Nortel Ethernet Routing Switch 5000 Series

Configuration - Quality of Service

NN47200-504

Document status: Standard
Document version: 04.01
Document date: 12 November 2008

Sourced in Canada and the United States of America

LEGAL NOTICE

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

Microsoft and Windows are trademarks of Microsoft Corporation.

IEEE is a trademark of the Institute of Electrical and Electronics Engineers, Inc.

All other trademarks are the property of their respective owners.

Nortel Networks Inc. software license agreement

This Software License Agreement ("License Agreement") is between you, the end user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer’s Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The foregoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

1. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

2. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

3. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

4. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

5. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

6. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

New in this Release

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

Features

- DoS Attack Prevention Package (DAPP)

Other changes

No other changes.

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 Web-based Management, Nortel Networks Command Line Interface (NNCLI), SNMP, and the 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).

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

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 intolerant, fixed bandwidth	Premium	Interhuman communications requiring interaction (such as VoIP).	Absolute bounded priority over user traffic. No packet loss for in-profile traffic. Virtual leased line with lowest amount of latency. Provisioned for peak rate.
Real time, delay tolerant, low variable bandwidth	Platinum	Interhuman communications requiring interaction with additional minimal delay (such as low-cost VoIP).	Higher-priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Real time, delay tolerant, high variable bandwidth	Gold	Single human communication with no interaction (such as web site streaming video).	High-priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Non-real time, mission critical, interactive	Silver	Transaction processing (such as Telnet, web browsing).	Medium priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Non-real time, mission critical, non-interactive	Bronze	For example, e-mail, FTP, SNMP.	Lower-priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Non-real time, non-mission critical	Standard	Bulk transfer (such as large FTP transfers, after-hours tape backup).	Best-effort delivery. Uses remaining available bandwidth.

Specifying interface groups

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

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.

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_CFSEC)*.

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)

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

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 1: 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.

Note 2: On the 5600 Series switch, known/unknown IP multicast packets are not impacted by related System Classifier objects. Non-IP multicast packets are controlled.

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 (not identical actions or meters, but also 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.

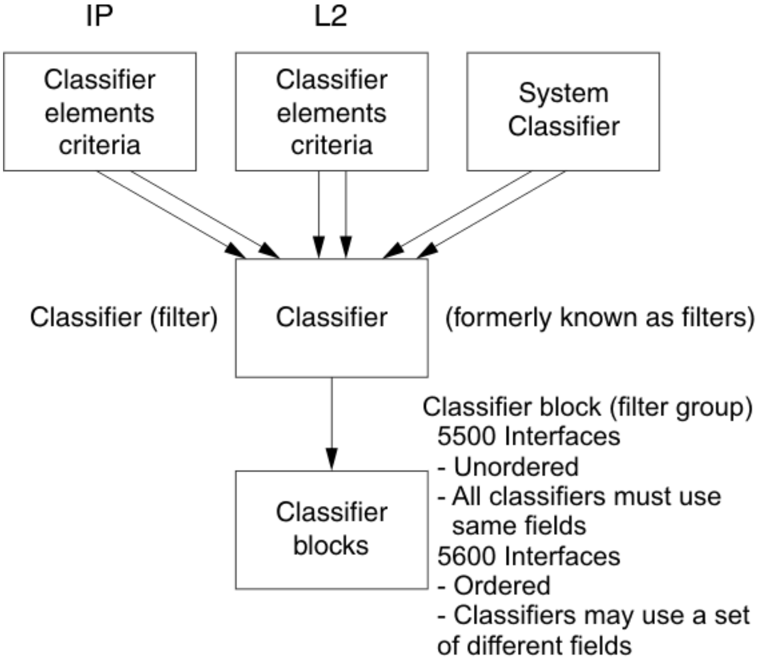
Each classifier or classifier block is associated with actions that are executed when the packet matches the filter criteria in the group. The filter criteria and the associated actions, metering criteria, and ports or interface groups are referenced by a policy, which dictates the overall traffic treatment (refer to "Flowchart of QoS Actions" (page 28) 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, not individual classifiers that comprise a block, can be associated with a meter or action.

"Relationship of classifier elements, classifiers, and classifier blocks" (page 26) displays the relationship between the classifier elements, classifiers, and classifier blocks.

Relationship of classifier elements, classifiers, and classifier blocks


IP
L2
Classifier elements criteria
Classifier elements criteria
System Classifier
Classifier (filter)
Classifier
(formerly known as filters)
Classifier block (filter group)
5500 Interfaces
- Unordered
- All classifiers must use same fields
5600 Interfaces
- Ordered
- Classifiers may use a set of different fields
Classifier blocks

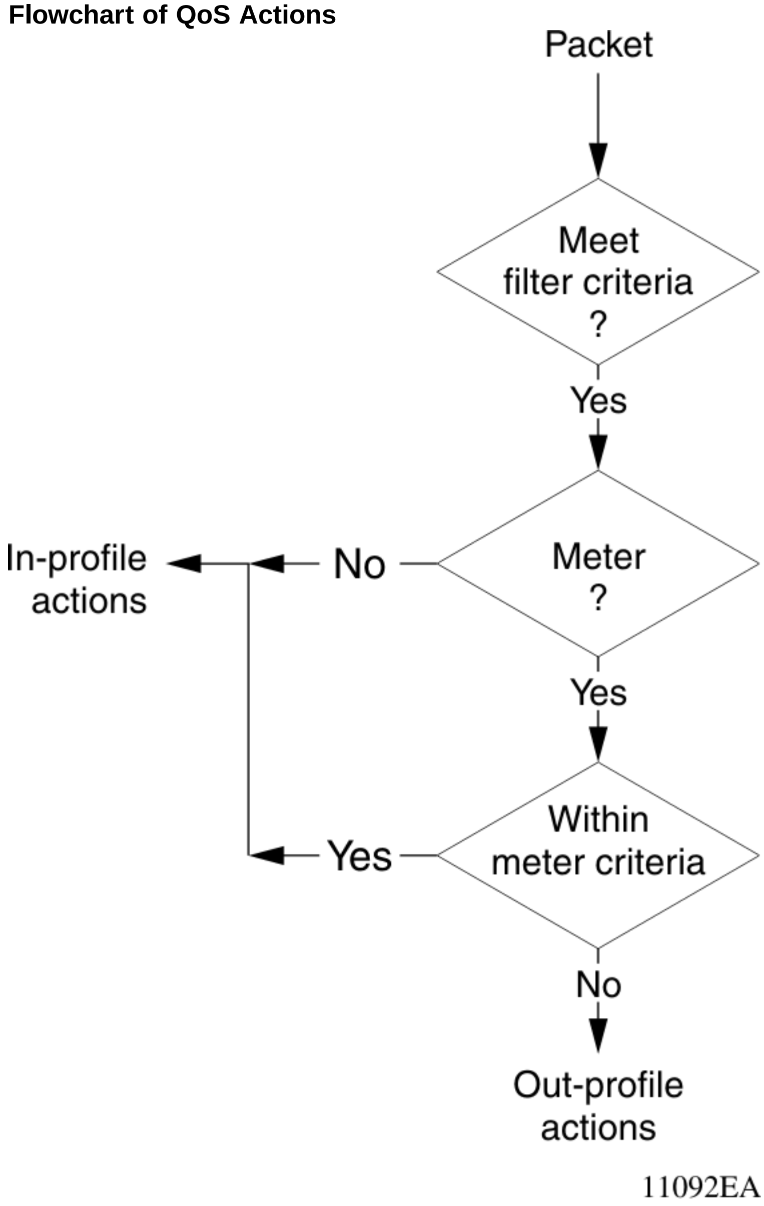
In summary, classifiers combine different classifier elements. In the case of the 5500 Series switch, classifier blocks combine classifiers to form an unordered set of classification data. Unordered data means that all classifiers associated with a policy are applied as if simultaneously, with no precedence.

> ***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

"Flowchart of QoS Actions" (page 28) summarizes how QoS matches packets with actions.

Flowchart of QoS Actions



"Summary of Allowable Actions" (page 28) shows a summary of the allowable actions for different matching criteria. This information is applicable to the 5500 Series switch only.

Summary of Allowable Actions

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

Actions	In-Profile	Out-Of-Profile	Non-Matching
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.

"Summary of allowable interface action extensions" (page 30) shows a summary of the allowable interface action extensions for different matching criteria. This information is applicable to the 5500 Series switch only.

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.

"Default QoS fields by class of interface--IPv4 only" (page 33) 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.

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

Type of filter	Action	Trusted	Untrusted	Unrestricted
	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.

"Default mapping of DSCP to QoS class and IEEE 802.1p" (page 35) describes the default DSCP, QoS class, IEEE 802.1p, and egress queue assignment for packets in each traffic class.

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(0 x1C), 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 "Default mapping of DSCP to QoS class and IEEE 802.1p" (page 35), 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.

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").

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).

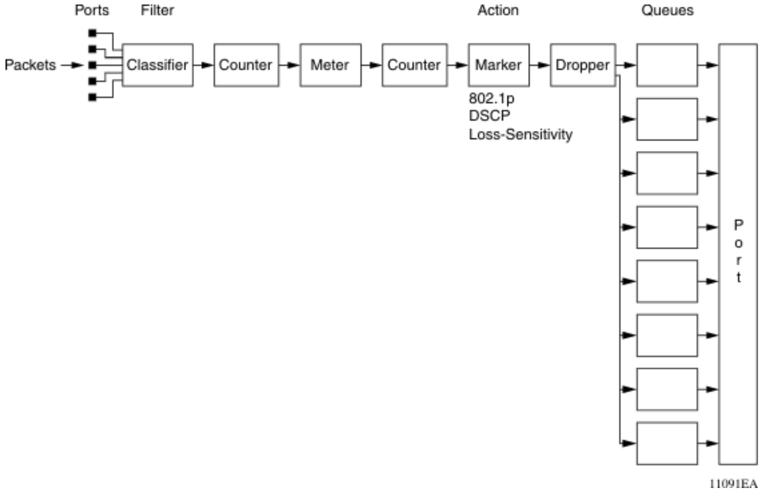
Meters, operating at ingress, keep the sorted packets within certain parameters. A committed rate of traffic can be configured, allowing for a certain amount of temporary burst traffic, as In-Profile traffic. All other traffic is configured as Out-of-Profile traffic. If you choose not to meter the flow,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

"QoS Policy Schematic" (page 39) provides a schematic overview of QoS policies.

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 port type.
- 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.

The user-configurable parameters for the queue sets take effect only after the next system reset. These configuration parameters are saved in NVRAM.

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

> ***Note:*** Changes affecting the egress interface queue set do not take effect until the system is reset. However, if the default queue configuration is queried after configuring a new queue set and prior to resetting the system, the system returns the newly configured (not yet effective) queue set.

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

> ***Note:*** The system must be reset for the modified buffer resource allocation to take effect. However, if the buffer resource is queried after modifying the buffer resource allocation and prior to resetting the system, the system returns the newly configured (not yet effective) buffer resource.

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 0xaaaaaaa, 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.

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

```
show qos { acl-assign <1 - 65535> |
action [user | system | all | <1-65535>] |
agent [details]|
arp {spoofing [port] } |
bpdu {blocker [port] } |
capability [meter|shaper] |
classifier [user | system | all | <1-65535>] |
classifier-block [user | system | all |<1-65535> ] |
dhcp {snooping [port] | spoofing [port] } |
diag [unit] |
dos {nachia [port] | sqlslam [port] | tcp-dnsport
[port] |
egressmap [ds| status]|
if-action-extension [user | system | all | <1-65535>] |
if-assign [port] |
if-group |
if-shaper [port] |
ingressmap |
ip-acl <1 - 65535> |
ip-element [user | system | all | <1-65535>] |
l2-acl <1 - 65535> |
l2-element [user | system | all | <1-65535>] |
meter [user | system | all | <1-65535>] |
nsna |
policy [user | system | all | <1-65535>] |
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.
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 not available on 5600 Series.
bpdu blocker	Displays QoS BPDU settings. blocker - Displays QoS BPDU blocker settings. This parameter not available on 5600 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.

Variable	Value
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.
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 not available on 5600 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.

Variable	Value
	- xmas - Displays QoS DoS Xmas settings. This parameter not available on 5600 Series.
egressmap	Displays the association between the DSCP and the 802.1p priority and drop precedence.
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-shaper [port]	Displays the interface shaping parameters. port - List of ports. Displays the configuration for particular ports
ingressmap	Displays the 802.1p priority to DSCP mapping.
ip-acl <1 - 65535>	Displays the specified IP access list assignment entry. - <1-65535> - Displays a particular entry.
ip-element [<1-65535> | all | system | user]	Displays the IP classifier element entries. The applicable values are: - <1-65535> - Displays a particular entry. - all - Displays all user-created, default, and system entries. - system - Displays only system entries. - user - Displays only user-created and default entries. Default is all.
l2-acl <1 - 65535>	Displays the specified Layer 2 access list assignment entry. - <1-65535> - Displays a particular entry.

Variable	Value
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 - Specify the label to display a particular NSNA template entry.
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.
queue-set	Displays the queue set configuration.
queue-set-assignment	Displays the association between the 802.1p priority to that of a specific queue.

Variable	Value
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	To display QoS capability policy configuration, use 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 - 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 - 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 To assign ports to an access list, use 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>	The list of ports assigned to the specified access list.
acl-type {ip | l2}	The type of access list used; IP or Layer 2.
name <name>	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	To remove an access list assignment, use 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 To create an access list, use 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>	The name assigned to this access list.
addr-type <addrtype>	The IP address type to use for the access list.
src-ip <source_ip>	The source IP address to use for this access list.
dst-ip <destination_ip>	The destination IP address to use for this access list.
ds-field <dscp>	The DSCP value to use for this access list.
{protocol <protocol_type> | next_header <header>}	The protocol type or IP header to use with this access list.
src-port-min <port> src-port-max <port>	The minimum and maximum source ports to use with this access list. Both values must be specified.
dst-port-min <port> dst-port-max <port>	The minimum and maximum destination ports to use with the access list. Both values must be specified.
flow-id <flowid>	The flow ID to use with this access list.
drop-action {drop | pass}	The drop action to use for this access list.
update-dscp <0 - 63>	The DSCP value to update for this access list.
update-1p <0 - 7>	The 802.1p value to update for this access list.
set-drop-prec {high drop | low drop}	The drop precedence to configure for this access list.
block <block_name>	The block name to associate with the access list.

Removing an IP access list

Use the following procedure to remove an IP access list.

Procedure steps

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

Removing a Layer 2 access list

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

Procedure steps

Step **Action**

1 To remove an access list, use 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 "Displaying QoS Parameters" (page 49).

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

Enabling QoS ARP spoofing

Use 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 To enable the QoS ARP spoofing application, use the following command from Interface Configuration mode.

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

—End—

Variable definitions

Variable	Value
port <port_list>	The list of ports on which to enable the QoS ARP spoofing application.
default-gateway <A.B.C.D>	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	To disable the QoS ARP spoofing application, use 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	To enable the BPDU blocker application, use 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	To disable the BPDU blocker application, use 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 To enable snooping, use the following command from Interface Configuration mode.

```
qos dhcp snooping port <port_list> enable interface-t
ype {access | core}
```

2 To enable spoofing, use 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>	The ports to enable the selected QoS DHCP application on.
interface-type {access | core}	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 To disable snooping, use the following command from Interface Configuration mode.

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

2 To disable spoofing, use the following command from Interface Configuration mode.

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

—End—

Variable definitions

Variable	Value
port <port_list>	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 To enable QoS DoS applications, use 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}	The type of QoS DoS application to enable on the selected ports.
port <port_list>	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	To disable QoS DoS applications, use 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}	The type of QoS DoS application to disable on the selected ports.
port <port_list>	The ports to disable the application on.

Configuring the QoS Agent

The default queue configuration can be configured and modified using the following NNCLI commands.

Configuring a default queue set

Use the following procedure to specify the default queue set.

Procedure steps

Step	Action
1	To configure the queue set, use the following command from Global Configuration mode.

```
default qos agent [buffer | dos-attack-prevention
| nt-mode | nvram-delay | queue-set <1-8> |
statistics-tracking | ubp]
```

—End—

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

Variable definitions

Variable	Value
buffer	Restore default QoS resource buffer allocation.
dos-attack-prevention	Restore default QoS DoS Attack Prevention. This parameter is only available on the 5600 Series switch.
nt-mode	Restore default QoS NT application traffic processing mode.
nvram-delay	Restore default maximum time in seconds to write config data to a non-volatile storage.
queue-set	Restore default QoS queue set
statistics-tracking	Restore default QoS statistics tracking support.
ubp	Restore default QoS UBP support level.

Job aid: Viewing the QoS agent

The following is an example for viewing the **`qos agent`**

```
5530-24TFD(config)#show qos agent
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
QoS NT mode:  Disabled
```

Modifying default queue configuration

Use the following procedure to modify the default queue configuration.

Procedure steps

Step	Action
1	To modify the configuration, use 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	To default the resource buffer, use the following command from Global Configuration mode. `default qos agent buffer`

—End—

Note: The switch must be reset once changes are made to the QoS queue set or QoS buffering for those changes to take effect.

Modifying QoS resource buffer allocation

Use the following procedure to modify QoS resource buffer allocation.

Procedure steps

Step	Action
1	To modify resource buffer allocation, use the following command from Global Configuration mode. `qos agent buffer <regular │ large │ maximum>`

—End—

Note: The switch must be reset once changes are made to the QoS queue set or QoS buffering for those changes to take effect.

Variable definitions

Variable	Value
buffer	Enter one of the following to specify the buffer allocation mode for all QoS interfaces after the next system reboot: • regular • large • maximum ***Note:*** The buffer mode determines the level of resource sharing across interfaces sharing the same port hardware.

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 To configure priority values, use 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>	Enter a number from 1 to 56 to specify the queue set to modify.

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

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 To add ports, use 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>	Enter the ports to add to interface group.
name <WORD>	Specify 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 To delete ports, use 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	To create interface groups, use the following command from Global Configuration mode. `qos if-group name <WORD> class <trusted	untrusted	unrestricted>`

—End—

Variable definitions

Variable	Value
name <WORD>	Enter the name of the interface group; maximum is 32 US-ASCII. Name must begin with a letter a..z or A..Z.
class <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	To delete interface groups, use the following command from Global Configuration mode. `no qos if-group name <WORD>`

—End—

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

—End—

Variable definitions

Variable	Value
name <WORD>	Specify the label for the egress mapping.
ds <0-63>	Enter 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.

Variable	Value
1p <0-7>	Enter the 802.1p priority value associated with the DSCP; range is between 0 and 7.
dp <low-drop | high-drop>	Enter the drop precedence values associated with the DSCP: • low-drop • high-drop

Restoring egress mapping entries to default

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

Procedure steps

Step	Action
1	To reset the entries, use 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	To configure priority, use the following command from Global Configuration mode. `qos ingressmap [name <WORD>] 1p <0-7> ds  <0-63>`

—End—

Variable definitions

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

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 To reset the entries, use 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 To add and configure classifier entries, use the following command from Global Configuration mode.

```
qos ip-element <cid> [addr-type  <addrtype>][src-ip
<src-ip-info>][dst-ip  <dst-ip-info>][ds-field
<dscp>][protocol <protocoltype>][src-port-min
<port>  src-port-max  <port>][next-header
<nextheader>][dst-port-min  <port>  dst-port-max
<port>]  [flow-id  <flowid>]  [session-id]
```

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
<cid>	Enter an integer to specify the element ID. The allowable range of values is 1 to 55000.
addr-type <addrtype>	Specify the address type, either ipv4 or ipv6. Default is ipv4.
src-ip <src-ip-info>	Enter 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-ip <dst-ip-info>	Enter 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.
ds-field <0-63>	Enter 6-bit DSCP value; range is 0 to 63. Default is ignore.
protocol <protocoltype>	Specify the IPv4 protocol classifier criteria; range is 0 to 255.
src-port-min <port> src-port-max <port>	Specify the L4 source port minimum value and maximum value filter criteria.

Variable	Value
dst-port-min <port> dst-port-max <port>	Specify the L4 destination port minimum value and maximum value filter criteria.
next-header	Specify the IPv6 next header classifier criteria; range is 0 to 255.
flow-id <flowid>	Specify the IPv6 flow identifier.
session-id	Specify the session ID.

Removing IP classifier entries

Use the following procedure to remove IP classifier entries.

Procedure steps

Step	Action
1	To remove IP classifier entries, use 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	To add Layer 2 elements, use the following command from Global Configuration mode.

```
qos l2-element  <1-55000>  [src-mac
<src-mac>][src-mac-mask <src-mac-mask>][dst-mac
<dst-mac>][dst-mac-mask <dst-mac-mask>][vlan-min
<vid-min>  vlan-max  <vid-max>][vlan-tag
<format>][ethertype  <etype>][priority  <ieee1p-seq>]
```

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—

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

Variable definitions

Variable	Value
<1-55000>	Enter an integer to specify the element ID; range is 1 to 55000.
src-mac <src-mac>	Specify the source MAC element criteria. Enter in the format H.H.H.
src-mac-mask <src-mac-mask>	Specify the source MAC mask element criteria. Enter in the format H.H.H.
dst-mac <dst-mac>	Specify the destination MAC element criteria. Enter in the format H.H.H.
dst-mac-mask <dst-mac-mask>	Specify the destination MAC mask element criteria. Enter in the format H.H.H.
vlan-min <vid-min>	Specify the VLAN ID minimum value element criteria. Range is 1 to 4094.
vlan-max <vid-max>	Specify the VLAN ID maximum value element criteria. Range is 1 to 4094.
vlan-tag <format>	Specify the packet format element criteria: • untagged • tagged The default is Ignore.

Variable	Value
ethertype <etype>	Enter the Ethernet type in the form of 0xXXXX, for example, 0x0801. Default is ignore.
priority <ieee1p-seq>	Enter the 802.1p priority values; range from 0 to 7 or all. Default is ignore.

Removing Layer 2 elements

Use the following procedure to delete Layer 2 element entries.

Procedure steps

Step Action

1 To delete element entries, use 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 To link elements, use the following command from Global Configuration mode.

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

—End—

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

Variable definitions

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

Removing classifier entries

Use the following procedure to delete classifier entries.

Procedure steps

Step Action

1 To delete classifier entries, use 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 To combine individual classifiers, use 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>	Enter an integer to specify the classifier block ID; range is 1 to 55000.
block-number <1-55000>	Specify the classifier block number; range is 1 to 55000.
name <WORD>	Specify the label for the classifier block; maximum is 16 alphanumeric characters.
set-id <1-55000>	Specify the classifier set to be linked to the classifier block; range is 1 to 55000.
set-name <WORD>	Specify the classifier set name to be linked to the classifier block; maximum is 16 alphanumeric characters.
in-profile-action <1-55000>	Specify the in profile action to be linked to the filter block; range is 1 to 55000.
in-profile-action-name <WORD>	Specify the in profile action name to be linked to the classifier block; maximum is 16 alphanumeric characters.
meter <1-55000>	Specify the meter to be linked to the classifier block; range is 1 to 55000.
meter-name <WORD>	Specify 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	To delete classifier block entries, use 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	To configure system classifier element parameters, use the following command from Global Configuration mode.

```
qos system-element <1-55000> [known-mcast |
unknown-mcast | unknown-ucast] [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>	System classifier element entry id; range is 1 to 55000.
known-mcast	Filter on known multicast destination address.
unknown-mcast	Filter on unknown multicast destination address.
unknown-ucast	Filter on unknown unicast destination address.

Variable	Value
pattern-format { tagged | untagged }	Specifies the format of data/mask pattern. The available values are: • tagged - Data/mask pattern describes a tagged packet • untagged - Data/mask pattern describes an untagged packet
pattern-data <WORD>	Byte pattern data to filter on. ***Note:*** The format of the WORD string is in the form of XX:XX:XX:.....:XX.
pattern-mask <WORD>	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	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	Specify the session ID.

Removing system classifier element entries

Use the following procedure to remove system classifier element entries.

Procedure steps

Step	Action
1	To remove system classifier element entries, use 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	To create or update QoS actions, use 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>	Enter an integer to specify the QoS action; range is 10 to 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

Variable	Value
drop-action<enable | disable | deferred-pass>	Specifies whether packets are dropped or not: • enable--drop the traffic flow • disable--do not drop the traffic flow • deferred-pass--traffic flow decision deferred to other installed policies Default is deferred pass. ***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>	Enter the drop precedence value: • low-drop • high-drop Default is low-drop.
action-ext <1-55000>	Enter an integer to specify the action extension; range is 1 to 55000.
action-ext-name <WORD>	Specify 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	To delete QoS action entries, use 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 Interface 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	To create interface action extension entries, use 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>	Enter an integer to specify the QoS action. The range is 1 to 55000
name <WORD>	Assigns a name to a QoS action with the designated action ID. Enter the name for the action; maximum is 16 alphanumeric characters
egress-ucast <port> | egress-non-ucast <port>	Specify redirection of unicast/non-unicast to specified port.

Removing interface action extension entries

Use the following procedure to remove interface action extension entries.

Procedure steps

Step	Action
1	To remove interface action extension entries, use 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	To create QoS meter entries, use 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>	Enter an integer to specify the QoS meter; range is 1 to 55000.
name <WORD>	Specify name for meter; maximum is 16 alphanumeric characters.
committed-rate <64-10230000>	Specifies rate that traffic must not exceed for extended periods to be considered in-profile. Enter the rate in Kb/s for in-profile traffic in increments of 1000 Kbits/sec; range is 64 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 to 4294967295 ms.
in-profile-action <1-55000>	Specify the in-profile action ID; range is 1 to 55000.
in-profile-action-name <WORD>	Specify the in-profile action name.
out-profile-action <1,9-55000>	Specify 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	To remove QoS meter entries, use the following command from Global Configuration mode. `no qos meter <1-55000>`

—End—

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 To configure interface shaping, use 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>]}
```

—End—

Variable definitions

Variable	Value
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.
port <portlist>	Ports to configure shaping parameters.
name <WORD>	Specify name for if-shaper; maximum is 16 alphanumeric characters.
shape-rate <64-10230000>	Shaping rate in kilobits/sec; range is 64-10230000 kilobits/sec.

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 to 4294967295 ms.

Disabling interface shaping

Use the following procedure to disable interface shaping.

Procedure steps

Step	Action
1	To disable interface shaping, use the following command from Interface Configuration mode.

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

—End—

Configuring QoS Policies

Use the following NNCLI commands to configure QoS policies.

Configuring QoS policies

Use the following procedure to create and configure QoS policies.

Procedure steps

Step	Action
1	To create a QoS policy, use 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

qos policy parameters

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

Variable	Value
non-match-action <1-55000>	Enter the action ID for non-match traffic; range is 1 to 55000. This parameter is not applicable to 5600 Series switches.
non-match-action-name <WORD>	Enter 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 to 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	To remove QoS policy entries, use the following command from Global Configuration mode. `no qos policy <1-55000>`

—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	To configure QoS for Nortel SNA filters, use 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.

—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 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. • 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.

Variable	Value
	• 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-nm-action] [drop-out-action] [max-burst-rate] [max-burst-duration] [update-dscp-out-action]	Creates the QoS Nortel SNA set. Optional parameters: • commited-rate specifies the commited rate in Kbps. • drop-nm-action specifies the action to take when the packet is non-matching. This action is applied to all traffic that was not previously matched by the specified filtering data. Options are **enable** (packet is dropped) and **disable** (packet is not dropped). • drop-out-action specifies the action to take when a packet is out-of-profile. This action is only applied if metering is being enforced, and if the traffic is

Variable	Value
	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	To delete an entire filter set, use the following command from the Global configuration mode. `no qos nsna name <filter name>`
2	To delete a classifier, use the following command from the Global configuration mode. `no qos nsna name <filter name> eval-order <value>`

—End—

> ***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	To view Nortel SNA filter parameters, use the following command from the Privileged EXEC configuration mode. `show qos nsna`
2	To view the parameters for a specific filter set, use the following command from the Privileged EXEC configuration mode. `show qos nsna name <filter name>`
3	To view ports and the filter sets assigned to those ports, use the following command from the Privileged EXEC configuration mode. `show qos nsna interface`

4 To view classifier entries, use 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	To configure User Based Policies, use 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. • 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.

Variable	Value
	• 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-nm-action] [drop-out-action] [max-burst-rate] [max-burst-duration] [update-dscp-out-action] [set-priority]	Creates the User Based Policy set. Optional parameters: • commited-rate specifies the commited rate in Kbps. • drop-nm-action specifies the action to take when the packet is non-matching. This action is applied to all traffic that was not previously matched by the specified filtering data. Options are **`enable`** (packet is dropped) and **`disable`** (packet is not dropped). • drop-out-action specifies the action to take when a packet is out-of-profile. This action is only applied if metering is being enforced, and if the traffic is

Variable	Value
	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 To delete an entire filter set, use 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.

2 To delete a classifier, use 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 To view User Based Policy filter parameters, use the following command from the Privileged EXEC configuration mode.

```
show qos ubp
```

2 To view the parameters for a specific filter set, use the following command from the Privileged EXEC configuration mode.

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

3 To view ports and the filter sets assigned to those ports, use the following command from the Privileged EXEC configuration mode.

```
show qos ubp interface
```

4 To view classifier entries, use 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.

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	To reset QoS to factory defaults, use 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

This procedure describes how to configure the QoS Agent NT mode.

Procedure steps

Step	Action
1	To configure QoS NT mode, use 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	To configure the UBP support level, use 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

This procedure describes the steps necessary to configure the type of statistics tracking used with QoS.

Procedure steps

Step	Action
1	To configure the QoS statistics tracking type, use 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	To configure NVRAM delay, use 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 To reset NVRAM delay to default, use 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 To reset the QoS agent, use 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

This procedure describes the steps necessary to enable DAPP.

Procedure steps

Step Action

1 To enable DAPP, use 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

This procedure describes how to configure DAPP status tracking.

Procedure steps

Step	Action
1	To enable DAPP status tracking, use 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

This procedure describes how to set the minimum TCP header size used by DAPP.

Procedure steps

Step	Action
1	To set the minimum TCP header size, use the following command from Global Configuration mode: `qos agent dos-attack-prevention min-tcp-header <0-255>`

—End—

Configuring DAPP maximum IPv4 ICMP length

This procedure describes how to set the maximum IPv4 ICMP length used by DAPP.

Procedure steps

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

—End—

Configuring DAPP maximum IPv6 ICMP length

This procedure describes how to set the maximum IPv6 ICMP length used by DAPP.

Procedure steps

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

—End—

Configuring Quality of Service (QoS) using Web based management

This chapter discusses how to configure DiffServ and QoS parameters for policy-enabled networks using Web-based Management.

Quality of Service Wizards

The QoS Wizards provide a streamlined QoS policy configuration mechanism. The user is prompted for only the information needed to install a specific category (type) of QoS policy. These categories include VLAN and IP application traffic prioritization, user-defined flow, network access-list support, filter set definition, and other interface security applications.

Individual entries in the appropriate currently defined QoS tables (DiffServ Multi-Field Classifier Table, Layer 2 Multi-Field Classifier Table, Base Action Table, Meter Table, Policy Table, and so on) are then created based on the user data behind the scenes, relieving the user of this responsibility. The QoS Wizard application provides a means for all users, regardless of experience, to configure effective QoS policies.

These wizards can be accessed by selecting **Application > QoS > QoS Wizard** from the menu.

"QoS Wizards" (page 105) describes the four available wizards.

QoS Wizards

Name	Menu Location	Description
QoS Configuration Wizard	**Application > QoS > QoS Wizard > QoS Wizard Config**	Used to create QoS policies.
QoS Management Wizard	**Application > QoS > QoS Wizard > QoS Wizard Mgmt**	Used to manage QoS policies previously created using the QoS Configuration Wizard.

Name	Menu Location	Description
Interface Shaper Wizard	**Application > QoS > QoS Wizard > Interface Shaper**	Used in the configuration and management of interface shaping.
Interface Applications Wizard	**Application > QoS > QoS Wizard > Interface Apps**	Used in the configuration and management of interface applications. ***Note:*** Due to hardware limitations, the Ethernet Routing Switch 5500 only supports 11 masks/precedence levels per port in a default configuration. This information applies only to the 5500 Series switch.

To use a wizard, select it from the menu as described in "QoS Wizards" (page 105). The following sections describe the use of these wizards.

> ***Note:*** Use the **Submit** and **Back** buttons provided on the wizard pages. The use of web browser **Back** and **Forward** buttons is not recommended, and can cause the wizard to function improperly.

QoS Configuration Wizard

The QoS Configuration Wizard provides a way to quickly configure quality of service policies on a switch. This wizard can be used to configure quality of service based on VLANs, IP applications such as HTTP and SMTP, user-defined flows, Layer 2 to 4 access lists, and filter sets.

To use the wizard, follow this procedure:

Procedure steps

Step	Action
1	Open the QoS Configuration Wizard by selecting **Application > QoS > QoS Wizard > QoS Wizard Config** from the menu.
2	The first screen of the configuration wizard asks the user whether they want to reset all QoS parameters before continuing. If this is desired, select **Yes**. Otherwise, select **No**. Click **Next** to continue.
3	The second screen of the configuration wizard selects the type of traffic upon which the new QoS policy is based. Valid selections are **VLAN, IP Application, User Defined Flow, L2 - L4 Access List**, or **Filter Set**.

4 The third screen of the configuration wizard names the new policy or filter set to be created. Enter the policy or filter set name in the **Name** field.

5 The next step in the configuration wizard is dependent on the selection made when prompted for a traffic type. Refer to the subsections appropriate to the traffic type selected.

a. **VLAN** -- Enter the number of a valid VLAN to which this policy applies.

b. **IP Application** -- Select the IP application on which to base the policy.

c. **User Defined Flows** -- When configuring user defined flow policies it is a two step process. The first step is to define the type of filter to apply, either IP or Layer 2.

The second step is to designate the classification parameters for this policy.

d. **Layer 2 - Layer 4 Access List** -- When configuring Layer 2 - Layer 4 Access List policies, it is a two step process. The first step is to select whether an IP Access List or Layer 2 Access List policy is to be created.

The second step is to define classification parameters for the policy.

e. **Filter Sets** -- When configuring filter sets, it is a two step process. The first step is to select whether a NSNA or User Policy filter set is to be created.

The second step is to designate the filter set parameters for the policy. Since both types of filter sets contain the same parameters, they share a common configuration page.

6 The next step in the configuration wizard again depends on the type of traffic originally selected. If policy configuration is taking place for the **VLAN, IP Application**, and **User Defined Flow** traffic types, a screen is displayed asking to add more blocks to the policy. To add more blocks to a policy, repeat step 5.

If policy configuration is taking place for the **Layer 2 - Layer 4 Access List** or **Filter set** traffic types, a screen is displayed prompting for a service class to be selected for the policy. After the service class is selected, the user is prompted to add more blocks to the policy or elements to the filter set.

7 The next step in the configuration wizard is to apply any metering to the policy. The user is first asked if they want to apply metering

to the policy. If so, the metering parameters window is displayed for configuration. If not, the user is taken to the next step.

> ***Note:*** Not at all applications support metering. This step may not apply in some configurations.

8 This step applies only to the **VLAN, IP Application**, and **User Defined Flows** traffic types. In this step, the wizard asks for the service class to apply to the policy. This action is handled in step 6 for the **Layer 2 - Layer 4 Access List** and **Filter set** traffic types.

9 With the exception of configuring filter sets, the last step in the configuration wizard is to apply the new policy to a set of ports. This policy can be applied to one port, multiple ports, or all ports.

Click **Finish** when ports are selected.

If you created a filter set, the next screen in the wizard asks for the non-match action.

Click **Next**.

10 Specify a filter set priority value.

Click **Next** to finish the wizard.

11 The new policy is applied to the switch and saved. A confirmation screen is displayed to provide visual confirmation of the successful completion of the wizard.

—End—

QoS Management Wizard

The QoS Management Wizard manages quality of service policies previously created in the QoS Configuration Wizard.

To manage a policy using this wizard, follow this procedure:

Procedure steps

Step **Action**

1 Open the management wizard by selecting **Application > QoS > QoS Wizard > QoS Wizard Mgmt** from the menu.

Select the type of policy to be managed to continue.

2 The next wizard screen displays the policies of the type selected in the previous step. From this screen, the policy can be edited using the **Edit** button, deleted using the **Delete** button, or its state can be changed using the **State** list.

3 If the **Edit** button is selected in step 2, the wizard edit screen is displayed. On this screen, policy details can be viewed and the ports that the policy applies to can be changed. This screen varies with the type of policy edited.

a. VLAN

b. IP Applications

c. User Defined Flows

d. Layer 2 - Layer 4 Access List

e. Filter Sets

—End—

QoS Interface Shaper Wizard

The QoS Interface Shaper wizard configures interface shaping on a group of switch ports.

To configure interface shaping using this wizard, follow this procedure:

Procedure steps

Step	Action
1	Open the Interface Shaper wizard by selecting **Application > QoS > QoS Wizard > Interface Shaper** from the menu. To add an interface shaper, select **Add** at the top of the screen, select the ports it will be added to, and click **Submit**. To delete an interface shaper, select **Delete** at the top of the screen, select the desired ports, and click **Submit**.
2	If adding an interface shaper, the wizard displays the Interface Shaper screen. Use this screen to set the parameters for the new interface shaper. Click **Submit** when finished.

—End—

Variable definitions

Variable	Value
Name	A name for this interface shaper.
Shaping Rate	The shaping rate in kilobits per second.
Maximum Burst Rate	The maximum allowable burst rate in kilobits per second.
Maximum Burst Duration	The duration in milliseconds that the shaping rate is allowed to be exceeded.

QoS Interface Applications Wizard

The QoS Interface Applications wizard sets up the security applications available for switch ports.

This information is only applicable to the 5500 Series switch.

> ***Note:*** Due to hardware limitations, the Ethernet Routing Switch 5500 model only supports 11 masks/precedence levels per port in a default configuration.

To use the QoS Interface Applications wizard, follow this procedure:

Procedure steps

Step **Action**

1 Open the Interface Applications wizard by selecting **Application > QoS > QoS Wizard > Interface Applications** from the menu.

2 On the first wizard screen, select the ports that are to be configured in the **Ports** column. Select **Enable** at the top of the screen to enable an interface application or **Disable** to disable one previously configured.

3 Click **Submit**.

4 The second wizard screen configures the applications. Select or de-select the applications to apply against the designated ports.

a. Three interface applications require additional information to enable them. These interface applications are:

- **ARP Spoofing** -- requires the specification of a Default Gateway IP address in the Default Gateway field.
- **DHCP Snooping** -- requires the selection of an interface type from the Interface Type list.

- **DHCP Spoofing** -- requires the specification of DHCP Server IP address in the DHCP Server field.

—End—

Configuring an Interface Group

This section describes the procedures for viewing existing interface groups as well as their creation and management.

Creating an Interface Group Configuration

To create an interface group configuration, use the following procedure:

Procedure steps

Step	Action
1	Open the Interface Config screen by selecting **Applications > QoS > QoS Advanced > Devices > Interface Config** from the menu.
2	In the **Interface Group Creation** section, type a role combination name in the **Role Combination** field and select an interface class from the **Interface Class** list.
3	Click **Submit**. The new interface group configuration is displayed in the **Interface Group Table** section.

—End—

Displaying Interface ID Table

To display the Interface ID Table, use the following procedure:

Procedure steps

Step	Action
1	Open the **Interface Config** screen by selecting **Applications > QoS > QoS Advanced > Devices > Interface Config** from the menu.
2	Click **Display Interface ID Table**.

The **Interface ID** screen opens. The table displays all interfaces and the interface group (role combination) to which it belongs. If an interface does not belong to an interface group (role combination), it does not display in the table.

The table displays a mapping of each interface to its interface group.

—End—

Adding or Removing Interface Group Members

To select or deselect ports as members of an existing interface group, use the following procedure.

Procedure steps

Step	Action
1	Open the **Interface Config** screen by selecting **Applications > QoS > QoS Advanced > Devices > Interface Config** from the menu.
2	In the **Interface Group Table** section, click the **Modify** icon in the row to be modified. The **Interface Group Assignment** screen opens.
3	In the **Ports** field, select or de-select the ports that are to be part of this **Interface Group**.
4	Click **Submit**.

—End—

Deleting an Interface Group

To delete an Interface Group configuration, use the following procedure.

Procedure steps

Step	Action
1	Open the **Interface Config** screen by selecting **Applications > QoS > QoS Advanced > Devices > Interface Config** from the menu.
2	In the **Interface Group Table** section, click the **Modify** icon in the row of the group to be deleted.
3	In the **Ports** field, de-select all ports associated with the interface group.

4 Click **Submit**.

5 In the **Interface Group Table** section, click the **Delete** icon in the row of the interface group that is being removed.

A message asks for confirmation of the requested action.

6 Click **Yes**.

—End—

Configuring 802.1p priority queue assignment

> ***Note:*** Nortel Networks recommends using the default 802.1p assignments to ensure end-to-end QoS connectivity.

802.1p user priority values can be assigned to a queue for each interface with a specific queue set. This information is used for assigning egress traffic to outbound queues.

Use the following procedure to configure 802.1p user priority.

Procedure steps

Step	Action
1	Open the **Priority Queue Assignment** screen by selecting **Applications > QoS > QoS Advanced > Devices > Priority Q Assign** from the menu.
2	In the **802.1p Priority Assignment (View By)** section, select the queue set to view from the Queue Set drop-down.
3	Click the **Submit** button immediately under the **802.1p Priority Assignment (View By)** section.
4	The information for the selected queue set is displayed in the **802.1p Priority Assignment Table** section. In the **Queue** field, assign a number that signifies the desired queue in the specified queue set with which this priority is associated.
5	Click the **Submit** button immediately under the **802.1p Priority Assignment Table** section.

—End—

Configuring 802.1p priority mapping

> ***Note:*** Nortel Networks recommends using the default 802.1p priority to DSCP mappings to ensure end-to-end QoS connectivity.

To configure 802.1p priority to DSCP mapping, use the following procedure:

Procedure steps

Step	Action
1	Open the **Priority Mapping** screen by selecting **Applications > QoS > QoS Advanced > Devices > Priority Mapping** from the menu.
2	In the fields provided, enter the priority mapping information.
3	Click **Submit**.

—End—

Variable definitions

Variable	Value
802.1p Priority	The 802.1p user priority to map to a DSCP value at ingress.
DSCP	Type the DSCP value to associate with the specified 802.1p user priority value at ingress.
Name	Enter a name that describes the mapping, using 16 alphanumeric characters.

Configuring DSCP mapping

> ***Note:*** Nortel Networks recommends using the default DSCP mappings to ensure end-to-end QoS connectivity.

To configure DSCP to 802.1p user priority/drop precedence mapping, use the following procedure:

Procedure steps

Step	Action
1	Open the **DSCP Mapping** screen by selecting **Applications > QoS > QoS Advanced > Devices > DSCP Mapping** from the menu.

2 Click the icon in the **Action** column of the row to be configured. The **DSCP Mapping Modification** screen opens.

3 In the fields provided, modify the mapping scheme.

4 Click **Submit**.

—End—

Variable definitions

Variable	Value
802.1p Priority	Choose the IEEE802 CoS value to use when mapping the DSCP value.
Drop Precedence	Choose the drop value precedence to use for traffic with the associated 802.1p user priority value with the identified queue: • High Drop • Low Drop ***Note:*** Generally, low packet drop precedence receives preferential treatment.
Service Class	Enter the service class. ***Note:*** This field corresponds to the adjacent user priority levels.
	Note: Mappings created on the DSCP mapping modification page are used at egress for marking traffic.

Displaying QoS Meter Capability

Use the following procedure to display QoS interface meter capabilities.

Procedure steps

Step	Action
1	Open the **Interface Meter Capability** screen by selecting **Applications > QoS > QoS Advanced > Devices > Meter Capability** from the menu.

—End—

Variable definitions

Variable	Value
Port	The port that the meter is applied to.
Meter Support	The metering algorithms supported.
Meter Rate (Kbps)	Displays maximum supported Meter Rate capability.
Meter Bucket (KBytes)	Displays the maximum supported Meter Bucket size capability.
Meter Granularity (Kbps)	Displays the supported Meter Granularity.

Displaying QoS shaper capability

Use the following procedure to display QoS interface shaper capabilities.

Procedure steps

Step	Action
1	Open the **Interface Shaper Capability** screen by selecting **Applications > QoS > QoS Advanced > Devices >Shaper Capability** from the menu.

—End—

Variable definitions

Variable	Value
Port	The port to which the meter is applied.
Shaper Support	Displays where the shaper is applied.

Variable	Value
Shaper Rate (Kbps)	Displays maximum supported Shaper Rate.
Shaper Bucket (KBytes)	Displays maximum supported Shaper Bucket size.
Shaper Granularity (Kbps)	Displays supported Shaper Granularity.

Configuring IP classifier elements

An IP classifier element is created to enable the switch to classify traffic. In turn, IP classifier elements are then referenced by classifiers, which determine access to, and denial of, network services.

Creating an IP classifier element

Use the following procedure to create an IP classifier element.

Procedure steps

Step	Action
1	Open the **IP Classifier Element** screen by selecting **Applications > QoS > QoS Advanced > Rules > IP Classifier Element** from the menu.
2	To create a new IP classifier element, edit the fields in the **IP Classifier Element Creation** section. Any field in this section can be ignored for the purposes of the classifier element by selecting the **Ignore** option button.
3	Click **Submit**. The new element is displayed in the **IP Classifier Element Table** section of the screen.

—End—

Variable definitions

Variable	Value
Address Type	The type of IP address this classifier uses.
Destination Address	The destination IP address this classifier uses.
Source Address	The source IP address this classifier uses.
DSCP	The DSCP setting this classifier uses.

Variable	Value
IPv4 Protocol / IPv6 Next Header	The IPv4 protocol or IPv6 next header the classifier element will match.
Destination Layer4 Port	The value that the packet's layer 4 destination port number must have to match this classifier element.
Source Layer4 Port	The value that the packet's layer 4 source port number must have to match this classifier element.
IPv6 Flow ID	Enter the hexidecimal value of the flow identifier to match.
Session-ID	Specifies the session ID.

Deleting an IP classifier element configuration

Use the following procedure to delete a IP classifier element configuration.

Procedure steps

Step Action

1 Open the **IP Classifier Element** screen by selecting **Applications > QoS > QoS Advanced > Rules > IP Classifier Element** from the menu.

2 In the **IP Classifier Element** Table section, click the **Delete** icon beside the element to be deleted.

3 A message prompts for confirmation of the request. Click **Yes.**

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

—End—

Configuring Layer 2 classifier elements

Layer 2 classifier elements can be configured by defining IEEE 802-based parameters. Layer 2 classifiers are defined by specifying the layer 2 classifier element to be included in the given classifier or classifier blocks.

Creating a Layer 2 classifier element configuration

Use the following procedure to create a Layer 2 classifier element configuration.

Procedure steps

Step	Action
1	Open the **Layer2 Classifier Element** screen by selecting **Applications > QoS > QoS Advanced > Rules > Layer2 Classifier Element** from the menu.
2	In the fields provided in the **Layer2 Classifier Element Creation** section, specify the parameters for the new classifier element. Any field can remain unused in the classifier element by selecting the **Ignore** option.
3	Click **Submit**. The new Layer 2 Classifier Element is displayed in **Layer2 Classifier Element Table.**

—End—

Variable definitions

Variable	Value
Destination MAC Address	The destination MAC address to use for the classifier.
Source MAC Address	The source MAC address to use for the classifier.
VLAN	The VLAN ID range to use for the classifier.
VLAN Tag	Whether the classifier element looks for tagged or untagged VLANs.
EtherType	The type of ethernet protocol the classifier uses.
802.1p Priority	The 802.1p priority level this classifier uses.

Deleting a layer 2 classifier element configuration

Use the following procedure to delete a layer 2 classifier element configuration.

Procedure steps

Step	Action
1	Open the **Layer2 Classifier Element screen** by selecting **Applications > QoS > QoS Advanced > Rules > Layer2 Classifier Element** from the menu.

2 In the **Layer2 Classifier Element Table**, click the **Delete** icon in the row of the classifier element to be deleted.

3 A message opens prompting for confirmation of the request. Click **Yes.**

> ***Note:*** A Layer 2 classifier element configuration cannot be modified. The configuration must be deleted and recreated.
>
> A Layer 2 classifier element that is referenced by a classifier cannot be deleted.

—End—

Configuring System Classifier Element

The System Classifier Element supports traffic identification which is based on Layer 2 destination MAC address type. The benefits offered by System Classifier Element are:

- Supports pattern matching or offset filtering capabilities.
- Using offset filtering you can identify fields within protocol headers to identify traffic for additional QoS processing.
- Extends classification capabilities of the Nortel Ethernet Routing Switch 5000 Series by eliminating the limitations caused by supporting only a few protocol header fields (for example IP source address, IP protocol field, VLAN ID).
- Allows for the definition of fully-customized classifiers to match non-IP-based traffic and to identify IP-based traffic using non-typical fields in Layers 2, 3, 4 and beyond.

The System Classifier Element feature can be used by advanced QoS users whose classification requirements are not supported using traditional IP and Layer 2 classification support.

Use the following procedure to configure a System Classifier Element follow this procedure.

The Nortel Ethernet Routing Switch 5500 Series switch supports selection of 32 bytes within the first 80 bytes of a packet.

The Nortel Ethernet Routing Switch 5600 Series Content Aware Processor (CAP) lookup engine supports selection of 16 bytes within the first 128 bytes of the packet.

Procedure steps

Step	Action
1	Open the **System Classifier Element** screen by selecting **Applications > QoS > QoS Advanced > Rules > System Clfr Elem** from the menu.
2	In the **System Classifier Element Creation** section, edit the fields provided to create the new classifier element.
3	Click **Submit.**

—End—

Variable definitions

Variable	Value
Dst MAC Address Type	The destination MAC address type.
Pattern	The pattern data can be entered, or use the pattern data and mask byte template as a starting point for modifications. Existing classifiers (and the associated referenced elements) can also be used, using the "Fill in" list, or typical protocol header data fields, using the radio buttons and check boxes to initialize the offset filtering components. ***Note:*** For ports on a 5600 Series switch, you must specify version 2 and select an address type for patterns to be installed.

Classifier Configurations

Viewing Existing Classifiers

To view existing classifiers, follow this procedure:

Procedure steps

Step	Action
1	Open the **Classifiers** screen by selecting **Applications > QoS > QoS Advanced > Rules > Classifier**.
2	Click the **View** icon beside the desired classifier.

—End—

Creating a Classifier

To create a new classifier, follow this procedure:

Procedure steps

Step	Action
1	Open the **Classifiers** screen by selecting **Applications > QoS > QoS Advanced > Rules > Classifier**.
2	Click **Create Classifier**.
3	The **Create Classifier** screen opens.
4	Enter a name for the classifier in the **Classifier Name** field. One will be assigned to the classifier if not designated.
5	Select one classifier element from the **IP classifier element** from the IP Classifier Element section and one **L2 Classifier Element** section. Classifiers can have either one IP element and one L2 element or just one IP element or just one L2 element.
6	Click **Submit**.

—End—

Deleting a classifier

Use the following procedure to delete a classifier.

Procedure steps

Step	Action
1	Open the **Classifiers** screen by selecting **Applications > QoS > QoS Advanced > Rules > Classifier**.
2	Click the **Delete** icon next to the row with the classifier to be deleted. ***Note:*** A classifier or classifier block that is referenced by a policy cannot be deleted. The policy must be deleted first.

—End—

Classifier Block Configurations

Note: Each classifier in a classifier block on a 5000 Series switch must match the same parameters and the same mask, range, and VLAN tag type. Additionally, all members of a classifier block must be configured consistently regarding meters and actions--that is, they must all specify meters or they must all not specify meters, and they must all specify actions or they must all not specify actions.

Viewing Classifier Blocks

To view classifier blocks, use the following procedure:

Procedure steps

Step	Action
1	Open the **Classifier Blocks** screen by selecting **Applications > QoS > QoS Advanced > Rules > Classifier Block** from the menu.
2	Click the **View** icon in the row of the classifier block to be viewed.

—End—

Creating Classifier Blocks

To create a classifier block, follow this procedure:

Procedure steps

Step	Action
1	Open the **Classifier Blocks** screen by selecting **Applications > QoS > QoS Advanced > Rules > Classifier Block** from the menu.
2	Click **Create Classifier Block**.
3	The **Create Classifier Block** screen opens.
4	Enter a name for the block in the **Classifier Block Name** field.
5	Select the classifiers to include in the block from the **Classifier Block Members** section.
6	Click **Submit**.

—End—

Deleting a Classifier Block

To delete a classifier block, follow this procedure:

Procedure steps

Step	Action
1	Open the **Classifier Blocks** screen by selecting **Applications > QoS > QoS Advanced > Rules > Classifier Block** from the menu.
2	Click the **Delete** icon in the row of the classifier block to be deleted.

—End—

Configuring QoS actions

After an action is created, the action is associated with policies, meters, and classifier blocks. An action specifies the type of behavior a policy that applies to a flow of packets. When the filters match the incoming packets, the created actions are performed on those packets.

Creating an Action

To create an action, follow this procedure:

Procedure steps

Step	Action
1	Open the **Action** screen by selecting **Applications > QoS > QoS Advanced > Action** from the menu.
2	In the fields provided, use the **Action Creation** section to create the new action.
3	Click **Submit**.

—End—

Variable definitions

Variable	Value
Action Name	The name to associate with this action.

Variable	Value
Drop Frame	Choose whether the frame being evaluated is dropped or transmitted by this attribute: • Deferred Pass - traffic flow decision deferred to other installed policies • No - do not drop the traffic flow • Yes - drop the traffic flow The default setting is Deferred Pass.
Update DSCP	Choose a value. When this field is defined, it causes the value contained in the Differentiated Services (DS) field of an associated IP datagram to be updated with the value of this object. The default setting is Ignore.
Set Drop Precedence	Choose a packet drop precedence value. ***Note:*** Generally, low packet drop precedence receives preferential treatment. The default setting is Low Drop.
Update 802.1p Priority	Choose the action attribute that causes the value contained in the 802.1p priority field to be updated based on the value of this object. The update priority range values are 0 (lowest priority) to 7 (highest priority). The default setting is Ignore.
Extension	Choose either No Extension or one of the extensions created on the Interface Action Extension page. The default setting is None.

Modifying an action configuration

Use the following procedure to modify an action configuration.

Procedure steps

Step	Action
1	Open the **Action** screen by selecting **Applications > QoS > QoS Advanced > Action** from the menu.
2	In the **Action Table** section, click the **Modify** icon in the row of the action to be modified.
3	The **Action Modification** screen opens with the fields displaying the current data for that action.
4	In the fields provided, modify the Action.
5	Click **Submit**.

—End—

Deleting an Action

To delete an action configuration, follow this procedure:

Procedure steps

Step	Action
1	Open the **Action** screen by selecting **Applications > QoS > QoS Advanced > Action** from the menu.
2	In the **Action Table** section, click the Delete icon in the row that represents the Action to be deleted.
3	A message prompts for confirmation of the request.
4	Click **Yes**. ***Note:*** An action that is referenced by a meter, classifier block, or policy cannot be deleted. The associated item must first be deleted. A system default or system created action cannot be deleted.

—End—

Using the Interface Action Extension

Action extensions are created by using the Interface Action Extension page. These extensions filter on:

- Set an egress unicast
- Set an egress non-unicast

Creating an Interface Action Extension

To create an interface action extension, follow this procedure:

> ***Note:*** The 5600 Series switch must specify the same port with both egress unicast and non-egress unicast.

Procedure steps

Step	Action
1	Open the **Interface Action Extension** screen by selecting **Applications > QoS > QoS Advanced > Interface Action Ext**.
2	In the **Interface Action Extension Creation** section, use the fields provided to create the new action extension.
3	Click **Submit**.

—End—

Variable definitions

Variable	Value
Action Name	The name for this action extension.
Set Egress Unicast	Choose either: • Ignore - the system does not set an egress unicast port • Choose the port for the egress unicasts. The default setting is Ignore.

Variable	Value
Set Egress Non-Unicast	Choose either: • Ignore - the system does not set an egress unicast port • Choose the port for the egress non-unicasts. The default setting is Ignore.

Deleting an interface action extension configuration

Use the following procedure to delete an interface action extension.

Procedure steps

Step	Action
1	Open the **Interface Action Extension** screen by selecting **Applications > QoS > QoS Advanced > Interface Action Ext**.
2	In the **Interface Action Extension Table** section, click the **Delete** icon in the row of the action extension to be deleted.
3	A message prompts for confirmation of the request. Click **Yes**. ***Note:*** An interface action extension that is referenced by an action cannot be deleted. Delete the action first.

—End—

Using QoS Meters

Use the QoS screens to view, create, modify, and delete QoS meters.

Creating a QoS Meter

To create a QoS meter, follow this procedure:

Procedure steps

Step	Action
1	Open the **Meter** screen by selecting **Applications > QoS > QoS Advanced > Meter** from the menu.
2	In the Meter Creation section, use the fields provided to create the new meter.
3	Click **Submit**.

—End—

Variable definitions

Variable	Value
Name	Enter the name for the meter you are creating.
Committed Rate	Enter the Committed Rate in Kbps here. ***Note:*** The committed rate must be entered in multiples of 64 or 1000 Kbps.
Committed Burst Size	• Maximum Burst Rate - Enter the Maximum Burst Rate in Kbps. • Duration - From the list, choose 1 of up to 12 durations for the period that the Maximum Burst Rate is allowed.
In-Profile Action	Choose from the list of: • Default actions • All actions you created using the Action page The default setting is Drop Traffic.
Out-of-Profile Action	Choose from the list of: • Default actions

Variable	Value
	• All actions you created using the Action page The default setting is Drop Traffic.

Viewing meters

Use the following procedure to view a meter.

Procedure steps

Step	Action
1	Open the **Meter** screen by selecting **Applications > QoS > QoS Advanced > Meter** from the menu.
2	View created meters in the **Meter Table**.

—End—

Deleting a meter

Use the following procedure to delete a meter.

Procedure steps

Step	Action
1	Open the **Meter** screen by selecting **Applications > QoS > QoS Advanced > Meter** from the menu.
2	In the **Meter Table** section, click the **Delete** icon to delete the meter.
3	A message prompts for confirmation of the request. Click **Yes**.

—End—

Configuring QoS Interface Shaper

Interface Shaping is a method that involves limiting the traffic rate at egress through a specific interface. Interface-based shaping allows administrators to limit egress traffic generation independent of other QoS components. It provides limited shaping capabilities with minimal configuration requirements.

Configuring Interface Shaping parameters

Use the following procedure to add interface shaping parameters for a port or set of ports.

Procedure steps

Step	Action
1	Open the **Interface Shaper** screen by selection **Applications > QoS > QoS Advanced > Interface Shaper**.
2	Click on the **Add** option button and select the desired ports.
3	Click **Submit**.
4	The **Interface Shaper Creation** screen is displayed.
5	Using the fields provided, enter the parameters for the new interface shaper entry.
6	Click **Submit**.

—End—

Variable definitions

Variable	Value
Name	Denotes the name of the Interface.
Shaping Rate	Signifies the shaping rate in multiples of 64 or 1000 Kbps.
Maximum Burst Rate	Denotes the maximum burst rate in Kbps.
Maximum Burst Duration	Signifies the period that the maximum burst rate is allowed.

Deleting Interface Shaping Parameters

Interface Shaping parameters can be deleted for a single port or multiple ports.

Use the following procedure to delete the parameters.

Procedure steps

Step	Action
1	Open the **Interface Shaper** screen by selection **Applications > QoS > QoS Advanced > Interface Shaper**.
2	In the **Interface Shaper Setting** section, select the **Del** option and the ports that the configuration parameters are to be deleted from.
3	Click **Submit**.

—End—

Configuring QoS policies

QoS policies are created by creating filters in the hardware that apply a set of packet-filtering criteria and actions to individual interfaces.

If data is to be metered, the In-Profile action and the Out-Profile action are referenced from the meter entry. The In-Profile action directs the switch how to handle the data flow that is within the meter you set, and the Out-Profile directs the switch how to handle all other data.

Installing defined filters

Use the following procedure to create a hardware policy filter configuration.

Procedure steps

Step	Action
1	Open the **Policy** screen by selecting **Application > QoS > QoS Advanced > Policy** from the menu.
2	In the **Policy Creation** section, enter the information for the policy in the fields provided.
3	Click **Submit**.

—End—

Variable definitions

Variable	Value
Policy Name	Type a character string to create a unique name to identify this policy.

Variable	Value
Classifier Type	Choose the type of filter to associate with this policy.
Classifier Name	Choose the name of the classifier or classifier block to associate with this policy.
Role/Port	Choose the type of interface to which this policy applies either specified in terms of a role combination, from a list of all Role Combinations created so far, or by selecting a port from the Port dropdown.
Policy Precedence	Enter a number from 1 to 15 to use as a determinate of the order of precedence for this filter. ***Note:*** The highest value for precedence is evaluated first.
Meter	Choose either: • None - no meter is associated with this policy • one of the user-defined meters
In-Profile Action	Choose the action to be taken for the data associated with this policy. ***Note:*** If this policy is metered the In-Profile Action is derived from the Meter entry.
Non-Match Action	Choose the action to take associated with this policy for data that does not match the configured set of packet-filtering criteria. ***Note:*** Not applicable to 5600 Series switch.
Track Statistics	Choose whether to track statistics for this policy and the granularity of the statistics desired. The default setting is No.

Viewing hardware policy statistics

To view statistics for a selected hardware policy configuration, use the following procedure:

Procedure steps

Step	Action
1	Open the **Policy** screen by selecting **Application > QoS > QoS Advanced > Policy** from the menu.
2	Click the View icon in the Policy Table section for the policy to be viewed. The Policy Statistics screen opens.

—End—

Deleting a hardware policy configuration

Use the following procedure to delete a hardware policy configuration.

Procedure steps

Step	Action
1	Open the **Policy** screen by selecting **Application > QoS > QoS Advanced > Policy** from the menu.
2	Click the Delete icon in the Policy Table section for the policy being deleted.
3	A message prompts for confirmation of the request. Click **Yes**.

—End—

Configuring QoS Policy Agent (QPA) characteristics

QPA operational parameters can be configured in Web-based Management.

To open the configure QPA parameters follow this procedure:

Procedure steps

Step	Action
1	Open the **Agent Configuration** screen by selecting **Application > QoS > QoS Advanced > Agent > Configuration** from the menu.
2	In the **QoS Configuration** section, configure the agent parameters using the fields provided.
3	Click **Submit**.

—End—

Variable definitions

Variable	Value
QoS Policy Agent Reset to Defaults	Choose whether or not to reset the policy agent to the default settings.
NVRAM Commit Delay	Type the time, in seconds, before the configuration is saved to NVRAM.
Queue Set	Choose the default QoS CoS queue set. Default queue count is specified.
Buffering	Choose the QoS resource buffer allocation scheme.
UBP Support Level	Configure or disable UBP support level.
Default Statistics Tracking	Configure the statistics tracking method. Options are: • Disabled • Individual • Aggregate
DoS Attack Prevention	• **Mode**: Enables or Disables DAPP • **Minimum TCP header**: Configure minimum TCP header size in the range 0 to 255 • **Maximum IPv4 ICMP**: Configure maximum IPv4 ICMP in the range 0 to 1023 • **Maximum IPv6 ICMP**: Configure maximum IPv6 ICMP in the range 0 to 16383
QoS NT Mode	Configure QoS NT Mode. Options are: • Disabled • NT without egress DSCP remapping • NT with egress DSCP remapping
QoS WEB Display Mode	Choose to display either only user-created parameters, only system-created parameters, or all parameters for QoS.

Using QoS diagnostics

The Diagnostics screen is used to:

- view how many filters, masks, meters, and counters are used.
- validate configuration ranges.

- examine the raw bit form of the classifiers placed into a classifier block in order to compare the masks.

  Note: Classifiers must be configured already to display the rules and masks; the value and mask for a range can be displayed before configuring that range.

Use the following procedure to open the Diagnostics screen.

Procedure steps

Step	Action
1	Open the **Diagnostics** screen by selecting **Application > QoS > QoS Advanced > Agent > Diagnostic** from the menu.
2	To display a valid range: a. Use the **QoS Valid Range** section to enter the beginning number of the desired range. b. From the list, choose the end of the range from the system-provided choices. c. Click **Submit**.

—End—

Variable definitions

Screen Section	Variable	Value
QoS Resource Allocation Table	Interface	Displays the port or interface number.
	QoS Masks Consumed	Displays total number of masks consumed from QoS application.
	QoS Filters Consumed	Displays total number of filters consumed from QoS application.
	QoS Meters Consumed	Displays total number of meters consumed from QoS application.
	QoS Counters Consumed	Displays total number of counters consumed from QoS application.

Screen Section	Variable	Value
	Non-QoS Masks Consumed	Displays total number of masks consumed by non-QoS applications.
	Non-QoS Filters Consumed	Displays total number of filters consumed by non-QoS applications.
	Non-QoS Meters Consumed	Displays total number of meters consumed by non-QoS applications.
QoS Valid Range	Range	Enter beginning variable for any QoS range (such as VLANs, L4 Source Port, L4 Destination Port) and choose the end variable from among the system-provided values on the pull-down menu.
	Value	Displays the corresponding rule value in the IRULE entry in hardware.
QoS Valid Range (continued)	Mask	Displays the corresponding mask value in the IMASK entry in hardware.

Configuring Quality of Service (QoS) using Device Manager

This chapter describes using the 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.

Managing interface groups

Interface queues and groups can be displayed.

Displaying interface queues

To display interface queues, use the following procedure:

Procedure steps

Step	Action
1	Open the **QosDevice** screen by selecting **QoS > QoS Devices** from the menu. Select the **Interface Queue** tab.

—End—

Variable definitions

Variable	Value
SetId	Displays an integer between 1 and 65535 that identifies the specific queue set.
QueueId	Displays an integer that uniquely identifies a specific queue within a set of queues.

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

Displaying interface groups

Device Manager lets you display the interface groups.

To display interface groups:

Procedure steps

Step	Action
1	Open the **QosDevice** screen by selecting **QoS > QoS Devices** from the menu. Select the **Interface Group** tab.

—End—

Variable definitions

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

Variable	Value
Role	The tag used to identify interfaces with the characteristics specified by the attributes of this class instance. These identifiers can be used within a number of classes to identify a physical set of interfaces to which policy rules and actions can apply.
Capabilities	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	The type of traffic interfaces associated with the specified role combination.
StatsTrackingType	The type of statistics tracking. Options are aggregate or disabled.
StorageType	Displays storage type for this interface group: • Volatile • nonVolatile (default) • readOnly

Assigning ports to an interface group

Device Manager lets you assign ports to an interface group.

To assign ports to an interface group:

Procedure steps

Step	Action
1	Open the **QosDevice** screen by selecting **QoS > QoS Devices** from the menu. Select the **Interface Group** tab.
2	Click **Interface Assignment**. The **Group Assignment** screen opens.
3	Click the port numbers to add to the interface group.
4	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 Device Manager to time out.

—End—

Deleting ports from an interface group

Device Manager lets you remove ports from an interface group.

To remove ports from an interface group:

Procedure steps

Step	Action
1	Open the **QosDevice** screen by selecting **QoS > QoS Devices** from the menu. Select the **Interface Group** tab.
2	Highlight the interface group from which to delete ports.
3	Click **Interface Assignment**.
4	The **Group Assignment** screen opens.
5	Click the port numbers to delete from the interface group.
6	Click **OK**.

—End—

Adding interface groups

Device Manager lets you add interface groups.

To add an interface group, use the following procedure:

Procedure steps

Step	Action
1	Open the **QosDevice** screen by selecting **QoS > QoS Devices** from the menu. Select the **Interface Group** tab.
2	Click **Insert**.
3	The **Insert Interface Group** screen opens.
4	Enter the desired ID number.
5	Enter the **Role** combination tag for this Interface Group.

6 Select the interface class desired for this interface group: **trusted**, **nonTrusted**, or **unrestricted**.

7 Click **Insert**.

—End—

Deleting interface groups

Device Manager lets you delete interface groups.

To delete an interface group:

Procedure steps

Step	Action
1	Open the **QosDevice** screen by selecting **QoS > QoS Devices** from the menu. Select the **Interface Group** tab.
2	Highlight the interface group to delete.
3	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—

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

Displaying an interface ID

To display the interface ID, use the following procedure:

Procedure steps

Step	Action
1	Open the **QosDevice** screen by selecting **QoS > QoS Devices** from the menu. Select the **Interface ID Assignments** tab. **Interface ID Assignments tab fields**

—End—

Variable definitions

Variable	Value
RoleCombination	Displays the role combination associated with the interface.
QueueSet	Displays the queue set associated with this interface.

Filtering Interface ID Assignments table

To display selected parts of the Interface ID Assignments tab:

Procedure steps

Step	Action

1 Open the **QosDevice** screen by selecting **QoS > QoS Devices** from the menu. Select the **Interface ID Assignments** tab.

2 Click the **Filter** button.

The **Insert Filter** dialog opens.

3 Set the conditions to be used to filter the display of the **Interface ID Assignments** table:

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

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

c. From **Column**, select the parameters to designate table contents.

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

e. To display the entries in the table by interface, select **IfIndex** and enter the **IfIndex** string to display.

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

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

4 Click **Filter**.

—End—

Variable definitions

Variable	Value
Condition	Select one of the following: • **AND** to include all entries in the table that include *all* specified parameters • **OR** to include *any* of the specified parameters
Ignore case	Select **Ignore case** to include all entries with the parameters being set, whether in lowercase or uppercase.
Column	Select any of the following criteria: • **contains** to include only information that contains the specified parameters • **does not contain** to exclude specific parameters • **equals to**to include only information that matches the specific parameters • **does not equal to**to include only information that does not match the parameters
All records	Displays all entries in the table.
RoleCombination	Enter the role combination values associated with the interface to display in the table.
QueueSet	Enter the queue set values associated with the interface to display in the table.

Displaying priority queue assignments

Device Manager allows for the display Priority Q Assignments.

To display priority queue assignments:

Procedure steps

Step	Action
1	Open the **QosDevice** screen by selecting **QoS > QoS Devices** from the menu. Select the **Priority Q Assign** tab.

—End—

Variable definitions

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

Filtering priority queue assignments

The priority queue assignments table can be filtered to display only those records that are of interest. To filter the priority queue assignments table, follow this procedure:

Procedure steps

Step Action

1 Open the **QosDevice** screen by selecting **QoS > QoS Devices** from the menu. Select the **Priority Q Assign** tab.

2 Click **Filter**.

The **Insert Filter** dialog opens.

3 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.

4 Click **Filter**.

—End—

Displaying priority mapping

Device Manager lets you display priority mapping.

To display priority mapping:

Procedure steps

Step **Action**

1 Open the **QosDevice** screen by selecting **QoS > QoS Devices** from the menu. Select the **Priority Mapping** tab.

—End—

Variable definitions

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

Displaying DSCP mappings

Device Manager lets you display DSCP mapping.

To display DSCP mappings:

Procedure steps

Step	Action
1	Open the **QosDevice** screen by selecting **QoS > QoS Devices** from the menu. Select the **DSCP** tab.

—End—

Variable definitions

Variable	Value
Dscp	Shows the DSCP value. This field is read-only.
802.1pPriority	Displays the user priority value associated with the DSCP. To change a value, double-click in the cell and edit the value. The valid range is 0..7.
DropPrecedence	The drop precedence setting. The available settings are: • lowDropPrec • highDropPrec Traffic associated with low drop precedence is generally given priority over traffic with high drop precedence during resource allocation. To change the setting, click in a cell and choose the setting.
ServiceClass	Specifies the type of service.

Displaying Meter Capability

To display QoS interface meter capabilities, use the following procedure.

Procedure steps

Step	Action
1	From the Device Manager main menu, select **QoS >QoS Devices**. The **QoSDevice** dialog box appears with the Interface Queue tab open.
2	Select the **Meter Capability** tab.

—End—

Variable definitions

Variable	Value
Port	The port to which the meter is applied.
MeterSupport	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

Use the following procedure to configure Meter Capability filtering.

Procedure steps

Step	Action
1	Click the **Filter** button to set Meter Capability table view filtering criteria. The **QOSDevice, Meter Capability - Filter** dialog opens.
2	Select filtering criteria and enter port, meter support, and meter rate parameters.
3	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—

Displaying Shaper Capability

To display QoS interface shaper capabilities, use the following procedure.

Procedure steps

Step	Action
1	From the Device Manager main menu, select **QoS > QoS Devices**. The **QOSDevice** dialog appears with the Interface Queue tab open.
2	Select the **Shaper Capability** tab. The **Shaper Capability** tab appears.

—End—

Variable definitions

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

Shaper Capability filtering

Use the following procedure to configure Shaper Capability filtering.

Procedure steps

Step	Action
1	Click the **Filter** button to set Shaper Capability table filtering. The **QOSDevice, Shaper Capability - Filter** dialog opens.
2	Select filtering criteria and enter port, meter support, and meter rate parameters.
3	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—

Managing QoS rules

This section discusses the management of QoS rules using the DM.

Displaying IP classifier elements

To display the IP classifier elements:

Procedure steps

Step	Action
1	Open the **QosRules** screen by selecting **QoS > QoS Rules** from the menu. The **IP Classifier Element** tab is selected.

—End—

Variable definitions

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 a packet's destination IP address.
DstMaskLength	Specifies the length of the destination address mask.
SrcAddr	Specifies the IP address to match against a packet's source IP address.
SrcMasklength	Specifies the length of the source address mask.
Dscp	Specifies the value for the DSCP in a packet.
Version	Specifies the version type.
Protocol/NextHeader	Specifies the IP protocol value.
DstL4Port	Specifies the value for the Layer 4 destination port number in a packet.
SrcL4Port	Specifies the value for the Layer 4 source port number in a packet.
IPv6FlowId	Specifies the flow identifier for IPv6 packets.

Variable	Value
SessionId	Specifies the session identification number.
Storage	Specifies the type of storage: • volatile • nonVolatile (default) • readOnly

Adding IP classifier elements

Device Manager lets you add the IP classifier elements.

To add an IP classifier element:

Procedure steps

Step	Action
1	Open the **QosRules** screen by selecting **QoS > QoS Rules** from the menu. The **IP Classifier Element** tab is selected.
2	Click **Insert**. The **Insert IP Classifier Element** screen opens.
3	Enter the information you want to use for this IP classifier element.
4	Click Insert.

—End—

Deleting IP classifier elements

Device Manager lets you delete IP classifier elements.

To delete an IP classifier element:

Procedure steps

Step	Action
1	Open the **QosRules** screen by selecting **QoS > QoS Rules** from the menu. The **IP Classifier Element** tab is selected.

2 Highlight the IP classifier element to delete.

3 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—

Displaying L2 classifier elements

Device Manager lets you display classifiers.

To display L2 classifiers:

Procedure steps

Step Action

1 Open the**QosRules** screen by selecting **QoS > QoS Rules** from the menu. Select the **L2 Classifier Element** tab.

—End—

Variable definitions

Variable	Value
Id	Specifies the index that enumerates the classifier entries.
Name	Specifies the L2 Classifier Element name.
DstMacAddr	Specifies the MAC address against which the MAC destination address of incoming packets will be compared
DstMacAddrMask	Specifies a mask identifying the destination MAC address.
SrcMacAddr	Specifies the MAC source address of incoming packets.
SrcMacAddrMask	Specifies a mask identifying the source MAC address.
VlanId	Specifies the value for the VLAN ID in a packet.

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

Adding L2 classifier elements

Use the following procedure to add L2 classifier elements:

Procedure steps

Step	Action
1	Open the **QosRules** screen by selecting **QoS > QoS Rules** from the menu. Select the **L2 Classifier Element** tab.
2	Click **Insert**. TheInsert **L2 Classifier Element** dialog opens.
3	Enter the information to use for this L2 classifier element.
4	Click **Insert**.

—End—

Deleting L2 classifier elements

Device Manager lets you delete L2 classifier elements.

To delete a L2 classifier elements:

Procedure steps

Step	Action
1	Open the **QosRules** screen by selecting **QoS > QoS Rules** from the menu. Select the **L2 Classifier Element** tab.
2	Highlight any table cell of the L2 classifier element to delete.
3	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**.

—End—

Displaying System Classifier Elements

Device Manager lets you display classifiers.

To display System Classifier Elements:

Procedure steps

Step	Action
1	Open the **QosRules** screen by selecting **QoS > QoS Rules** from the menu. Select the **System Clfr Element** tab.

—End—

Variable definitions

Variable	Value
Id	The index that enumerates the system classifier entries.
UnknownUcastFrames	If true(1), frames containing an unknown unicast destination address will match this classification entry. A value of false(2) indicates that no classification is requested based on this address type.

Variable	Value
UnknownMcastFrames	If true(1), frames containing an unknown multicast destination address will match this classification entry. A value of false(2) indicates that no classification is requested based on this address type.
KnownMcastFrames	If true(1), frames containing a known multicast destination address will match this classification entry. A value of false(2) indicates that no classification is requested based on this address type
PatternFormat	This field indicates the data link layer packet format that is used when specifying pattern match data. A value of untagged (1) indicates that the specified pattern match data does not include an 802.1Q tag. A value of tagged (2) indicates that the specified pattern match data does include an 802.1Q tag. The default value is tagged (2).
SessionId	The number assigned to the session displays in this column.
Storage	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’.
PatternIPVersion	Specifies the pattern IP version.
Version	Specifies the version.

Viewing the System Classifier Pattern

Use the following procedure to view the System Classifier pattern:

Procedure steps

Step	Action
1	Open the **QosRules** screen by selecting **QoS > QoS Rules** from the menu. Select the **System Clfr Element** tab.
2	Highlight an entry in the **System Clfr Element** table.
3	Click **Pattern**. The **System Classifier Element # Pattern (Data/Position)** screen opens.

—End—

Adding System Classifier Elements

Use the following procedure to add System Classifier Elements:

Procedure steps

Step	Action
1	Open the **QosRules** screen by selecting **QoS > QoS Rules** from the menu. Select the **System Clfr Element** tab.
2	Click **Insert**. The **Insert System Clfr Element** dialog opens.
3	Select the **DestAddressType**.
4	Type the**PatternData** or **PatternPosition** information manually. Alternatively, click on the ellipses to view the **Pattern** screen.
5	The **Pattern** screen configures the data and position of the pattern to be used by this system classifier.
6	The **System Classifier Element Pattern (Data/Position)** screen opens.
7	Select **IPv4, IPv6,** or **non-IP**.
8	Select **tagged** or **untagged**.
9	Select the version, 1 or 2. ***Note:*** This setting is only available on hybrid stacks to create system classifiers that can be used only on 5500 Series switches (version 1) or only on 5600 Series switches (version 2).
10	Select the required fields to set up a template guide so that it will be easier to configure the data and position of the pattern.
11	Type the desired **Data** and **Position** in two-digit hex number format.
12	Click **Ok**.
13	Click **Insert**.

—End—

Deleting System Classifier Elements

Use the following procedure to delete System Classifier Elements:

Procedure steps

Step	Action
1	Open the **QosRules** screen by selecting **QoS > QoS Rules** from the menu. Select the **System Clfr Element** tab.
2	Highlight the System Classifier Element to delete.
3	Click **Delete**.

—End—

Displaying Classifiers

Use the following procedure to display classifiers:

Procedure steps

Step	Action
1	Open the **QosRules** screen by selecting **QoS > QoS Rules** from the menu. Select the **Classifier** tab.

—End—

Variable definitions

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.

Variable	Value
SessionId	Specifies the numerical identification associated with the session.
Storage	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.

Adding classifiers

Use the following procedure to add classifiers.

Procedure steps

Step	Action

1 Open the **QosRules** screen by selecting **QoS > QoS Rules** from the menu. Select the **Classifier** tab.

2 Click **Insert**.

The **Insert Classifier** screen opens.

3 Type the name of the classifier element.

4 Select the **IP Classifier Element, L2 Classifier Element,** or **System Classifier Element**.

5 Click **Insert**.

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

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

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 should not be configured on the system element.

—End—

Deleting classifiers

Use the following procedure to delete classifiers.

Procedure steps

Step **Action**

1 Open the **QosRules** screen by selecting **QoS > QoS Rules** from the menu.Select the **Classifier** tab.

2 Highlight the classifier to delete.

3 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.

Procedure steps

Step **Action**

1 Open the **QosRules** screen by selecting **QoS > QoS Rules** from the menu. Select the **Classifier** tab.

2 Click **Filter**.

The **Insert Filter** screen opens.

3 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.

4 Click **Filter**.

—End—

Displaying Classifier Blocks

Use the following procedure to display classifier blocks:

Procedure steps

Step **Action**

1 Open the **QosRules** screen by selecting **QoS > QoS Rules** from the menu. Select the **Classifier Block** tab. the following illustration.

—End—

Variable definitions

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.

Variable	Value
ClassifierSetId	Displays the ID number assigned to that classifier (from the Classifier screen).
Meter	Displays the meter associated with the classifier block.
Action	Displays the action followed for those flows not being metered. (For those flows being metered, this attribute is not applied.)
SessionId	Displays the numerical identification for the current session.
Storage	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.

Appending Classifier Blocks

Use the following procedure to append a classifier block:

Procedure steps

Step	Action
1	Open the **QosRules** screen by selecting **QoS > QoS Rules** from the menu. Select the **Classifier** Block tab.
2	Click **Append Classifier**. The **Insert Classifier Block** dialog opens.
3	Select the Classifier to append to the Classifier Block.
4	Click **Insert**.

—End—

Adding Classifier Blocks

Use the following procedure to add classifier blocks.

Procedure steps

Step	Action

1 Open the **QosRules** screen by selecting **QoS > QoS Rules** from the menu. Select the **Classifier Block** tab.

2 Click **Insert**.

The **Insert Classifier Block** screen opens.

3 Enter the name of the classifier block.

4 Select the **Classifier, Meter**, and **Action**.

5 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

Use the following procedure to delete classifier blocks.

Procedure steps

Step	Action

1 Open the **QosRules** screen by selecting **QoS > QoS Rules** from the menu.Select the **Classifier Block** tab.

2 Highlight the classifier block to delete.

3 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**.

—End—

Filtering Classifier Blocks

Use the following procedure to filter a classifier block:

Procedure steps

Step	Action
1	Open the **QosRules** screen by selecting **QoS > QoS Rules** from the menu. Select the **Classifier Block** tab.
2	Click **Filter**. The **QOSRules Classifier Block - Filter** dialog opens .
3	Select the filtering condition, case, and column criteria.
4	Enter the **BlockNum** and **Name**.
5	Click **Filter**.

—End—

Managing QoS actions, Interface action extensions, Meters, Policies, Interface Shapers, and Interface Applications

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

Displaying QoS actions

Use the following procedure to display a QoS action:

Procedure steps

Step	Action
1	Open the **QoS** screen by selecting **QoS > QoS** from the menu. Select the **Action** tab.

—End—

Variable definitions

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

Adding QoS actions

Use the following procedure to add a QoS action:

Procedure steps

Step	Action
1	Open the **QoS** screen by selecting **QoS > QoS** from the menu. Select the **Action** tab.
2	Click **Insert**. The **Insert Action** dialog opens.
3	Enter the information and select the parameters to use for this QoS action.
4	Click **Insert**.

—End—

Deleting QoS actions

Use the following procedure to delete a QoS action:

Procedure steps

Step	Action
1	Open the **QoS** screen by selecting **QoS > QoS** from the menu. Select the **Action** tab.
2	Highlight the QoS action to delete.
3	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—

Displaying Interface action extensions

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

Procedure steps

Step	Action
1	Open the **QoS** screen by selecting **QoS > QoS** from the menu. Select the **Interface Action Ext** tab.

—End—

Variable definitions

Variable	Value
Id	Specifies the number of the interface action extension.
Name	Specifies a label for the interface action extension.
SetEgressUnicastPort	Specifies redirection of normally-switched unicast packets to a specified interface.

Variable	Value
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 non-volatile.

Adding Interface action extensions

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

Procedure steps

Step	Action
1	Open the **QoS** screen by selecting **QoS > QoS** from the menu. Select the **Interface Action Ext** tab.
2	Click **Insert**. The **Insert Interface Action Ext** screen opens.
3	Enter the information and make the selections to use for this Interface action extension.
4	Click **Insert**.

—End—

Deleting Interface action extensions

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

Procedure steps

Step	Action
1	Open the **QoS** screen by selecting **QoS > QoS** from the menu. Select the **Interface Action Ext** tab.
2	Highlight the interface action extension to delete.
3	Click **Delete**. ***Note:*** A QoS interface action extension that is referenced by an action entry cannot be deleted. First delete the action.

—End—

Displaying QoS meters

Use the following procedure to display a QoS meter:

Procedure steps

Step **Action**

1 Open the **QoS** screen by selecting **QoS > QoS** from the menu. Select the **Meter** tab.

—End—

Variable definitions

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

Adding QoS meters

Use the following procedure to add a QoS meter:

Procedure steps

Step **Action**

1 Open the **QoS** screen by selecting **QoS > QoS** from the menu. Select the **Meter** tab.

2 Click **Insert**.

The **Insert Meter** dialog opens.

3 Enter the information and make the selections to use for this QoS meter.

4 Click **Insert**.

—End—

Deleting QoS meters

Use the following procedure to delete QoS meters.

Procedure steps

Step **Action**

1 Open the **QoS** screen by selecting **QoS > QoS** from the menu. Select the **Meter** tab.

2 Highlight the QoS meter to delete.

3 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—

Displaying QoS Interface Shapers

Use the following procedure to display QoS policies.

Procedure steps

Step **Action**

1 Open the **QoS** screen by selecting **QoS > QoS** from the menu. Select the **Interface Shaper** tab.

—End—

Variable definitions

Variable	Value
Port	The port associated with interface shaping.
Name	The name applied to the interface shaping data.

Variable	Value
ShapingRate	The token-bucket rate, in kilobits per second (kbps). This attribute is used for CIR for Simple Token Bucket CIR in RFC 2697 for srTCM CIR and PIR in RFC 2698 for trTCM CTR and PTR in RFC 2859 for TSWTCM AverageRate in RFC 3290.
BurstSize	The maximum number of bytes in a single transmission burst. This attribute is used for Token bucket size for Simple Token Bucket CBS and EBS in RFC 2697 for srTCM CBS and PBS in RFC 2698 for trTCM Burst Size in RFC 3290.

Adding Interface Shapers

Use the following procedure to add QoS Interface Shapers:

Procedure steps

Step	Action
1	Open the **QoS** screen by selecting **QoS > QoS** from the menu. Select the **Interface Shaper** tab.
2	Click **Insert**. The **Insert Interface Shaper** screen opens.
3	Click the ellipses to select the ports for the interface shaper. The **ntnQoSIfShapingPorts** screen opens.
4	Select the required ports.
5	Click **Ok**.
6	Type the **Label**, **Shapingrate**, and **MaximumBurstRate**.
7	Select the **Duration** in milliseconds.
8	Click **Insert**.

—End—

Deleting an Interface Shaper

Use the following procedure to delete an Interface Shaper.

Procedure steps

Step	Action
1	Open the **QoS** screen by selecting **QoS > QoS** from the menu. Select the **Interface Shaper** tab.
2	Highlight the Interface Shaper that to delete.
3	Click **Delete**.

—End—

Displaying QoS policies

Use the following procedure to display QoS policies.

Procedure steps

Step	Action
1	Open the **QoS** screen by selecting **QoS > QoS** from the menu. Select the **Policy** tab.

—End—

Variable definitions

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 (refer to "Managing interface groups" (page 139)) prior to associating it with a policy.

Variable	Value
InterfaceIndex	The ifIndex field identifies the interface to which the policy is to be applied. A policy is associated with an interface explicitly using this attribute or implicitly using a role combination through the ntnQosPolicyInterfaceRole attribute. An interface must be identified by one and only one of these attributes. This attribute can identify an interface that does not currently exist in the system, as long as the specified interface index represents a potentially valid system interface. ***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.

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

Adding QoS policies

Use the following procedure to add QoS policies.

Procedure steps

Step	Action
1	Open the **QoS** screen by selecting **QoS > QoS** from the menu. Select the **Policy** tab.
2	Click **Insert**. The **Insert QoS Policy** screen opens.
3	Enter the information to use for this QoS policy.
4	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—

Deleting QoS policies

Use the following procedure to delete QoS policies.

Procedure steps

Step	Action
1	Open the **QoS** screen by selecting **QoS > QoS** from the menu. Select the **Policy** tab.
2	Highlight the QoS policy to delete.
3	Click **Delete**.

—End—

QoS Policy Stats

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

Procedure steps

Step	Action
1	Select **QoS > QoS** from the Device Manager main menu.
2	Select the **Policy** tab.
3	Select a policy from the list.
4	Click **Graph**. The **Policy Aggregate Stats** window opens.

—End—

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

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

If the Policy Stats type is set to individual, the individual stats, consisting of in-profile and out-profile packets, appears. If policy meter is set to none, no out-profile packet information is available. **TIP**: Individual stats are provided per policy, per filter, per port.

Viewing QoS Interface Applications

> ***Note:*** Due to hardware limitations, the Ethernet Routing Switch 5500 Series switch supports only 11 interface applications per port.

Use the following procedure to view configured QoS interface applications

Procedure steps

Step	Action
1	Open the **QoS** screen by selecting **QoS > QoS** from the menu. Select the **Interface Apps** tab.

—End—

Variable definitions

Variable	Value
IfIndex	The ports that this QoS application applies to.
AppEnable	The applications enabled for the interface (port) specified in IfIndex field.
DefaultGateway	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**.

Variable	Value
	3. Double-click the **AppEnable** field, select **arpSpoofing**, and edit the **DefaultGateway** field. 4. Click **Apply**.
IfType	The interface type configured for the **dhcpSnooping** application.
DHCPServer	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: 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**.

Adding an Interface Application

Use the following procedure to add an Interface Application.

Procedure steps

Step	Action
1	Open the **QoS** screen by selecting **QoS > QoS** from the menu. Select the **Interface Apps** tab.
2	Click **Insert**. The **Insert Interface Apps** screen opens.
3	In the fields provided, enter the information for the new entry.
4	Click **Insert**. The new Interface Application entry is displayed on the **Interface App** tab.

—End—

Variable definitions

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	The default gateway configured for the **arpSpoofing** application.
IfType	The interface type configured for the **dhcpSnooping** application.
DHCPServer	The DHCP server configured for the **dhcpSpoofing** application.

Deleting an Interface Application

Use the following procedure to delete an Interface Application.

Procedure steps

Step	Action
1	Open the**QoS** screen by selecting **QoS > QoS** from the menu. Select the **Interface Apps** tab.
2	Select the Interface Application to delete.
3	Click **Delete**.

—End—

Configuring User Based Policies and the Nortel SNA solution

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.

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** dialog box.

Inserting a classifier

Use the following procedure to configure a classifier for the Nortel SNA solution or a User Based Policy:

Procedure steps

Step	Action
1	Select **QoS > QoS NSNA/UBP** from the Device Manager menu. The **QOS_NSNA_UBP** dialog box opens with the **Classifier** tab selected.
2	Click **Insert**. The **QOS_NSNA_UBP, Insert Classifier** dialog box opens.
3	Using the **Type** radio options, choose whether to create a classifier for the Nortel SNA solution (**NsnaClfr**) or for a User Based Policy (**UbpClfr**).
4	Enter the classifier information in the fields.
5	Change values in any fields that present default values if you want to configure specific parameters.
6	Click **Insert**. The information for the classifier appears in the **Classifier** tab of the **QOS_NSNA_UBP** dialog box.

—End—

Variable definitions

Variable	Value
Id	Specifies the ID number of the classifier.
Type	The type of classifier. Options are NSNA and UBP.
Name	Specifies the name of the classifier. All classifiers with the same name are part of the same filter set. That filter set has the same name as the classifiers.

Variable	Value
Block	Specifies the block name with which the classifier is associated.
EvalPrec	Specifies the evaluation order number of the classifier in that filter set. Two classifiers in the same filter set cannot have the same evaluation order. A higher eval order means a lower precedence for the corresponding policy.
AddrType	Specifies the type of IP address used by this classifier entry.
DstIpAddr	Specifies the IP address to match against the destination IP address of a packet.
DstIpPrefixLength	Specifies the length of the destination address mask.
SrcIpAddr	Specifies the IP address to match against the source IP address of a packet.
SrcIpPrefixLength	Specifies the length of the source address mask.
Dscp	Specifies the value for a DiffServ Codepoint (DSCP) in a packet.
Protocol/NextHeader	Specifies the IPv4 protocol value, or the IPv6 next-header value. Values are the following: • 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	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.

Variable	Value
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.
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).

Deleting a classifier

Use the following procedure to delete a classifier.

Procedure steps

Step	Action
1	Select **QoS > QoS NSNA/UBP** from the Device Manager menu. The **QOS_NSNA_UBP** dialog box opens with the Classifier tab selected.
2	Select the classifier you want to delete.
3	Click **Delete**.

—End—

Configuring a set

Use the following procedure to configure a set:

Procedure steps

Step	Action
1	Select **QoS > Qos NSNA/UBP** from the Device Manager menu. The **QOS_NSNA_UBP** dialog box opens with the Classifier tab selected.
2	Click the **Set** tab. The **Set** tab is selected.
3	Click **Insert**. The **QOS_NSNA_UBP, Insert Set** dialog box opens.
4	Enter the set information in the fields.
5	Click **Insert**. The information for the set appears in the **Set** tab of the **QOS_NSNA_UBP** dialog box.

—End—

Variable definitions

Variable	Value
AclType	Specifies the type of ACL (NSNA or UBP).
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.
CommittedRate	Specifies the committed rate (in Kbps).
BurstSize	Specifies the maximum number of bytes in a single transmission burst.

Variable	Value
OutActionDrop	Specifies the action to take when packet is out-of-profile. This action is applied only if metering is being enforced, and if the traffic is deemed out-of-profile based on the level of traffic and the metering criteria. (Metering is applied only to traffic matching the filtering data.) Options are the following: • drop (packet is dropped) • pass (packet is not dropped) The default value is **pass**.
NonMatchActionDrop	Specifies the action to take when a packet is non-matching. This action is applied to all traffic that was not previously matched by the specified filtering data. Options are the following: • drop (packet is dropped) • pass (packet not dropped) • defer (no explicit drop/pass action is specified; the decision is deferred) The default value is **defer**.
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 to 63.
SetPriority	Specifies the priority in the range 1 to 255.
Storage	Specifies the type of storage.

Deleting a set

Use the following procedure to delete a QoS NSNA UBP set.

Procedure steps

Step	Action
1	From the Device Manager main menu, select **QoS**. The QoS menu appears.
2	Select **QoS_NSNA/UBP**. The QOS_NSNA_UBP window opens with the Classifier tab open.

3 Click the **Set** tab. The Set dialog opens.

4 Select a set to delete.

5 Click **Delete**.

—End—

Filtering a set

Use the following procedure to filter a QoS NSNA UBP set.

Procedure steps

Step	Action
1	From the Device Manager main menu, select **QoS**. The QoS menu appears.
2	Select **QoS_NSNA/UBP**. The QOS_NSNA_UBP window opens with the Classifier tab open.
3	Click the **Set** tab. The Set dialog opens.
4	Select a set to filter.
5	Click **Filter**. The QOS_NSNA_UBP, Set - Filter dialog opens.
6	Set the filter parameters in the dialog.
7	Click **Filter**.

—End—

Displaying User Based Policy session information

Use the following procedure to view user based policy information for the active session.

Procedure steps

Step	Action
1	Select **QoS > QoS** from the Device Manager menu. The **QoS** window appears with the **Action** tab open.
2	Select the **User Based Policy** tab.

—End—

Variable definitions

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.
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

This section contains information on working with QoS agents.

Displaying QoS agent configuration

Use the following procedure to display QoS agent configuration:

Procedure steps

Step	Action
1	Open the**QoSAgent** screen by selecting **QoS > QoS Agent** from the menu.Select the **Configuration** tab.

—End—

Variable definitions

Variable	Value
NVRamCommitDelay	Specifies the maximum time before non-volatile QoS data is written to NVRAM.
ResetToDefaults	Click to reset all policy information to factory default values.
QueueCfg	Determines the queue set that is associated with all egress interfaces by default. You must restart the system if you change the current attribute.
BufferingCaps	The value of this attribute 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. You must restart the system if you change the current attribute.
UBPSupportLevel	The value of this attribute sets the level of User Based Policy support.
TrackStatistics	Specifies the type of statistics tracking.
NTApplicationMode	Specifies the behavior of NT application mode.

Displaying policy class support

Use the following procedure to display policy class support:

Procedure steps

Step	Action
1	Open the**QoSAgent** screen by selecting **QoS > QoS Agent** from the menu. Select the **Policy Class Support** tab.

—End—

Variable definitions

Variable	Value
PolicyClassName	Identifies the Policy Rule Classes (PRCs) supported by the device. A PRC is synonymous to a MIB table; therefore, the supported PRCs indicate which MIB tables are supported for QoS processing purposes.
CurrentInstances	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	The maximum number of PRIs that can be installed and/or modified by a user for a specific PRC (equates to the number of MIB table entries that can be created or modified by a user).

Displaying policy device identification

Use the following procedure to display policy device identification data.

Procedure steps

Step	Action
1	Open the **QoSAgent** screen by selecting **QoS > QoS Agent** from the menu. Select the **Policy Device Identification** tab.

—End—

Variable definitions

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	The maximum message size in octets that the device can support.

Displaying resource allocation on the 5500 Series switch

Use the following procedure to display QoS diagnostics information for the 5500 Series switch.

Procedure steps

Step	Action
1	Open the **QoSAgent** screen by selecting **QoS > QoS Agent** from the menu. Select the **Resource Allocation (ERS5500)** tab.

—End—

Variable definitions

Variable	Value
Port	Identifies the interface unit and port.
MasksConsumed	Displays the number of classification masks in use by policy and filter data by that interface.
FiltersConsumed	Displays the number of rules (filters) in use by policy and filter data by that interface.
MetersConsumed	Displays the number of meters in use by policy data by that interface.
CountersConsumed	Displays the number of counters in use by that interface.
NonQosMasksConsumed	Displays the number of classification masks in use *not* from policy and filter data by that interface.

Variable	Value
NonQosFiltersConsumed	Displays the number of rules (filters) in use *not* from policy and filter data by that interface.
NonQosMetersConsumed	Displays the number of meters in use *not* from policy data by that interface. These are meter resources used by other applications besides QoS; none of these are currently supported on the 5000 Series switch.

Displaying resource allocation on the 5600 Series switch

Use the following procedure to display QoS resource Allocation information on the 5600 Series switch.

Procedure steps

Step	Action
1	Open the **QoSAgent** screen by selecting **QoS > QoS Agent** from the menu. Select the **Resource Allocation (ERS5600)** tab.

—End—

Variable Definitions

Field	Description
Precedence	Displays the applied precedence (from 1 to 8).
Port	Displays the Port number.
FiltersConsumed	Displays the number of rules (filters) in use by policy and filter data by that interface.
MetersConsumed	Displays the number of meters in use by policy data by that interface.
CountersConsumed	Displays the number of counters in use by that interface.
NonQosFiltersConsumed	Tracks the current number of filters in use, not due to installed 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).

Field	Description
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.

Filtering the resource allocation table

To filter the resource allocation table, use this procedure.

Procedure steps

Step	Action
1	Select **QoS > QoS Agent**.
2	Select the **Resource Allocation** tab.
3	Click **Filter**.
4	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.
5	Click **Filter.**

—End—

Configuring DoS Attack Prevention Package

This section contains procedures used to configure the DoS Attack Prevention Package (DAPP).

Enabling DAPP

This procedure describes the steps necessary to enable DAPP.

Procedure steps

Step **Action**

1 From the Device Manager main window, choose **QoS > QoS Agent**
The **QOSAgent** window opens.

2 On the Configuration tab, under the **DAPP** section, choose the mode for DAPP enabling.

- **disable** (Default) - Disables DAPP.
- **enableWithoutStatusTracking** - Enables DAPP without enabling status tracking.
- **enableWithStatusTracking** - Enables DAPP and enables status tracking.

3 Click **Apply**.

4 Click **Close**.

—End—

Configuring DAPP minimum TCP header size

This procedure describes how to set the minimum TCP header size used by DAPP.

Procedure steps

Step **Action**

1 From the Device Manager main window, choose **QoS > QoS Agent**
The **QOSAgent** window opens.

2 On the Configuration tab, under the **DAPP** section, enter a value in the range 0 to 255 in the **DappMinTspHdrSize** text box.

3 Click **Apply**.

4 Click **Close**.

—End—

Configuring DAPP maximum IPv4 ICMP length

This procedure describes how to set the maximum IPv4 ICMP length used by DAPP.

Procedure steps

Step	Action
1	From the Device Manager main window, choose **QoS > QoS Agent** The **QOSAgent** window opens.
2	On the Configuration tab, under the **DAPP** section, enter a value in the range 0 to 1023 in the **DappIpv4IcmpMaxLength** text box.
3	Click **Apply**.
4	Click **Close**.

—End—

Configuring DAPP maximum IPv6 ICMP length

This procedure describes how to set the maximum IPv6 ICMP length used by DAPP.

Procedure steps

Step	Action
1	From the Device Manager main window, choose **QoS > QoS Agent** The **QOSAgent** window opens.
2	On the Configuration tab, under the **DAPP** section, enter a value in the range 0 to 16383 in the **DappIpv6IcmpMaxLength** text box.
3	Click **Apply**.
4	Click **Close**.

—End—

Nortel Ethernet Routing Switch 5000 Series

Configuration - Quality of Service

Publication: NN47200-504
Document status: Standard
Document version: 04.01
Document date: 12 November 2008

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.

Sourced in Canada and the United States of America.

The information in this document is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.