
4	Click **Filter**.
	The **Insert Filter** dialog opens.
5	Set the conditions to be used to filter the display of the **Priority Q Assign** table:
	a Select **AND** to include all entries in the table that include *all* specified parameters, or select **OR** to include *any* of the specified parameters.
	b Select **Ignore Case** to include all entries with the parameters being set, whether in lowercase or uppercase.
	c Select any of the criteria from **Column** to include entries matching the criteria. **Contains** if the table is to show all entries that contain the parameters set or **Equal To** to show only those entries that are equal to the parameters being set.
	d Select **All records** to display all the entries in the table.
	e To display the entries in the table by queue set, select **QSet** and enter the **QSet** values to display.
6	Click **Filter**.

--End--

For more information , see Table 10 "QoS Devices Priority Q Assign tab parameters" (page 136).

Viewing Priority Mapping
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Priority Mapping tab.

Procedure steps

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

--End--

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

Table 11
QoS Devices Priority Mapping tab parameters

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

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

DSCP mapping tab navigation

-
-

Viewing egress mapping using EDM

Use the following procedure to view egress mapping using EDM.

Procedure steps

Step	Action
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.

--End--

Variable definitions

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

Table 12
DSCP Mapping tab parameters

Variable	Value
Dscp	Indicates the DSCP value. This is a read-only cell.
802.1pPriority	Specifies the user priority value associated with the DSCP. 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 16 characters.

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.

Prerequisites

- Open one of the supported browsers.

- Enter the IP address of the switch to open an EDM session.

Procedure steps

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

--End--

Variable definitions

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

Table 13
DSCP Mapping tab parameters

Variable	Value
Dscp	Indicates the DSCP value. This is a read-only cell.

Table 13
DSCP Mapping tab parameters (cont'd.)

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 16 characters.

Viewing Meter Capability
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Meter Capability tab.

Procedure steps

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

--End--

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

Table 14
QoS Devices Meter Capability tab parameters

Variable	Value
Port	Specifies the port to which the meter is applied.
MeterSupport	Specifies the supported Token Bucket metering algorithm.
Meter Rate (Kbps)/Bucket (KBytes)/Granularity (Kbps)	Displays maximum supported Meter Rate, Meter Bucket size and Meter Granularity.

Meter Capability filtering
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to configure Meter Capability filtering.

Procedure steps

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

--End--

For more information, see Table 14 "QoS Devices Meter Capability tab parameters" (page 142).

Viewing Shaper Capability
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Shaper Capability tab.

Procedure steps

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

--End--

Table 15
Shaper Capability tab parameters

Variable	Value
Port	Displays the port number.
ShaperSupport	Displays the shaper support as: • Interface • Cos (Class of Service)
Shaper Rate(Kbps)/Bucket(Kbytes)/Granularity(Kbps)	Displays the • Shaper rate in Kilobytes per second • Bucket size in Kilobytes • Granularity in Kilobytes per second

Shaper Capability filtering
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to configure Shaper Capability filtering.

Procedure steps

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

--End--

QoS Rules dialog box

Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the QoS Rules dialog box.

Procedure steps

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

--End--

This section contains information about the following topics:

- "Viewing the IP Classifier Element tab" (page 145)
- "Viewing the L2 Classifier Element" (page 147)
- "Viewing System Clfr Elements " (page 150)
- "Viewing Classifiers " (page 155)
- "Viewing the Classifier Block " (page 160)

Viewing the IP Classifier Element tab

Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the IP Classifier Element tab.

Procedure steps

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

--End--

Variable definitions

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

Table 16
QoS Rules IP Classifier Element tab parameters

Variable	Value
Id	Specifies the number of the IP classifier element.
Name	Specifies the IP classifier element name.
AddressType	Specifies the type of IP address used by this classifier entry. The type is limited to IPv4 and IPv6 addresses.
DstAddr	Specifies the IP address to match against the destination IP address of packet.
DstMaskLength	Specifies the length of the destination address mask.
SrcAddr	Specifies the IP address to match against the source IP address of packet.
SrcMasklength	Specifies the length of the source address mask.
Dscp	Specifies the value for the DSCP in a packet.
Protocol/NextHeader	Specifies the IP protocol value.
DstL4Port	Specifies the value for the Layer 4 destination port number in a packet.

Table 16
QoS Rules IP Classifier Element tab parameters (cont'd.)

Variable	Value
SrcL4Port	Specifies the value for the Layer 4 source port number in a packet.
IPv6FlowId	Specifies the flow identifier for IPv6 packets.
IpFlags	Specifies the value of flags present in an IPv4 header.
TcpCtrlFlags	Specifies the control flags present in an TCP header.
Ipv4Options	Specifies whether the Option field is present in the packet header. Valid values are • 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.
SessionId	Specifies the session identification number.
Storage	Specifies the type of storage: • volatile • nonVolatile (default) • readOnly

This section contains information about the following topics:

- "Adding IP classifier elements" (page 146)
- "Deleting IP classifier elements" (page 147)

Adding IP classifier elements
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to add an IP classifier element.

Procedure steps

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

3   Select the **IP Classifier Element** tab.

4   Click **Insert**.

The **Insert IP Classifier Element** screen opens.

5   Enter the information you want to use for this IP classifier element.

6   Click **Insert**.

--End--

Deleting IP classifier elements
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to delete an IP classifier element.

Procedure steps

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

Note: An IP classifier element cannot be deleted 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**.

--End--

Viewing the L2 Classifier Element
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the L2 Classifier Element tab.

Procedure steps

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

--End--

Variable definitions

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

Table 17
QoS Rules L2 Classifier Element tab parameters

Variable	Value
Id	Specifies the index that enumerates the classifier entries.
Name	Specifies the Layer 2 Classifier Element name.
DstMacAddr	Specifies the MAC address against which the MAC destination address of incoming packets are compared.
DstMacAddrMask	Specifies a mask identifying the destination MAC address.
SrcMacAddr	Specifies the MAC source address of incoming packets.
SrcMacAddrMask	Specifies a mask identifying the source MAC address.
VlanId	Specifies the value for the VLAN ID in a packet.
VlanTag	Specifies the type of VLAN tagging in a packet: • untagged • tagged • ignore
EtherType	Specifies a value for the Ethertype.
802.1pPriority	Specifies a value for the 802.1p user priority.

Table 17
QoS Rules L2 Classifier Element tab parameters (cont'd.)

Variable	Value
PktType	Specifies the packet frame format. - etherII—indicates that only Ethernet II format frames match this classifier component. - snap—indicates that only EEE 802 SNAP format frames match this classifier component. - llc—indicates that only IEEE 802 LLC format frames match this classifier component.
Version	Specifies the version.
SessionId	Specifies the session identification number.
Storage	Specifies the type of storage.

This section contains information about the following topics:

Adding L2 classifier elements
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to add L2 classifier elements.

Procedure steps

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

--End--

For more information, see Table 17 "QoS Rules L2 Classifier Element tab parameters" (page 148).

Deleting L2 classifier elements
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to delete L2 classifier elements.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS Rules**.
3	Select the **L2 Classifier Element** tab.
4	Highlight any table cell of the L2 classifier element to delete.
5	Click **Delete**.

Device Manager deletes the entire L2 classifier element.

> *Note:* 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**.

<div align="center">

--End--

</div>

For more information, see Table 17 "QoS Rules L2 Classifier Element tab parameters" (page 148).

Viewing System Clfr Elements
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the System Clfr Element tab.

Procedure steps

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

--End--

Variable definitions

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

Table 18
QoS Rules System Clfr Element tab parameters

Variable	Value
Id	Specifies the index that enumerates the system classifier entries.
Name	Specifies the System Classifier Element name.
UnknownUcastFrames	Identifies frames with an unknown unicast destination address. • true—indicates frames containing an unknown unicast destination address match this classification entry. • false—indicates that no classification is requested based on this address type.
UnknownMcastFrames	Identifies frames with an unknown multicast destination address. • true—indicates frames containing an unknown multicast destination address match this classification entry. • false—indicates that no classification is requested based on this address type.
KnownMcastFrames	Identifies frames with a known multicast destination address. • true—indicates frames containing a known multicast destination address match this classification entry. • false—indicates that no classification is requested based on this address type.

Table 18
QoS Rules System Clfr Element tab parameters (cont'd.)

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	Supports targeting non-IP traffic. • true—indicates that non IP packets match this classification entry. • false—indicates that no classification is requested based on this packet type.

Table 18
QoS Rules System Clfr Element tab parameters (cont'd.)

Variable	Value
PatternFormat	Indicates that 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. Default value is tagged.
PatternIPVersion	Specifies the pattern IP version.
PatternL2Format	Specifies the Layer 2 pattern format (ethernet 2, llc, or snap).
Version	Specifies the version.
SessionId	Specifies the number assigned to the session displays in this column.
Storage	Specifies the storage type for this conceptual row. Conceptual rows that have the value permanent need not allow write-access to any columnar objects in the row. This object may not be modified if the associated status object is equal to active.

This section contains information about the following topics:

Viewing the System Classifier Pattern
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to view the System Classifier pattern.

Procedure steps

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

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

3   Select the **System Clfr Element** tab.

4   Highlight an entry in the **System Clfr Element** table.

5   Click **Pattern**.

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

--End--

Adding System Classifier Elements
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to add System Classifier Elements.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS Rules**.
3	Select the **System Clfr Element** tab.
4	Click **Insert**. The **Insert System Clfr Element** dialog opens.
5	Select the **DestAddressType**.
6	Type the**PatternData** or **PatternPosition** information manually. Alternatively, click on the ellipses to view the **Pattern** screen.
7	The **Pattern** screen configures the data and position of the pattern to be used by this system classifier.
8	The **System Classifier Element Pattern (Data/Position)** screen opens.
9	Select **IPv4, IPv6,** or **non-IP**.
10	Select **tagged** or **untagged**.
11	Select the version, 1 or 2. *Note:* This setting is available to create system classifiers that can be used only on 5500 Series switches (version 1) or only on 5600 Series switches (version 2).

12	Select the required fields to set up a template guide so that it will be easier to configure the data and position of the pattern.
13	Type the desired **Data** and **Position** in two-digit hex number format.
14	Click **Ok**.
15	Click **Insert**.

--End--

Deleting System Classifier Elements
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to delete System Classifier Elements.

Procedure steps

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

--End--

Viewing Classifiers
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Classifier tab.

Procedure steps

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

--End--

Variable definitions

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

Table 19
QoS Rules Classifier tab parameters

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

This section contains information about the following topics:

- "Adding classifiers" (page 157)
- "Deleting classifiers" (page 158)
- "Filtering Classifiers" (page 159)

Adding classifiers
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to add classifiers.

Procedure steps

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

7 Click **Insert**.

> *Note:* A classifier can be created by using the following combination:
>
> - *one system classifier element*
> - *one L2 classifier element*
> - *one IP classifier element*
> - *one IP classifier, one system classifier*
> - *one L2 classifier, one system classifier*
> - *one L2 classifier, one IP classifier*
> - *one IP, one L2, plus one system classifier*
>
> Entries with the same **SetId** belong to the same classifier. Click on the **SetId** column header to sort the table by **SetId** value; this makes it very easy to see which entries have the same **SetId** value.Limitations on classifier creation are:
> - when creating a classifer with L2 and IP elements the L2 element should contain ethertype 0x800.
> - when creating a classifer with a system element and IP element, the pattern data on the system element must contain the ethertype value.

--End--

Deleting classifiers
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to delete classifiers.:

Procedure steps

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

5 Click **Delete**.

> *Note:* 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**.

--End--

Filtering Classifiers

Use the following procedure to filter the display of classifiers.

Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to filter the display of classifiers.

Procedure steps

Step	Action

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

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

3 Select the **Classifier** tab.

4 Click **Filter**.

The **Insert Filter** screen opens.

5 Set the conditions to filter the display of the **Classifiers** table:

a Select **AND** to include all entries in the table that include *all* specified parameters, or select **OR** to include any of the specified parameters.

b Select **Ignore Case** to include all entries with the parameters being set, whether in lowercase or uppercase.

c Select **contains** to include in the table all entries that contain the parameters set, **does not contain** to exclude a parameter from the table, **does not equal to** to include entries that are not equal to a set parameter, or **equals to** to show only those entries that are equal to the parameters being set.

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

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

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

6 Click **Filter**.

--End--

Viewing the Classifier Block
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Classifier Block tab.

Procedure steps

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

--End--

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

Table 20
QoS Rules Classifier Block tab parameters

Variable	Value
BlockNum	Entries with the same BlockNum belong to the same classifier block. *Note:* 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).

Table 20
QoS Rules Classifier Block tab parameters (cont'd.)

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

This section contains information about the following topics:

- "Appending Classifier Blocks" (page 161)

- "Adding Classifier Blocks" (page 162)

- "Deleting Classifier Blocks" (page 163)

- "Filtering Classifier Blocks" (page 163)

Appending Classifier Blocks
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to append a classifier block.

Procedure steps

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

5   Select the Classifier to append to the Classifier Block.

6   Click **Insert**.

--End--

Adding Classifier Blocks
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to add classifier blocks.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS Rules**.
3	Select the **Classifier Block** tab.
4	Click **Insert**.
	The **Insert Classifier Block** screen opens.
5	Enter the name of the classifier block.
6	Select the **Classifier, Meter**, and **Action**.
7	Click **Insert.**

> *Note:* If one of the classifiers in a classifier block has associated actions or meters, then all classifier elements of that classifier block must also have associated actions or meters (not identical values for the actions or meters, but also associated actions or meters).Entries with the same **BlockNum** belong to the same classifier block. Click on the **BlockNum** column header to sort the table by **Block Number** value.

--End--

Deleting Classifier Blocks
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to delete classifier blocks.

Procedure steps

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

> *Note:* 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**.

<div align="center">

--End--

</div>

Filtering Classifier Blocks
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to filter a classifier block.

Procedure steps

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

The **QOSRules Classifier Block - Filter** dialog opens .

5 Select the filtering condition, case, and column criteria.

6 Enter the **BlockNum** and **Name**.

7 Click **Filter**.

--End--

QoS dialog box

Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the QoS dialog box.

Procedure steps

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

--End--

This section has information about the following topics:

Viewing Actions

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

Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the action tab.

Procedure steps

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

--End--

Variable definitions

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

Table 21
QoS Action tab parameters

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

This section contains information about the following topics:

Adding QoS actions
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to add a QoS action.

Procedure steps

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

<div align="center">

--End--

</div>

Deleting QoS actions
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to delete a QoS action.

Procedure steps

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

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

3   Select the **Action** tab.

4   Highlight the QoS action to delete.

5   Click **Delete**.

> *Note:* 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**.

--End--

Viewing Interface Action Ext
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Interface Action Ext tab.

Procedure steps

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

--End--

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

Table 22
QoS Interface Action Ext tab parameters

Variable	Value
Id	Specifies the number of the interface action extension.
Name	Specifies a label for the interface action extension.

Table 22
QoS Interface Action Ext tab parameters (cont'd.)

Variable	Value
SetEgressUnicastPort	Specifies redirection of normally-switched unicast packets to a specified interface.
SetEgressNonUnicastPort	Specifies redirection of normally-switched non-unicast packets (broadcast and multicast traffic) to a specified interface.
SessionId	Specifies the numerical identification for the current session.
Storage	Specifies the type of storage, either volatile or nonvolatile.

This section contains information about the following topics:

Adding Interface action extensions
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

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

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS**.
3	Select the **Interface Action Ext** tab.
4	Click **Insert**. The **Insert Interface Action Ext** screen opens.
5	Enter the information and make the selections to use for this Interface action extension.
6	Click **Insert**.

--End--

Deleting Interface action extensions
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

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

Procedure steps

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

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

--End--

Viewing the Meters
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Meter tab.

Procedure steps

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

--End--

Variable definitions

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

Table 23
QoS Meter tab parameters

Variable	Value
Id	Specifies the unique identifier for this entry.
Name	Specifies a name for this entry.
CommittedRate	Specifies the committed rate (in Kbps).
BurstSize	Specifies the committed burst (in bytes).
InProfileAction	Specifies in profile action.
OutOfProfileAction	Specifies out of profile action.
SessionId	Specifies the numerical identification of the current session.
Storage	Specifies the type of storage.
Version	Specifies the version.

This section contains information about the following topics:

Adding QoS meters
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to add a QoS meter.

Procedure steps

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

6   Click **Insert**.

--End--

Deleting QoS meters
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to delete QoS meters.

Procedure steps

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

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

--End--

Viewing Policies
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

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

Use the following procedure to open the Policy tab.

Procedure steps

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

--End--

Variable definitions

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

Table 24
QoS Policy tab parameters

Variable	Value
Id	Specifies the number of the QoS policy.
Status	Allows you to enable or disable the policy.
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. *Note:* You must configure the role combinations prior to associating it with a policy.
InterfaceIndex	Specifies the interface to which the policy is to be applied. A policy is associated with an interface explicitly using this attribute or implicitly using a role combination through the ntnQosPolicyInterfaceRole attribute. An interface must be identified by one and only one of these attributes. This attribute can identify an interface that does not currently exist in the system, as long as the specified interface index represents a potentially valid system interface.

Table 24
QoS Policy tab parameters (cont'd.)

Variable	Value
	Note: The InterfaceRoles and InterfaceIndex fields are mutually exclusive. When the InterfaceIndex field is not zero, the InterfaceRoles must be empty (select none when insert the policy). When the InterfaceRoles specifies a valid role combination, the InterfaceIndex field must be 0.
Precedence	Specifies the order in which multiple policies are associated with the same interface. Policies with greater precedence have higher numbers. ***Note:*** 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. ***Note:*** 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. ***Note:*** You must configure actions before associating them with a policy.
NonMatchAction	Identifies action taken for flows that do not match policy criteria.
StatsType	Specifies statistics tracking: • none—no statistics tracked for this policy • individual—separate counters allocated, space permitting, for each classifier referenced by the policy • aggregate—a single counter accumulates all the statistics for all the classifiers referenced by the policy
SessionId	Specifies the numerical identification for the current session.

Table 24
QoS Policy tab parameters (cont'd.)

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

This section contains information about the following topics:

- "Adding QoS policies" (page 174)

- "Deleting QoS policies" (page 175)

- "Viewing QoS Policy Stats" (page 175)

Adding QoS policies
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

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

Use the following procedure to add QoS policies.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS**.
3	Select the **Policy** tab.
4	Click **Insert**. The **Insert QoS Policy** screen opens.
5	Enter the information to use for this QoS policy.

6   Click **Insert**.

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

--End--

For more information, see Table 24 "QoS Policy tab parameters" (page
172).

Deleting QoS policies
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to delete QoS policies.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS**.
3	Select the **Policy** tab.
4	Highlight the QoS policy to delete.
5	Click **Delete**.

--End--

For more information, see Table 24 "QoS Policy tab parameters" (page
172).

Viewing QoS Policy Stats
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

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

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS**.
3	Select the **Policy** tab.
4	Select a policy from the list.
5	Click **Graph**. The **Policy Aggregate Stats** window opens.

> *Note:* When StatsType is aggregate, the aggregate stats are available.
> When StatsType is individual, the individual stats are available.

--End--

For more information, see Table 24 "QoS Policy tab parameters" (page 172).

Viewing the Interface Shaper
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Interface Shaper tab.

Procedure steps

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

--End--

Variable definitions
The following table outlines the parameters of the **Interface Shaper** tab.

Table 25
QoS Interface Shaper tab parameters

Variable	Value
Port	Specifies the port associated with interface shaping.
Name	Specifies the name applied to the interface shaping data.
ShapingRate	Specifies the token-bucket rate, in kilobits per second (kbps).
BurstSize	Specifies the maximum number of bytes in a single transmission burst.

This section contains information about the following topics:

-

-

Adding an Interface Shaper
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to add QoS Interface Shapers.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS**.
3	Select the **Interface Shaper** tab.
4	Click **Insert**.
	The **Insert Interface Shaper** screen opens.
5	Click the ellipses to select the ports for the interface shaper.
	The **ntnQoSIfShapingPorts** screen opens.
6	Select the required ports.
7	Click **Ok**.
8	Type the **Label**, **Shapingrate**, and **MaximumBurstRate**.
9	Select the **Duration** in milliseconds.

10   Click **Insert**.

--End--

Deleting an Interface Shaper
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to delete an Interface Shaper.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS**.
3	Select the **Interface Shaper** tab.
4	Highlight the Interface Shaper that to delete.
5	Click **Delete**.

--End--

Interface queue shaper configuration
The following sections describe the Interface queue shaper.

Interface queue shaper navigation

Viewing QoS interface queue shaper information using EDM
Use the following procedure to view QoS interface queue shaper information.

Procedure steps

Step	Action
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.

--End--

Variable definitions

Use the data in the following table to help you understand QoS interface queue shaper information.

Table 26
Interface Queue Shaper parameters

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

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

--End--

Variable Definitions

Use the data in the following table to help you create a new QoS interface queue shaper.

Table 27
Interface Queue Shaper parameters

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

Table 27
Interface Queue Shaper parameters (cont'd.)

Variable	Value
ShapingRate	Specifies the QoS interface queue shaping rate, in kilobits per second (Kbps). Values range from 64 to 10230000 Kbps. The value must be a multiple of 64 or 1000 Kbps.
ShapingMinRate	Specifies the minimum QoS interface queue shaping rate, in kilobits per second (Kbps). Values range from 0 to 10230000 Kbps. The value must be a multiple of 64 or 1000 Kbps.

Deleting a QoS interface queue shaper using EDM
Use the following procedure to delete a QoS interface shaper.

Procedure steps

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

--End--

Interface Apps configuration

> *Note:* Due to hardware limitations, the Ethernet Routing Switch 5500 Series switch supports only 11 interface applications per port.

ATTENTION
This tab is only available when there exists ERS5500 unit, and it only allowed for ERS5500 ports.

Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Interface Apps tab.

Procedure steps

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

--End--

Variable definitions

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

Table 28
QoS Interface Apps tab parameters

Variable	Value
IfIndex	Specifies the ports that this QoS application applies to.
AppEnable	Specifies the applications enabled for the interface (port) specified in IfIndex field.
DefaultGateway	Specifies the default gateway configured for the **arpSpoofing** application. The default gateway cannot be directly modified. To modify the default gateway for the **arpSpoofing** application, do the following: 1. Double-click the **AppEnable** field and de-select **arpSpoofing**. 2. Click **Apply**. 3. Double-click the **AppEnable** field, select **arpSpoofing**, and edit the **DefaultGateway** field. 4. Click **Apply**.
IfType	Specifies the interface type configured for the **dhcpSnooping** application.
DHCPServer	Specifies the DHCP server configured for the **dhcpSpoofing** application. The DHCP server cannot be directly modified. To modify the DHCP server for the **dhcpSpoofing** application, do the following:

Table 28
QoS Interface Apps tab parameters (cont'd.)

Variable	Value
	1. Double-click the **AppEnable** field and de-select **dhcpSpoofing**. 2. Click **Apply**. 3. Double-click the **AppEnable** field, select **dhcpSpoofing**, and edit the **DHCPServer** field. 4. Click **Apply**.

This section contains information about the following topics:

* "Adding an Interface Application" (page 183)
* "Deleting an Interface Application" (page 184)

Adding an Interface Application
Prerequisites

* Open one of the supported Web browsers.
* Access the switch.
* Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to add an Interface Application.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS**.
3	Select the **Interface Apps** tab.
4	Click **Insert**. The **Insert Interface Apps** screen opens.
5	In the fields provided, enter the information for the new entry.
6	Click **Insert**. The new Interface Application entry is displayed on the **Interface App** tab.

--End--

Variable definitions

The following table outlines the parameters of the **Insert Interface Apps** dialog box.

Table 29
QoS Insert Interface Apps dialog box parameters

Variable	Value
Ports	Click the ellipse button and select the ports to be configured for the QoS application.
AppEnable	Select the applications enabled for the ports selected in the **Ports** field.
DefaultGateway	Specifies the default gateway configured for the **arpSpoofing** application.
IfType	Specifies the interface type configured for the **dhcpSnooping** application.
DHCPServer	Specifies the DHCP server configured for the **dhcpSpoofing** application.

Deleting an Interface Application
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to delete an Interface Application.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS**.
3	Select the **Interface Apps** tab.
4	Select the Interface Application to delete.
5	Click **Delete**.

--End--

Viewing User Based Policies
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the User Based Policy tab.

Procedure steps

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

--End--

Variable definitions
The following table outlines the parameters of the **User Based Policy** tab.

Table 30
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.
SessionId	Displays the system-assigned session identifier used to track instances of this user policy entry.
SessionStart	Displays the system-assigned session start timestamp. The value in this field corresponds to the value of the **sysUpTime**, converted to seconds, at the instand this user policy entry is created or updated.

Table 30
QoS User Based Pollicy tab parameters (cont'd.)

Variable	Value
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 Agent dialog box

This section contains information on working with QoS agents.

Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the QoS Agent dialog box.

Procedure steps

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

--End--

This section contains information about the following topics:

- "Viewing the QoS Configuration" (page 187)

- "Viewing Policy Class Support " (page 193)

- "Viewing Policy Device Identifications " (page 194)

- "Resource Allocation (ERS5XXX) Configuration" (page 195)

Viewing the QoS Configuration
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Configuration tab.

Procedure steps

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

--End--

Variable definitions
The following table outlines the parameters of the **Configuration** tab.

Table 31
QoS Agent Configuration tab parameters

Variable	Value
QosOperMode	Specifies whether the QoS Agent support is enabled or disabled.
NVRamCommitDelay	Specifies the maximum time before nonvolatile QoS data is written to NVRAM.
ResetToPartialDefaults	Resets QoS condigurations to deafult ecept for quque-set and buffering type.
ResetToDefaults	Resets all policy information to factory default values.
QueueCfg	Determines the queue set that is associated with all egress interfaces by default.
BufferingCaps	Determines the method through which buffering resources are allocated to ports sharing a pool of buffers. The value of this attribute determines the level of buffer sharing or over-allocation that can take place among ports sharing a buffer pool. Higher levels of over-allocation increase the likelihood (under heavy load) of a relatively few number of ports consuming all the buffers in a pool, causing packets to be dropped on other ports due to buffer starvation.

Table 31
QoS Agent Configuration tab parameters (cont'd.)

Variable	Value
UBPSupportLevel	Sets the level of User Based Policy support.
TrackStatistics	Specifies the type of statistics tracking.
AQApplicationMode	Specifies the behavior of Auto Qos application mode.
TrustedProcessingMode	Indicates the QoS trusted processing mode status. The trusted processing mode parameter is available only for a mixed stack of ERS 5500 series switches.
TrustedProcessingMode	Trusted processing mode: partialDscpMapping (less QoS filters used) or fullDscpMapping (64 QoS filters used)
DappEnable	DoS Attack Prevention Package for ERS 5600 switches only: disable (default), enableWithoutStatusTracking (enabled without logging messages), enableWithStatusTracking (enabled with logging messages).
DappMinTcpHdrSize	Dapp minimum TCP header size
DappIpv4IcmpMaxLength	Dapp maximum length for IPv4 ICMP packets
DappIpv6IcmpMaxLength	Dapp maximum length for IPv6 ICMP packets

This section contains information about the following topics:

- "Enabling and disabling QoS Agent support" (page 188)
- "Enabling Automatic QoS" (page 189)
- "Disabling Automatic QoS" (page 190)
- "Configuring the QoS trusted processing mode" (page 190)
- "Enabling DoS Attack Prevention Package (DAPP)" (page 191)
- "Configuring DAPP minimum TCP header size" (page 191)
- "Configuring DAPP maximum IPv4 ICMP length" (page 192)
- "Configuring DAPP maximum IPv6 ICMP length" (page 193)

Enabling and disabling QoS Agent support
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to enable and disable QoS Agent support.

Procedure steps

Step	Action
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.

--End--

Enabling Automatic QoS
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to enable Automatic QoS support.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS Agent**.
3	Select the **Configuration** tab.
4	Select the appropriate mode in the **AQApplicationMode** section from the following: • **enablePureMode** - Enables Automatic QoS functionality with DSCP remarking at egress disabled. • **enableMixedMode** - Enables Automatic QoS functionality with DSCP remarking at egress enabled.
5	Click **Apply**.

--End--

Disabling Automatic QoS
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to disable Automatic QoS support.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS Agent**.
3	Select the **Configuration** tab.
4	Select **Disable** in the **AQApplicationMode** section.
5	Click **Apply**.

--End--

Configuring the QoS trusted processing mode
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to configure the trusted processing mode.

Procedure steps

Step	Action
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**.

--End--

Enabling DoS Attack Prevention Package (DAPP)
Prerequisites

*   Open one of the supported Web browsers.

*   Access the switch.

*   Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to enable DAPP.

Procedure steps

Step	Action
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**.

--End--

Configuring DAPP minimum TCP header size
Prerequisites

*   Open one of the supported Web browsers.

*   Access the switch.

*   Click the Configuration arrowhead to open the navigation tree.

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

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS Agent**.
3	Select the **Configuration** tab.
4	Under the DoS Attack Prevention Package section, enter a value in the range 0 to 255 in the **DappMinTcpHdrSize** text box.
5	Click **Apply**.

--End--

Configuring DAPP maximum IPv4 ICMP length
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

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

Procedure steps

Step	Action
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**.

--End--

Configuring DAPP maximum IPv6 ICMP length
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

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

Procedure steps

Step	Action
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**.

--End--

Viewing Policy Class Support
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Policy Class Support tab.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS Agent**.
3	Select the **Policy Class Support** tab.

--End--

Variable definitions

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

Table 32
QoS Agent Policy Class Support tab parameters

Variable	Value
PolicyClassName	Identifies the Policy Rule Classes (PRCs) 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	Specifies the current number of Policy Rules Instances (PRIs) that are installed for a specific PRC (equates to the current number of entries in a given MIB table).
MaximumInstalledInstances	Specifies the maximum number of PRIs that 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).

Viewing Policy Device Identifications

Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Policy Device Identification tab.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS Agent**.
3	Select the **Policy Device Identification** tab.

--End--

Variable definitions

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

Table 33
QoS Agent Policy Device Identification tab parameters

Variable	Value
Descr	A description of the policy agent. *Note:* The description must include the name and version identification of the policy agent hardware and software.
MaxMsg	Specifies the maximum message size in octets that the device can support.

Resource Allocation (ERS5XXX) Configuration
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Resource Allocation 5XXX tab.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS Agent**.
3	Select the **Resource Allocation (ERS5XXX)** tab.

--End--

Variable definitions
The following table outlines the parameters of the **Resource Allocation (ERS5XXX)** tab.

Table 34
QoS Agent Resource Allocation (ERS5XXX) tab parameters

Variable	Value
Precedence	Displays the applied precedence.
Port	Displays the Port number.
FiltersConsumed	Displays the number of rules (filters) in use by policy and filter data by that interface.
MetersConsumed	Displays the number of meters in use by policy data by that interface.

Table 34
QoS Agent Resource Allocation (ERS5XXX) tab parameters (cont'd.)

Variable	Value
CountersConsumed	Displays the number of counters in use by that interface.
NonQosFiltersConsumed	Tracks the current number of filters in use, not due to installed filter data, for a given precedence level and interface.
NonQosMetersConsumed	Tracks the current number of meters in use, not due to installed policy data, for a given precedence level and interface.
TotalFiltersAvail	Displays the maximum number of filters available (for each precedence and for each ASIC).
TotalMetersAvail	Displays the maximum number of meters available (for each precedence and for each ASIC).
TotalCountersAvail	Displays the maximum number of counters available (for each precedence and for each ASIC).
RangeCheckersConsumed	Displays the number of range checkers consumed by QoS.

This section contains information about the following topics:

- "Filtering the resource allocation table" (page 196)

Filtering the resource allocation table
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to filter the resource allocation table.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS Agent**.
3	Select the **Resource Allocation (ERS5XXX)** tab.
4	Click **Filter**.
5	Set the filter conditions.

    a Select **AND** to include all entries in the table that include all specified parameters, or select **OR** to include any of the specified parameters.

    b Select **IGNORE CASE** to include all entries with the parameters being set, whether in lower case or upper case.

    c Define the search to return all cases in which an entry **CONTAINS, DOES NOT CONTAIN, EQUALS TO, DOES NOT EQUAL TO** the set parameters.

    d Select **ALL RECORDS** to display all entries in the table.

    e Set **Precedence** to filter by order of precedence.

    f Select **Port** to display the entries by port.

6 Click **Filter.**

--End--

QoS Filter Limiting configuration using Enterprise Device Manager

You can use the procedures in this section to disable, re-enable, and display information about QoS Filter Limiting, a feature that controls the maximum number of user-defined protocol VLANs.

Displaying QoS Filter Limiting using EDM

Use this procedure to display the QoS Filter Limiting status.

Step	Action
1	From the navigation tree, click **QoS**.
2	From the QoS tree, click **QoS**.
3	In the working area, click the **Filter Limiting** tab.

--End--

Disabling QoS Filter Limiting using EDM

Use this procedure to disable QoS Filter Limiting. Filter Limiting is enabled by default.

Step	Action
1	From the navigation tree, click **QoS**.
2	From the QoS tree, click **QoS**.
3	In the working area, click the **Filter Limiting** tab.

4   Click the **AdminEnabled** check box to change the status.

5   On the tool bar, click **Apply**.

6   Reset the switch.

--End--

Enabling QoS Filter Limiting using EDM

Filter Limiting is enabled by default. If you have disabled Filter Limiting, use this procedure to enable the feature.

Step	Action
1	From the navigation tree, click **QoS**.
2	From the QoS tree, click **QoS**.
3	In the working area, click the **Filter Limiting** tab.
4	Click the **AdminEnabled** check box to change the status.
5	On the tool bar, click **Apply**.
6	Reset the switch.

--End--

Table 35
Filter Limiting parameters

Variable	Value
AdminEnabled	The filter limiting next-boot status,
OperEnabled	The filter limiting current status. This is a read only field.

QoS NSNA/UBP/Traffic Profile dialog box

The procedures for configuring User Based Policies and the Nortel SNA solution are nearly identical. When you assign a filter name to a VLAN (for example, redFilter), the switch automatically creates all the necessary QoS classifiers with the name you assigned (in this case, redFilter) if that filter does not already exist.

Traffic Profile applies the QoS policy on port(s) that you specify. UBP applies the QoS policy when a user is authenticated by EAPOL or non-EAPOL.

If you had previously defined the filter, then that pre-existent filter is used. Once a filter is created (either by you or automatically by the switch), it can be modified (that is, entries can be deleted or added) on the QoS NSNA/UBP/Traffic Profile dialog box.

Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

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

Use the following procedure to open the QoS NSNA/UBP/Traffic Profile dialog box.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS NSNA/UBP/Traffic Profile**.

<div align="center">**--End--**</div>

This section contains information about the following topics:

- "Viewing Classifiers " (page 199)

- "Viewing traffic profile sets" (page 204)

Viewing Classifiers
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Classifier tab.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS NSNA/UBP/Traffic Profile**.
3	Select the **Classifier** tab.

--End--

Variable definitions

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

Table 36
QoS NSNA/UBP/Traffic Profile Classifier tab parameters

Variable	Value
Id	Specifies the ID number of the classifier.
Type	Specifies the type of classifier., Options are NSNA, UBP, and TGraffic Profile.
Name	Specifies the name of the classifier. All classifiers with the same name are part of the same filter set. That filter set has the same name as the classifiers.
Block	Specifies the block name with which the classifier is associated.
EvalPrec	Specifies the evaluation order number of the classifier in that filter set. Two classifiers in the same filter set cannot have the same evaluation order. A higher eval order means a lower precedence for the corresponding policy. The save eval-order can be used for multiple classifiers within the same block.
AddrType	Specifies the type of IP address used by this classifier entry.
DstIpAddr	Specifies the IP address to match against the destination IP address of a packet.
DstIpPrefixLength	Specifies the length of the destination address mask.
SrcIpAddr	Specifies the IP address to match against the source IP address of a packet.
SrcIpPrefixLength	Specifies the length of the source address mask.
Dscp	Specifies the value for a DiffServ Codepoint (DSCP) in a packet.

Table 36
QoS NSNA/UBP/Traffic Profile Classifier tab parameters (cont'd.)

Variable	Value
Protocol/NextHeader	Specifies the IPv4 protocol value, or the IPv6 next-header value. Values are the following: • 1 = ICMP-IPv4 • 2 = IGMP • 6 = TCP • 17 = UDP • 46 = RSVP • 58 = ICMP-IPv6
DstL4PortMin	Specifies the minimum value for the Layer 4 destination port number in a packet.
DstL4PortMax	Specifies the maximum value for the Layer 4 destination port number in a packet.
SrcL4PortMin	Specifies the minimum value for the Layer 4 source port number in a packet.
SrcL4PortMax	Specifies the maximum value for the Layer 4 source port number in a packet.
Ipv6FlowId	Specifies the flow identifier for IPv6 packets.
Storage	Specifies the type of storage used.
DstMacAddr	Specifies the MAC address against which the MAC destination address of incoming packets is compared.
DstMacAddrMask	Specifies a mask identifying the destination MAC address.
SrcMacAddr	Specifies a MAC source address of incoming packets.
SrcMacAddrMask	Specifies a mask identifying the source MAC address.
VlanIdMin	Specifies the minimum value for the VLAN ID in a packet.
VlanIdMax	Specifies the maximum value for the VLAN ID in a packet.
VlanTag	Specifies the type of VLAN tagging in a packet: • untagged • tagged • ignore
EtherType	Specifies the value for the Ether type.
UserPriority	Specifies the value for the 802.1p user priority.

Table 36
QoS NSNA/UBP/Traffic Profile Classifier tab parameters (cont'd.)

Variable	Value
ActionDrop	Specifies whether or not to drop the traffic matching filtering data.
UpdateDscp	Specifies a value used to update the DSCP field in an IPv4 packet.
UpdateUserPriority	Specifies 802.1p value used to update user priority.
ActionSetPrec	Specifies automatic drop precedence (high or low).
IpFlags	Specifies the IP flags.
TcpCtrlFlags	Specifies the TCP control flags.
Ipv4Options	Specifies whether IPv4 options are present.
PktType	Specifies the Layer 2 packet type.
MasterBlockMember	Specifies whether the master classifier is within the block or not.(Traffic Profile).
Rate	Specifies the Traffic Profile classifier meter rate (Traffic Profile Per-policy-individual-metering or Per-classifier-metering).
BurstSize	Specifies the Traffic Profile burst size (Traffic Profile Per-policy-individual-metering or Per-classifier-metering).
OutActionDrop	Specifies the drop action for out-of-profile packets (Traffic Profile Per-policy-individual-metering or Per-classifier-metering).
OutActionRemarkDscp	Specifies the remark DSCP action for out-profile-packets (Traffic Profile Per-policy-individual-metering or Per-classifier-metering).
OutActionSetPrec	Specifies the set precedence for out-profile-packets (Traffic Profile Per-policy-individual-metering or Per-classifier-metering).

This section contains information about the following topics:

Inserting a classifier
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to configure a classifier for the Nortel SNA solution, Based Policy, or Traffic Profile.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS NSNA/UBP/Traffic Profile**.
3	Select the **Classifier** tab.
4	Click **Insert**.
	The **Insert Classifier** dialog box opens.
5	Using the **Type** radio options, choose whether to create a classifier for the Nortel SNA solution (**NsnaClfr**), for a User Based Policy (**UbpClfr**) or a Traffic Profile (**Traffic Profile**).
6	Enter the classifier information in the fields.
7	Change values in any fields that present default values if you want to configure specific parameters.
8	Click **Insert**.

<div align="center">**--End--**</div>

Deleting a classifier
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to delete a classifier.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS NSNA/UBP/Traffic Profile**.
3	Select the **Classifier** tab.
4	Select the classifier you want to delete.

5   Click **Delete**.

--End--

Use this procedure to filter a classifier.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS NSNA/UBP/Traffic Profile**.
3	Select the **Classifier** tab.
4	Select the classifier you want to filter.
5	On the toolbar, click **Filter**.

--End--

Viewing traffic profile sets
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to open the Set tab.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS NSNA/UBP/Traffic Profile**.
3	Select the **Set** tab.

--End--

Variable definitions
The following table outlines the parameters of the **Set** tab.

Table 37
QoS NSNA/UBP/Traffic Profile Set tab parameters

Variable	Value
AclType	Specifies the type of ACL (NSNA, UBP, or Traffic Profile).
Name	Specifies a name for this entry. The name must be an existing classifier name. All classifiers with this name are part of this filter set. The filter set itself has this name.
IfIndex	Specifies the logical interface index assigned to the VLAN or the physical interface.
MeteringMode	Specifies the Traffic Profile metering Mode as: • noMetering • perPolicyUniformRateMetering • perPolicyIndividualRateMetring • perClassifierMetering
CommittedRate	Specifies the committed rate (in Kbps).
BurstSize	Specifies the maximum number of bytes in a single transmission burst.
OutActionDrop	Specifies the action to take when packet is out-of-profile. This action is applied only if metering is being enforced, and if the traffic is deemed out-of-profile based on the level of traffic and the metering criteria. (Metering is applied only to traffic matching the filtering data.) Options are the following: • drop (packet is dropped) • pass (packet is not dropped)
OutActionUpdateDscp	Specifies the action to take to update DSCP when a packet is out-of-profile. The default value is **-1**. The value range is between -1–63.
SetPriority	Specifies the priority in the range 1–255. You can only change this field for a User Based Policy set. .
Status	Enables or disables the Traffic Profile set policy. .
Storage	Specifies the type of storage for this entry.

This section contains information about the following topcis:

Configuring a set
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to configure a set.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS NSNA/UBP/Traffic Profile**.
3	Select the **Set** tab.
4	Click **Insert**. The **Insert Set** dialog box opens.
5	Enter the set information in the fields.
6	Click **Insert**.

--End--

Deleting a set
Prerequisites

- Open one of the supported Web browsers.
- Access the switch.
- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to delete a set.

Procedure steps

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

2   From the QoS tree, double-click **QoS NSNA/UBP/Traffic Profile**.

3   Select the **Set** tab.

4   Select a set to delete.

5   Click **Delete**.

--End--

Filtering a set
Prerequisites

- Open one of the supported Web browsers.

- Access the switch.

- Click the Configuration arrowhead to open the navigation tree.

Use the following procedure to filter a set.

Procedure steps

Step	Action
1	From the navigation tree, double-click **QoS**.
2	From the QoS tree, double-click **QoS NSNA/UBP/Traffic Profile**.
3	Select the **Set** tab.
4	Select a set to filter.
5	Click **Filter**.
6	Set the filter parameters in the dialog.
7	Click **Filter**.

--End--

Nortel Ethernet Routing Switch 5000 Series

Configuration - Quality of Service

Release: 6.2
Publication: NN47200-504
Document revision: 06.01
Document release date: 28 June 2010

NORTEL