



Nortel Ethernet Routing Switch 5500 Series

Configuration - Quality of Service

Document status: Standard
Document version: 03.01
Document date: 27 August 2007

Copyright © 2005 - 2007, Nortel Networks
All Rights Reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks reserves the right to make changes to the products described in this document without notice.

Nortel Networks does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

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

a) 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).

b) 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.

c) 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.

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

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

f) 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.

Revision History

Date Revised	Version	Reason for revision
July 2005	1.00	New document for Software Release 4.2.
July 2006	2.00	Updated for software release 5.0
June 2007	3.01	Updated for software release 5.1
August 2007	3.01	Updated for software release 5.1

6 Revision History

Nortel Ethernet Routing Switch 5500 Series
Configuration - Quality of Service
NN47200-504 03.01 Standard
5.1 27 August 2007

Contents

Preface	13
Nortel Ethernet Routing Switch 5500 Series	13
Related Publications	14
How to get help	15
<hr/>	
An Introduction to Policy-Enabled Networks	17
Summary	17
Port-based and Role-based QoS Policies	18
QoS overview	18
DiffServ Concepts	19
QoS components	19
Specifying interface groups	21
Interface shaping	22
The Nortel SNA solution	22
User based policies	22
Rules	23
Classifier definition	23
IP classifier elements	24
Layer 2 classifier elements	24
System classifier elements	24
Classifiers and classifier blocks	25
Specifying actions	26
Specifying interface action extensions	28
Specifying meters	29
Trusted, untrusted, and unrestricted interfaces	30
Specifying policies	33
Packet flow using QoS	35
Queue sets	37
Modifying queue set characteristics	38
Modifying CoS-to-queue priorities	40
QoS configuration guidelines	40
Troubleshooting tips	40
QoS Interface Applications	40
ARP Spoofing	41

- DHCP Snooping 41
- DHCP Spoofing 41
- SQLSlam 42
- Nachia 42
- Xmas 42
- TCP SynFinScan 42
- TCP FtpPort 42
- TCP DnsPort 43
- BPDU Blocker 43

Configuring Quality of Service (QoS) with the CLI	45
Displaying QoS Parameters	45
Configuring QoS Access Lists	51
qos acl-assign command	51
no qos acl-assign command	52
qos ip-acl command	53
no qos ip-acl command	54
qos l2-acl command	54
no qos l2-acl command	56
Configuring QoS Security	56
qos arp spoofing command	56
no qos arp spoofing command	57
qos bpdu blocker command	57
no qos bpdu blocker command	57
qos dhcp command	58
no qos dhcp command	58
qos dos command	59
no qos dos command	59
Configuring and Modifying Default Queue Set	60
default qos agent command	60
qos agent queue-set command	61
Configuring Default Buffering Capabilities	61
default qos agent buffer command	61
qos agent buffer command	62
Configuring the CoS-to-Queue Assignments	62
qos queue-set-assignment command	62
Configuring QoS Interface Groups	63
qos if-assign command	63
no qos if-assign command	63
qos if-group command	64
no qos if-group command	64
Configuring DSCP and 802.1p and Queue Associations	65
qos egressmap command	65
default qos egressmap command	65

qos ingressmap command	66
default qos ingress command	66
Configuring QoS Elements, Classifiers, and Classifier Blocks	66
qos ip-element command	67
no qos ip-element command	68
qos l2-element command	68
no qos l2-element command	70
qos classifier command	70
no qos classifier command	71
qos classifier-block command	71
no qos classifier-block command	72
Configuring QoS system-element	72
qos system-element command	72
no qos system-element command	73
Configuring QoS Actions	74
qos action command	74
no qos action command	75
Configuring QoS Interface Action Extensions	76
qos if-action-extension command	76
no qos if-action-extension command	76
Configuring QoS Meters	77
qos meter command	77
no qos meter command	78
Configuring QoS Interface Shaper	78
qos if-shaper command	78
no qos if-shaper command	79
Configuring QoS Policies	79
qos policy command	79
no qos policy command	82
Configuring QoS for the Nortel SNA solution	82
Example: using qos nsna commands	84
Deleting a classifier, classifier block, or an entire filter set	85
Viewing filter descriptions	85
Configuring User Based Policies	87
Example: using qos ubp commands	89
Deleting a classifier, classifier block, or an entire filter set	90
Viewing filter descriptions	91
Maintaining the QoS Agent	91
qos agent reset-default command	91
qos agent nvram-delay command	91
default qos agent nvram-delay	92
default qos agent command	92

Configuring Quality of Service (QoS) with the Web-based Management Interface	93
Quality of Service Wizards	93
QoS Configuration Wizard	94
QoS Management Wizard	105
QoS Interface Shaper Wizard	109
QoS Interface Applications Wizard	110
Configuring an Interface Group	112
Creating an Interface Group Configuration	112
Displaying Interface ID Table	113
Adding or Removing Interface Group Members	114
Deleting an Interface Group	115
Configuring 802.1p priority queue assignment	116
Configuring 802.1p priority mapping	117
Configuring DSCP mapping	118
Displaying QoS Meter Capability	120
Displaying QoS shaper capability	121
Configuring IP classifier elements	122
Creating an IP classifier element	122
Deleting an IP classifier element configuration	123
Configuring Layer 2 classifier elements	124
Creating a Layer 2 classifier element configuration	124
Deleting a layer 2 classifier element configuration	125
Configuring System Classifier Element	125
Classifier Configurations	127
Viewing Existing Classifiers	127
Creating a Classifier	128
Deleting a classifier	128
Classifier Block Configurations	129
Viewing Classifier Blocks	129
Creating Classifier Blocks	130
Deleting a Classifier Block	130
Configuring QoS actions	131
Creating an Action	131
Modifying an action configuration	133
Deleting an Action	134
Using the Interface Action Extension	134
Creating an Interface Action Extension	134
Deleting an interface action extension configuration	136
Using QoS Meters	136
Creating a QoS Meter	136
Viewing meters	138

Deleting a meter	138
Configuring QoS Interface Shaper	138
Configuring Interface Shaping parameters	138
Deleting Interface Shaping Parameters	140
Configuring QoS policies	140
Installing defined filters	140
Viewing hardware policy statistics	142
Deleting a hardware policy configuration	143
Configuring QoS Policy Agent (QPA) characteristics	144
Using QoS diagnostics	145

Configuring Quality of Service (QoS) with the Java Device Manager (JDM) 151

Managing interface groups	151
Displaying interface queues	151
Displaying interface groups	153
Assigning ports to an interface group	154
Deleting ports from an interface group	155
Adding interface groups	156
Deleting interface groups	157
Displaying an interface ID	157
Displaying priority queue assignments	161
Displaying priority mapping	163
Displaying DSCP mappings	164
Displaying Meter Capability	166
Meter Capability filtering	167
Displaying Shaper Capability	167
Shaper Capability filtering	168
Managing QoS rules	169
Displaying IP classifier elements	169
Adding IP classifier elements	170
Deleting IP classifier elements	171
Displaying L2 classifier elements	172
Adding L2 classifier elements	173
Deleting L2 classifier elements	174
Displaying System Classifier Elements	175
Viewing the System Classifier Pattern	176
Adding System Classifier Elements	177
Deleting System Classifier Elements	179
Displaying Classifiers	179
Adding classifiers	181
Deleting classifiers	182
Filtering Classifiers	183
Displaying Classifier Blocks	184

Appending Classifier Blocks	185
Adding Classifier Blocks	186
Deleting Classifier Blocks	187
Filtering Classifier Blocks	188
Managing QoS actions, Interface action extensions, Meters, Policies, Interface Shapers, and Interface Applications	189
Displaying QoS actions	189
Adding QoS actions	190
Deleting QoS actions	191
Displaying Interface action extensions	192
Adding Interface action extensions	193
Deleting Interface action extensions	194
Displaying QoS meters	194
Adding QoS meters	195
Deleting QoS meters	196
Displaying QoS Interface Shapers	197
Adding Interface Shapers	198
Deleting an Interface Shaper	199
Displaying QoS policies	199
Adding QoS policies	202
Deleting QoS policies	203
QoS Policy Stats	204
Viewing QoS Interface Applications	204
Adding an Interface Application	206
Deleting an Interface Application	207
Configuring User Based Policies and the Nortel SNA solution	208
Inserting a classifier	208
Deleting a classifier	211
Configuring a set	212
Displaying User Based Policy session information	215
QoS agent	216
Displaying QoS agent configuration	217
Displaying policy class support	218
Displaying policy device identification	220
Displaying diagnostics	221

Index

223

Preface

This guide provides information and instructions on the configuration of quality of service and IP filtering on the 5500 Series Nortel Ethernet Routing Switch. Please consult any documentation included with the switch and the product release notes (see "[Related Publications](#)" (page 14)) for any errata before beginning the configuration process.

Nortel Ethernet Routing Switch 5500 Series

"[5500 Series Switch Platforms](#)" (page 13) outlines the switches that are part of the 5500 Series of Nortel Ethernet Routing Switches

5500 Series Switch Platforms

5500 Series Switch Model	Key Features
Nortel Ethernet Routing Switch 5510-24T	A 24 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch. This switch contains two shared SFP ports.
Nortel Ethernet Routing Switch 5510-48T	A 48 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch. This switch contains two shared SFP ports.
Nortel Ethernet Routing Switch 5520-24T-PWR	A 24 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch with full Power over Ethernet (PoE) capability on all copper ports. This switch contains four shared SFP ports.
Nortel Ethernet Routing Switch 5520-48T-PWR	A 48 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch with full Power over Ethernet (PoE) capability on all copper ports. This switch contains four shared SFP ports.
Nortel Ethernet Routing Switch 5530-24TFD	A 24 port, 10/100/1GBase-T, Layer 4, diffserv-capable, stackable Ethernet switch. This switch contains twelve shared SFP ports and two XFP ports.

Related Publications

For more information about the management, configuration, and usage of the Nortel Ethernet Routing Switch 5500 Series, refer to the publications listed in "[Nortel Ethernet Routing Switch 5500 Series Documentation](#)" (page 14).

Nortel Ethernet Routing Switch 5500 Series Documentation

Title	Description	Part Number
<i>Nortel Ethernet Routing Switch 5500 Series Installation</i>	Instructions for the installation of a switch in the Nortel Ethernet Routing Switch 5500 Series. It also provides an overview of hardware key to the installation, configuration, and maintenance of the switch.	NN47200-300
<i>Nortel Ethernet Routing Switch 5500 Series Overview - System Configuration</i>	Instructions for the general configuration of switches in the 5500 Series that are not covered by the other documentation.	NN47200-500
<i>Nortel Ethernet Routing Switch 5500 Series Security - Configuration</i>	Instructions for the configuration and management of security for switches in the 5500 Series.	NN47200-501
<i>Nortel Ethernet Routing Switch 5500 Series Configuration - VLANs, Spanning Tree, and MultiLink Trunking</i>	Instructions for the configuration of spanning and trunking protocols on 5500 Series switches.	NN47200-502
<i>Nortel Ethernet Routing Switch 5500 Series Configuration - IP Routing</i>	Instructions for the configuration of IP routing protocols on 5500 Series switches.	NN47200-503
<i>Nortel Ethernet Routing Switch 5500 Series Configuration - Quality of Service</i>	Instructions for the configuration and implementation of QoS and filtering on 5500 Series switches.	NN47200-504
<i>Nortel Ethernet Routing Switch 5500 Series Configuration - System Monitoring</i>	Instructions for the configuration, implementation, and usage of system monitoring on 5500 Series switches.	NN47200-505

Title	Description	Part Number
<i>Nortel Ethernet Routing Switch 5500 Series Release Notes - Software Release 5.1</i>	Overview of new features, fixes, and limitations of the 5500 Series switches. Also includes supplementary documentation and document errata.	NN47200-400
<i>Installing the Nortel Ethernet Redundant Power Supply Unit 15</i>	Instructions for the installation and usage of the Nortel Ethernet RPSU 15.	217070-A
<i>DC-DC Converter Module for the Baystack 5000 Series Switch</i>	Instructions for the installation and usage of the DC-DC power converter.	215081-A
<i>Installing SFP and XFP Transceivers and GBICs</i>	Instructions for the installation and usage of small form-factor pluggable transceivers and gigabit interface converters.	318034-C

All technical documentation can be accessed online at the Nortel Technical Support web site located at <http://www.nortel.com/support>. Use the following procedure to access documents on the Technical Support web site:

- If it is not already selected, click the **Browse product support** tab.
- From the list provided in the product family box, select **Nortel Ethernet Routing Switch**.
- From the product list, select the desired 5500 Series Switch.
- From the content list, select **Documentation**.
- Click **Go**.

Documentation can be viewed online, downloaded for future reference, or printed. All documents accessed on the Technical Support web site are in Adobe Portable Document Format (PDF) format. Adobe Acrobat Reader can be used to view and print these documents. Adobe Acrobat Reader is a free product of Adobe Systems and can be downloaded from the Adobe web site at <http://www.adobe.com>.

How to get help

If a service contract is purchased with this Nortel product from a distributor or authorized reseller, contact the technical support for that distributor or reseller for technical assistance.

If a Nortel service program is purchased with this product, contact Nortel Technical Support.

The following information is available online:

- contact information for Nortel Technical Support
- information about the Nortel Technical Solutions Centers
- information about the Express Routing Code (ERC) for your product

An Express Routing Code (ERC) is available for many Nortel products. When used, an ERC allows a technical assistance call to be routed to a technical support personnel who specialize in that service or product. The ERC for a particular product or service is available online.

The main Nortel support portal is available at <http://www.nortel.com/support>

An Introduction to Policy-Enabled Networks

This chapter provides an overview of the Differentiated Services (DiffServ) Quality of Service (QoS) network architecture. The Nortel Ethernet Routing Switch 5500 Series provides a Web-based Management Interface, Command Line Interface (CLI), and the Java Device Manager (JDM) 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

Software Release 5.0 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 was 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 5500 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.

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

Specifying interface groups

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

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

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

Note: 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.

Interface shaping

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

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

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

The Nortel SNA solution

The Ethernet Routing Switch 5500 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 5500 Series can be configured to manage access with user based policies. User based policies revolve around the new User Policy Table, which has been enhanced to support 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:

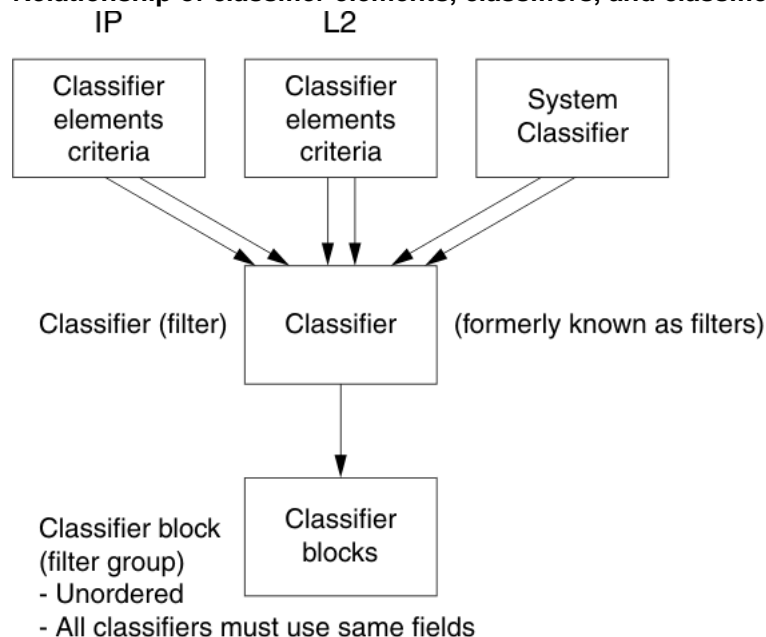
- Layer 2 (L2) classifier elements
- IP classifier elements
- System classifier

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.

"[Relationship of classifier elements, classifiers, and classifier blocks](#)" (page 23) displays the relationship between the classifier elements, classifiers, and classifier blocks.

Relationship of classifier elements, classifiers, and classifier blocks



11437EA

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

IP classifier elements

The Nortel Ethernet Routing Switch 5500 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 (range of)

Layer 2 classifier elements

The Nortel Ethernet Routing Switch 5500 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.

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, 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.

All classifiers that are part of a single classifier block (that is, with the same block number) must each filter on identically the same parameters at the packet level. This includes the same mask, range, and VLAN tag type. If this criterion is not met, an error message is generated 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).

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

Each classifier or classifier block is associated with actions that are executed when the packet matches the filter criteria in the group. The filter criteria and the associated actions, metering criteria, and interface groups are referenced by a policy, which dictates the overall traffic treatment (refer to ["Flowchart of QoS Actions"](#) (page 27) for an illustration of the traffic treatment).

Classifier elements, through individual classifiers or a classifier block, are associated with an interface group, action, and metering through a policy. Multiple policies can be applied to a given flow. The policy evaluation order is determined by the policy precedence. The order of precedence is from the highest precedence value to the lowest precedence (that is, a value of 8 is evaluated before a value of 7).

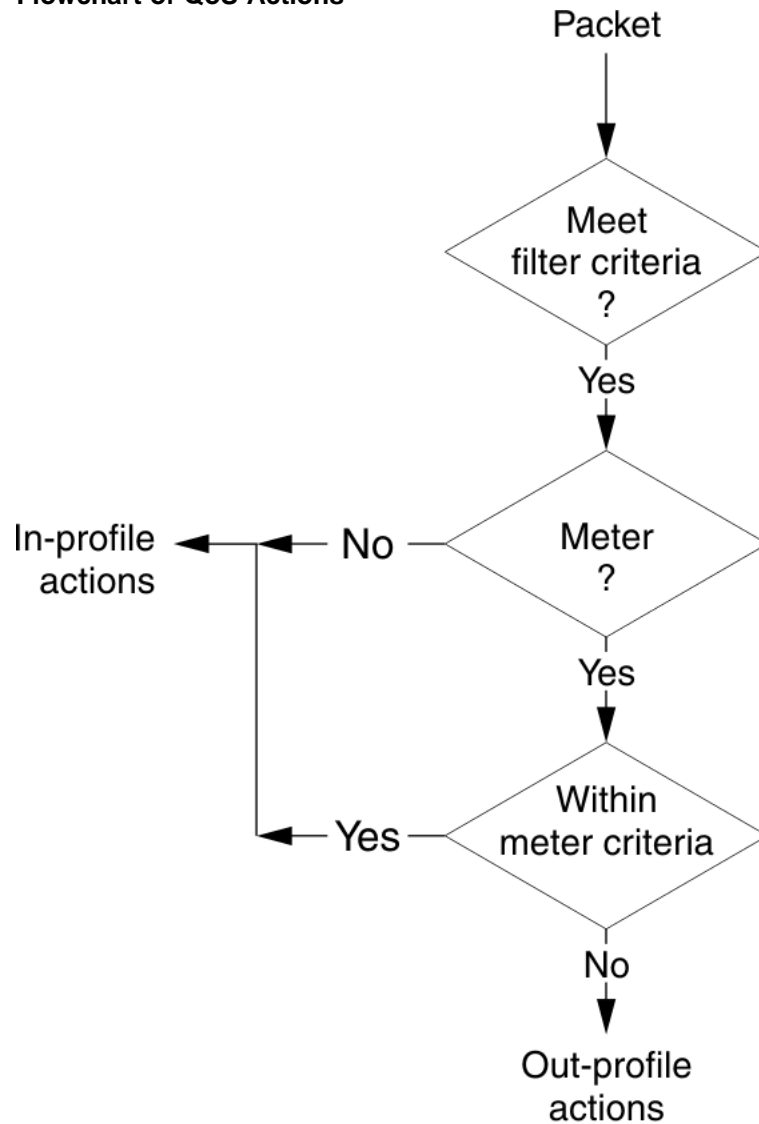
Note: Classifier blocks, not individual classifiers that comprise a block, can be associated with a meter or action.

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

Specifying actions

["Flowchart of QoS Actions"](#) (page 27) summarizes how QoS matches packets with actions.

Flowchart of QoS Actions



11092EA

"Summary of Allowable Actions" (page 27) shows a summary of the allowable actions for different matching criteria.

Summary of Allowable Actions

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

The Nortel Ethernet Routing Switch 5500 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 with the lowest precedence 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 29) shows a summary of the allowable interface action extensions for different matching criteria.

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

The Nortel Ethernet Routing Switch 5500 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 definition.

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

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

Using meters, a Committed Rate in 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: The range for the committed rate is 1000 to < 1023000 Kb/s. The rate is set in increments of 1000 Kb/s (1 megabit) 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).

Note: On 5530-24TFD, 5520-24T/48T 10/100/1000 Mbps 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. For more information see "[show qos capability parameters](#)" (page 51).

Trusted, untrusted, and unrestricted interfaces

Nortel Ethernet Routing Switch 5500 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. Remapping occurs, by default, only for standardized DSCP values (for example, EF, AFXX) and any proprietary Nortel values. The DSCP values that are remapped are associated with a non-zero 802.1p user priority value in the DSCP-to-COS Mapping Table.
- Untrusted interfaces -- IPv4 traffic received on untrusted interfaces is re-marked at the layer 3 level--that is, the DSCP value is updated. The new DSCP value is determined differently depending on whether the packet is untagged or tagged:

— Untagged frames

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

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

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

— Tagged frames

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

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

"Default QoS fields by class of interface--IPv4 only" (page 32) 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	<ul style="list-style-type: none"> Tagged--Updates to 0 (Standard) Untagged--Updates using mapping table and port's default value 	Does not change
	IEEE 802.1p	Updates based on DSCP mapping table value	Updates based on DSCP mapping table value	Does not change

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 5500 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.

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 is not dropped, the Nortel Ethernet Routing Switch 5500 Series uses default system classifiers to change the packet IEEE 802.1p and drop precedence based on the DSCP of the packet.

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 5500 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 5500 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 DSCP-to-CoS mapping table to determine the DSCP value.

"Default mapping of DSCP to QoS class and IEEE 802.1p" (page 33) 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(0x1C), AF33(0x1E), CS3(0x18)	Gold	4	4
AF21(0x12), AF22(0x14), AF23(0x16), CS2(0x10)	Silver	5	3
AF11(0xA), AF12(0xC), AF13(0xE), CS1(0x8)	Bronze	6	2
DE(0x0), CS0(0x0), all undefined DSCPs	Standard	7	0

As displayed in "Default mapping of DSCP to QoS class and IEEE 802.1p" (page 33), 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.

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 lowest 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)**, 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** 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" CLI 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

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 5500 Series supports per policy and per policy, classifier, or interface statistics tracking.

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.

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.

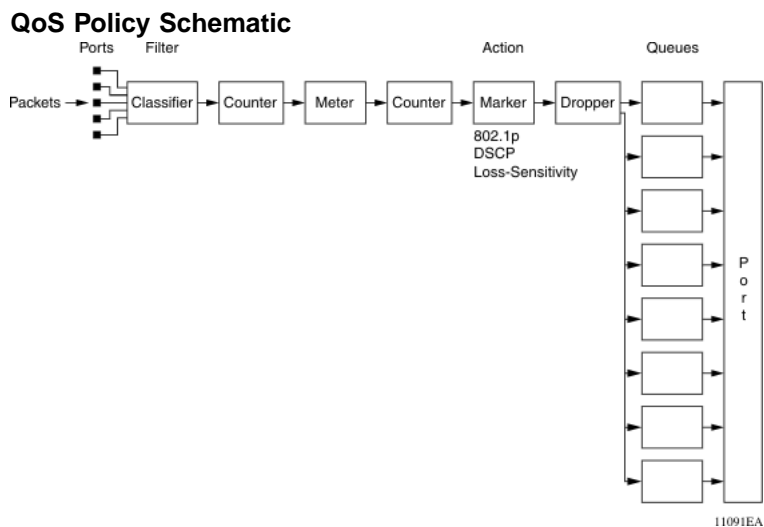
The classifiers/classifier blocks are associated with policies, and policies are organized into a hierarchy. The policy with the highest precedence is evaluated first. The classifier elements, classifiers, and classifier blocks are associated with interface groups, in that packets from a specific port 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 a certain size for a temporary burst, as In-Profile traffic. All other traffic is configured as Out-of-Profile traffic. If you choose not to meter the flow, you do not configure meters.

Actions determine how the traffic is treated.

The overall total of all the interacting QoS factors on a group of packets is a policy. Policies 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 36) provides a schematic overview of QoS policies.



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 5500 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.
- the buffering resources consumed by the egress QoS interface -- you select regular, large, or maximum to allocate the resources.

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 sets, 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 not 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, the switch is locked from further use.

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

- Up to 15 policies per interface group can be configured.
- Up to 63 meters per interface (port) can be configured.
- Up to 100 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).

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; this can explain why an effect is not immediately seen after modifying the values.

QoS Interface Applications

Software Release 5.0 supports several new 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.

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 5520 model only supports 11 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. Pass all broadcast ARP requests.
2. Drop all non-broadcast ARP requests.
3. Drop all ARP packets with a source IP address equal to the identified default gateway.
4. Drop all ARP packets with a target IP address equal to the identified default gateway.
5. Pass all ARP responses.

DHCP Snooping

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

DHCP Spoofing

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

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

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

2. Drop DHCP traffic originated by all other hosts.

SQLSlam

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

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

Nachia

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

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

Xmas

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

TCP SynFinScan

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

TCP FtpPort

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

TCP DnsPort

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

BPDU Blocker

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

Note: BPDU blocker application is no longer supported in 5.1 builds. Please use spanning-tree bpdu filtering. The following error is displayed when using "qos bpdu" CLI commands: "QoS BPDU Blocker not supported in hardware" .

Configuring Quality of Service (QoS) with the CLI

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

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

Displaying QoS Parameters

QoS parameters are displayed using the `show qos` command.

The `show qos` command displays the current QoS policy configuration.

The syntax for the `show qos` command is:

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

```

bpdud {blocker [port] } |
dhcp {snooping [port] | spoofing [port] } |
dos {nachia [port] | sqlslam [port] | tcp-dnsport [port] |
tcp-ftpport [port] | tcp-synfinscan [port] | xmas [port] } |
ip-acl <1 - 65535> |
l2-acl <1 - 65535> }

```

"show qos parameters" (page 46) outlines the parameters for this command.

show qos parameters

Parameter	Description
acl-assign <1 - 65535>	Displays the specified access list assignment entry. <ul style="list-style-type: none"> <1-65535> - Displays a particular entry.
action [<1-65535> all system user]	Displays the base action entries. The applicable values are: <ul style="list-style-type: none"> <1-65535> - Displays a particular entry. all - Displays user-created, default, and system entries. system - Displays only system entries. user - Displays only user-created and default entries. 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.
bpdud <blocker>	Displays QoS BPDU settings. blocker - Displays QoS BPDU blocker settings.
capability [meter shaper]	Displays QoS port capabilities. The applicable values are: <ul style="list-style-type: none"> meter - Displays QoS port meter capabilities. shaper - Displays QoS port shaper capabilities.

Parameter	Description
classifier [<1-65535> all system user]	<p>Displays the classifier set entries. The applicable values are:</p> <ul style="list-style-type: none"> • <1-65535> - Displays a particular entry. • all - Displays all user-created, default, and system entries. • system - Displays only system entries. • user - Displays only user-created and default entries. <p>Default is all.</p>
classifier-block [<1-65535> all system user]	<p>Displays the classifier block entries. The applicable values are:</p> <ul style="list-style-type: none"> • <1-65535> - Displays a particular entry. • all - Displays all user-created, default, and system entries. • system - Displays only system entries. • user - Displays only user-created and default entries. <p>Default is all.</p>
dhcp [snoothing spoofing]	<p>Displays QoS DHCP settings. The applicable values are:</p> <ul style="list-style-type: none"> • snoothing - Displays QoS DHCP snoothing settings. • spoofing - Displays QoS DHCP spoofing prevention settings.
diag [unit]	<p>Displays the diagnostics entries. unit <1-8> - Displays diagnostic entries for particular unit</p>
dos [nachia prevent-package sqlslam tcp-dnsport tcp-ftpport tcp-synfinscan xmas]	<p>Displays QoS DoS settings. The applicable values are:</p> <ul style="list-style-type: none"> • nachia - Displays QoS DoS Nachia settings. • prevent-package - Displays QoS DoS Attack prevention package 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.

Parameter	Description
	<ul style="list-style-type: none"> xmas - Displays QoS DoS Xmas settings.
egressmap [ds status]	<p>Displays the association between the DSCP and the 802.1p priority and drop precedence.</p> <ul style="list-style-type: none"> ds <1-63> - Display egressmap for one particular DSCP value. status - Display egressmap for all DSCP values.
if-action-extension [<1-65535> all system user]	<p>Displays the interface action extension entries. The applicable values are:</p> <ul style="list-style-type: none"> <1-65535> - Displays a particular entry. all - Displays all user-created, default, and system entries. system - Displays only system entries. user - Displays only user-created and default entries. <p>Default is all.</p>
if-assign [port]	<p>Displays the list of interface assignments.</p> <p>port - List of ports. Displays the configuration for particular ports</p>
if-group	Displays the interface groups.
if-shaper [port]	<p>Displays the interface shaping parameters.</p> <p>port - List of ports. Displays the configuration for particular ports</p>
ingressmap	Displays the 802.1p priority to DSCP mapping.
ip-acl <1 - 65535>	<p>Displays the specified IP access list assignment entry.</p> <ul style="list-style-type: none"> <1-65535> - Displays a particular entry.
ip-element [<1-65535> all system user]	<p>Displays the IP classifier element entries. The applicable values are:</p> <ul style="list-style-type: none"> <1-65535> - Displays a particular entry. all - Displays all user-created, default, and system entries. system - Displays only system entries. user - Displays only user-created and default entries. <p>Default is all.</p>

Parameter	Description
l2-acl <1 - 65535>	Displays the specified Layer 2 access list assignment entry. <ul style="list-style-type: none"> <1-65535> - Displays a particular entry.
l2-element [<1-65535> all system user]	Displays the Layer 2 classifier element entries. The applicable values are: <ul style="list-style-type: none"> <1-65535> - Displays a particular entry. all - Displays all user-created, default, and system entries. system - Displays only system entries. user - Displays only user-created and default entries. Default is all.
meter [<1-65535> all system user]	Displays the meter entries. The applicable values are: <ul style="list-style-type: none"> <1-65535> - Displays a particular entry. all - Displays all user-created, default, and system entries. system - Displays only system entries. user - Displays only user-created and default entries. Default is all.
nsna [classifier interface name]	Displays QoS NSNA entries. The applicable values are: <ul style="list-style-type: none"> classifier - Displays QoS NSNA classifier entries. interface - Displays QoS NSNA interface entries. name - Specify the label to display a particular NSNA template entry.
policy [<1-65535> all system user]	Displays the policy entries. The applicable values are: <ul style="list-style-type: none"> <1-65535> - Displays a particular entry. all - Displays all user-created, default, and system entries. system - Displays only system entries. user - Displays only user-created and default entries. Default is all.
queue-set	Displays the queue set configuration.

Parameter	Description
queue-set-assignment	Displays the association between the 802.1p priority to that of a specific queue.
statistics <1-65535>	Displays the policy and filter statistics values. <ul style="list-style-type: none"> <1-65535> - Displays a particular entry.
system-element [<1-65535> all system user]	Displays the system classifier element entries. The applicable values are: <ul style="list-style-type: none"> <1-65535> - Displays a particular entry. all - Displays all user-created, default, and system entries. system - Displays only system entries. user - Displays only user-created and default entries.
ubp [classifier interface name]	Displays QoS UBP entries. The applicable values are: <ul style="list-style-type: none"> classifier - Displays QoS UBP classifier entries. interface - Displays QoS UBP interface entries. name - Specifies the label to display a particular UBP template entry.
user-policy	Displays QoS User Policy entries.

The **show qos** command is executed in the Privileged EXEC command mode.

The **show qos capability** command displays the current QoS capability policy configuration.

The syntax for the **show qos capability** command is:

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

"[show qos capability parameters](#)" (page 51) outlines the parameters for this command.

show qos capability parameters

Parameter	Description
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

The `show qos capability` command is executed in the Privileged EXEC command mode.

Configuring QoS Access Lists

The CLI commands detailed in this section allow for the configuration and management of QoS access lists. For information on displaying this information, refer to ["Displaying QoS Parameters" \(page 45\)](#).

qos acl-assign command

The `qos acl-assign` command is used to assign ports to an access list.

The syntax for the `qos acl-assign` command is:

```
qos acl-assign  aclassid <1 - 55000>
                port <port_list>
                acl-type {ip | 12}
                name <name>
                [committed-rate <1000 - 10230000>]
                [max-burst-rate <1 - 4294967295>]
                [max-burst-duration <1 - 4294967295>]
                [out-prof-drop-action {drop | pass}]
                [out-prof-update-dscp <0 - 63>]
                [out-prof-update-lp <0 - 7>]
                [out-prof-set-drop-prec {high drop |
                low drop}]
                [track-statistics {aggregate |
                individual}]
```

["qos acl-assign parameters" \(page 52\)](#) outlines the parameters for this command.

qos acl-assign parameters

Parameter	Description
aclassignid <1 - 55000>	A unique identifier for the access list assignment.
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. Refer to "qos ip-acl command" (page 53) and "qos l2-acl command" (page 54) for information on performing these tasks.
committed-rate <1000 - 10230000>	The committed rate in kilobits per second configured for this access list assignment.
max-burst-rate <1 - 4294967295>	The maximum burst rate in kilobits per second allowed under this access list assignment.
max-burst-duration <1 - 4294967295>	The maximum burst duration in milliseconds allowed under this access list assignment.
out-prof-drop-action {drop pass}	The out of profile drop action.
out-prof-update-dscp <0 - 63>	The out of profile DSCP update action.
out-prof-update-1p <0 - 7>	The out of profile 802.1p update action.
out-prof-set-drop-prec {high drop low drop}	The out of profile drop precedence.
track-statistics {aggregate individual}	The type of statistics gathered about this access list assignment.

This command is executed in the Global Configuration command mode.

no qos acl-assign command

The `no qos acl-assign` command is used to remove an access list assignment.

The syntax for this command is:

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

Substitute <aclassignid> above with the unique identifier of the access list assignment to remove.

The `no qos acl-assign` command is executed in the Global Configuration command mode.

qos ip-acl command

The `qos ip-acl` command is used to create an IP access list.

The syntax for this command is:

```
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-tp <0 - 7>]
            [set-drop-prec {high drop | low drop}]
            [block <block_name>]
```

"[qos ip-acl parameters](#)" (page 53) outlines the parameters for this command.

qos ip-acl parameters

Parameter	Description
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. See note below.
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. See note below.
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.

Parameter	Description
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.

Note: Possible values for src-port-max and dst-port-max are based on the binary value of the respective port-min, and are obtained by replacing consecutive trailing zeros in this binary value with ones, starting at the right-most position.

For example, if port-min = 200, then there are 4 possible values for port-max:

11001000 (200)

11001001 (201)

11001011 (203)

11001111 (207)

The value of port-max is $\text{port-min} + 2^n - 1$, where n is the number of consecutive trailing zeros replaced.

This command is executed in the Global Configuration command mode.

no qos ip-acl command

The `no qos ip-acl` command is used to remove an IP access list.

The syntax for this command is:

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

Substitute <aclid> above with the unique identifier of the IP access list to remove. This value is between 1 and 55000.

This command is executed in the Global Configuration command mode.

qos l2-acl command

The `qos l2-acl` command is used to create a Layer 2 access list.

The syntax for this command is:

```
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>]

```

"qos l2-acl parameters" (page 55) outlines the parameters for this command.

qos l2-acl parameters

Parameter	Description
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. See note below.
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.

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 + 2n - 1`, where `n` is the number of consecutive trailing zeros replaced.

This command is executed in the Global Configuration command mode.

no qos l2-acl command

The `no qos l2-acl` command is used to remove a Layer 2 access list.

The syntax for this command is:

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

Substitute `<aclid>` above with the unique identifier of the IP access list to remove. This value is between 1 and 55000.

This command is executed in the Global Configuration command mode.

Configuring QoS Security

The CLI 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 45).

Note: Due to hardware limitations, the Ethernet Routing Switch 5520 model only supports 11 QoS security applications per port.

qos arp spoofing command

The `qos arp spoofing` command enables QoS ARP spoofing application on the designated switch ports.

The syntax for this command is:

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

"[qos arp spoofing parameters](#)" (page 56) outlines the parameters for this command.

qos arp spoofing parameters

Parameter	Description
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.

The `qos arp spoofing` command is executed in the Interface Configuration command mode.

no qos arp spoofing command

The `no qos arp spoofing` command disables the QoS ARP spoofing application on the designated switch ports.

The syntax for this command is:

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

Substitute `<port_list>` above with the ports on which the ARP spoofing application is disabled.

The `no qos arp spoofing` command is executed in the Interface Configuration command mode.

qos bpdu blocker command

The `qos bpdu blocker` command enables the QoS BPDU blocker application on the designated switch ports.

The syntax for this command is:

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

Substitute `<port_list>` above with the ports on which the BPDU blocker application is enabled.

The `qos bpdu blocker` command is executed in the Interface Configuration command mode.

Note: BPDU blocker application is no longer supported in 5.1 builds. Please use spanning-tree bpdu-filtering. The following error is displayed when using qos bpdu CLI commands: "QoS BPDU Blocker not supported in hardware"

no qos bpdu blocker command

The `no qos bpdu blocker` command disables the QoS BPDU blocker application on the designated switch ports.

The syntax for this command is:

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

Substitute `<port_list>` above with the ports on which the BPDU blocker application is disabled.

The `no qos bpdu blocker` command is executed in the Interface Configuration command mode.

Note: BPDU blocker application is no longer supported in 5.1 builds. Please use spanning-tree bpdu-filtering. The following error is displayed when using qos bpdu CLI commands: "QoS BPDU Blocker not supported in hardware"

qos dhcp command

The `qos dhcp` command enables the QoS DHCP snooping and spoofing applications on the designated switch ports.

The syntax for this command is:

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

"[qos dhcp parameters](#)" (page 58) outlines the parameters for this command.

qos dhcp parameters

Parameter	Description
{snooping spoofing}	The type of QoS DHCP application to enable.
port <port_list>	The ports to enable the selected QoS DHCP application on.
interface-type {access core}	The interface type to use.

The `qos dhcp` command is executed in the Interface Configuration command mode.

no qos dhcp command

The `no qos dhcp` command disables the QoS DHCP snooping and spoofing applications on the designated switch ports.

The syntax for this command is:

```
no qos dhcp {snooping | spoofing} port <port_list>
```

"[no qos dhcp parameters](#)" (page 59) outlines the parameters for this command.

no qos dhcp parameters

Parameter	Description
{snooping spoofing}	The type of QoS DHCP application to disable.
port <port_list>	The ports to disable the selected QoS DHCP application on.

The `no qos dhcp` command is executed in the Interface Configuration command mode.

qos dos command

The `qos dos` command enables QoS DoS applications on the designated switch ports.

The syntax for this command is:

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

"[qos dos parameters](#)" (page 59) outlines the parameters for this command.

qos dos parameters

Parameter	Description
{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.

The `qos dos` command is executed in the Interface Configuration command mode.

no qos dos command

The `no qos dos` command disables QoS DoS applications on the designated switch ports.

The syntax for this command is:

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

"[no qos dos parameters](#)" (page 60) outlines the parameters for this command.

no qos dos parameters

Parameter	Description
{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.

The `no qos dos` command is executed in the Interface Configuration command mode.

Configuring and Modifying Default Queue Set

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

default qos agent command

The `default qos agent` command specifies the default queue set.

The syntax for the default qos agent command is:

```
default qos agent [buffer | nvram-delay | queue-set <1-8>]
```

"default qos agent parameters" (page 60) describes the parameters for this command.

default qos agent parameters

Parameter	Description
buffer	Restore default QoS resource buffer allocation.
nvram-delay	Restore default maximum time in seconds to write config data to a non-volatile storage.
queue-set <1-8>	Enter a number from 1 to 8 to specify the queue set that will be associated with all QoS interfaces after the next system reset. Note: The default value is 2.

The `default qos agent` command is executed in the Global Configuration command mode.

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
5530-24TFD(config)#show eapol port 1/8,1/18
EAPOL Administrative State: Enabled
EAPOL User Based Policies: Enabled
EAPOL User Based Policies Filter On MAC Addresses: Disabled
Admin Admin Oper ReAuth ReAuth Quiet
Xmit Supplic Server Max
Port Status Auth Dir Dir Enable Period Period
Period Timeout Timeout Req
-----
-----
1/8 Auto No Both Both No 3600 60
30 30 30 2
1/18 Auto No Both Both No 3600 60
30 30 30 2

```

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

qos agent queue-set command

The `qos agent queue-set` command modifies the default queue configuration.

The syntax for the `qos agent queue-set` command is:

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

Substitute <1-8> above with the number of the queue set that is associated with all QoS interfaces after the next system reset. The default value is 8.

The `qos agent queue-set` command is executed in the Global Configuration command mode.

Configuring Default Buffering Capabilities

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

default qos agent buffer command

The `default qos agent buffer` command allocates the default QoS resource buffer.

The syntax for the `default qos agent buffer` command is:

```
default qos agent buffer
```

The `default qos agent buffer` command is executed in the Global Configuration command mode.

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

qos agent buffer command

The command modifies the QoS resource buffer allocation.

The syntax for `qos agent buffer` command is:

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

"qos agent buffer parameters" (page 62) outlines the parameters for this command.

qos agent buffer parameters

Parameter	Description
buffer-mode	Enter one of the following to specify the buffer allocation mode for all QoS interfaces after the next system reboot: <ul style="list-style-type: none"> regular large maximum

The `qos agent buffer` command is executed in the Global Configuration command mode.

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

Configuring the CoS-to-Queue Assignments

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

qos queue-set-assignment command

The `qos queue-set-assignment` command associates 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.

The syntax for the `qos queue-set-assignment` command is:

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

"[qos queue-set-assignment parameters](#)" (page 63) outlines the parameters for this command.

qos queue-set-assignment parameters

Parameter	Description
queue-set <1-8>	Enter a number from 1 to 8 to specify the queue set to modify.
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.

The `qos queue-set-assignment` command is executed in the Global Configuration command mode.

Configuring QoS Interface Groups

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

qos if-assign command

The `qos if-assign` command adds ports to a defined interface group.

The syntax for the `qos if-assign` command is:

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

"[qos if-assign parameters](#)" (page 63) describes the parameters for this command.

qos if-assign parameters

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

The `qos if-assign` command is executed in the Interface Configuration command mode.

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

no qos if-assign command

The `no qos if-assign` command deletes ports from a defined interface group.

The syntax for the `no qos if-assign` command is:

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

Substitute `port <portlist>` above with the ports to delete from the interface group.

The `no qos if-assign` command is executed in the Interface Configuration command mode.

qos if-group command

The `qos if-group` command creates interface groups.

The syntax for the `qos if-group` command is:

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

"[qos if-group parameters](#)" (page 64) outlines the parameters for this command.

qos if-group parameters

Parameter	Description
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: <ul style="list-style-type: none"> • trusted • untrusted • unrestricted

The `qos if-group` command is executed in the Global Configuration command mode.

no qos if-group command

The `no qos if-group` command deletes interface groups.

The syntax for the `no qos if-group` command is:

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

Substitute `<WORD>` above with the name of the interface group to delete.

The `no qos if-group` command is executed in the Global Configuration command mode.

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

Configuring DSCP and 802.1p and Queue Associations

DSCP, IEEE 802.1p priority, and queue set association can be configured using the CLI. This section covers the CLI following commands.

qos egressmap command

The `qos egressmap` command configures 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.

The syntax for the `qos egressmap` command is:

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

"[qos egressmap parameters](#)" (page 65) outlines the parameters for this command.

qos egressmap parameters

Parameter	Description
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.
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: <ul style="list-style-type: none"> low-drop high-drop

The `qos egressmap` command is executed in the Global Configuration command mode.

default qos egressmap command

The `default qos egressmap` command resets the egress mapping entries to factory default values.

The syntax for the `default qos egressmap` command is:

```
default qos egressmap
```

The `default qos egressmap` command is executed in the Global Configuration command mode.

qos ingressmap command

The `qos ingressmap` command configures 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.

The syntax for the `qos ingressmap` command is:

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

"[qos ingressmap parameters](#)" (page 66) outlines the parameters for this command.

qos ingressmap parameters

Parameter	Description
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.

The `qos ingressmap` command is executed in the Global Configuration command mode.

default qos ingress command

The `default qos ingressmap` command resets the ingress mapping entries to factory default values.

The syntax for the `default qos ingressmap` command is:

```
default qos ingressmap
```

The `default qos ingressmap` command is executed in the Global Configuration command mode.

Configuring QoS Elements, Classifiers, and Classifier Blocks

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

qos ip-element command

The `qos ip-element` command adds IP classifier element entries.

The syntax for the `qos ip-element` command is:

```
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>]
```

"[qos ip-element parameters](#)" (page 67) outlines the parameters for this command.

qos ip-element parameters

Parameter	Description
<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 or a.b.c.d x.x.x.x for IPv4, or 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 or a.b.c.d x.x.x.x for IPv4, or 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. See note below.
dst-port-min <port> dst-port-max <port>	Specify the L4 destination port minimum value and maximum value filter criteria. See note below.

Parameter	Description
next-header	Specify the IPv6 next header classifier criteria; range is 0 to 255.
flow-id <flowid>	Specify the IPv6 flow identifier.

Note: Possible values for src-port-max and dst-port-max are based on the binary value of the respective port-min, and are obtained by replacing consecutive trailing zeros in this binary value with ones, starting at the right-most position.

For example, if port-min = 200, then there are 4 possible values for port-max:

11001000 (200)

11001001 (201)

11001011 (203)

11001111 (207)

The value of port-max is $\text{port-min} + 2^n - 1$, where n is the number of consecutive trailing zeros replaced.

The `qos ip-element` command is executed in the Global Configuration command mode.

no qos ip-element command

The `no qos ip-element` command deletes IP classifier element entries.

The syntax for the `no qos ip-element` command is:

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

Substitute <1-55000> above with the element ID.

The `no qos ip-element` command can be executed in the Global Configuration command mode.

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

qos l2-element command

The `qos l2-element` command adds Layer 2 elements.

The syntax for the `qos l2-element` command is:

```
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>]
```

"qos l2-element parameters" (page 69) outlines the parameters for this command.

qos l2-element parameters

Parameter	Description
<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. See note below.
vlan-tag <format>	Specify the packet format element criteria: <ul style="list-style-type: none"> • untagged • tagged <p>The default is Ignore.</p>
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.

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 + 2n - 1`, where `n` is the number of consecutive trailing zeros replaced.

The `qos 12-element` command is executed in the Global Configuration command mode.

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

no qos 12-element command

The `no qos 12-element` command deletes Layer 2 element entries.

The syntax for the `no qos 12-element` command is:

```
no qos 12-element <1-55000>
```

Substitute `<1-55000>` above with the ID of the element to be deleted.

The `no qos 12-element` command is executed in the Global Configuration command mode.

qos classifier command

The `qos classifier` command facilitates the linking of individual IP and L2 classifier elements into a single classifier.

The syntax for the `qos classifier` command is:

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

"[qos classifier parameters](#)" (page 70) outlines the parameters for this command.

qos classifier parameters

Parameter	Description
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.

The `qos classifier` command is executed in the Global Configuration command mode.

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

no qos classifier command

The `no qos classifier` command deletes classifier entries.

The syntax for the `no qos classifier` command is:

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

Substitute `<1-55000>` above with the classifier ID of the classifier to be deleted.

The `no qos classifier` command is executed in the Global Configuration command mode.

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.

qos classifier-block command

The `qos classifier-block` command combines individual classifiers.

The syntax for the `qos classifier-block` command is:

```
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>} ]
```

"[qos classifier-block parameters](#)" (page 71) outlines the parameters for this command.

qos classifier-block parameters

Parameter	Description
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.

Parameter	Description
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.

The `qos classifier-block` command is executed in the Global Configuration command mode.

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

no qos classifier-block command

The `no qos classifier-block` command deletes classifier block entries.

The syntax for the `no qos classifier-block` command is:

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

Substitute <1-55000> above with the ID of the classifier block to be deleted.

The `no qos classifier-block` command is executed in the Global Configuration command mode.

Configuring QoS system-element

qos system-element command

The `qos system-element` command configures the system classifier element parameters that may be used in QoS policies.

The syntax for the `qos system element` command is:

```
qos system-element <1-55000> [known-mcast | unknown-mcast
| unknown-ucast] [pattern-format {tagged | untagged}]
[pattern-data <WORD> pattern-mask <WORD>]
```


"qos system-element parameters" (page 73) outlines the parameters for this command.

qos system-element parameters

Parameter	Description
<1-55000>	System classifier element entry id; range is 1 to 55000.
know-mcast	Filter on known multicast destination address.
unknow-mcast	Filter on unknown multicast destination address.
unknow-ucast	Filter on unknown unicast destination address.
pattern-format { tagged untagged }	Specifies the format of data/mask pattern. The available values are: <ul style="list-style-type: none"> tagged - Data/mask pattern describes a tagged packet untagged - Data/mask pattern describes an untagged packet
pattern-data <WORD>	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: The format of the WORD string is in the form of XX:XX:XX:.....:XX.

Note: 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.

The `qos system-element` command is executed in the Global Configuration command mode.

no qos system-element command

The `no qos system-element` command deletes the system classifier element entry.

The syntax for the `no qos system-element` command is:

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

Substitute <1-55000> above with the classifier element entry ID of the classifier element to be deleted.

The `no qos system-element` command is executed in the Global Configuration command mode.

Configuring QoS Actions

The configuration of QoS actions directs the Nortel Ethernet Routing Switch 5500 Series to take specific action on each packet. This section covers the following CLI commands.

qos action command

The `qos action` command creates or updates a QoS action.

The syntax for the `qos action` command is:

```
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>]
```

"qos action parameters" (page 74) outlines the parameters for this command.

qos action parameters

Parameter	Description
<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
drop-action<enable disable deferred-pass>	Specifies whether packets are dropped or not: <ul style="list-style-type: none"> • enable--drop the traffic flow • disable--do not drop the traffic flow • deferred-pass--traffic flow decision deferred to other installed policies <p>Default is deferred pass.</p> <p>Note: If you omit this parameter, the default value applies.</p>

Parameter	Description
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: <ul style="list-style-type: none"> • ieee1p--enter the value you want; range is 0 to 7 • use-egress--uses the egress map to assign value • use-tos-prec--uses the type of service precedence to assign value. Default is ignore.
set-drop-prec <low-drop high-drop>	Enter the loss-sensitivity value: <ul style="list-style-type: none"> • 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.

The `qos action` command is executed in the Global Configuration command mode.

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.

no qos action command

The `no qos action` command deletes QoS action entries.

The syntax for the `no qos action` command is:

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

Substitute <10-55000> above with the ID of the QoS action to be deleted.

The `no qos action` command is executed in the Global Configuration command mode.

Configuring QoS Interface Action Extensions

QoS interface action extensions direct the Nortel Ethernet Routing Switch 5500 Series to take specific action on each packet. This section covers the following CLI commands.

qos if-action-extension command

The `qos if-action-extension` command creates interface action extension entries.

The syntax for the `qos if-action-extension` command is:

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

"[qos if-action-extension parameters](#)" (page 76) describes the parameters for this command.

qos if-action-extension parameters

Parameter	Description
<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.

The `qos if-action-extension` command is executed in the Global Configuration command mode.

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

no qos if-action-extension command

The `no qos if-action-extension` command deletes interface action extension entries.

The syntax for the `no qos if-action-extension` command is:

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

Substitute <1-55000> above with the ID of the QoS action extension to be deleted.

The `no qos if-action-extension` command is executed in the Global Configuration command mode.

Configuring QoS Meters

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

qos meter command

The `qos meter` command creates QoS meter entries.

The syntax for the `qos meter` command is:

```
qos meter <1-55000> [name <WORD>] committed-rate
<64-10230000> 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>}
```

"[qos meter parameters](#)" (page 77) describes the parameters for this command.

qos meter parameters

Parameter	Description
<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.
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.

Parameter	Description
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.

The `qos meter` command is executed in the Global Configuration command mode.

no qos meter command

The `no qos meter` command deletes QoS meter entries.

The syntax for the `no qos meter` command is:

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

Substitute <1-55000> above with the ID of the QoS meter to be deleted.

The `no qos meter` command is executed in the Global Configuration command mode.

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

Configuring QoS Interface Shaper

qos if-shaper command

The `qos if-shaper` command configures the interface shaping parameters for a set of ports.

The syntax for the `qos if-shaper` command is:

```
qos if-shaper [port <portlist>] [name <WORD>] shape-rate  
<64-10230000> max-burst-rate <64-4294967295>  
[max-burst-duration <1-4294967295>]
```

"[qos if-shaper parameters](#)" (page 78) outlines the parameters for this command.

qos if-shaper parameters

Parameter	Description
<portlist>	Ports to configure shaping parameters.
<WORD>	Specify name for if-shaper; maximum is 16 alphanumeric characters.

Parameter	Description
shape-rate <64-10230000>	Shaping rate in kilobits/sec; range is 64-10230000 kilobits/sec.
max-burst-rate <64-4294967295>	Maximum burst rate in kilobits/sec; range is 64-4294967295Kbits/sec.
max-burst-duration <1-4294967295>	Maximum burst duration in milliseconds; range is 1 to 4294967295 ms.

The `qos if-shaper` command is executed in the Interface Configuration mode.

no qos if-shaper command

The `no qos if-shaper` command disables the interface shaping for a set of ports.

The syntax for the `no qos if-shaper` command is:

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

Substitute `<portlist>` above with the ports on which to disable shaping.

The `no qos if-shaper` command is executed in the Interface Configuration mode.

Configuring QoS Policies

Use the following CLI commands to configure QoS policies.

qos policy command

The `qos policy` command creates a QoS policy.

The syntax for the `qos policy` command is:

```
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 <1-11>
[track-statistics <individual | aggregate>]}
```

"[qos policy parameters](#)" (page 80) describes the parameters for this command.

qos policy parameters

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

Parameter	Description
track-statistics <individual aggregate>	Specifies statistics tracking on this policy, either: <ul style="list-style-type: none"> • individual--statistics on individual classifiers • aggregate--aggregate statistics

The `qos policy` command is executed in the Global Configuration command mode.

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)#
```

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.

no qos policy command

The `no qos policy` command deletes QoS policy entries.

The syntax for the `no qos policy` command is:

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

Substitute `<1-55000>` above with the ID of the QoS policy to be deleted.

The `no qos policy` command is executed in the Global Configuration command mode.

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.

To configure QoS for Nortel SNA filters, use the following command from the Global configuration mode:

```
qos nsna
```

This command includes the following parameters:

Parameter	Description
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: <ul style="list-style-type: none"> • addr-type {ipv4 ipv6} specifies the type of IP address used by this classifier entry. The type is limited to IPv4 and IPv6 addresses. • block specifies the label to identify access list elements that are of the same block. • drop-action specifies whether or not to drop non-conforming traffic. • ds-field specifies the value for the DiffServ Codepoint (DSCP) in a packet. • dst-ip specifies the IP address to match against the destination IP address of a packet. • dst-mac specifies the MAC address against which the MAC destination address of incoming packets is compared. • dst-port-min specifies the minimum value for the layer 4 destination port number in a packet. • 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 automatic 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. • 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.

Parameter	Description
	<ul style="list-style-type: none"> vlan-min specifies the minimum value for the VLAN ID in a packet. vlan-tag specifies the type of VLAN tagging in a packet.
set name [committed-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: <ul style="list-style-type: none"> committed-rate specifies the committed 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 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 the action to take when a dscp filed in an IPv4 packet is out of profile.

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

Example: 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

To delete an entire filter set, use the following command from the Global configuration mode:

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

where <filter name> is the label used to reference the Nortel SNA entry.

To delete a classifier, use the following command from the Global configuration mode:

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

where <filter name> is the label used to reference the Nortel SNA entry and <value> is the evaluation order identifier that references the specific Nortel SNA entry.

To delete a classifier block, use the command for deleting a classifier to delete all the classifier members in that block.

Note: You cannot delete all the classifiers in a filter set. There should always be at least one remaining.

Viewing filter descriptions

To view Nortel SNA filter parameters, use the following command from the Privileged EXEC configuration mode:

```
show qos nsna
```

Example

```
5530-24TFD(config)#show qos ubp
Id: 1
Unit/Port: 0 (TEMPLATE)
Name: no_pc3
Block:
Eval Order: 1
Address Type: IPv4
Destination Addr/Mask: 10.100.111.1/32
Source Addr/Mask: Ignore
DSCP: Ignore
IPv4 Protocol / IPv6 Next Header: Ignore
Destination L4 Port Min: Ignore
Destination L4 Port Max: Ignore
Source L4 Port Min: Ignore
Source L4 Port Max: Ignore
IPv6 Flow Id: Ignore
Destination MAC Addr: Ignore
Destination MAC Mask: Ignore
Source MAC Addr: Ignore
Source MAC Mask: Ignore
VLAN: Ignore
VLAN Tag: Ignore
EtherType: 0x0800
802.1p Priority: All
Action Drop: Yes
Action Update DSCP: Ignore
Action Update 802.1p Priority: Ignore
Action Set Drop Precedence: Low Drop
Non-Match Action: Defer
Storage Type: NonVolatile
Id: 2
Unit/Port: 0 (TEMPLATE)
Name: meter_pc3
Block:
Eval Order: 1
Address Type: IPv4
Destination Addr/Mask: 10.100.111.1/32
Source Addr/Mask: Ignore
DSCP: Ignore
IPv4 Protocol / IPv6 Next Header: Ignore
Destination L4 Port Min: Ignore
Destination L4 Port Max: Ignore
Source L4 Port Min: Ignore
Source L4 Port Max: Ignore
IPv6 Flow Id: Ignore
Destination MAC Addr: Ignore
Destination MAC Mask: Ignore
```

```

Source MAC Addr: Ignore
Source MAC Mask: Ignore
VLAN: Ignore VLAN Tag: Ignore
EtherType: 0x0800
802.1p Priority: All
Action Drop: No
Action Update DSCP: Ignore
Action Update 802.1p Priority: Ignore
Action Set Drop Precedence: Low Drop
Commit Rate: 1000 Kbps
Commit Burst: 524288 Bytes
Out-Profile Drop Action: Drop
Out-Profile Remark DSCP Action: None
Non-Match Action: Defer
Storage Type: NonVolatile

```

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>
```

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
```

To view classifier entries, use the following command from the Privileged EXEC configuration mode:

```
show qos nsna classifier
```

Configuring User Based Policies

To configure User Based Policies, use the following command from the Global configuration mode:

```
qos ubp
```

This command includes the following parameters:

Parameter	Description
classifier name [addr-type {ipv4 ipv6}] [block] [drop-action] [ds-field] [dst-ip] [dst-mac] [dst-port-min] [ethertype] [eval-order] [flow-id] [next-header] [priority] [protocol] [set-drop-prec] [src-ip] [src-mac] [src-port-min] [update-1p] [update-dscp] [vlan-min] [vlan-tag]	Creates the User Based Policy classifier entry. Optional parameters: <ul style="list-style-type: none"> addr-type {ipv4 ipv6} specifies the type of IP address used by this classifier entry. The type is limited to IPv4 and IPv6 addresses. block specifies the label to identify access list elements that are of the same block.

Parameter	Description
	<ul style="list-style-type: none"> • drop-action specifies whether or not to drop non-conforming traffic. • ds-field specifies the value for the DiffServ Codepoint (DSCP) in a packet. • dst-ip specifies the IP address to match against the destination IP address of a packet. • dst-mac specifies the MAC address against which the MAC destination address of incoming packets is compared. • dst-port-min specifies the minimum value for the layer 4 destination port number in a packet. • 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 automatic 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. • 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.

Parameter	Description
	<ul style="list-style-type: none"> vlan-tag specifies the type of VLAN tagging in a packet.
set name [committed-rate] [drop-nm-action] [drop-out-action] [max-burst-rate] [max-burst-duration] [update-dscp-out-action]	Creates the User Based Policy set. Optional parameters: <ul style="list-style-type: none"> committed-rate specifies the committed 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 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 the action to take when a dscp filed in an IPv4 packet is out of profile.

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

Example: 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

To delete an entire filter set, use the following command from the Global configuration mode:

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

where <filter name> is the label used to reference the User Based Policy entry.

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

To delete a classifier, use the following command from the Global configuration mode:

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

where <filter name> is the label used to reference the User Based Policy entry and <value> is the evaluation order identifier that references the specific User Based Policy entry.

To delete a classifier block, use the command for deleting a classifier to delete all the classifier members in that block.

Note: You cannot delete all the classifiers in a filter set. There should always be at least one remaining.

Viewing filter descriptions

To view User Based Policy filter parameters, use the following command from the Privileged EXEC configuration mode:

```
show qos ubp
```

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>
```

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
```

To view classifier entries, use the following command from the Privileged EXEC configuration mode:

```
show qos ubp classifier
```

Maintaining the QoS Agent

Use the following CLI commands to maintain the QoS agent.

qos agent reset-default command

The `qos agent reset-default` command deletes all user-defined entries, removes all installed policies, and resets the system to its QoS factory default values.

The syntax for the `qos agent reset-default` command is:

```
qos agent reset-default
```

The `qos agent reset-default` command is executed in the Global Configuration command mode.

qos agent nvram-delay command

The `qos agent nvram-delay` command specifies 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.

The syntax for the `qos agent nvram-delay` command is:

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

Substitute `<0-604800>` above with the maximum amount of time (in seconds) before non-volatile QoS configuration data is written to non-volatile storage. The default is 10 seconds.

The `qos agent nvram-delay` command is executed in the Global Configuration command mode.

default qos agent nvram-delay

The `default qos agent nvram-delay` command resets the NVRAM delay time to factory default.

The syntax for the `default qos agent nvram-delay` command is:

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

The `default qos agent nvram-delay` command is executed in the Global Configuration command mode.

default qos agent command

The `default qos agent` command deletes all user-defined entries, removes all installed policies, and resets the system to its QoS factory default values.

The syntax for the `default qos agent` command is:

```
default qos agent
```

The `default qos agent` command is executed in the Global Configuration command mode.

Configuring Quality of Service (QoS) with the Web-based Management Interface

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

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, 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 93](#)) 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 5520 model only supports 11 interface applications per port.

To use a wizard, select it from the menu as described in "[QoS Wizards](#)" (page 93). 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.

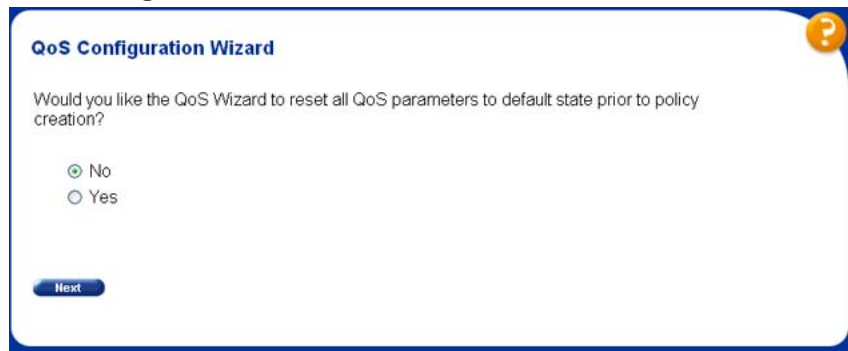
QoS Configuration Wizard

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:

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 . This screen is illustrated in " QoS Configuration Wizard, Screen 1 " (page 95). Click Next to continue.

QoS Configuration Wizard, Screen 1



QoS Configuration Wizard

Would you like the QoS Wizard to reset all QoS parameters to default state prior to policy creation?

No
 Yes

Next

- 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**. This screen is illustrated in "QoS Configuration Wizard, Screen 2" (page 95).

QoS Configuration Wizard, Screen 2



QoS Configuration Wizard

Select a traffic type.

VLAN
 IP Application (e.g., HTTP, SMTP)
 User Defined Flow
 L2 - L4 Access List
 Filter Set

Back **Next**

- 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. The screen for a new policy is illustrated in "QoS Configuration Wizard, Screen 3" (page 96).

QoS Configuration Wizard, Screen 3



QoS Configuration Wizard

Step 1 - Policy Label | Step 2 - VLAN | Step 3 - Block | Step 4 - Meter | Step 5 - Service | Step 6 - Ports

Provide a label name for the policy.

Name

[Back](#) [Next](#)

- 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. This screen is illustrated in "QoS Configuration Wizard, Screen 4 - VLAN" (page 96).

QoS Configuration Wizard, Screen 4 - VLAN



QoS Configuration Wizard

Step 1 - Policy Label | Step 2 - VLAN | Step 3 - Block | Step 4 - Meter | Step 5 - Service | Step 6 - Ports

VLAN Elements: 0

Enter a VLAN.

VLAN

[Back](#) [Next](#)

- b. **IP Application** -- Select the IP application on which to base the policy. This screen is illustrated in "QoS Configuration Wizard, Screen 4 - IP Application" (page 97).

QoS Configuration Wizard, Screen 4 - IP Application

QoS Configuration Wizard

Step 1 - Policy Label | **Step 2 - IP Application** | Step 3 - Block | Step 4 - Meter | Step 5 - Service | Step 6 - Ports

IP Application Elements: 0

You can configure a QoS policy based on the following management traffic.

- Web Browsing (http)
- Secure Web Browsing (https)
- E-Mail (smtp)
- File Transfers (ftp)
- Keyboard I/O (telnet)
- SNMP

[Back](#) [Next](#)

- c. **User Defined Flows** -- When configuring user defined flow policies it is a two step process. The first step (illustrated in "QoS Configuration Wizard, Screen 4A - User Defined Flows" (page 97)) is to define the type of filter to apply, either IP or Layer 2.

QoS Configuration Wizard, Screen 4A - User Defined Flows

QoS Configuration Wizard

Step 1 - Policy Label | **Step 2 - Policy Definition** | Step 3 - Meter | Step 4 - Service | Step 5 - Ports

Select the type of filter.

- IP Filter
- Layer2 Filter

[Back](#) [Next](#)

The second step is to designate the classification parameters for this policy. This screen is illustrated in "QoS Configuration Wizard, Screen 4B - User Defined Flows" (page 98).

QoS Configuration Wizard, Screen 4B - User Defined Flows

Provide the policy parameters to classify on.

Address Type	<input checked="" type="radio"/> IPv4 (e.g. A.B.C.D / 0-32) <input type="radio"/> IPv6 (e.g. X:X:X:X:X:X / 0-128)
Destination IP Address	<input checked="" type="radio"/> Ignore <input type="radio"/> 0.0.0.0 <input type="text" value="0"/> <small>Address Mask Length</small>
Source IP Address	<input checked="" type="radio"/> Ignore <input type="radio"/> 0.0.0.0 <input type="text" value="0"/> <small>Address Mask Length</small>
DSCP	Ignore <input type="button" value="v"/>
IPv4 Protocol / IPv6 Next Header	<input checked="" type="radio"/> Ignore <input type="radio"/> Preconfigured Protocol <input type="text" value="TCP"/> <input type="radio"/> User Defined Protocol <input type="text" value="0"/>
Destination Layer4 Port	<input checked="" type="radio"/> Ignore <input type="radio"/> Preconfigured Port # <input type="text" value="TFTP"/> <input type="radio"/> User Defined Port # <input type="text" value="0"/> to <input type="text" value="65535"/> (0..65535)
Source Layer4 Port	<input checked="" type="radio"/> Ignore <input type="radio"/> Preconfigured Port # <input type="text" value="TFTP"/> <input type="radio"/> User Defined Port # <input type="text" value="0"/> to <input type="text" value="65535"/> (0..65535)
IPv6 Flow Id	<input checked="" type="radio"/> Ignore <input type="radio"/> 0x0 (e.g. 0xF2843)

- 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. This is illustrated in "QoS Configuration Wizard, Screen 4A - Access Lists" (page 98).

QoS Configuration Wizard, Screen 4A - Access Lists

QoS Configuration Wizard

Step 1 - Access List Label | **Step 2 - Access List Definition** | Step 3 - Service | Step 4 - Ports

Select the type of access list.

IP Access List
 Layer2 Access List

The second step is to define classification parameters for the policy. If **IP Access List** is selected on the screen in "QoS Configuration Wizard, Screen 4A - Access Lists" (page 98), the screen in "QoS Configuration Wizard, Screen 4B - IP Access List" (page 99) is displayed. Otherwise, if **Layer 2 Access List** is selected, the screen in "QoS Configuration Wizard, Screen 4B - Layer 2 Access List" (page 99) is displayed.

QoS Configuration Wizard, Screen 4B - IP Access List

Provide the access list element parameters to classify on.

Address Type	<input checked="" type="radio"/> IPv4 (e.g. A.B.C.D / 0-32) <input type="radio"/> IPv6 (e.g. X.X.X.X:X.X.X.X / 0-128)
Destination IP Address	<input checked="" type="radio"/> Ignore <input type="radio"/> 0.0.0.0 <input type="text" value="0"/> Address Mask Length
Source IP Address	<input checked="" type="radio"/> Ignore <input type="radio"/> 0.0.0.0 <input type="text" value="0"/> Address Mask Length
DSCP	Ignore <input type="button" value="v"/>
IPv4 Protocol / IPv6 Next Header	<input checked="" type="radio"/> Ignore <input type="radio"/> Preconfigured Protocol TCP <input type="button" value="v"/> <input type="radio"/> User Defined Protocol <input type="text" value="0"/>
Destination Layer4 Port	<input checked="" type="radio"/> Ignore <input type="radio"/> Preconfigured Port # TFTP <input type="button" value="v"/> <input type="radio"/> User Defined Port # <input type="text" value="0"/> to <input type="text" value="65535"/> <input type="button" value="v"/> (0..65535)
Source Layer4 Port	<input checked="" type="radio"/> Ignore <input type="radio"/> Preconfigured Port # TFTP <input type="button" value="v"/> <input type="radio"/> User Defined Port # <input type="text" value="0"/> to <input type="text" value="65535"/> <input type="button" value="v"/> (0..65535)
IPv6 Flow Id	<input checked="" type="radio"/> Ignore <input type="radio"/> 0x0 (e.g. 0xF2843)
Block	<input type="text"/>

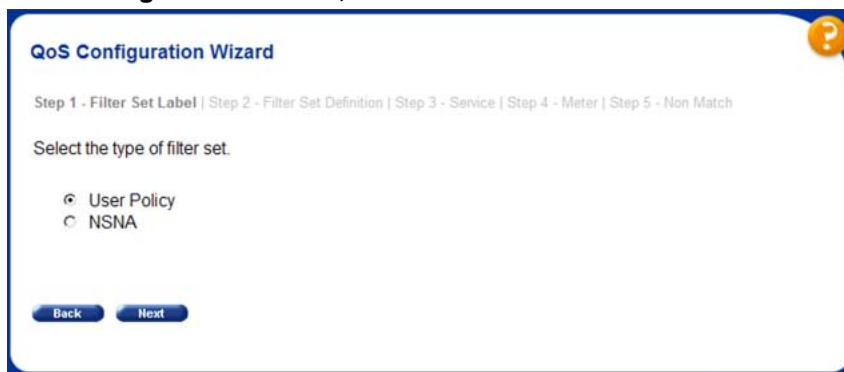
QoS Configuration Wizard, Screen 4B - Layer 2 Access List

Provide the access list element parameters to classify on.

Destination MAC Address	<input checked="" type="radio"/> Ignore <input type="radio"/> 00-00-00-00-00-00 <input type="text" value="00-00-00-00-00-00"/> MAC Addr MAC Addr Mask
Source MAC Address	<input checked="" type="radio"/> Ignore <input type="radio"/> 00-00-00-00-00-00 <input type="text" value="00-00-00-00-00-00"/> MAC Addr MAC Addr Mask
VLAN	<input checked="" type="radio"/> Ignore <input type="radio"/> VLAN Range <input type="text" value="1"/> to <input type="text" value="1"/> <input type="button" value="v"/> (1..4094)
VLAN Tag	Ignore <input type="button" value="v"/>
EtherType	<input type="radio"/> Ignore <input checked="" type="radio"/> Preconfigured IP <input type="button" value="v"/> <input type="radio"/> User Defined 0x0800 (e.g. 0x8137)
802.1p Priority	Ignore <input type="button" value="v"/>
Block	<input type="text"/>

- 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. This is illustrated in "QoS Configuration Wizard, Screen 4 - Filter Sets" (page 100).

QoS Configuration Wizard, Screen 4 - Filter Sets



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 as shown in "QoS Configuration Wizard, Screen 4A - Filter Sets" (page 101).

QoS Configuration Wizard, Screen 4A - Filter Sets

Address Type	<input checked="" type="radio"/> IPv4 (e.g. A.B.C.D / 0-32) <input type="radio"/> IPv6 (e.g. X.X.X.X.X.X.X / 0-128)
Destination IP Address	<input checked="" type="radio"/> Ignore <input type="radio"/> <input type="text" value="0.0.0.0"/> <input type="text" value="0"/> Address Mask Length
Source IP Address	<input checked="" type="radio"/> Ignore <input type="radio"/> <input type="text" value="0.0.0.0"/> <input type="text" value="0"/> Address Mask Length
DSCP	Ignore <input type="text" value=""/>
IPv4 Protocol / IPv6 Next Header	<input checked="" type="radio"/> Ignore <input type="radio"/> Preconfigured Protocol <input type="text" value="TCP"/> <input type="radio"/> User Defined Protocol <input type="text" value="0"/>
Destination Layer4 Port	<input checked="" type="radio"/> Ignore <input type="radio"/> Preconfigured Port # <input type="text" value="TFTP"/> <input type="radio"/> User Defined Port # <input type="text" value="0"/> to <input type="text" value="65535"/> (0..65535)
Source Layer4 Port	<input checked="" type="radio"/> Ignore <input type="radio"/> Preconfigured Port # <input type="text" value="TFTP"/> <input type="radio"/> User Defined Port # <input type="text" value="0"/> to <input type="text" value="65535"/> (0..65535)
IPv6 Flow Id	<input checked="" type="radio"/> Ignore <input type="radio"/> <input type="text" value="0x0"/> (e.g. 0xF2843)
Destination MAC Address	<input checked="" type="radio"/> Ignore <input type="radio"/> <input type="text" value="00-00-00-00-00-00"/> <input type="text" value="00-00-00-00-00-00"/> MAC Addr MAC Addr Mask
Source MAC Address	<input checked="" type="radio"/> Ignore <input type="radio"/> <input type="text" value="00-00-00-00-00-00"/> <input type="text" value="00-00-00-00-00-00"/> MAC Addr MAC Addr Mask
VLAN	<input checked="" type="radio"/> Ignore <input type="radio"/> VLAN Range <input type="text" value="1"/> to <input type="text" value="1"/> (1..4094)
VLAN Tag	Ignore <input type="text" value=""/>
EtherType	<input type="radio"/> Ignore <input checked="" type="radio"/> Preconfigured <input type="text" value="IP"/> <input type="radio"/> User Defined <input type="text" value="0x0800"/> (e.g. 0x8137)
802.1p Priority	Ignore <input type="text" value=""/>
Eval Precedence	<input type="text" value="1"/>
Block	<input type="text" value=""/>

- 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 similar to the one in "[QoS Configuration Wizard, Screen 5](#)" (page 102) asking to add more blocks to the policy. To add more blocks to a policy, repeat step 5.

QoS Configuration Wizard, Screen 5

QoS Configuration Wizard

Step 1 - Policy Label | Step 2 - VLAN | Step 3 - Block | Step 4 - Meter | Step 5 - Service | Step 6 - Ports

VLAN Elements: 1

Would you like to add additional VLANs into the block?

No
 Yes Block Name

If policy configuration is taking place for the **Layer 2 - Layer 4 Access List** or **Filter set** traffic types, the corresponding screen illustrated in "QoS Configuration Wizard, Screen 5 - Access Lists" (page 102) 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 from a screen similar to the one illustrated in "QoS Configuration Wizard, Screen 5" (page 102).

QoS Configuration Wizard, Screen 5 - Access Lists

QoS Configuration Wizard

Step 1 - Access List Label | Step 2 - Access List Definition | Step 3 - Service | Step 4 - Ports

Access List Elements: 0
Access List Blocks: 0

Select the service class or action.

Service

- 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 ("QoS Configuration Wizard, Screen 6A" (page 103)). If so, the metering parameters window is displayed for configuration ("QoS Configuration Wizard, Screen 6B" (page 103)). If not, the user is taken to the next step.

QoS Configuration Wizard, Screen 6A

QoS Configuration Wizard

Step 1 - Policy Label | Step 2 - VLAN | Step 3 - Block | **Step 4 - Meter** | Step 5 - Service | Step 6 - Ports

Would you like to meter the traffic?

No
 Yes

Back **Next**

QoS Configuration Wizard, Screen 6B

QoS Configuration Wizard

Step 1 - Policy Label | Step 2 - VLAN | Step 3 - Block | **Step 4 - Meter** | Step 5 - Service | Step 6 - Ports

Enter the metering parameters.

Committed Rate kbps (1000 bits per second)
Maximum Burst Rate kbps (1000 bits per second)
Maximum Burst Duration

Back **Next**

- 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. This wizard screen is illustrated in "QoS Configuration Wizard, Screen 7" (page 103).

QoS Configuration Wizard, Screen 7

QoS Configuration Wizard

Step 1 - Policy Label | Step 2 - VLAN | Step 3 - Block | Step 4 - Meter | **Step 5 - Service** | Step 6 - Ports

Select the service class or action.

In-Profile Service
Out-of-Profile Service

Back **Next**

- 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. This wizard screen is illustrated in "QoS Configuration Wizard, Screen 8" (page 104).

QoS Configuration Wizard, Screen 8

QoS Configuration Wizard

Step 1 - Policy Label | Step 2 - VLAN | Step 3 - Block | Step 4 - Meter | Step 5 - Service | Step 6 - Ports

Select the ports on which the policy will be installed.

Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Click **Finish** when ports are selected.

If you created a filter set, the final screen in the wizard asks for the non-match action as shown in "QoS Configuration Wizard, Screen 8A- Filter Sets" (page 104).

Click **Next** to finish the wizard.

QoS Configuration Wizard, Screen 8A- Filter Sets

QoS Configuration Wizard

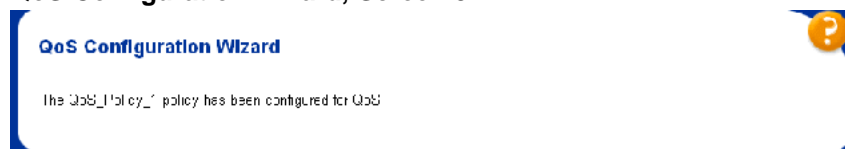
Step 1 - Filter Set Label | Step 2 - Filter Set Definition | Step 3 - Service | Step 5 - Non Match

Select the non-match action.

Non-Match Action:

- 10 The new policy is applied to the switch and saved. A confirmation screen similar to the one illustrated in "QoS Configuration Wizard, Screen 9" (page 105), is displayed to provide visual confirmation of the successful completion of the wizard.

QoS Configuration Wizard, Screen 9



—End—

QoS Management Wizard

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

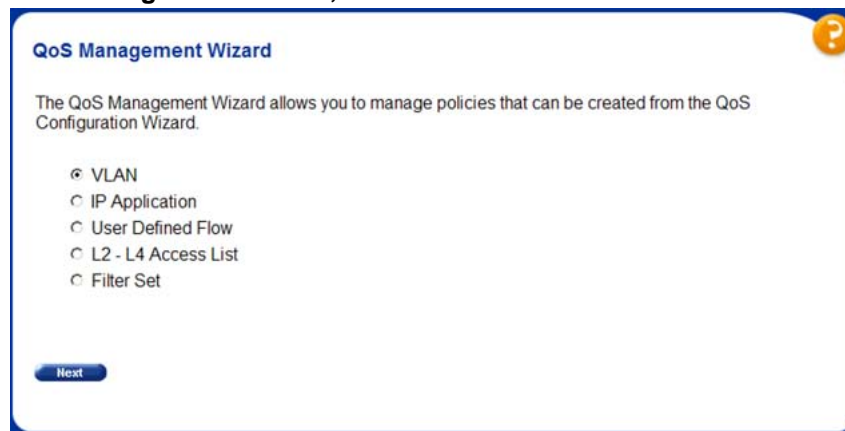
To manage a policy using this wizard, follow this procedure:

Step	Action
------	--------

- | | |
|---|--|
| 1 | Open the management wizard by selecting Application > QoS > QoS Wizard > QoS Wizard Mgmt from the menu. The screen illustrated in "QoS Management Wizard, Screen 1" (page 105) is displayed. |
|---|--|

Select the type of policy to be managed to continue.

QoS Management Wizard, Screen 1



- | | |
|---|---|
| 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. This screen is illustrated in "QoS Management Wizard, Screen 2" (page 106). |
|---|---|

QoS Management Wizard, Screen 2



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. "QoS Management Wizard, Screen 3 - VLAN" (page 106), "QoS Management Wizard, Screen 3 - IP Applications" (page 107), "QoS Management Wizard, Screen 3 - User Defined Flows" (page 107), "QoS Management Wizard, Screen 3 - Access Lists" (page 108), and (SS Here) display this screen for each policy type.

a. VLAN

QoS Management Wizard, Screen 3 - VLAN

QoS Management Wizard

Name QoS_Policy_1

Destination MAC Addr/Mask	Source MAC Addr/Mask	VLAN	VLAN Tag	EtherType	802.1p Priority	Block
Ignore	Ignore	1	Ignore	IP	Ignore	

Meter Committed Rate	1000 Kbps
Meter Committed Burst Size	512 Kbytes
In-Profile Action Drop	No
In-Profile Action Remark DSCP	0x0
In-Profile Action Remark COS	Priority 0
In-Profile Action Drop Precedence	High Drop
Out-Profile Action Drop	Yes
Out-Profile Action Remark DSCP	Ignore
Out-Profile Action Remark COS	Ignore
Out-Profile Action Drop Precedence	High Drop
Total In-Profile Packets	0
Total Out-Profile Packets	0

Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>																						

b. IP Applications

QoS Management Wizard, Screen 3 - IP Applications

QoS Management Wizard

Name QoS_Policy_2

Address Type	Destination IP Addr/Mask Length	Source IP Addr/Mask Length	DSCP	IPv4 Protocol / IPv6 Next Header	Destination L4 Port	Source L4 Port	IPv6 Flow Id	Block
IPv4	Ignore	Ignore	Ignore	TCP	Ignore	80	Ignore	
IPv4	Ignore	Ignore	Ignore	TCP	80	Ignore	Ignore	

Meter Committed Rate	1000 Kbps
Meter Committed Burst Size	512 Kbytes
In-Profile Action Drop	No
In-Profile Action Remark DSCP	0x0
In-Profile Action Remark COS	Priority 0
In-Profile Action Drop Precedence	High Drop
Out-Profile Action Drop	Yes
Out-Profile Action Remark DSCP	Ignore
Out-Profile Action Remark COS	Ignore
Out-Profile Action Drop Precedence	High Drop
Total In-Profile Packets	0
Total Out-Profile Packets	0

Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

c. User Defined Flows

QoS Management Wizard, Screen 3 - User Defined Flows

QoS Management Wizard

Name QoS_Policy_3

Destination MAC Addr/Mask	Source MAC Addr/Mask	VLAN	VLAN Tag	EtherType	802.1p Priority	Block
Ignore	Ignore	1	Tagged	IP	Ignore	

Meter Committed Rate	1000 Kbps
Meter Committed Burst Size	512 Kbytes
In-Profile Action Drop	No
In-Profile Action Remark DSCP	0x0
In-Profile Action Remark COS	Priority 0
In-Profile Action Drop Precedence	High Drop
Out-Profile Action Drop	Yes
Out-Profile Action Remark DSCP	Ignore
Out-Profile Action Remark COS	Ignore
Out-Profile Action Drop Precedence	High Drop
Total In-Profile Packets	0
Total Out-Profile Packets	0

Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

d. Layer 2 - Layer 4 Access List

QoS Management Wizard, Screen 3 - Access Lists

QoS Management Wizard

Name

Destination MAC Addr/Mask	Source MAC Addr/Mask	VLAN	VLAN Tag	EtherType	802.1p Priority	Block	Action Drop	Action Remark DSCP	Action Remark COS	Action Drop Precedence
Ignore	Ignore	Ignore	Ignore	IP	Ignore		No	DxD	Priority 0	High Drop

Total Packets

Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
		25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input type="checkbox"/>																							

e. Filter Sets

QoS Management Wizard, Screen 3 - Filter Sets

QoS Management Wizard

Name

Action Id	Address Type	Destination IP Addr/Mask Length	Source IP Addr/Mask Length	DSCP	IPv4 Protocol / IPv6 Next Header	Destination L4 Port	Source L4 Port	IPv6 Flow Id	Destination MAC Addr/Mask
<input checked="" type="checkbox"/>	6 IPv4	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore

Meter Committed Rate	<input type="text" value="1000"/> Kbps
Meter Committed Burst Size	<input type="text" value="512"/> KBytes
Out-Profile Action Drop	<input type="text" value="Yes"/>
Out-Profile Action Remark DSCP	Ignore
Out-Profile Action Remark COS	Ignore
Out-Profile Action Drop Precedence	High Drop
Non Match Action	Defer

Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
		25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48

—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:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the Interface Shaper wizard by selecting Application > QoS > QoS Wizard > Interface Shaper from the menu. The screen illustrated in "QoS Interface Shaper Wizard, Screen 1" (page 109) is displayed. |
|---|---|

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**.

QoS Interface Shaper Wizard, Screen 1

Interface Shaper Setting			
<input type="radio"/> Add	Port	Name	Rate (Kbps)
<input type="radio"/> Delete			Burst Size (Bytes)
<input type="checkbox"/>	1		
<input type="checkbox"/>	2		
<input type="checkbox"/>	3		
<input type="checkbox"/>	4		
<input type="checkbox"/>	5		
<input type="checkbox"/>	6		
<input type="checkbox"/>	7		
<input type="checkbox"/>	8		
<input type="checkbox"/>	9		
<input type="checkbox"/>	10		
<input type="checkbox"/>	11		
<input type="checkbox"/>	12		
<input type="checkbox"/>	Switch		

Submit

[Ports 13 - 24](#) [Ports 25 - 26](#)

- | | |
|---|--|
| 2 | If adding an interface shaper, the wizard displays the screen illustrated in "QoS Interface Shaper Wizard, Screen 2" (page 110). Use this screen to set the parameters for the new interface shaper. |
|---|--|

QoS Interface Shaper Wizard, Screen 2

"Interface Shaper Creation fields" (page 110) outlines the fields on this screen.

Interface Shaper Creation fields

Field	Description
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.

Click **Submit** when finished.

—End—

QoS Interface Applications Wizard

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

Note: Due to hardware limitations, the Ethernet Routing Switch 5520 model only supports 11 interface applications per port.

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

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the Interface Applications wizard by selecting Application > QoS > QoS Wizard > Interface Applications from the menu. This screen is illustrated in "QoS Interface Applications Wizard - Screen 1" (page 111). |
|---|---|

- 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**.

QoS Interface Applications Wizard - Screen 1

Application > QoS > Interface Applications

Interface Applications Setting

<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Action	Port	ARP Spoofing	Default Gateway	DHCP Snooping	Interface Type	DHCP Spoofing	DHCP Server	DoS SQLSlam	DoS Nachia	DoS Xmas	DoS TCP SynFinScan
<input type="checkbox"/>		1										
<input type="checkbox"/>		2										
<input type="checkbox"/>		3										
<input type="checkbox"/>		4										
<input type="checkbox"/>		5										
<input type="checkbox"/>		6										
<input type="checkbox"/>		7										
<input type="checkbox"/>		8										
<input type="checkbox"/>		9										
<input type="checkbox"/>		10										
<input type="checkbox"/>		11										
<input type="checkbox"/>		12										
<input type="checkbox"/>		Switch										

[Ports 13 - 24](#) [Ports 25 - 26](#)

- 4 The second wizard screen configures the applications. Select or de-select the applications to apply against the designated ports. This screen is illustrated in "QoS Interface Applications Wizard - Screen 2" (page 112).
 - 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.

QoS Interface Applications Wizard - Screen 2

Application > QoS > Interface Applications

Interface Applications Creation

<input type="checkbox"/>	ARP Spoofing	Default Gateway	<input type="text"/>
<input type="checkbox"/>	DHCP Snooping	Interface Type	Access
<input type="checkbox"/>	DHCP Spoofing	DHCP Server	<input type="text"/>
<input type="checkbox"/>	DoS SQLSlam		
<input type="checkbox"/>	DoS Nachia		
<input type="checkbox"/>	DoS Xmas		
<input type="checkbox"/>	DoS TCP SynFinScan		
<input type="checkbox"/>	DoS TCP FtpPort		
<input type="checkbox"/>	DoS TCP DnsPort		
<input type="checkbox"/>	BPDU Blocker		

Submit Back

—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, perform the following procedure:

Step	Action
------	--------

- | | |
|---|--|
| 1 | Open the Interface Config screen by selecting Applications > QoS > QoS Advanced > Devices > Interface Config from the menu. This screen is illustrated in " Interface Config screen " (page 113). |
|---|--|

Interface Config screen

The screenshot shows the Nortel configuration interface for 'Interface Configuration'. On the left is a navigation tree with 'Access (RW)' expanded to 'Devices' and 'Interface Config'. The main area displays the 'Interface Queue Table' with the following data:

Set ID	Queue ID	General Discipline	Bandwidth %	Absolute Bandwidth (Kbps)	Bandwidth Allocation	Service Order	Size (Bytes)
1	1	Priority Queuing	100	0	Relative	1	262144
1	1	Priority Queuing	100	0	Relative	1	190224
2	2	Priority Queuing	100	0	Relative	2	81920
1	1	Priority Queuing	100	0	Relative	1	109568
3	2	Weighted Round Robin	75	0	Relative	2	87040
3	3	Weighted Round Robin	25	0	Relative	2	65536
1	1	Priority Queuing	100	0	Relative	1	81920
2	2	Weighted Round Robin	65	0	Relative	2	74240
3	3	Weighted Round Robin	26	0	Relative	2	61440
4	4	Weighted Round Robin	9	0	Relative	2	44544
1	1	Priority Queuing	100	0	Relative	1	64000
2	2	Weighted Round Robin	58	0	Relative	2	59904
3	3	Weighted Round Robin	27	0	Relative	2	53760
1	1	Weighted Round Robin	11	0	Relative	2	46080
5	5	Weighted Round Robin	4	0	Relative	2	38400
1	1	Priority Queuing	100	0	Relative	1	51200
2	2	Weighted Round Robin	52	0	Relative	2	49152
3	3	Weighted Round Robin	24	0	Relative	2	47104
4	4	Weighted Round Robin	14	0	Relative	2	43008
5	5	Weighted Round Robin	7	0	Relative	2	37376
6	6	Weighted Round Robin	3	0	Relative	2	34304
1	1	Priority Queuing	100	0	Relative	1	49152
2	2	Weighted Round Robin	45	0	Relative	2	46080
3	3	Weighted Round Robin	21	0	Relative	2	39936
7	4	Weighted Round Robin	15	0	Relative	2	33280

- 2 In the **Interface Group Creation** section ("Interface Group Creation section" (page 113)), type a role combination name in the **Role Combination** field and select an interface class from the **Interface Class** list.

Interface Group Creation section

The screenshot shows the 'Interface Group Creation' section. It contains two input fields: 'Role Combination' (empty) and 'Interface Class' (set to 'Unrestricted'). Below these fields is a 'Submit' button.

- 3 Click **Submit**.

The new interface group configuration is displayed in the **Interface Group Table** section.

—End—

Displaying Interface ID Table

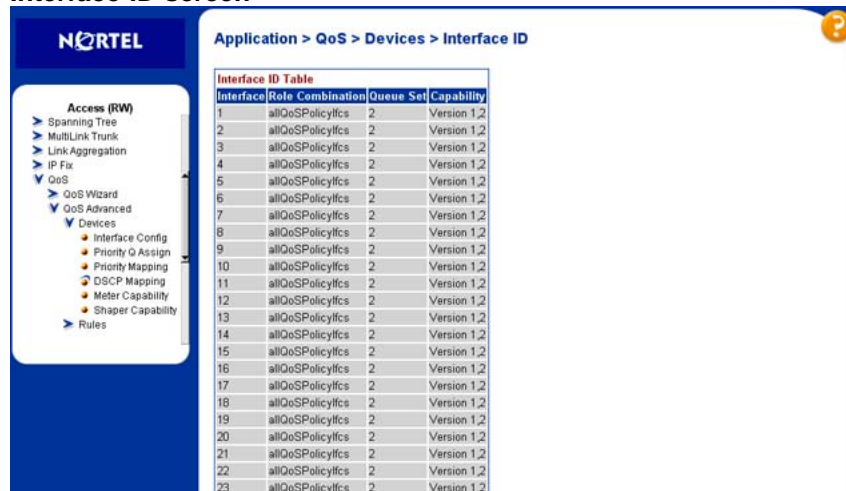
To display the Interface ID Table, use the following procedure:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the Interface Config screen by selecting Applications > QoS > QoS Advanced > Devices > Interface Config from the menu. This screen is illustrated in "Interface Config screen" (page 113). |
| 2 | Click Display Interface ID Table . |

The **Interface ID** screen opens ("Interface ID screen" (page 114)). 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.

Interface ID screen



—End—

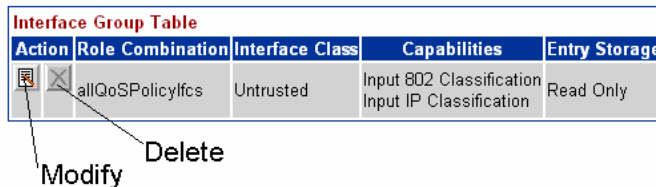
Adding or Removing Interface Group Members

To select or de-select ports as members of an existing interface group perform these tasks:

Step Action

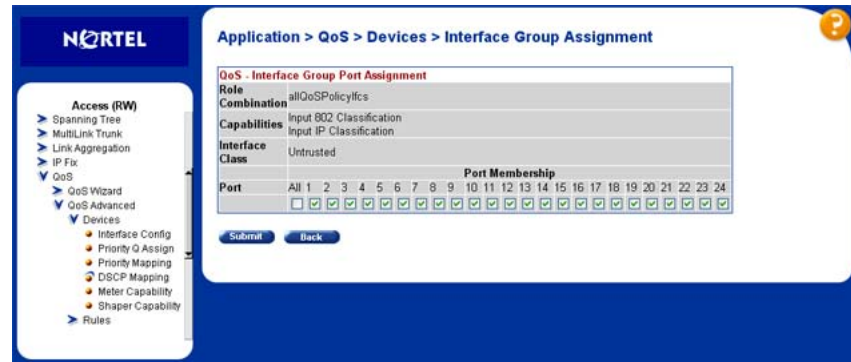
- 1 Open the **Interface Config** screen by selecting **Applications > QoS > QoS Advanced > Devices > Interface Config** from the menu. This screen is illustrated in "Interface Config screen" (page 113).
- 2 In the **Interface Group Table** section, click the **Modify** icon in the row to be modified. This section is illustrated in "Interface Group Table section" (page 114).

Interface Group Table section



The **Interface Group Assignment** screen opens ("Interface Group Assignment screen" (page 115)).

Interface Group Assignment screen



- 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:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the Interface Config screen by selecting Applications > QoS > QoS Advanced > Devices > Interface Config from the menu. This screen is illustrated in "Interface Config screen" (page 113). |
| 2 | In the Interface Group Table section ("Interface Group Table section" (page 114)), 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.

To configure 802.1p user priority:

Step Action

- 1 Open the **Priority Queue Assignment** screen by selecting **Applications > QoS > QoS Advanced > Devices > Priority Q Assign** from the menu. This screen is illustrated in "[Priority Queue Assignment screen](#)" (page 116).

Priority Queue Assignment screen

The screenshot shows the Nortel web-based management interface. The breadcrumb trail at the top reads: Application > QoS > Devices > 802.1p Priority Queue Assignment. The main content area is titled "802.1p Priority Assignment (View By)". It features a "Queue Set" dropdown menu currently set to "1" and a "Submit" button below it. Below the dropdown is a table titled "802.1p Priority Assignment Table". The table has two columns: "802.1p Priority" and "Queue". The rows are numbered 0 through 7. Each row has a small input field in the "Queue" column, all of which currently contain the value "1". There is another "Submit" button at the bottom of the table.

- 2 In the **802.1p Priority Assignment (View By)** section, select the queue 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 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.

- Click the **Submit** button immediately under the **802.1p Priority Assignment Table** section.

—End—

Configuring 802.1p priority mapping

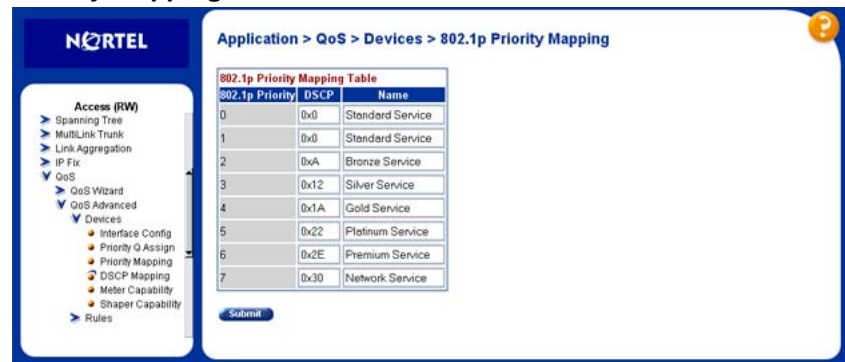
Note: Nortel Networks recommends using the default 802.1p priority to DSCP mappings to ensure end-to-end QoS connectivity.

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

Step	Action
------	--------

- Open the **Priority Mapping** screen by selecting **Applications > QoS > QoS Advanced > Devices > Priority Mapping** from the menu. This screen is illustrated in "Priority Mapping screen" (page 117).

Priority Mapping screen



- In the fields provided, enter the priority mapping information. "Priority Mapping fields" (page 117) outlines the fields on this screen.

Priority Mapping fields

Field	Description
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.

- Click **Submit**.

—End—

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:

Step	Action
------	--------

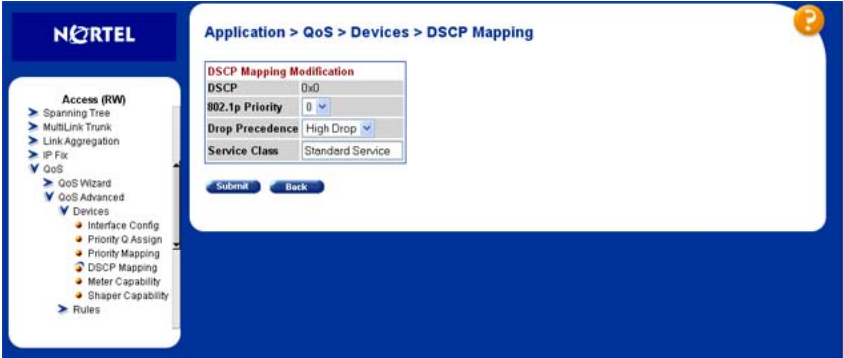
- 1 Open the **DSCP Mapping** screen by selecting **Applications > QoS > QoS Advanced > Devices > DSCP Mapping** from the menu. This screen is illustrated in "DSCP Mapping screen" (page 118).

DSCP Mapping screen

Action	DSCP	802.1p Priority	Drop Precedence	Service Class
	0x0	0	High Drop	Standard Service
	0x1	0	High Drop	Standard Service
	0x2	0	High Drop	Standard Service
	0x3	0	High Drop	Standard Service
	0x4	0	High Drop	Standard Service
	0x5	0	High Drop	Standard Service
	0x6	0	High Drop	Standard Service
	0x7	0	High Drop	Standard Service
	0x8	2	High Drop	Bronze Service
	0x9	0	High Drop	Standard Service
	0xA	2	Low Drop	Bronze Service
	0xB	0	High Drop	Standard Service
	0xC	2	High Drop	Bronze Service
	0xD	0	High Drop	Standard Service
	0xE	2	High Drop	Bronze Service
	0xF	0	High Drop	Standard Service
	0x10	3	High Drop	Silver Service
	0x11	0	High Drop	Standard Service
	0x12	3	Low Drop	Silver Service
	0x13	0	High Drop	Standard Service

- 2 Click the icon in the **Action** column of the row to be configured. The **DSCP Mapping Modification** screen opens. This screen is illustrated in "DSCP Mapping Modification screen" (page 119).

DSCP Mapping Modification screen



3 In the fields provided, modify the mapping scheme. "DSCP Mapping Modification fields" (page 119) describes the fields on this screen.

DSCP Mapping Modification fields

Field	Description
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: <ul style="list-style-type: none"> • High Drop • Low Drop <p>Note: Generally, low packet drop precedence receives preferential treatment.</p>
Service Class	Enter the service class. <p>Note: This field corresponds to the adjacent user priority levels.</p>
	Note: Mappings created on the DSCP mapping modification page are used at egress for marking traffic.

4 Click **Submit**.

—End—

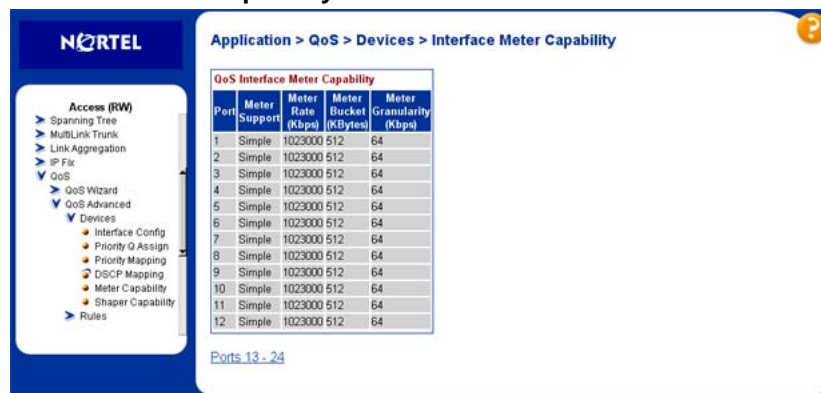
Displaying QoS Meter Capability

To display QoS interface meter capabilities:

Step	Action
------	--------

- | | |
|---|--|
| 1 | Open the Interface Meter Capability screen by selecting Applications > QoS > QoS Advanced > Devices > Meter Capability from the menu. This screen is illustrated in "Interface Meter Capability" (page 120). |
|---|--|

Interface Meter Capability



"Interface Meter Capability fields" (page 120) outlines the fields on this screen.

Interface Meter Capability fields

Field	Description
Port	The port that the meter is applied to.
Meter Support	The supported Token Bucket metering algorithm..
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.

—End—

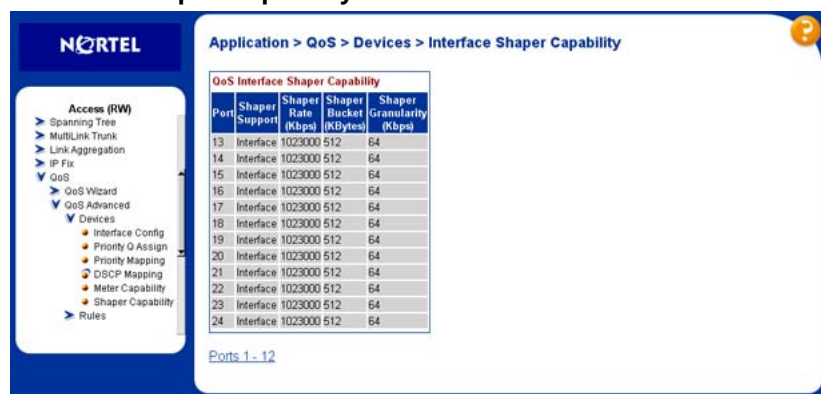
Displaying QoS shaper capability

To display QoS interface shaper capabilities:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the Interface Shaper Capability screen by selecting Applications > QoS > QoS Advanced > Devices > Shaper Capability from the menu. This screen is illustrated in "Interface Shaper Capability" (page 121). |
|---|---|

Interface Shaper Capability



"Interface Shaper Capability fields" (page 121) outlines the fields on this screen.

Interface Shaper Capability fields

Field	Description
Port	The port to which the meter is applied.
Shaper Support	Displays where the shaper is applied.
Shaper Rate (Kbps)	Displays maximum supported Shaper Rate.
Shaper Bucket (KBytes)	Displays maximum supported Shaper Bucket size.
Shaper Granularity (Kbps)	Displays supported Shaper Granularity.

—End—

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 and classifier blocks, which determine access to, and denial of, network services.

Creating an IP classifier element

To create an IP classifier element:

Step	Action
------	--------

- | | |
|---|--|
| 1 | Open the IP Classifier Element screen by selecting Applications > QoS > QoS Advanced > Rules > IP Classifier Element from the menu. This screen is illustrated in "IP Classifier Element screen" (page 122). |
|---|--|

IP Classifier Element screen

- | | |
|---|---|
| 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. "IP Classifier Element Creation fields" (page 122) describes the fields in this section. |
|---|---|

IP Classifier Element Creation fields

Field	Description
Address Type	The type of IP address this classifier uses.

Field	Description
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.
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 hexadecimal value of the flow identifier to match.

3 Click **Submit**.

The new element is displayed in the **IP Classifier Element Table** section of the screen.

—End—

Deleting an IP classifier element configuration

To delete a IP classifier element configuration:

Step	Action
------	--------

- | | |
|----------|--|
| 1 | Open the IP Classifier Element screen by selecting Applications > QoS > QoS Advanced > Rules > IP Classifier Element from the menu. This screen is illustrated in " IP Classifier Element screen " (page 122). |
| 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 or classifier block 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

To create a Layer 2 classifier element configuration:

Step	Action
------	--------

- | | |
|---|--|
| 1 | Open the Layer2 Classifier Element screen by selecting Applications > QoS > QoS Advanced > Rules > Layer2 Classifier Element from the menu. This screen is illustrated in " Layer2 Classifier Element screen " (page 124). |
|---|--|

Layer2 Classifier Element screen

The screenshot shows the 'Layer2 Classifier Element' configuration screen. On the left is a navigation tree with 'Rules' expanded to 'Layer2 Classifier Element'. The main content area has a breadcrumb 'Application > QoS > Rules > Layer2 Classifier Element'. Below this is a table titled 'L2 Classifier Element Table' with columns: Action, Instance, Destination MAC Addr, Destination MAC Addr Mask, Source MAC Addr, Source MAC Addr Mask, VLAN, VLAN Tag, EtherType, 802.1p Priority, and Storage Type. Two rows are shown with instances 55001 and 55002. Below the table is the 'Layer2 Classifier Element Creation' form. It has radio buttons for 'Ignore' and input fields for 'Destination MAC Address' and 'Source MAC Address'. There are also radio buttons for 'VLAN' (Ignore or VLAN Range) and 'EtherType' (Ignore, Preconfigured, or User Defined). A 'Submit' button is at the bottom.

- | | |
|---|---|
| 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. " Layer2 Classifier Element Creation fields " (page 124) describes the fields in this section. |
|---|---|

Layer2 Classifier Element Creation fields

Field	Description
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.

Field	Description
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.

- 3 Click **Submit**.

The new Layer 2 Classifier Element is displayed in **Layer2 Classifier Element Table**.

—End—

Deleting a layer 2 classifier element configuration

To delete a layer 2 classifier element configuration:

Step	Action
------	--------

- 1 Open the **Layer2 Classifier Element screen** by selecting **Applications > QoS > QoS Advanced > Rules > Layer2 Classifier Element** from the menu. This screen is illustrated in "[Layer2 Classifier Element screen](#)" (page 124).
- 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 or classifier block 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 5500 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.

To configure a System Classifier Element follow this procedure:

Step Action

- 1 Open the **System Classifier Element** screen by selecting **Applications > QoS > QoS Advanced > Rules > System Clfr Elem** from the menu. This screen is illustrated in "[System Classifier Element screen](#)" (page 126).

System Classifier Element screen

Application > QoS > Rules > System Classifier Element

Action	Instance	Unknown Ucast Frames	Unknown Mcast Frames	Known Mcast Frames	Pattern	Session ID	Storage Type
--------	----------	----------------------	----------------------	--------------------	---------	------------	--------------

System Classifier Element Creation

Ignore
 Unknown Unicast
 Unknown Multicast
 Known Multicast

Dst MAC Addr Type

Pattern

Fill with: Zeroes

Address Type: IPv4 IPv6
VLAN Tag: Tagged Untagged

Dst MAC Address
 Src MAC Address
 802.1p Priority
 VLAN ID
 EtherType
 IP Version
 DSCP
 Protocol/Next Header
 Src IP Address

Data (hex)															
1	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
9	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
17	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
25	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
33	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
41	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
49	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
57	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
65	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

- 2 In the **System Classifier Element Creation** section, edit the fields provided to create the new classifier element. "[System Classifier Element Creation fields](#)" (page 127) outlines the fields in this section.

System Classifier Element Creation fields

Field	Description
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.

- 3 Click **Submit**.

—End—

Classifier Configurations

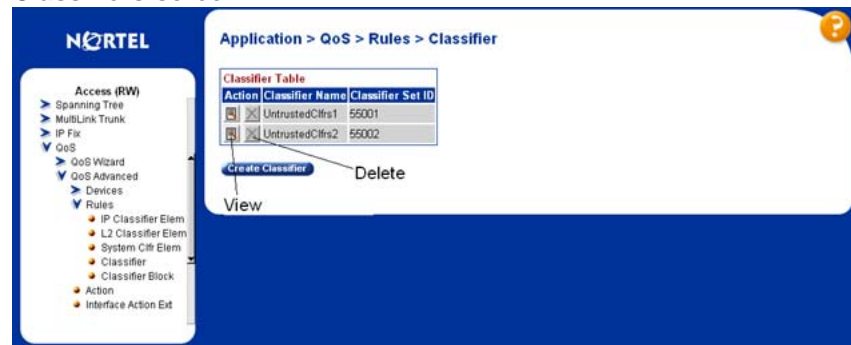
Viewing Existing Classifiers

To view existing classifiers, follow this procedure:

Step Action

- 1 Open the **Classifiers** screen by selecting **Applications > QoS > QoS Advanced > Rules > Classifier**. This screen is illustrated in "Classifiers screen" (page 127).

Classifiers screen



- 2 Click the **View** icon beside the desired classifier.

—End—

Creating a Classifier

To create a new classifier, follow this procedure:

Step Action

- 1 Open the **Classifiers** screen by selecting **Applications > QoS > QoS Advanced > Rules > Classifier**. This screen is illustrated in "Classifiers screen" (page 127).
- 2 Click **Create Classifier**.
- 3 The **Create Classifier** screen opens. This screen is illustrated "Create Classifier screen" (page 128).

Create Classifier screen

- 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

To delete a classifier:

Step	Action
1	Open the Classifiers screen by selecting Applications > QoS > QoS Advanced > Rules > Classifier . This screen is illustrated in "Classifiers screen" (page 127).
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

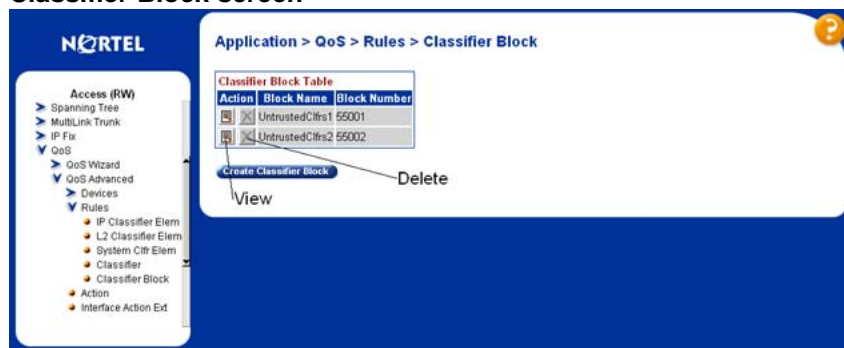
Note: Each classifier in a classifier block must match the same parameters and the same mask, range, and VLAN tag type. Additionally, all members of a classifier block must be configured consistently regarding meters and actions--that is, they must all specify meters or they must all not specify meters,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

Viewing Classifier Blocks

To view classifier blocks, use the following procedure:

Step	Action
1	Open the Classifier Blocks screen by selecting Applications > QoS > QoS Advanced > Rules > Classifier Block from the menu. This screen is illustrated in "Classifier Block screen" (page 129).

Classifier Block screen



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:

- | Step | Action |
|------|--|
| 1 | Open the Classifier Blocks screen by selecting Applications > QoS > QoS Advanced > Rules > Classifier Block from the menu. This screen is illustrated in "Classifier Block screen" (page 129). |
| 2 | Click Create Classifier Block . |
| 3 | The Create Classifier Block screen opens. This screen is illustrated in "Create Classifier Block screen" (page 130). |

Create Classifier Block screen



- 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:

Step Action

- 1 Open the **Classifier Blocks** screen by selecting **Applications > QoS > QoS Advanced > Rules > Classifier Block** from the menu. This screen is illustrated in "[Classifier Block screen](#)" (page 129).
 - 2 Click the **Delete** icon in the row of the classifier block to be deleted.
-

—End—

Configuring QoS actions

When an action is created, the action is associated with specific classifiers and classifier blocks. An action specifies the type of behavior a policy to 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:

Step Action

- 1 Open the **Action** screen by selecting **Applications > QoS > QoS Advanced > Action** from the menu. This screen is illustrated in "[Action screen](#)" (page 131).

Action screen

Application > QoS > Action

Action	Action Name	Instance	Drop Frame	Update DSCP	Set Drop Precedence	Update 802.1p Priority	Extension	Storage Type
	Drop_Traffic	1	Yes	Ignore	High Drop	Ignore	None	Read Only
	Standard_Service	2	No	Dx0	High Drop	Priority 0	None	Read Only
	Bronze_Service	3	No	DxA	Low Drop	Priority 2	None	Read Only
	Silver_Service	4	No	Dx12	Low Drop	Priority 3	None	Read Only
	Gold_Service	5	No	Dx1A	Low Drop	Priority 4	None	Read Only
	Platinum_Service	6	No	Dx22	Low Drop	Priority 5	None	Read Only
	Premium_Service	7	No	Dx2E	Low Drop	Priority 6	None	Read Only
	Network_Service	8	No	Dx30	Low Drop	Priority 7	None	Read Only
	Null_Action	9	No	Ignore	Low Drop	Ignore	None	Read Only
	UntrustedClrs1	55001	Deferred Pass	Derive from Ingress Priority	Low Drop	Ignore	None	Other
	UntrustedClrs2	55002	Deferred Pass	Dx0	High Drop	Priority 0	None	Other

Action Creation

Action Name:

Drop Frame:

Update DSCP:

Set Drop Precedence:

Update 802.1p Priority:

Extension:

- 2 In the fields provided, use the **Action Creation** section to create the new action. "[Action Creation fields](#)" (page 132) outlines the fields in this area.
-

Action Creation fields

Field	Description
Action Name	The name to associate with this action.
Drop Frame	<p>Choose whether the frame being evaluated is dropped or transmitted by this attribute:</p> <ul style="list-style-type: none"> • Deferred Pass - traffic flow decision deferred to other installed policies • No - do not drop the traffic flow • Yes - drop the traffic flow <p>The default setting is Deferred Pass.</p>
Update DSCP	<p>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.</p> <p>The default setting is Ignore.</p>
Set Drop Precedence	<p>Choose a packet drop precedence value.</p> <p>Note: Generally, low packet drop precedence receives preferential treatment.</p> <p>The default setting is Low Drop.</p>
Update 802.1p Priority	<p>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).</p> <p>The default setting is Ignore.</p>
Extension	Choose either No Extension or one of the extensions created on the Interface Action Extension page.

Field	Description
	The default setting is None.

- 3 Click **Submit**.

—End—

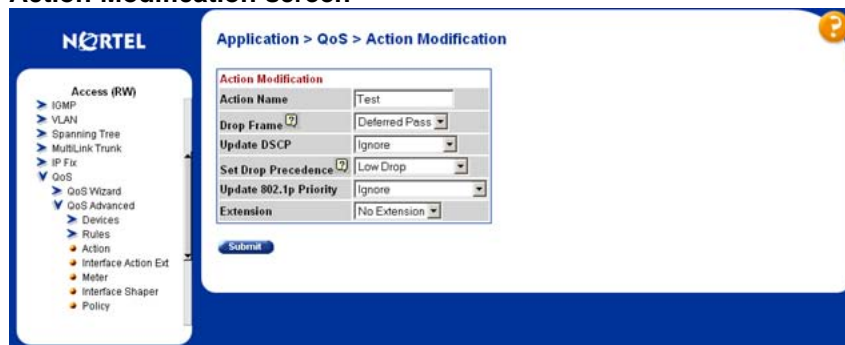
Modifying an action configuration

To modify an action configuration:

Step Action

- 1 Open the **Action** screen by selecting **Applications > QoS > QoS Advanced > Action** from the menu. This screen is illustrated in "Action screen" (page 131).
- 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. This screen is illustrated in "Action Modification screen" (page 133).

Action Modification screen



- 4 In the fields provided, modify the Action. Refer to "Action Creation fields" (page 132) for an explanation of these fields.
- 5 Click **Submit**.

—End—

Deleting an Action

To delete an action configuration, follow this procedure:

Step	Action
1	Open the Action screen by selecting Applications > QoS > QoS Advanced > Action from the menu. This screen is illustrated in " Action screen " (page 131).
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:

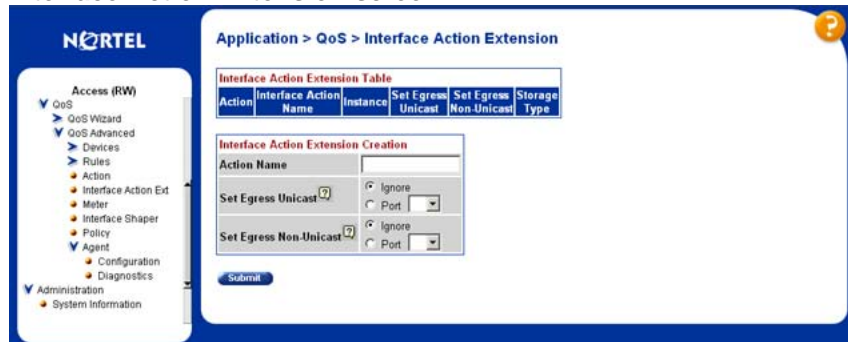
- Set an egress unicast
- Set an egress non-unicast

Creating an Interface Action Extension

To create an interface action extension follow this procedure:

Step	Action
1	Open the Interface Action Extension screen by selecting Applications > QoS > QoS Advanced > Interface Action Ext. This screen is illustrated in " Interface Action Extension screen " (page 135).

Interface Action Extension screen



- 2 In the **Interface Action Extension Creation** section, use the fields provided to create the new action extension. "[Interface Action Extension Creation fields](#)" (page 135) outlines the fields in this section.

Interface Action Extension Creation fields

Field	Description
Action Name	The name for this action extension.
Set Egress Unicast	Choose either: <ul style="list-style-type: none"> Ignore - the system does not set an egress unicast port Choose the port for the egress unicasts. <p>The default setting is Ignore.</p>
Set Egress Non-Unicast	Choose either: <ul style="list-style-type: none"> Ignore - the system does not set an egress unicast port Choose the port for the egress non-unicasts. <p>The default setting is Ignore.</p>

- 3 Click **Submit**.

—End—

Deleting an interface action extension configuration

To delete an interface action extension, complete these tasks:

- | Step | Action |
|------|--|
| 1 | Open the Interface Action Extension screen by selecting Applications > QoS > QoS Advanced > Interface Action Ext. This screen is illustrated in " Interface Action Extension screen " (page 135). |
| 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:

- | Step | Action |
|------|---|
| 1 | Open the Meter screen by selecting Applications > QoS > QoS Advanced > Meter from the menu. This screen is illustrated in " Meter screen " (page 136). |

Meter screen

The screenshot shows the 'Meter Creation' screen in the Nortel web-based management interface. The interface has a blue header with the Nortel logo and a navigation menu on the left. The main content area is titled 'Application > QoS > Meter'. It features a 'Meter Table' with columns for Action Name, Instance, Committed Rate (Kbps), Committed Burst Size (Bytes), In-Profile Action, Out-of-Profile Action, and Storage Type. Below the table is a 'Meter Creation' form with fields for Name, Committed Rate (Kbps), Committed Burst Size, Maximum Burst Rate (Kbps), Duration, In-Profile Action (Drop_Traffic), and Out-Of-Profile Action (Drop_Traffic). A 'Submit' button is located at the bottom of the form.

- 2 In the Meter Creation section, use the fields provided to create the new meter. "Meter Creation fields" (page 137) outlines the fields in this area.

Meter Creation fields

Field	Description
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	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Default actions All actions you created using the Action page The default setting is Drop Traffic.

- 3 Click **Submit**.

—End—

Viewing meters

To view a meter:

Step	Action
1	Open the Meter screen by selecting Applications > QoS > QoS Advanced > Meter from the menu. This screen is illustrated in "Meter screen" (page 136).
2	View created meters in the Meter Table .

—End—

Deleting a meter

To delete a meter:

Step	Action
1	Open the Meter screen by selecting Applications > QoS > QoS Advanced > Meter from the menu. This screen is illustrated in "Meter screen" (page 136).
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

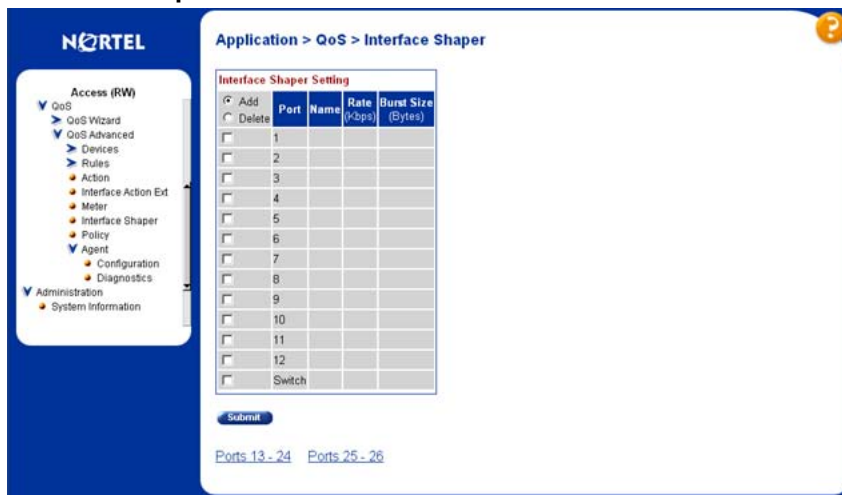
Interface Shaping is a method that involves limiting the traffic rate at egress through a specific interface. Interface-based shaping allows administrators to limit egress traffic generation independent of other QoS components. It provides limited shaping capabilities with minimal configuration requirements.

Configuring Interface Shaping parameters

To add interface shaping parameters for a port or set of ports:

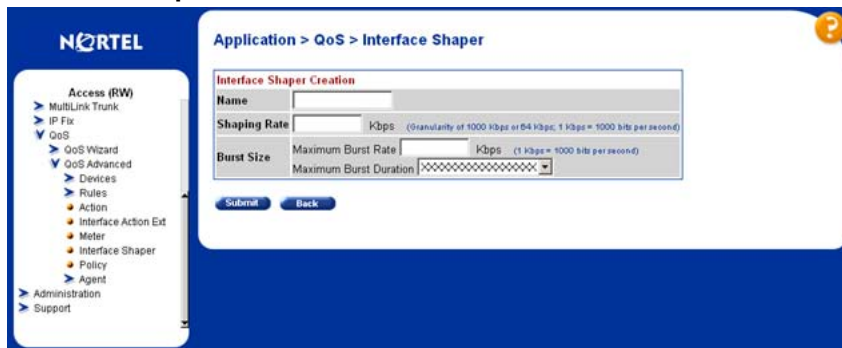
Step	Action
1	Open the Interface Shaper screen by selection Applications > QoS > QoS Advanced > Interface Shaper . This screen is illustrated in "Interface Shaper screen" (page 139).

Interface Shaper screen



- 2 Click on the **Add** option button and select the desired ports.
- 3 Click **Submit**.
- 4 The **Interface Shaper Creation** screen is displayed. This screen is displayed in "Interface Shaper Creation screen" (page 139).

Interface Shaper Creation screen



- 5 Using the fields provided, enter the parameters for the new interface shaper entry. "Interface Shaper Creation fields" (page 139) describes the fields on this screen.

Interface Shaper Creation fields

Field	Description
Name	Denotes the name of the Interface.
Shaping Rate	Signifies the shaping rate in multiples of 64 or 1000 Kbps.

Field	Description
Maximum Burst Rate	Denotes the maximum burst rate in Kbps.
Maximum Burst Duration	Signifies the period that the maximum burst rate is allowed.

6 Click **Submit**.

—End—

Deleting Interface Shaping Parameters

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

To delete the parameters:

Step	Action
1	Open the Interface Shaper screen by selection Applications > QoS > QoS Advanced > Interface Shaper . This screen is illustrated in "Interface Shaper screen" (page 139).
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

To create a hardware policy filter configuration, perform these tasks:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the Policy screen by selecting Application > QoS > QoS Advanced > Policy from the menu. This screen is illustrated in "Policy screen" (page 141). |
|---|---|

Policy screen

- | | |
|---|---|
| 2 | In the Policy Creation section, enter the information for the policy in the fields provided. "Policy Creation fields" (page 141) describes the fields in this section. |
|---|---|

Policy Creation fields

Field	Description
Policy Name	Type a character string to create a unique name to identify this policy.
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.

Field	Description
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: <ul style="list-style-type: none"> • 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, an In-Profile Action are not be chosen here; the policy is referenced from the Meter entry.
Non-Match Action	Choose the action to take associated with this policy for data that is not within the configured profile.
Track Statistics	Choose whether to track statistics for this policy and the granularity of the statistics desired. The default setting is No.

3 Click **Submit**.

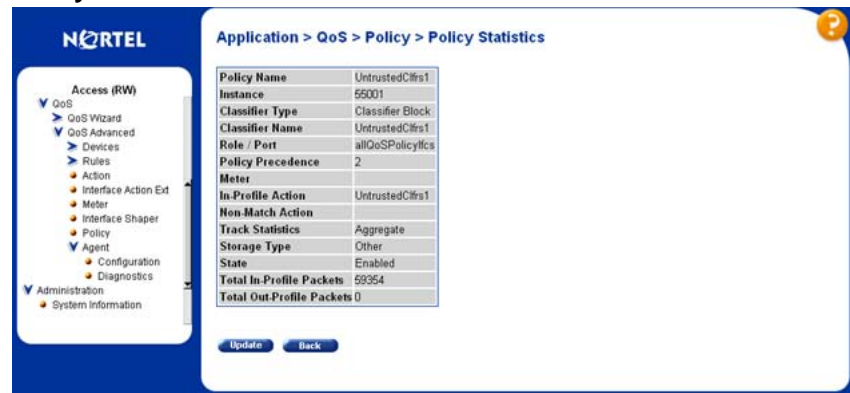
—End—

Viewing hardware policy statistics

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

- | Step | Action |
|------|---|
| 1 | Open the Policy screen by selecting Application > QoS > QoS Advanced > Policy from the menu. This screen is illustrated in "Policy screen" (page 141). |
| 2 | Click the View icon in the Policy Table section for the policy to be viewed. The Policy Statistics screen opens. This screen is illustrated in "Policy Statistics screen" (page 143). |

Policy Statistics screen



—End—

Deleting a hardware policy configuration

To delete a hardware policy configuration:

- | Step | Action |
|------|---|
| 1 | Open the Policy screen by selecting Application > QoS > QoS Advanced > Policy from the menu. This screen is illustrated in "Policy screen" (page 141). |
| 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 the Web-based Management Interface.

To open the configure QPA parameters follow this procedure:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the Agent Configuration screen by selecting Application > QoS > QoS Advanced > Agent > Configuration from the menu. This screen is illustrated in "Agent Configuration screen" (page 144). |
|---|---|

Agent Configuration screen

Policy Class Name	Current Instances	Maximum Installed Instances
ntrnQoSPrctSupportSupportedPrct	25	0
ntrnQoSPrctDeviceIdentDescr	1	0
ntrnQoSInterfaceTypeTable	1	100
ntrnQoSIfQueueSetId	36	0
ntrnQoSIfAssignmentRoleCombination	26	512
ntrnQoSDiscpToCosDiscp	64	64
ntrnQoSCosToDiscpCos	8	8
ntrnQoSQsetPriAssignmentQset	64	8
ntrnDsMultiFieldCltrAddrType	0	200
ntrnL2MultiFieldCltrDstAddr	2	200
ntrnSystemCltrUnknownUcastFrames	0	100
ntrnCltrComponentSpecific	2	400
ntrnCltrBlockNumber	2	200

- | | |
|---|---|
| 2 | In the QoS Configuration section, configure the agent parameters using the fields provided. "QoS Configuration fields" (page 144) describes the fields in this area. |
|---|---|

QoS Configuration fields

Field	Description
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.
Buffering	Choose the QoS resource buffer allocation scheme.
QoS WEB Display Mode	Choose to display either only user-created parameters, only system-created parameters, or all parameters for QoS.

3 Click **Submit**.

—End—

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.

To open the Diagnostics screen:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the Diagnostics screen by selecting Application > QoS > QoS Advanced > Agent > Diagnostic from the menu. This screen is illustrated in "Diagnostics screen (1 of 3)" (page 145), "Diagnostics screen (2 of 3)" (page 146), and "Diagnostics screen (3 of 3)" (page 146). |
|---|---|

Diagnostics screen (1 of 3)

The screenshot shows the Nortel QoS Diagnostics screen. On the left is a navigation tree with 'QoS' expanded to 'Agent' > 'Diagnostics'. The main area displays the 'QoS Resource Allocation Table' with the following data:

Interface	QoS Masks Consumed	QoS Filters Consumed	QoS Meters Consumed	QoS Counters Consumed	Non-QoS Masks Consumed	Non-QoS Filters Consumed	Non-QoS Meters Consumed
1	2	2	0	2	6	15	0
2	2	2	0	2	6	15	0
3	2	2	0	2	6	15	0
4	2	2	0	2	6	15	0
5	2	2	0	2	6	15	0
6	2	2	0	2	6	15	0
7	2	2	0	2	6	15	0
8	2	2	0	2	6	15	0
9	2	2	0	2	6	15	0
10	2	2	0	2	6	15	0
11	2	2	0	2	6	15	0
12	2	2	0	2	6	15	0
13	2	2	0	2	6	15	0
14	2	2	0	2	6	15	0
15	2	2	0	2	6	15	0
16	2	2	0	2	6	15	0
17	2	2	0	2	6	15	0
18	2	2	0	2	6	15	0
19	2	2	0	2	6	15	0
20	2	2	0	2	6	15	0
21	2	2	0	2	6	15	0
22	2	2	0	2	6	15	0
23	2	2	0	2	6	15	0
24	2	2	0	2	6	15	0

Diagnostics screen (2 of 3)

QoS Valid Range	
Minimum Value	<input type="text" value="0"/>
Maximum Value	<input type="text" value="65535"/>
Rule Value	<input type="text" value="0x0000"/>
Mask Value	<input type="text" value="0x0000"/>

Submit

QoS Encapsulating Range	
Low Value	<input type="text" value="0"/>
High Value	<input type="text" value="0"/>
Minimum Value	<input type="text" value="0"/>
Maximum Value	<input type="text" value="0"/>

Submit

Diagnostics screen (3 of 3)

QoS Classifier Rule/Mask Comparison				
Classifier	None Defined		None Defined	
	Rule	Mask	Rule	Mask
Dst MAC Address				
Src MAC Address				
User Priority				
VLAN				
EtherType				
IP Version				
IP Header Length				
DSCP				
IPv4 Protocol				
IPv6 Flow ID				
IPv6 Next Header				
Src IP Address				
Dst IP Address				
Src L4 Port				
Dst L4 Port				
VLAN Tag				
Dst MAC Addr Type				
Header				

Submit

"Diagnostic screen fields" (page 147) describes the fields on the **Diagnostics** screen.

Diagnostic screen fields

Screen Section	Field	Description
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.
	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.

Screen Section	Field	Description
QoS Classifier Rules/Mask Comparison	Classifier	Select the for which you want to display the rule and mask.
	Dst MAC Address	Displays the rule and mask for the destination MAC addresses configured.
	Src MAC Address	Displays the rule and mask for the source MAC addresses configured.
	User Priority	Displays the rule and mask for the user priority configured.
	VLAN	Displays the rule and mask for the VLANs configured.
	EtherType	Displays the rule and mask for the Ether types configured.
	IP Version	Displays the rule and mask for the IP versions configured.
	IP Header Length	Displays the rule and mask for the IP header lengths configured.
	DSCP	Displays the rule and mask for the DSCPs configured.
	IPv4 Protocol	Displays the rule and mask for the IPv4 protocols configured.
	IPv6 Flow ID	Displays the rule and mask for the IPv6 flow IDs configured.
	IPv6 Next Header	Displays the rule and mask for the IPv6 next headers configured.
	Src IP Address	Displays the rule and mask for the source IP addresses configured.
Dst IP Address	Displays the rule and mask for the destination IP addresses configured.	

Screen Section	Field	Description
	Src L4 Port	Displays the rule and mask for the source L4 ports configured.
	Dst L4 Port	Displays the rule and mask for the destination L4 ports configured.
	VLAN Tag	Displays the VLAN tag configured.
	Header	Displays the rule and mask for the first 80 bytes of the header configured.

- 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**.

- 3 To display the rule and mask in order to compare them for selected classifiers:
 - a. Choose the desired classifiers from the **QoS Classifier Rule / Mask Comparison** section using the provided lists.
 - b. Click **Submit**.

—End—

Configuring Quality of Service (QoS) with the Java Device Manager (JDM)

This chapter describes using the Java Device Manager to manage Quality of Service (QoS) parameters on the Nortel Ethernet Routing Switch 5500 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:

Step	Action
1	Open the QoSDevice screen by selecting QoS > QoS Devices from the menu. This screen is illustrated in " QoSDevice, Interface Queue tab " (page 152). Select the Interface Queue tab.

QoSDevice, Interface Queue tab

SetId	QueueId	Discipline	Bandwidth%	AbsBandwidth	BandwidthAllocation	Priority Q. Assign	Priority Mapping	DSCP Mapping	Meter Capability	Shaper Capability
1	1	priorityQueuing	100	0	relative					
2	1	priorityQueuing	100	0	relative					
2	2	priorityQueuing	100	0	relative					
3	1	priorityQueuing	100	0	relative					
3	2	weightedRoundRobin	75	0	relative					
3	3	weightedRoundRobin	25	0	relative					
4	1	priorityQueuing	100	0	relative					
4	2	weightedRoundRobin	65	0	relative					
4	3	weightedRoundRobin	20	0	relative					
4	4	weightedRoundRobin	9	0	relative					
5	1	priorityQueuing	100	0	relative					
5	2	weightedRoundRobin	58	0	relative					
5	3	weightedRoundRobin	27	0	relative					
5	4	weightedRoundRobin	11	0	relative					
5	5	weightedRoundRobin	4	0	relative					
5	1	priorityQueuing	100	0	relative					
5	2	weightedRoundRobin	52	0	relative					
5	3	weightedRoundRobin	24	0	relative					
5	4	weightedRoundRobin	14	0	relative					
5	5	weightedRoundRobin	7	0	relative					
5	6	weightedRoundRobin	3	0	relative					
7	1	priorityQueuing	100	0	relative					
7	2	weightedRoundRobin	45	0	relative					
7	3	weightedRoundRobin	21	0	relative					
7	4	weightedRoundRobin	15	0	relative					
7	5	weightedRoundRobin	10	0	relative					
7	6	weightedRoundRobin	6	0	relative					
7	7	weightedRoundRobin	3	0	relative					
8	1	priorityQueuing	100	0	relative					
8	2	weightedRoundRobin	41	0	relative					
8	3	weightedRoundRobin	19	0	relative					

Refresh Filter... Print Close Help...

AbsBandwidth(kbps) size(bytes), kbps = 1000 bps per second
30.106(s)

The following table "Interface Queue tab fields" (page 152) describes the Interface Queue tab fields.

Interface Queue tab fields

Field	Description
SetId	Displays an integer between 1 and 65535 that identifies the specific queue set.
QueueId	Displays an integer that uniquely identifies a specific queue within a set of queues.
Discipline	Displays the paradigm used to empty the queue: <ul style="list-style-type: none"> priorityQueuing weightedRoundRobin
Bandwidth%	Displays relative bandwidth available to a given queue with respect to other associated queues.
AbsBandwidth	Displays absolute bandwidth available to this queue, in Kb/s.
BandwidthAllocation	Displays bandwidth allocation: relative or absolute.

Field	Description
ServiceOrder	The order in which a queue is serviced based on the defined discipline.
Size	Displays the size of the queue in bytes.

—End—

See also

- "Displaying interface groups" (page 153)
- "Displaying an interface ID" (page 157)
- "Displaying priority queue assignments" (page 161)
- "Displaying priority mapping" (page 163)
- "Displaying DSCP mappings" (page 164)

Displaying interface groups

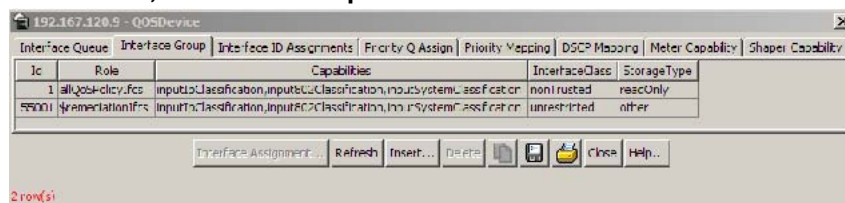
Device Manager lets you display the interface groups.

To display interface groups:

Step Action

- 1 Open the **QoSDevice** screen by selecting **QoS > QoS Devices** from the menu. This screen is illustrated in "["QoSDevice, Interface Queue tab"](#) (page 152). Select the **Interface Group** tab. This tab is illustrated in "["QoSDevice, Interface Group tab"](#) (page 153).

QoSDevice, Interface Group tab



The following table "["Interface Group tab fields"](#) (page 153) describes the Interface Group tab fields.

Interface Group tab fields

Field	Description
Id	Displays a unique identifier of an interface group.

Field	Description
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).
IfClass	The type of traffic interfaces associated with the specified role combination.
StorageType	Displays storage type for this interface group: <ul style="list-style-type: none"> • Volatile • nonVolatile (default) • readOnly

—End—

See also

- ["Assigning ports to an interface group" \(page 154\)](#)
- ["Deleting ports from an interface group" \(page 155\)](#)
- ["Adding interface groups" \(page 156\)](#)
- ["Deleting interface groups" \(page 157\)](#)
- ["Displaying an interface ID" \(page 157\)](#)
- ["Displaying priority queue assignments" \(page 161\)](#)
- ["Displaying priority mapping" \(page 163\)](#)
- ["Displaying DSCP mappings" \(page 164\)](#)

Assigning ports to an interface group

Device Manager lets you assign ports to an interface group.

To assign ports to an interface group:

-
- | Step | Action |
|------|--|
| 1 | Open the QoSDevice screen by selecting QoS > QoS Devices from the menu. This screen is illustrated in " QoSDevice, Interface Queue tab " (page 152). Select the Interface Group tab. This tab is illustrated in " QoSDevice, Interface Group tab " (page 153). |
| 2 | Click Interface Assignment .

The Group Assignment screen opens (" Group Assignment dialog box " (page 155)). |

Group Assignment dialog box



- | | |
|---|---|
| 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—

See also

- "[Deleting ports from an interface group](#)" (page 155)

Deleting ports from an interface group

Device Manager lets you remove ports from an interface group.

To remove ports from an interface group:

-
- | Step | Action |
|------|--|
| 1 | Open the QoSDevice screen by selecting QoS > QoS Devices from the menu. This screen is illustrated in " QoSDevice, Interface Queue tab " (page 152). Select the Interface Group tab. This tab is illustrated in " QoSDevice, Interface Group tab " (page 153). |
| 2 | Highlight the interface group from which to delete ports. |
| 3 | Click Interface Assignment . |
-

- 4 The **Group Assignment** screen opens ("Group Assignment dialog box" (page 155)).
- 5 Click the port numbers to delete from the interface group.
- 6 Click **OK**.

—End—

See also

- "Assigning ports to an interface group" (page 154)

Adding interface groups

Device Manager lets you add interface groups.

To add an interface group, use the following procedure:

Step	Action
------	--------

- 1 Open the **QoSDevice** screen by selecting **QoS > QoS Devices** from the menu. This screen is illustrated in "QoSDevice, Interface Queue tab" (page 152). Select the **Interface Group** tab. This tab is illustrated in "QoSDevice, Interface Group tab" (page 153).
- 2 Click **Insert**.
- 3 The **Insert Interface Group** screen opens ("Insert Interface Group dialog box" (page 156)).

Insert Interface Group dialog box



The screenshot shows a dialog box titled "192.168.151.170 - QoSDevice, Insert Int...". It contains the following fields and controls:

- Id:** A text box containing the value "2" and a label "1..64000".
- Role:** A text box containing the value "1..64000".
- IfClass:** Three radio buttons labeled "trusted", "nonTrusted", and "unrestricted".
- Buttons:** "Insert", "Close", and "Help..." at the bottom.

- 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—

See also

- ["Deleting interface groups" \(page 157\)](#)

Deleting interface groups

Device Manager lets you delete interface groups.

To delete an interface group:

Step	Action
1	Open the QoSDevice screen by selecting QoS > QoS Devices from the menu. This screen is illustrated in "QoSDevice, Interface Queue tab" (page 152) . Select the Interface Group tab. This tab is illustrated in "QoSDevice, Interface Group tab" (page 153) .
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—

See also

- ["Adding interface groups" \(page 156\)](#)

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:

Step	Action
1	Open the QoSDevice screen by selecting QoS > QoS Devices from the menu. This screen is illustrated in "QoSDevice, Interface Queue tab" (page 152) . Select the Interface ID Assignments tab.

This tab is illustrated in "QoSDevice, Interface ID Assignments tab" (page 158).

QoSDevice, Interface ID Assignments tab

Port	RoleCombination	QueueSet
1j1	allQoSPolicyIfcs	2
1j2	allQoSPolicyIfcs	2
1j3	allQoSPolicyIfcs	2
1j4	allQoSPolicyIfcs	2
1j5	allQoSPolicyIfcs	2
1j6	allQoSPolicyIfcs	2
1j7	allQoSPolicyIfcs	2
1j8	allQoSPolicyIfcs	2
1j9	allQoSPolicyIfcs	2
1j10	allQoSPolicyIfcs	2
1j11	allQoSPolicyIfcs	2
1j12	allQoSPolicyIfcs	2
1j13	allQoSPolicyIfcs	2
1j14	allQoSPolicyIfcs	2
1j15	allQoSPolicyIfcs	2
1j16	allQoSPolicyIfcs	2
1j17	allQoSPolicyIfcs	2
1j18	allQoSPolicyIfcs	2
1j19	allQoSPolicyIfcs	2
1j20	allQoSPolicyIfcs	2
1j21	allQoSPolicyIfcs	2
1j22	allQoSPolicyIfcs	2
1j23	allQoSPolicyIfcs	2
1j24	allQoSPolicyIfcs	2
1j25	allQoSPolicyIfcs	2
1j26	allQoSPolicyIfcs	2

To continue, go to:

- [Interface ID Assignments tab fields](#)

Interface ID Assignments tab fields

The following table "Interface ID Assignments tab fields" (page 158) describes the Interface ID Assignments tab fields.

Interface ID Assignments tab fields

Field	Description
lflIndex	Displays ports numbers.
Port	Display the unit and port numbers.
RoleCombination	Displays the role combination associated with the interface.
QueueSet	Displays the queue set associated with this interface.

—End—

See also

- ["Displaying interface queues" \(page 151\)](#)
- ["Displaying interface groups" \(page 153\)](#)

- "Displaying priority queue assignments" (page 161)
- "Displaying priority mapping" (page 163)
- "Displaying DSCP mappings" (page 164)

Filtering Interface ID Assignments table

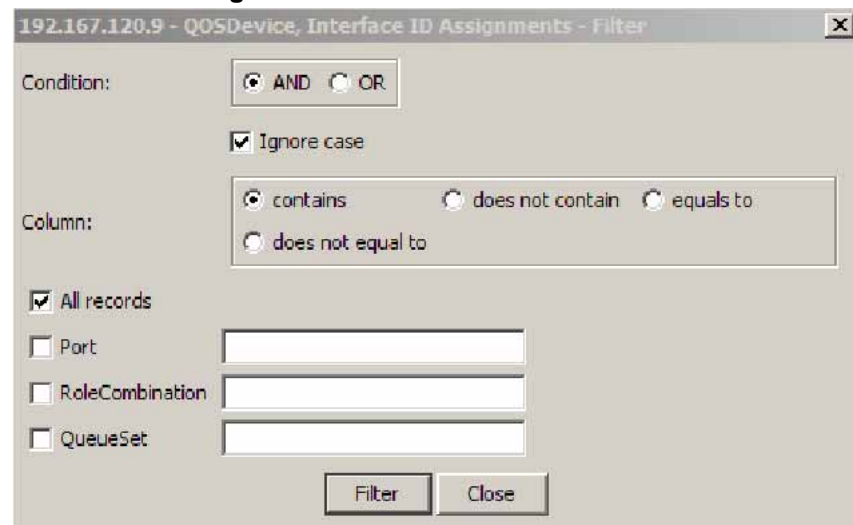
To display selected parts of the Interface ID Assignments tab:

Step Action

- 1 Open the **QoSDevice** screen by selecting **QoS > QoS Devices** from the menu. This screen is illustrated in "QoSDevice, Interface Queue tab" (page 152). Select the **Interface ID Assignments** tab. This tab is illustrated in "QoSDevice, Interface ID Assignments tab" (page 158).

- 2 Click the **Filter** button.

Insert Filter dialog



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

Interface ID Assignments Filter criteria

Field	Description
Condition	Select one of the following: <ul style="list-style-type: none"> • AND to include all entries in the table that include <i>all</i> specified parameters • OR to include <i>any</i> of the specified parameters

Field	Description
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: <ul style="list-style-type: none"> • 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.
Port	Enter the device and port for the table entries.
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.

- 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—

Displaying priority queue assignments

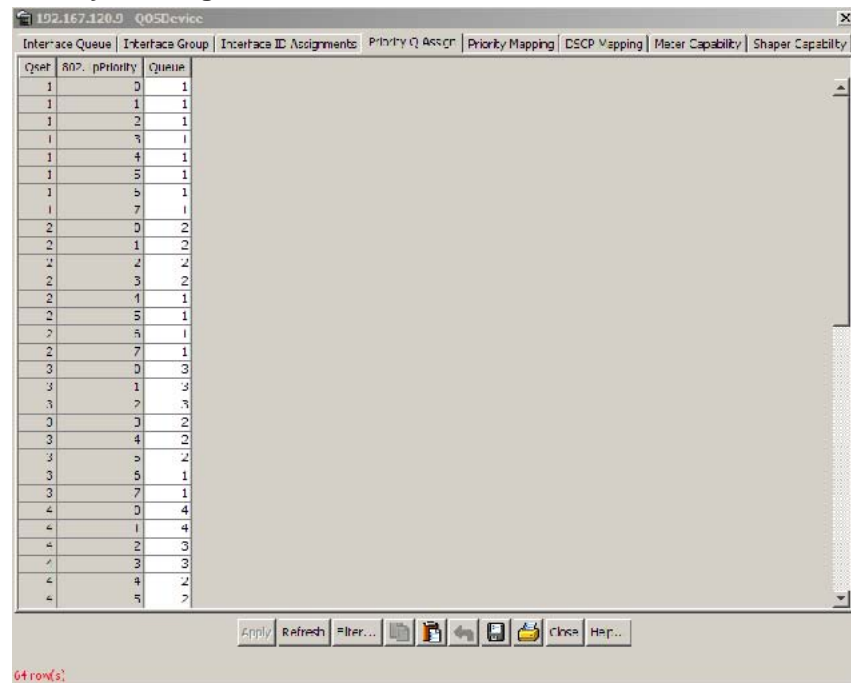
Device Manager allows for the display Priority Q Assignments.

To display priority queue assignments:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the QoSDevice screen by selecting QoS > QoS Devices from the menu. This screen is illustrated in " QoSDevice, Interface Queue tab " (page 152). Select the Priority Q Assign tab. This tab is illustrated in " Priority Q Assign tab " (page 161). |
|---|---|

Priority Q Assign tab



The following table "Priority Q Assign tab fields" (page 161) describes the **Priority Q Assign** tab fields.

Priority Q Assign tab fields

Field	Description
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.

Field	Description
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.

—End—

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:

Step Action

- 1 Open the **QoSDevice** screen by selecting **QoS > QoS Devices** from the menu. This screen is illustrated in "[QoSDevice, Interface Queue tab](#)" (page 152). Select the **Priority Q Assign** tab. This tab is illustrated in "[Priority Q Assign tab](#)" (page 161).

- 2 Click **Filter**.

The **Insert Filter** dialog opens. This screen is illustrated in "[Priority Queue Assignment Insert Filter dialog](#)" (page 162).

Priority Queue Assignment Insert Filter dialog

- 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—

See also

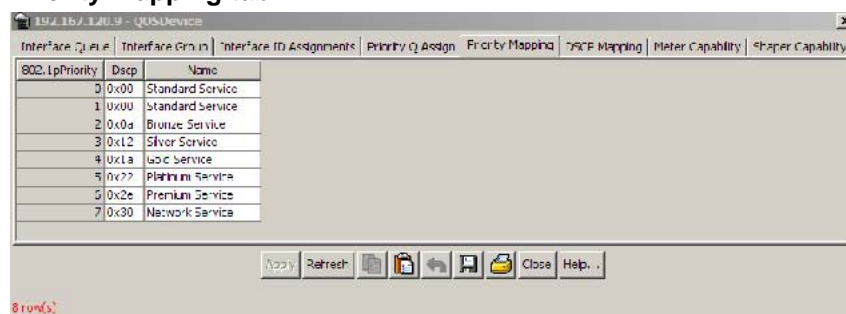
- ["Displaying interface queues" \(page 151\)](#)
- ["Displaying interface groups" \(page 153\)](#)
- ["Displaying an interface ID" \(page 157\)](#)
- ["Displaying priority queue assignments" \(page 161\)](#)
- ["Displaying priority mapping" \(page 163\)](#)
- ["Displaying DSCP mappings" \(page 164\)](#)

Displaying priority mapping

Device Manager lets you display priority mapping.

To display priority mapping:

Step	Action
1	Open the QoSDevice screen by selecting QoS > QoS Devices from the menu. This screen is illustrated in "QoSDevice, Interface Queue tab" (page 152) . Select the Priority Mapping tab. This tab is illustrated in "Priority mapping tab" (page 164) .

Priority mapping tab

The following table "Priority mapping tab fields" (page 164) describes the priority mapping tab fields.

Priority mapping tab fields

Field	Description
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.

—End—

See also

- "Displaying interface queues" (page 151)
- "Displaying interface groups" (page 153)
- "Displaying an interface ID" (page 157)
- "Displaying priority queue assignments" (page 161)
- "Displaying DSCP mappings" (page 164)

Displaying DSCP mappings

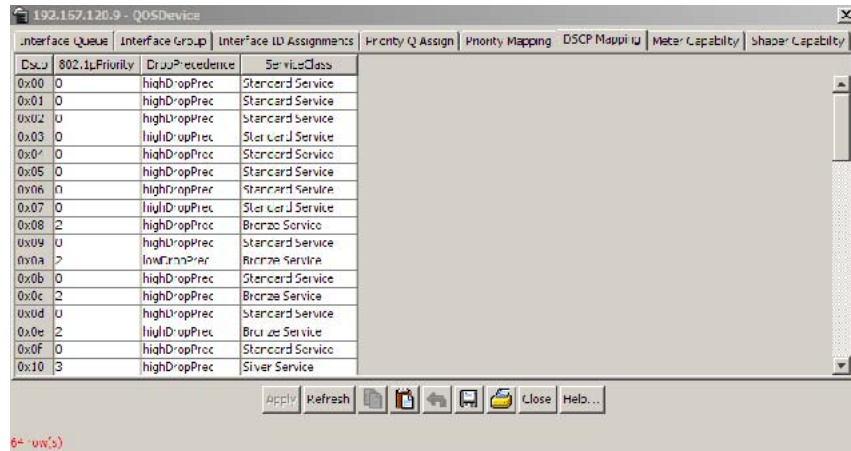
Device Manager lets you display DSCP mapping.

To display DSCP mappings:

Step Action

- 1 Open the **QoSDevice** screen by selecting **QoS > QoS Devices** from the menu. This screen is illustrated in "[QoSDevice, Interface Queue tab](#)" (page 152). Select the **DSCP** tab. This tab is illustrated in "[DSCP mapping tab](#)" (page 165).

DSCP mapping tab



The following table "[DSCP mapping tab fields](#)" (page 165) describes the DSCP mapping tab fields.

DSCP mapping tab fields

Field	Description
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	<p>The drop precedence setting. The available settings are:</p> <ul style="list-style-type: none"> • lowDropPrec • highDropPrec <p>Traffic associated with low drop precedence is generally given priority over traffic with high drop precedence during resource allocation.</p>

Field	Description
	To change the setting, click in a cell and choose the setting.
ServiceClass	Specifies the type of service.

—End—

See also

- ["Displaying interface queues" \(page 151\)](#)
- ["Displaying interface groups" \(page 153\)](#)
- ["Displaying an interface ID" \(page 157\)](#)
- ["Displaying priority queue assignments" \(page 161\)](#)
- ["Displaying priority mapping" \(page 163\)](#)

Displaying Meter Capability

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

Displaying QoS interface meter capabilities

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.

Meter Capability tab

Port	MeterSupport	Meter Rate (Kbps)/Bucket (KBytes)/Granularity (Kbps)
1/1	Simple	Rate1023000,Bucket:512,Granularity64
1/2	Simple	Rate1023000,Bucket:512,Granularity64
1/3	Simple	Rate1023000,Bucket:512,Granularity64
1/5	Simple	Rate1023000,Bucket:512,Granularity64
1/6	Simple	Rate1023000,Bucket:512,Granularity64
1/7	Simple	Rate1023000,Bucket:512,Granularity64
1/8	Simple	Rate1023000,Bucket:512,Granularity64
1/9	Simple	Rate1023000,Bucket:512,Granularity64
1/10	Simple	Rate1023000,Bucket:512,Granularity64
1/11	Simple	Rate1023000,Bucket:512,Granularity64
1/12	Simple	Rate1023000,Bucket:512,Granularity64
1/14	Simple	Rate1023000,Bucket:512,Granularity64
1/15	Simple	Rate1023000,Bucket:512,Granularity64
1/17	Simple	Rate1023000,Bucket:512,Granularity64
1/18	Simple	Rate1023000,Bucket:512,Granularity64
1/19	Simple	Rate1023000,Bucket:512,Granularity64
1/20	Simple	Rate1023000,Bucket:512,Granularity64
1/22	Simple	Rate1023000,Bucket:512,Granularity64
1/23	Simple	Rate1023000,Bucket:512,Granularity64
1/24	Simple	Rate1023000,Bucket:512,Granularity64
1/25	Simple	Rate1023000,Rate10230000,Bucket512,Bucket5192,Granularity1000
1/26	Simple	Rate1023000,Rate10230000,Bucket512,Bucket5192,Granularity1000

—End—

The following table describes the fields on the Meter Capability tab.

Meter Capability tab fields

Field	Description
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

Click the **Filter** button to set Meter Capability table view filtering criteria. The **QOSDevice, Meter Capability - Filter** dialog opens. Select filtering criteria and enter port, meter support, and meter rate parameters. To activate your selections, click the **Filter** button on the dialog, the **Meter Capability** window will display entries based on the filtering criteria specified.

Displaying Shaper Capability

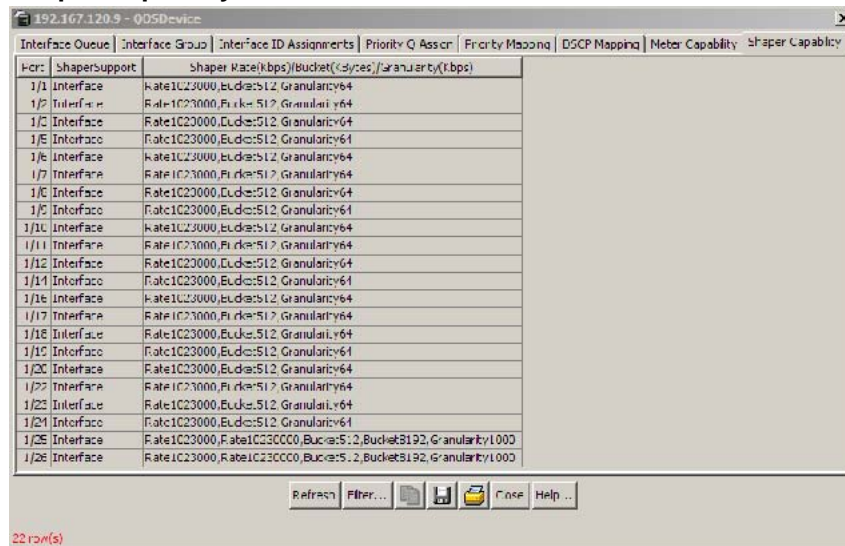
To display QoS interface shaper capabilities, use the following procedure.

Displaying QoS interface shaper capabilities

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.

Shaper Capability tab



Port	ShaperSupport	Shaper Rate(Kbps)/Bucket(Bytes)/Granularity(Kbps)
1/1	Interface	Rate1023000, Bucket:512, Granularity:64
1/2	Interface	Rate1023000, Bucket:512, Granularity:64
1/3	Interface	Rate1023000, Bucket:512, Granularity:64
1/4	Interface	Rate1023000, Bucket:512, Granularity:64
1/5	Interface	Rate1023000, Bucket:512, Granularity:64
1/6	Interface	Rate1023000, Bucket:512, Granularity:64
1/7	Interface	Rate1023000, Bucket:512, Granularity:64
1/8	Interface	Rate1023000, Bucket:512, Granularity:64
1/9	Interface	Rate1023000, Bucket:512, Granularity:64
1/10	Interface	Rate1023000, Bucket:512, Granularity:64
1/11	Interface	Rate1023000, Bucket:512, Granularity:64
1/12	Interface	Rate1023000, Bucket:512, Granularity:64
1/13	Interface	Rate1023000, Bucket:512, Granularity:64
1/14	Interface	Rate1023000, Bucket:512, Granularity:64
1/15	Interface	Rate1023000, Bucket:512, Granularity:64
1/16	Interface	Rate1023000, Bucket:512, Granularity:64
1/17	Interface	Rate1023000, Bucket:512, Granularity:64
1/18	Interface	Rate1023000, Bucket:512, Granularity:64
1/19	Interface	Rate1023000, Bucket:512, Granularity:64
1/20	Interface	Rate1023000, Bucket:512, Granularity:64
1/21	Interface	Rate1023000, Bucket:512, Granularity:64
1/22	Interface	Rate1023000, Bucket:512, Granularity:64
1/23	Interface	Rate1023000, Bucket:512, Granularity:64
1/24	Interface	Rate1023000, Bucket:512, Granularity:64
1/25	Interface	Rate1023000, Rate1023000, Bucket:512, Bucket:8192, Granularity:1000
1/26	Interface	Rate1023000, Rate1023000, Bucket:512, Bucket:8192, Granularity:1000

—End—

The following table describes the fields on the Shaper Capability tab.

Shaper Capability tab fields

Field	Description
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

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

Managing QoS rules

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

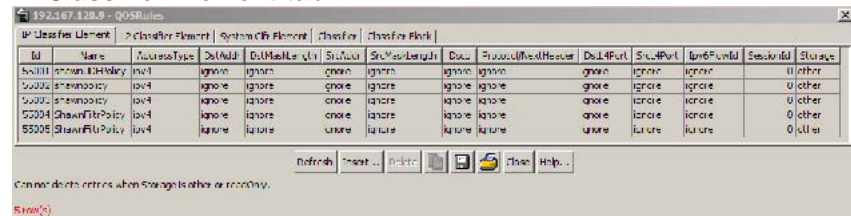
Displaying IP classifier elements

To display the IP classifier elements:

Step	Action
------	--------

- 1 Open the **QoSRules** screen by selecting **QoS > QoS Rules** from the menu. The **IP Classifier Element** tab is selected. This tab is illustrated in "IP Classifier Element tab" (page 169).

IP Classifier Element tab



The following table "IP Classifier Element tab fields" (page 169) describes the IP Classifier Element tab fields.

IP Classifier Element tab fields

Field	Description
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.
Protocol	Specifies the IP protocol value.

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

—End—

See also

- ["Displaying L2 classifier elements" \(page 172\)](#)
- ["Adding System Classifier Elements" \(page 177\)](#)
- ["Displaying Classifier Blocks" \(page 184\)](#)

Adding IP classifier elements

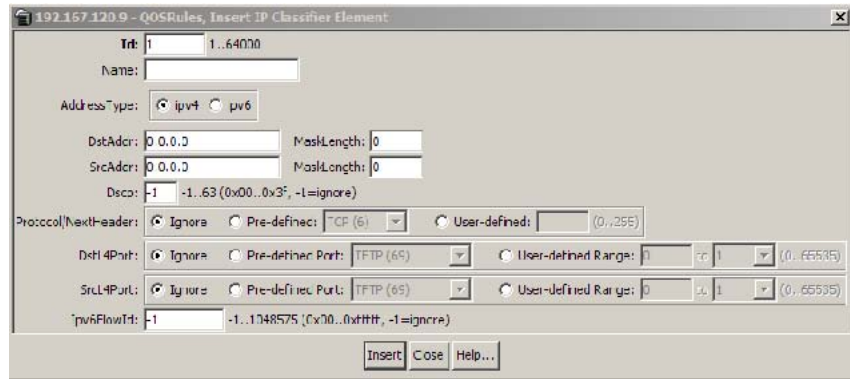
Device Manager lets you add the IP classifier elements.

To add an IP classifier element:

Step Action

- 1 Open the **QoSRules** screen by selecting **QoS > QoS Rules** from the menu. The **IP Classifier Element** tab is selected. This tab is illustrated in ["IP Classifier Element tab" \(page 169\)](#).
- 2 Click **Insert**.
The **Insert IP Classifier Element** screen opens (["Insert IP Classifier Element dialog box" \(page 171\)](#)).

Insert IP Classifier Element dialog box



- 3 Enter the information you want to use for this IP classifier element.
- 4 Click Insert.

—End—

See also

- ["Deleting IP classifier elements" \(page 171\)](#)

Deleting IP classifier elements

Device Manager lets you delete IP classifier elements.

To delete an IP classifier element:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the QoSRules screen by selecting QoS > QoS Rules from the menu. The IP Classifier Element tab is selected. This tab is illustrated in "IP Classifier Element tab" (page 169) . |
| 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—

See also

- "Adding IP classifier elements" (page 170)

Displaying L2 classifier elements

Device Manager lets you display classifiers.

To display L2 classifiers:

Step Action

- 1 Open the **QoSRules** screen by selecting **QoS > QoS Rules** from the menu. This screen is illustrated in "IP Classifier Element tab" (page 169). Select the **L2 Classifier Element** tab. This tab is illustrated in "L2 Classifier Element tab" (page 172).

L2 Classifier Element tab

Name	SetId	Specific	SessionId	Storage
UntrustedClfrs1	55001	L2 Classifier Element, Id=55001(UntrustedClfrs1)	0	other
UntrustedClfrs2	55002	L2 Classifier Element, Id=55002(UntrustedClfrs2)	0	other
shawnUDFPolicy	55003	IP Classifier Element, Id=55001(shawnUDFPolicy)	0	other
shawnVLANpolicy	55004	L2 Classifier Element, Id=55003(shawnVLANpolicy)	0	other
ShawnIPPolicy	55005	L2 Classifier Element, Id=55004(ShawnIPPolicy)	0	other
shawnpolicy	55006	IP Classifier Element, Id=55002(shawnpolicy)	0	other
shawnpolicy	55006	L2 Classifier Element, Id=55005(shawnpolicy)	0	other
shawnpolicy	55007	IP Classifier Element, Id=55003(shawnpolicy)	0	other
shawnpolicy	55007	L2 Classifier Element, Id=55006(shawnpolicy)	0	other
ShawnFiltrPolicy	55008	IP Classifier Element, Id=55004(ShawnFiltrPolicy)	0	other
ShawnFiltrPolicy	55008	L2 Classifier Element, Id=55007(ShawnFiltrPolicy)	0	other
ShawnFiltrPolicy	55009	IP Classifier Element, Id=55005(ShawnFiltrPolicy)	0	other
ShawnFiltrPolicy	55009	L2 Classifier Element, Id=55008(ShawnFiltrPolicy)	0	other
NachiaV1Def1	55010	System Classifier Element, Id=55001(NachiaV1Def1)	0	other

Can not delete entries when Storage is other or readOnly.
 Entries with same SetId belong to the same Classifier.
 14 row(s)

The following table "L2 Classifier Element tab fields" (page 172) describes the L2 Classifier Element tab fields.

L2 Classifier Element tab fields

Field	Description
Id	Specifies the index that enumerates the classifier entries.
Name	Specifies the L2 Classifier Element name.

Field	Description
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.
VlanTag	Specifies the type of VLAN tagging in a packet: <ul style="list-style-type: none"> • untagged • tagged • ignore
EtherType	Specifies a value for the Ethertype.
802.1pPriority	Specifies a value for the 802.1p user priority.
SessionId	Specifies the session identification number.
Storage	Specifies the type of storage.

—End—

See also

- ["Displaying IP classifier elements" \(page 169\)](#)
- ["Adding System Classifier Elements" \(page 177\)](#)
- ["Displaying Classifier Blocks" \(page 184\)](#)

Adding L2 classifier elements

To add L2 classifier elements:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the QoSRules screen by selecting QoS > QoS Rules from the menu. This screen is illustrated in "IP Classifier Element tab" (page |
|---|---|

169). Select the **L2 Classifier Element** tab. This tab is illustrated in "L2 Classifier Element tab" (page 172).

- 2 Click **Insert**.

The **Insert L2 Classifier Element** dialog opens ("Deleting interface groups" (page 157)).

Insert L2 Classifier Element dialog box

- 3 Enter the information to use for this L2 classifier element.
- 4 Click **Insert**.

—End—

See also

- "Deleting L2 classifier elements" (page 174)

Deleting L2 classifier elements

Device Manager lets you delete L2 classifier elements.

To delete a L2 classifier elements:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the QoSRules screen by selecting QoS > QoS Rules from the menu. This screen is illustrated in "IP Classifier Element tab" (page 169). Select the L2 Classifier Element tab. This tab is illustrated in "L2 Classifier Element tab" (page 172). |
| 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

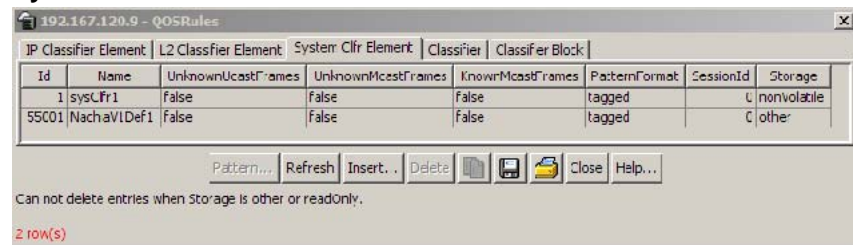
Device Manager lets you display classifiers.

To display System Classifier Elements:

Step	Action
------	--------

- | | |
|----------|---|
| 1 | Open the QoSRules screen by selecting QoS > QoS Rules from the menu. This screen is illustrated in "IP Classifier Element tab" (page 169). Select the System Clfr Element tab. This tab is illustrated in "System Clfr Element tab" (page 175). |
|----------|---|

System Clfr Element tab



"System Clfr Element tab fields" (page 175). The following table describes the System Clfr Element tab fields.

System Clfr Element tab fields

Field	Description
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.

Field	Description
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'.

—End—

Viewing the System Classifier Pattern

To view the pattern:

Device Manager lets you display classifiers.

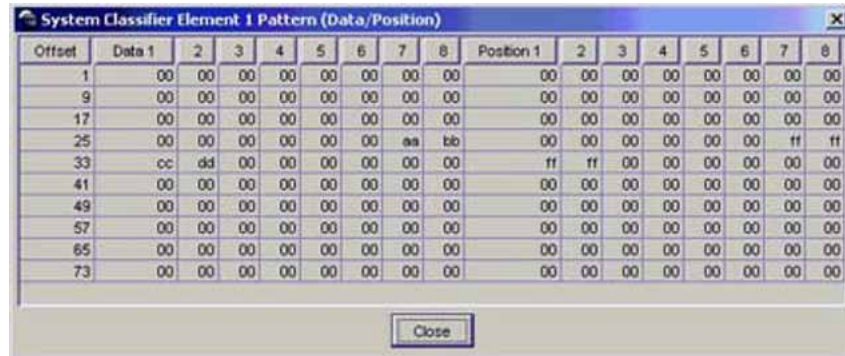
Step Action

- 1 Open the **QoSRules** screen by selecting **QoS > QoS Rules** from the menu. This screen is illustrated in "[IP Classifier Element tab](#)" (page 169). Select the **System Clfr Element** tab. This tab is illustrated in "[System Clfr Element tab](#)" (page 175).
- 2 Highlight an entry in the **System Clfr Element** table.

3 Click **Pattern**.

The **System Classifier Element # Pattern (Data/Position)** screen opens ("System Classifier Element 1 Pattern (Data Position) screen" (page 177)).

System Classifier Element 1 Pattern (Data Position) screen



—End—

See also:

- "Adding L2 classifier elements" (page 173)

Adding System Classifier Elements

To add System Classifier Elements:

Step	Action
1	Open the QoSRules screen by selecting QoS > QoS Rules from the menu. This screen is illustrated in "IP Classifier Element tab" (page 169). Select the System Clfr Element tab. This tab is illustrated in "System Clfr Element tab" (page 175).
2	Click Insert . The Insert System Clfr Element dialog opens ("QoSRules, Insert System Clfr Element dialog box" (page 178)).

QoSRules, Insert System Clfr Element dialog box

- 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 ("[System Classifier Element Pattern \(Data Position\) screen](#)" (page 178)).

System Classifier Element Pattern (Data Position) screen

Offset	Data 1	2	3	4	5	6	7	8	Position 1	2	3	4	5	6	7	8
1	00	00	00	00	00	00	00	00								
9	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
17	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
25	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
33	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
41	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
49	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
57	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
65	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
73	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

- 7 Select **IPv4** or **IPv6**.
- 8 Select **tagged** or **untagged**.
- 9 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.
- 10 Type the desired **Data** and **Position** in two-digit hex number format.
- 11 Click **Ok**.

-
- 12 Click **Insert**.
-

—End—

Deleting System Classifier Elements

To delete System Classifier Elements:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the QoSRules screen by selecting QoS > QoS Rules from the menu. This screen is illustrated in "IP Classifier Element tab" (page 169). Select the System Clfr Element tab. This tab is illustrated in "System Clfr Element tab" (page 175). |
| 2 | Highlight the System Classifier Element to delete. |
| 3 | Click Delete . |
-

—End—

Displaying Classifiers

To display classifiers:

Step	Action
------	--------

- | | |
|---|--|
| 1 | Open the QoSRules screen by selecting QoS > QoS Rules from the menu. This screen is illustrated in "IP Classifier Element tab" (page 169). Select the Classifier tab. This tab is illustrated in "Classifier tab" (page 180) the following illustration. |
|---|--|
-

Classifier tab

Name	SetId	Specific	SessionId	Storage
UntrustedClfrs1	55001	L2 Classifier Element, Id=55001(UntrustedClfrs1)	0	other
UntrustedClfrs2	55002	L2 Classifier Element, Id=55002(UntrustedClfrs2)	0	other
shawnUDFPolicy	55003	IP Classifier Element, Id=55001(shawnUDFPolicy)	0	other
shawnVLANpolicy	55004	L2 Classifier Element, Id=55003(shawnVLANpolicy)	0	other
ShawnIPPolicy	55005	L2 Classifier Element, Id=55004(ShawnIPPolicy)	0	other
shawnpolicy	55006	IP Classifier Element, Id=55002(shawnpolicy)	0	other
shawnpolicy	55006	L2 Classifier Element, Id=55005(shawnpolicy)	0	other
shawnpolicy	55007	IP Classifier Element, Id=55003(shawnpolicy)	0	other
shawnpolicy	55007	L2 Classifier Element, Id=55006(shawnpolicy)	0	other
ShawnFiltrPolicy	55008	IP Classifier Element, Id=55004(ShawnFiltrPolicy)	0	other
ShawnFiltrPolicy	55008	L2 Classifier Element, Id=55007(ShawnFiltrPolicy)	0	other
ShawnFiltrPolicy	55009	IP Classifier Element, Id=55005(ShawnFiltrPolicy)	0	other
ShawnFiltrPolicy	55009	L2 Classifier Element, Id=55008(ShawnFiltrPolicy)	0	other
NachiaV1Def1	55010	System Classifier Element, Id=55001(NachiaV1Def1)	0	other

Can not delete entries when Storage is other or readOnly.
 Entries with same SetId belong to the same Classifier.
 14 row(s)

The following table "Classifier tab fields" (page 180) describes the Classifier tab fields.

Classifier tab fields

Field	Description
Name	Specifies the name of the classifier.
SetId	Entries with the same SetId belong to the same classifier. Note: Click heading on this column to list entries in numerical order to view which entries have the same SetId.
Specific	Describes the specific classifier element and its ID number (from the IP Classifier Element screen, the L2 Classifier Element screen, or System Clfr Element screen) that is included in the classifier.
SessionId	Specifies the numerical identification associated with the session.
Storage	The storage type for this conceptual row. Conceptual rows that has the value <i>permanent</i> 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 <i>active</i> .

—End—

See also

- "Displaying IP classifier elements" (page 169)
- "Displaying L2 classifier elements" (page 172)
- "Displaying Classifier Blocks" (page 184)

Adding classifiers

Device Manager lets you add classifiers.

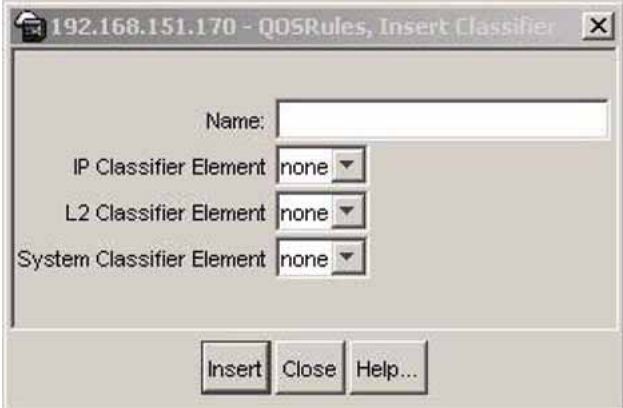
To add a classifier:

Step	Action
------	--------

1	Open the QoSRules screen by selecting QoS > QoS Rules from the menu. This screen is illustrated in "IP Classifier Element tab" (page 169). Select the Classifier tab. This tab is illustrated in "Classifier tab" (page 180).
---	---

2	Click Insert .
---	-----------------------

The **Insert Classifier** screen opens ("Insert Classifier screen" (page 181)).

Insert Classifier screen

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 using the following classifier combinations:

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

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

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

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

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

—End—

See also

- ["Deleting classifiers" \(page 182\)](#)

Deleting classifiers

Device Manager lets you delete classifiers.

To delete a classifier:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the QoSRules screen by selecting QoS > QoS Rules from the menu. This screen is illustrated in "IP Classifier Element tab" (page 169) . Select the Classifier tab. This tab is illustrated in "Classifier tab" (page 180) . |
| 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

To filter the display of classifiers, follow this procedure:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the QoSRules screen by selecting QoS > QoS Rules from the menu. This screen is illustrated in "IP Classifier Element tab" (page 169). Select the Classifier tab. This tab is illustrated in "Classifier tab" (page 180). |
| 2 | Click Filter . |

The **Insert Filter** screen opens. This screen is illustrated in "Classifier Insert Filter dialog" (page 183) the following illustration.

Classifier Insert Filter dialog

- | | |
|---|---|
| 3 | Set the conditions to filter the display of the Classifiers table: <ol style="list-style-type: none"> Select AND to include all entries in the table that include <i>all</i> specified parameters, or select OR to include any of the specified parameters. 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—

See also

- ["Adding classifiers" \(page 181\)](#)

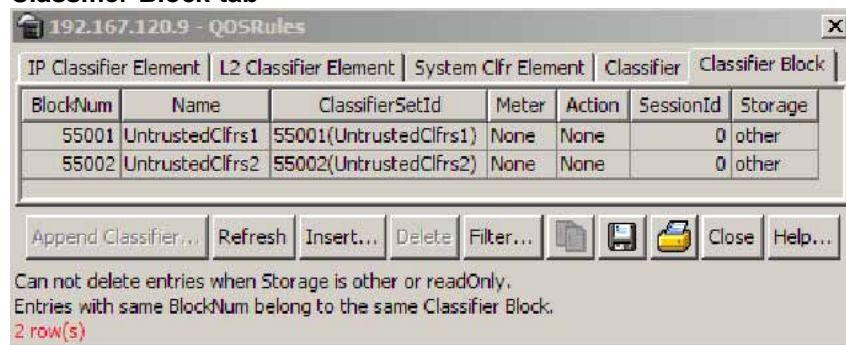
Displaying Classifier Blocks

To display classifier blocks:

Step Action

- 1 Open the **QoSRules** screen by selecting **QoS > QoS Rules** from the menu. This screen is illustrated in ["IP Classifier Element tab" \(page 169\)](#). Select the **Classifier Block** tab. This tab is illustrated in ["Classifier Block tab" \(page 184\)](#). the following illustration.

Classifier Block tab



The following table ["Classifier Block tab fields" \(page 185\)](#) describes the **Classifier Block** tab fields.

Classifier Block tab fields

Field	Description
BlockNum	Entries with the same BlockNum belong to the same classifier block. Note: Click heading on this column to list entries in numerical order to view which entries have the same BlockNum.
Name	Displays the name you assigned to that classifier block.
ClassifierSetId	Displays the ID number assigned to that classifier (from the Classifier screen).
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 <i>permanent</i> 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 <i>active</i> .

—End—

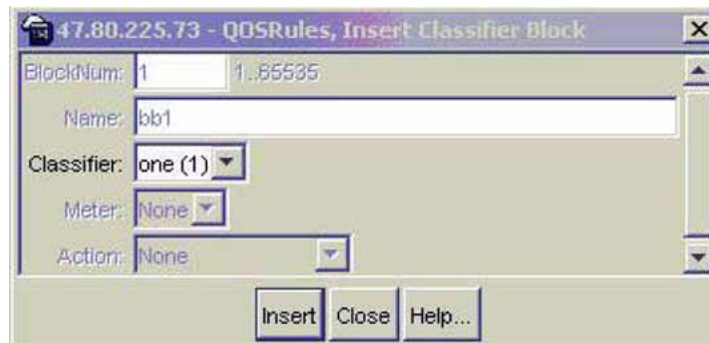
Appending Classifier Blocks

To append a classifier block:

Step	Action
1	Open the QoSRules screen by selecting QoS > QoS Rules from the menu. This screen is illustrated in " IP Classifier Element tab " (page 169). Select the Classifier Block tab. This tab is illustrated in " Classifier Block tab " (page 184).
2	Click Append Classifier .

The **Insert Classifier Block** dialog opens ("QoSRules, Insert Classifier Block" (page 186)).

QoSRules, Insert Classifier Block



- 3 Select the Classifier to append to the Classifier Block.
- 4 Click **Insert**.

—End—

See also

- "Displaying IP classifier elements" (page 169)
- "Displaying L2 classifier elements" (page 172)
- "Adding System Classifier Elements" (page 177)

Adding Classifier Blocks

Device Manager lets you add classifier blocks.

To add a classifier block:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the QoSRules screen by selecting QoS > QoS Rules from the menu. This screen is illustrated in "IP Classifier Element tab" (page 169). Select the Classifier Block tab. This tab is illustrated in "Classifier Block tab" (page 184). |
|---|---|

- | | |
|---|-----------------------|
| 2 | Click Insert . |
|---|-----------------------|

The **Insert Classifier Block** screen opens ("Insert Classifier Block screen" (page 187)).

Insert Classifier Block screen

- 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—

See also

- ["Deleting Classifier Blocks" \(page 187\)](#)

Deleting Classifier Blocks

Device Manager lets you delete classifier blocks.

To delete a classifier block:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the QoSRules screen by selecting QoS > QoS Rules from the menu. This screen is illustrated in " IP Classifier Element tab " (page 169). Select the Classifier Block tab. This tab is illustrated in " Classifier Block tab " (page 184). |
| 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

To filter a classifier block:

Step Action

- 1 Open the **QoSRules** screen by selecting **QoS > QoS Rules** from the menu. This screen is illustrated in "IP Classifier Element tab" (page 169). Select the **Classifier Block** tab. This tab is illustrated in "Classifier Block tab" (page 184).
- 2 Click **Filter**.

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

QOSRules, Classifier Block - Filter dialog

- 3 Select the filtering condition, case, and column criteria.
- 4 Enter the **BlockNum** and **Name**.
- 5 Click **Filter**.

—End—

See also

- "Adding Classifier Blocks" (page 186)

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.

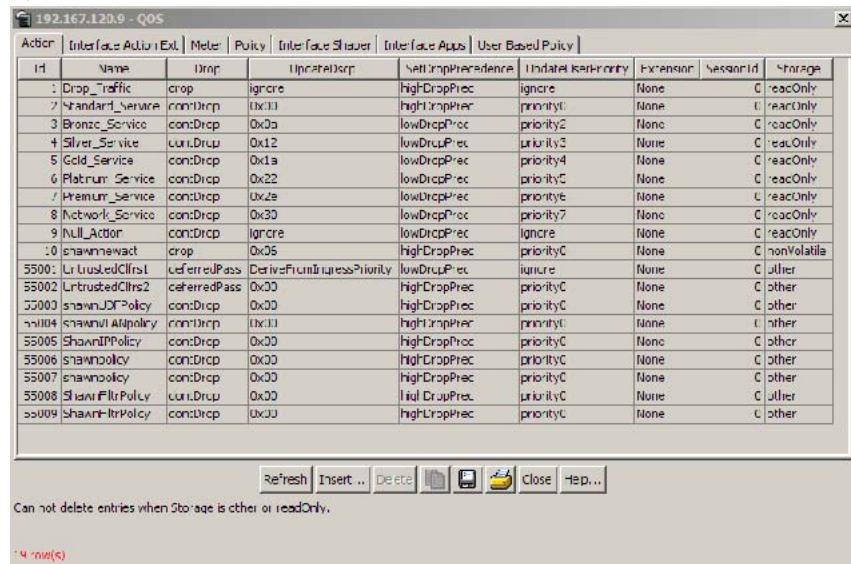
Displaying QoS actions

To display a QoS action:

Step Action

- 1 Open the **QoS** screen by selecting **QoS > QoS** from the menu. This screen is illustrated in "QoS Action tab" (page 189). Select the **Action** tab. This tab is illustrated in "QoS Action tab" (page 189).

QoS Action tab



The following table "QoS Action tab fields" (page 189) describes the QoS **Action** tab fields.

QoS Action tab fields

Field	Description
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.

Field	Description
UpdateDscp	Specifies a value used to update the DSCP field in an IPv4 packet.
SetDropPrecedence	Specifies automatic drop precedence.
UpdateUserPriority	Specifies a value for the 802.1p user priority.
Extension	Specifies linking additional actions. (These are defined on the Interface Action Ext Table.)
SessionId	Specifies the numerical identification for the active session.
Storage	Specifies the type of storage: <ul style="list-style-type: none"> • volatile • nonVvolatile • readOnly

—End—

See also

- ["Displaying Interface action extensions" \(page 192\)](#)
- [Click the ellipses to select the ports for the interface shaper.](#)

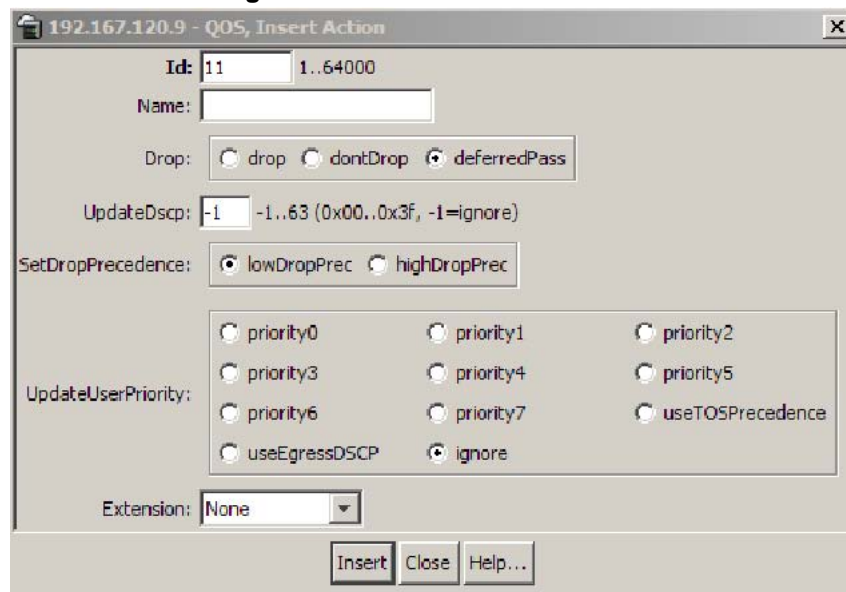
Adding QoS actions

To add a QoS action:

Step Action

- 1 Open the **QoS** screen by selecting **QoS > QoS** from the menu. This screen is illustrated in ["QoS Action tab" \(page 189\)](#). Select the **Action** tab. This tab is illustrated in ["QoS Action tab" \(page 189\)](#).
- 2 Click **Insert**.
The **Insert Action** dialog opens (["Insert Action dialog" \(page 191\)](#)).

Insert Action dialog



- 3 Enter the information and select the parameters to use for this QoS action.
- 4 Click **Insert**.

—End—

See also

- ["Deleting QoS actions" \(page 191\)](#)

Deleting QoS actions

To delete a QoS action:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the QoS screen by selecting QoS > QoS from the menu. This screen is illustrated in "QoS Action tab" (page 189) . Select the Action tab. This tab is illustrated in "QoS Action tab" (page 189) . |
| 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 if it is of the storage type of **other** or **readOnly**.

—End—

See also

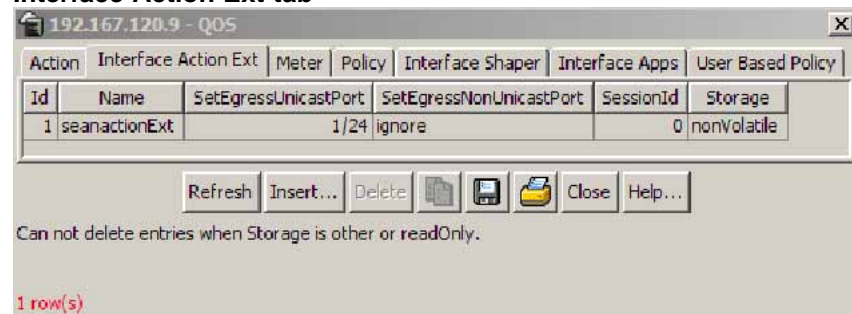
- ["Adding QoS actions" \(page 190\)](#)

Displaying Interface action extensions

To display a QoS interface action extension:

Step Action

- 1 Open the **QoS** screen by selecting **QoS > QoS** from the menu. This screen is illustrated in ["QoS Action tab" \(page 189\)](#). Select the **Interface Action Ext** tab. This tab is illustrated in ["Interface Action Ext tab" \(page 192\)](#).

Interface Action Ext tab

The following table ["Interface Action Ext tab fields" \(page 192\)](#) describes the Interface Action Ext tab fields.

Interface Action Ext tab fields

Field	Description
Id	Specifies the number of the interface action extension.
Name	Specifies a label for the interface action extension.
SetEgressUnicastPort	Specifies redirection of normally-switched unicast packets to a specified interface.
SetEgressNonUnicastPort	Specifies redirection of normally-switched non-unicast packets (broadcast and multicast traffic) to a specified interface.

Field	Description
SessionId	Specifies the numerical identification for the current session.
Storage	Specifies the type of storage, either volatile or non-volatile.

—End—

See also

- ["Displaying QoS actions" \(page 189\)](#)
- [Click the ellipses to select the ports for the interface shaper.](#)

Adding Interface action extensions

To add a QoS interface action extension:

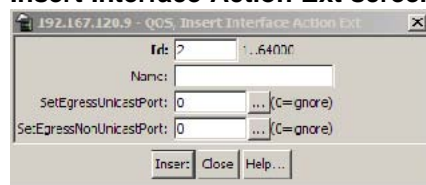
Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the QoS screen by selecting QoS > QoS from the menu. This screen is illustrated in "QoS Action tab" (page 189) . Select the Interface Action Ext tab. This tab is illustrated in "Interface Action Ext tab" (page 192) . |
|---|---|

- | | |
|---|-----------------------|
| 2 | Click Insert . |
|---|-----------------------|

The **Insert Interface Action Ext** screen opens (["Insert Interface Action Ext screen" \(page 193\)](#)).

Insert Interface Action Ext screen



- | | |
|---|---|
| 3 | Enter the information and make the selections to use for this Interface action extension. |
|---|---|

- | | |
|---|-----------------------|
| 4 | Click Insert . |
|---|-----------------------|

—End—

See also

- ["Deleting Interface action extensions" \(page 194\)](#)

Deleting Interface action extensions

To delete a QoS interface action extension:

Step	Action
1	Open the QoS screen by selecting QoS > QoS from the menu. This screen is illustrated in "QoS Action tab" (page 189) . Select the Interface Action Ext tab. This tab is illustrated in "Interface Action Ext tab" (page 192) .
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—

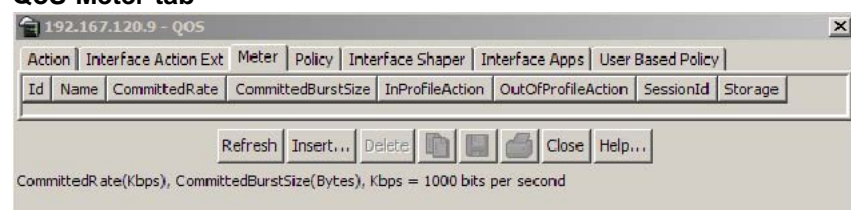
See also

- ["Adding Interface action extensions" \(page 193\)](#)

Displaying QoS meters

To display a QoS meter:

Step	Action
1	Open the QoS screen by selecting QoS > QoS from the menu. This screen is illustrated in "QoS Action tab" (page 189) . Select the Meter tab.

QoS Meter tab

The following table ["QoS Meter tab fields" \(page 195\)](#) describes the **QoS Meter** tab fields.

QoS Meter tab fields

Field	Description
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.

—End—

See also

- ["Displaying QoS actions" \(page 189\)](#)
- [Click the ellipses to select the ports for the interface shaper.](#)

Adding QoS meters

To add a QoS meter:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the QoS screen by selecting QoS > QoS from the menu. This screen is illustrated in "QoS Action tab" (page 189) . Select the Meter tab. This tab is illustrated in "QoS Meter tab" (page 194) . |
| 2 | Click Insert .
The Insert Meter dialog opens ("Insert Meter screen" (page 196)). |

Insert Meter screen

- 3 Enter the information and make the selections to use for this QoS meter.
- 4 Click **Insert**.

—End—

See also

- ["Deleting QoS meters" \(page 196\)](#)

Deleting QoS meters

Device Manager lets you delete QoS meters.

To delete a QoS meter:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the QoS screen by selecting QoS > QoS from the menu. This screen is illustrated in "QoS Action tab" (page 189) . Select the Meter tab. This tab is illustrated in "QoS Meter tab" (page 194) . |
| 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

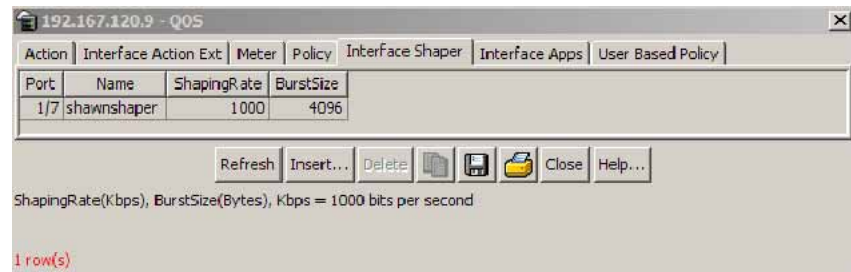
Device Manager lets you display QoS policies.

To display QoS Interface Shapers:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the QoS screen by selecting QoS > QoS from the menu. This screen is illustrated in "QoS Action tab" (page 189). Select the Interface Shaper tab. This tab is illustrated in "QoS Interface Shaper tab" (page 197). |
|---|---|

QoS Interface Shaper tab



The following table "Interface Shaper tab fields" (page 197) describes the **Interface Shaper** tab fields.

Interface Shaper tab fields

Field	Description
ifIndex	The ifIndex value that is associated with this instance of the ntnQosIfShapingEntry. The ifIndex value of this attribute must correspond to the ifTable entry with the same ifIndex value.
Label	A label used to reference the interface shaping data in a textual manner.
Port	The port associated with interface shaping.
Name	The name applied to the interface shaping data.

Field	Description
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.

—End—

Adding Interface Shapers

To add QoS Interface Shapers:

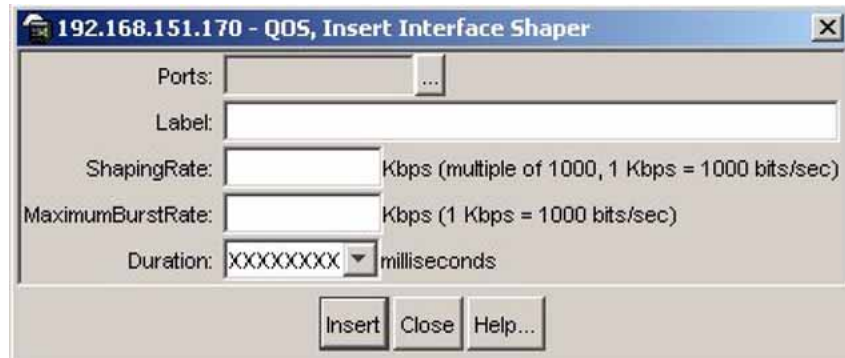
Step	Action
------	--------

1	Open the QoS screen by selecting QoS > QoS from the menu. This screen is illustrated in "QoS Action tab" (page 189). Select the Interface Shaper tab. This tab is illustrated in "QoS Interface Shaper tab" (page 197).
---	---

2	Click Insert .
---	-----------------------

The **Insert Interface Shaper** screen opens ("QoS, Insert Interface Shaper dialog box" (page 198)).

QoS, Insert Interface Shaper dialog box



3	Click the ellipses to select the ports for the interface shaper.
---	--

The **ntnQoSIfShapingPorts** screen opens ("ntnQoSIfShapingPorts screen" (page 199)).

ntnQoSIfShapingPorts screen



- 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

To delete an Interface Shaper, use the following procedure:

Step Action

- 1 Open the **QoS** screen by selecting **QoS > QoS** from the menu. This screen is illustrated in "QoS Action tab" (page 189). Select the **Interface Shaper** tab. This tab is illustrated in "QoS Interface Shaper tab" (page 197).
- 2 Highlight the Interface Shaper that to delete.
- 3 Click **Delete**.

—End—

Displaying QoS policies

To display QoS policies, use the following procedure:

Step Action

- 1 Open the **QoS** screen by selecting **QoS > QoS** from the menu. This screen is illustrated in "QoS Action tab" (page 189). Select the **Policy** tab. This tab is illustrated in "QoS Policy tab" (page 200).

QoS Policy tab

Id	Status	Name	ClassifierType	ClassifierName	InterfaceRoles	InterfaceIndex	Precedence	Weight	Classification	DropAction	StabType	BestEffort	Storage
5500	enabled	UnratedDiffs	classifierBlock	UnratedDiffs	allQoSInterfaces	0	2	none	UnratedDiffs	none	aggregate	0	other
5501	enabled	UnratedDiffs	classifierBlock	UnratedDiffs	allQoSInterfaces	0	1	none	UnratedDiffs	none	aggregate	0	other
5502	enabled	showAllPolicy	classifier	showAllPolicy		12	14	none	showAllPolicy	none	aggregate	0	other
5503	enabled	showAllPolicy	classifier	showAllPolicy		20	14	none	showAllPolicy	none	aggregate	0	other
5504	enabled	showUDPPolicy	classifier	showUDPPolicy		23	14	none	showUDPPolicy	none	aggregate	0	other
5505	enabled	showVLAN	classifier	showVLAN		31	14	none	showVLAN	none	aggregate	0	other

The following table "QoS Policy tab fields" (page 200) describes the **Policy** tab fields.

QoS Policy tab fields

Field	Description
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 151)) prior to associating it with a policy.
InterfaceIndex	The ifIndex field identifies the interface to which the policy is to be applied. A policy is associated with an interface explicitly using this attribute or implicitly using a role combination through the ntnQoSPolicyInterfaceRole attribute. An interface must be identified by one and only one of these attributes. This attribute can identify an interface that does not currently exist in the system, as long as the specified interface index represents a potentially valid system interface. Note: The InterfaceRoles and InterfaceIndex fields are mutually exclusive. When the InterfaceIndex field is not zero, the InterfaceRoles must be empty.

Field	Description
	(select none when insert the policy). When the InterfaceRoles specifies a valid role combination, the InterfaceIndex field must be 0.
Precedence	<p>Specifies the order in which multiple policies are associated with the same interface. Policies with greater precedence have higher numbers.</p> <p>Note: Policies with higher precedence values are applied before policies with lower precedence values.</p>
Meter	<p>Specifies metering associated with this policy. Specifying a metering component causes any action criteria specified explicitly by the policy to be rejected as an error.</p> <p>Note: You must configure meters before associating them with a policy.</p>
InProfileAction	<p>Identifies the action to be applied to traffic with this policy. This will not be used when a meter is specified.</p> <p>Note: You must configure actions before associating them with a policy.</p>
NonMatchAction	<p>Identifies action taken for flows that do not match policy criteria.</p>

Field	Description
StatsType	Specifies statistics tracking: <ul style="list-style-type: none"> • none--no statistics tracked for this policy • individual--separate counters allocated, space permitting, for each classifier referenced by the policy • aggregate--a single counter accumulates all the statistics for all the classifiers referenced by the policy
SessionId	Specifies the numerical identification for the current session.
Storage	Specifies the type of storage: <ul style="list-style-type: none"> • volatile • nonVolatile • readOnly

—End—

See also

- ["Displaying QoS actions" \(page 189\)](#)
- ["Displaying Interface action extensions" \(page 192\)](#)

Adding QoS policies

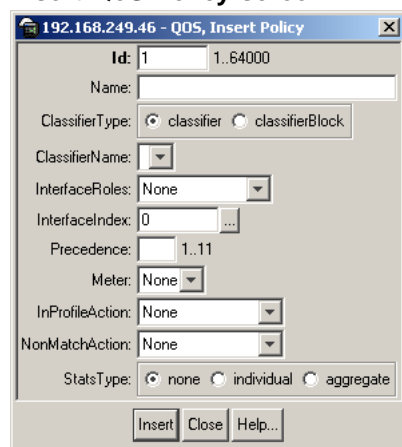
Use the Device Manager to add QoS policies.

To add a QoS policy, use the following procedure:

Step	Action
1	Open the QoS screen by selecting QoS > QoS from the menu. This screen is illustrated in " QoS Action tab " (page 189). Select the Policy tab. This tab is illustrated in " QoS Policy tab " (page 200).
2	Click Insert .

The **Insert QoS Policy** screen opens ("Insert QoS Policy screen" (page 203)).

Insert QoS Policy screen



- 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—

See also

- "Deleting QoS policies" (page 203)

Deleting QoS policies

Use the Device manager to delete QoS policies.

To delete a QoS policy, use the following procedure:

Step	Action
1	Open the QoS screen by selecting QoS > QoS from the menu. This screen is illustrated in "QoS Action tab" (page 189). Select the Policy tab. This tab is illustrated in "QoS Policy tab" (page 200).
2	Highlight the QoS policy to delete.
3	Click Delete .

—End—

QoS Policy Stats

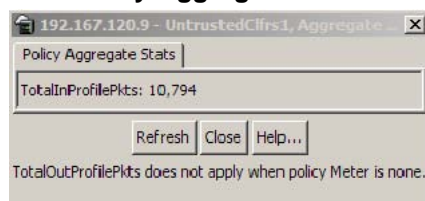
To view QoS Policy Stats information for a policy, follow this procedure.

Viewing QoS Policy Stats

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. |

QoS Policy Aggregate Stats tab



—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

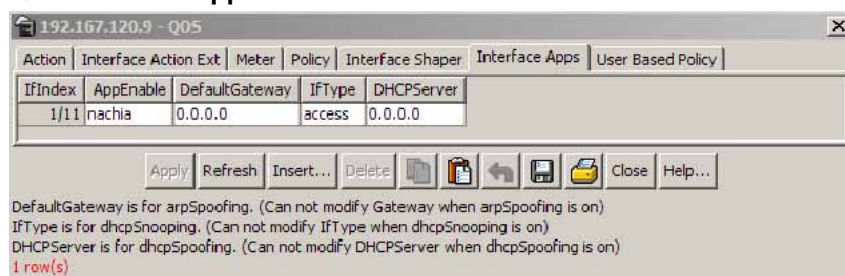
Note: Due to hardware limitations, the Ethernet Routing Switch 5520 model supports only 11 interface applications per port.

To view configured QoS interface applications, use the following procedure:

Step Action

- 1 Open the **QoS** screen by selecting **QoS > QoS** from the menu. Select the **Interface Apps** tab depicted in the following illustration.

QoS Interface Apps tab



"Interface Apps tab fields" (page 205) describes the fields on this tab.

Interface Apps tab fields

Field	Description
IfIndex	The ports that this QoS application applies to.
AppEnable	The applications enabled for the interface (port) specified in IfIndex field.
DefaultGateway	<p>The default gateway configured for the arpSpoofing application. The default gateway cannot be directly modified.</p> <p>To modify the default gateway for the arpSpoofing application, do the following:</p> <ol style="list-style-type: none"> 1. Double-click the AppEnable field and de-select arpSpoofing. 2. Click Apply. 3. Double-click the AppEnable field, select arpSpoofing, and edit the DefaultGateway field. 4. Click Apply.

Field	Description
IfType	The interface type configured for the dhcpSnooping application.
DHCP Server	<p>The DHCP server configured for the dhcpSpoofing application. The DHCP server cannot be directly modified.</p> <p>To modify the DHCP server for the dhcpSpoofing application, do the following:</p> <ol style="list-style-type: none"> 1. Double-click the AppEnable field and de-select dhcpSpoofing. 2. Click Apply. 3. Double-click the AppEnable field, select dhcpSpoofing, and edit the DHCP Server field. 4. Click Apply.

—End—

Adding an Interface Application

To add an Interface Application, follow this procedure:

Step	Action
1	Open the QoS screen by selecting QoS > QoS from the menu. Select the Interface Apps tab. This tab is illustrated in " QoS Interface Apps tab " (page 205).
2	Click Insert . The Insert Interface Apps screen opens. This screen is illustrated in " Insert Interface Apps tab " (page 207).

Insert Interface Apps tab



- 3 In the fields provided, enter the information for the new entry. "Insert Interface Apps screen fields" (page 207) outlines the fields on this screen.

Insert Interface Apps screen fields

Field	Description
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.

- 4 Click **Insert**.
The new Interface Application entry is displayed on the **Interface App** tab.

—End—

Deleting an Interface Application

To delete an Interface Application, follow this procedure:

Step	Action
1	Open the QoS screen by selecting QoS > QoS from the menu. Select the Interface Apps tab. This tab is illustrated in " QoS Interface Apps tab " (page 205).
2	Select the Interface Application to delete.
3	Click Delete .

—End—

See also

- "[Adding QoS policies](#)" (page 202)

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.

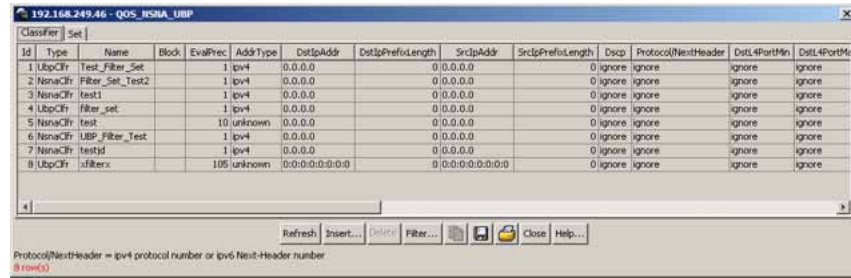
If you had previously defined the filter, then that pre-existent filter is used. Once a filter is created (either by you or automatically by the switch), it can be modified (that is, entries can be deleted or added) on the **QOS_NSNA** dialog box.

Inserting a classifier

To configure a classifier for the Nortel SNA solution or a User Based Policy:

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 (see " QOS_NSNA_UBP - Classifier dialog box " (page 209)).

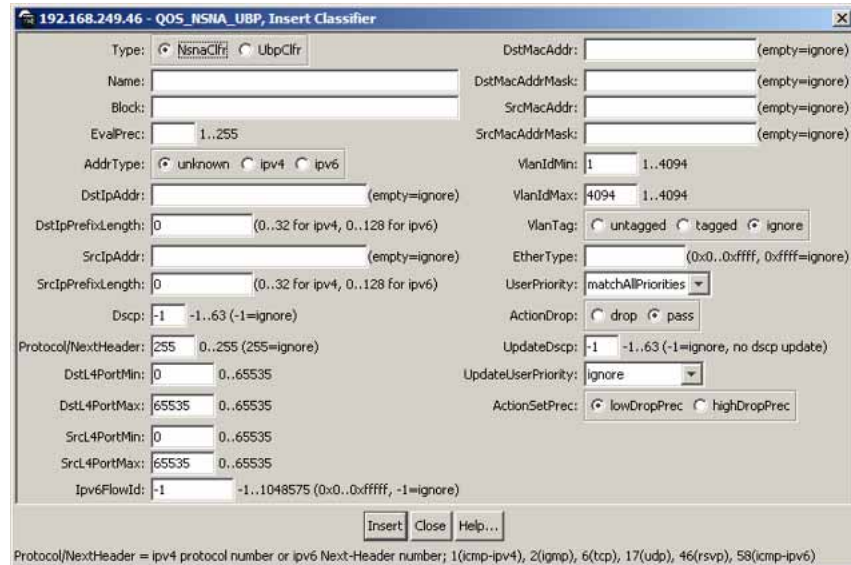
QOS_NSNA_UBP - Classifier dialog box



- 2 Click **Insert**.

The **QOS_NSNA_UBP, Insert Classifier** dialog box opens (see "QOS_NSNA_UBP, Insert Classifier dialog box" (page 209)).

QOS_NSNA_UBP, Insert Classifier dialog box



- 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.

Table describes the **QOS_NSNA_UBP Classifier** fields.

QOS_NSNA_UBP Classifier fields

Field	Description
Id	Specifies the ID number of the classifier.
Name	Specifies the name of the classifier. All classifiers with the same name are part of the same filter set. That filter set has the same name as the classifiers.
Block	Specifies the block name with which the classifier is associated.
EvalPrec	Specifies the evaluation order number of the classifier in that filter set. Two classifiers in the same filter set cannot have the same evaluation order. A higher eval order means a lower precedence for the corresponding policy.
AddrType	Specifies the type of IP address used by this classifier entry.
DstIpAddr	Specifies the IP address to match against the destination IP address of a packet.
DstIpPrefixLength	Specifies the length of the destination address mask.
SrcIpAddr	Specifies the IP address to match against the source IP address of a packet.
SrcIpPrefixLength	Specifies the length of the source address mask.
Dscp	Specifies the value for a DiffServ Codepoint (DSCP) in a packet.
Protocol/NextHeader	Specifies the IPv4 protocol value, or the IPv6 next-header value. Values are the following: <ul style="list-style-type: none"> • 1 = ICMP-IPv4 • 2 = IGMP • 6 = TCP • 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.

Field	Description
DstMacAddr	Specifies the MAC address against which the MAC destination address of incoming packets is compared.
DstMacAddrMask	Specifies a mask identifying the destination MAC address.
SrcMacAddr	Specifies a MAC source address of incoming packets.
SrcMacAddrMask	Specifies a mask identifying the source MAC address.
VlanIdMin	Specifies the minimum value for the VLAN ID in a packet.
VlanIdMax	Specifies the maximum value for the VLAN ID in a packet.
VlanTag	Specifies the type of VLAN tagging in a packet: <ul style="list-style-type: none"> • untagged • tagged • ignore
EtherType	Specifies the value for the 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).

—End—

Deleting a classifier

- | 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 (see " QOS_NSNA_UBP - Classifier dialog box " (page 209)). |
| 2 | Select the classifier you want to delete. |
| 3 | Click Delete . |

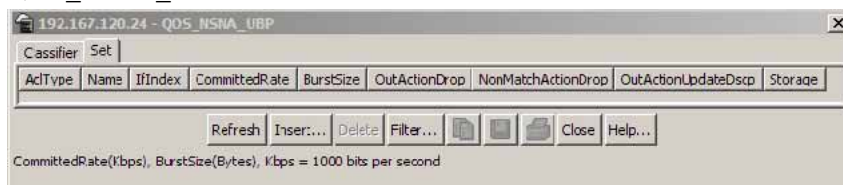
—End—

Configuring a set

To configure a set:

- | 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 (see " QOS_NSNA_UBP - Classifier dialog box " (page 209)). |
| 2 | Click the Set tab.
The Set tab is selected (see " QOS_NSNA_UBP Set tab " (page 212)). |

QOS_NSNA_UBP Set tab



"[QoS NSNA/UBP Set fields](#)" (page 212) describes the QoS NSNA/UBP Set fields.

QoS NSNA/UBP Set fields

Field	Description
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.

Field	Description
OutActionDrop	<p>Specifies the action to take when packet is out-of-profile.</p> <p>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.)</p> <p>Options are the following:</p> <ul style="list-style-type: none"> • drop (packet is dropped) • pass (packet is not dropped) <p>The default value is pass.</p>
NonMatchActionDrop	<p>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.</p> <p>Options are the following:</p> <ul style="list-style-type: none"> • drop (packet is dropped) • pass (packet not dropped) • defer (no explicit drop/pass action is specified; the decision is deferred) <p>The default value is defer.</p>
OutActionUpdateDscp	<p>Specifies the action to take to update DSCP when a packet is out-of-profile.</p> <p>The default value is -1. The value range is between -1 to 63.</p>
Storage	Specifies the type of storage.

3 Click **Insert**.

The **QOS_NSNA_UBP, Insert Set** dialog box opens (see "QOS_NSNA_UBP, Insert Set dialog" (page 214)).

QOS_NSNA_UBP, Insert Set dialog

- 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—

Deleting a set

To delete a QoS NSNA UBP set, use the following procedure:

Deleting a set**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—

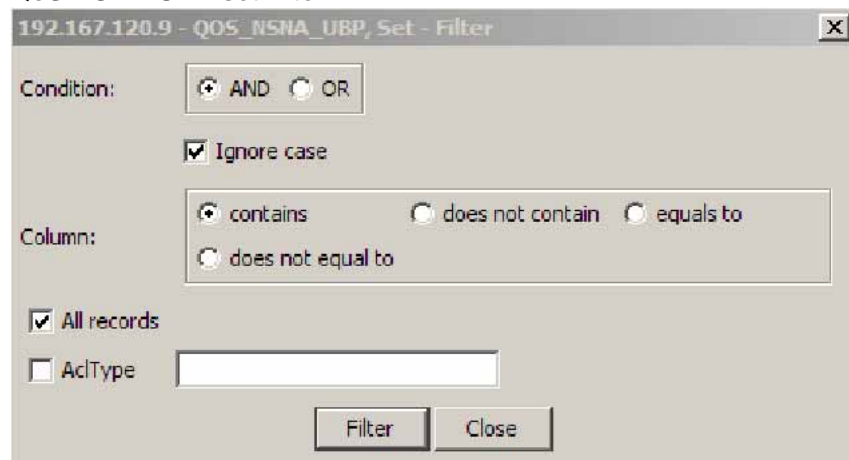
Filtering a set

To filter a QoS NSNA UBP set, use the following procedure:

Filtering a set

- | 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. |

QoS NSNA UBP set filter



- | | |
|---|--|
| 6 | Set the filter parameters in the dialog. |
| 7 | Click Filter . |

—End—

Displaying User Based Policy session information

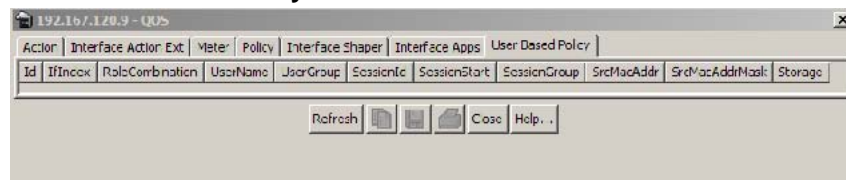
Use the following procedure to view user based policy information for the active session.

- | 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.

QoS User Based Policy tab



User Based Policy tab fields

Field	Description
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 be 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 instant this user policy entry is created or updated.
SessionGroup	Displays the system-assigned session group identifier. TIP: Multiple user sessions belong to the same group if they share the same role combination and have the same value for this field. SessionGroup is associated with installed policy criteria to identify users and interfaces to which the QoS policy is applied.
SrcMacAddr	Displays the source MAC address associated with the identified user.
SrcMacAddrMask	Specifies the bits in a source MAC address that should be considered when an 802 MAC SA comparison is performed against the address specified in the SrcMacAddr field.
Storage	Specifies the storage type for this entry.

—End—

QoS agent

This section contains information on working with QoS agents.

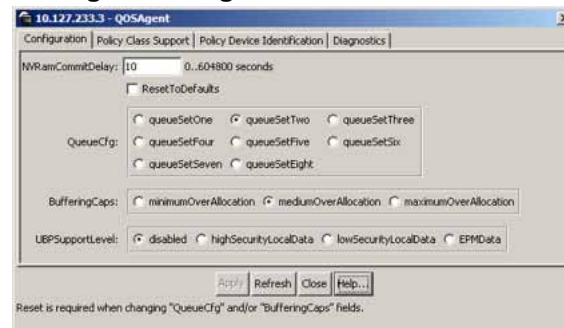
Displaying QoS agent configuration

To display QoS agent configuration:

Step	Action
------	--------

- | | |
|---|---|
| 1 | Open the QoSAgent screen by selecting QoS > QoS Agent from the menu. This screen is illustrated in " QoSAgent Configuration tab " (page 217). Select the Configuration tab. This tab is illustrated in " QoSAgent Configuration tab " (page 217). |
|---|---|

QoSAgent Configuration tab



The following table "[Configuration tab fields](#)" (page 217) describes the **Configuration** tab fields.

Configuration tab fields

Field	Description
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.

Field	Description
BufferingCaps	<p>The value of this attribute determines the method through which buffering resources are allocated to ports sharing a pool of buffers.</p> <p>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.</p> <p>You must restart the system if you change the current attribute.</p>
UBPSupportLevel	The value of this attribute sets the level of User Based Policy support.

—End—

See also

- ["Displaying policy class support" \(page 218\)](#)
- ["Displaying policy device identification" \(page 220\)](#)
- ["Displaying diagnostics" \(page 221\)](#)

Displaying policy class support

To display policy class support:

Step Action

- 1 Open the **QoSAgent** screen by selecting **QoS > QoS Agent** from the menu. This screen is illustrated in "[QoSAgent Configuration tab](#)" (page 217). Select the **Policy Class Support** tab. This tab is illustrated in "[Policy Class Support tab](#)" (page 219).

Policy Class Support tab

PolicyClassName	CurrentInstances	MaxInstalledInstances
ntrnQosPrcSupportTable	25	0
ntrnQosPolicyDeviceIdentTable	1	0
ntrnQosInterfaceTypeTable	1	100
ntrnQosIfQueueTable	36	0
ntrnQosIfAssignmentTable	26	512
ntrnQosDscpToCosTable	64	64
ntrnQosCosToDscpTable	8	8
ntrnQosQsetPriAssignmentTable	64	8
ntrnDsMultiFieldClfrTable	0	200
ntrnL2MultiFieldClfrTable	2	200
ntrnSystemClfrTable	0	100
ntrnClfrComponentTable	2	400
ntrnClfrBlockTable	2	200
ntrnQosIfcActionTable	0	64
ntrnQosBaseActionTable	11	128

The following table "Policy Class Support tab fields" (page 219) describes the **Policy Class Support** tab fields.

Policy Class Support tab fields

Field	Description
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).

—End—

See also

- "Displaying QoS agent configuration" (page 217)
- "Displaying policy device identification" (page 220)

- "Displaying diagnostics" (page 221)

Displaying policy device identification

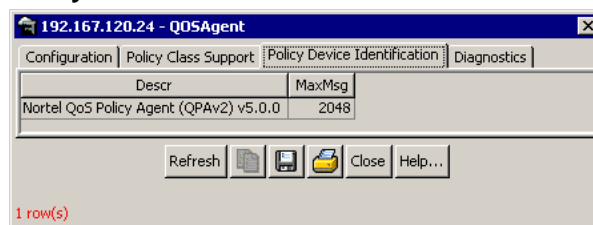
Use the Device Manager to display policy device identification data.

To display policy device identification data use the following procedure.

Step Action

- 1 Open the **QoSAgent** screen by selecting **QoS > QoS Agent** from the menu. This screen is illustrated in "QoSAgent Configuration tab" (page 217). Select the **Policy Device Identification** tab. This tab is illustrated in "Policy Device Identification tab" (page 220).

Policy Device Identification tab



The following table "Policy Device Identification tab fields" (page 220) describes the **Policy Device Identification** tab fields.

Policy Device Identification tab fields

Field	Description
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.

—End—

See also

- "Displaying QoS agent configuration" (page 217)
- "Displaying policy class support" (page 218)
- "Displaying diagnostics" (page 221)

Displaying diagnostics

To display QoS diagnostics information:

Step	Action
------	--------

- | | |
|---|--|
| 1 | Open the QoSAgent screen by selecting QoS > QoS Agent from the menu. This screen is illustrated in " QoSAgent Configuration tab " (page 217). Select the Diagnostics tab. This tab is illustrated in " Diagnostics tab " (page 221). |
|---|--|

Diagnostics tab

Port	MasksConsumed	FiltersConsumed	MetersConsumed	CountersConsumed	NonQosMasksConsumed	NonQosFiltersConsumed	NonQosMetersConsumed
1/1	2	2	0	2	5	6	0
1/2	3	3	0	3	5	6	0
1/3	2	2	0	2	5	6	0
1/5	2	2	0	2	5	6	0
1/6	?	?	0	?	5	6	0
1/7	?	?	0	?	5	6	0
1/8	?	?	0	?	5	6	0
1/9	?	?	0	?	5	6	0
1/10	?	?	0	?	5	6	0
1/11	3	3	0	3	5	6	0
1/12	2	2	0	2	5	6	0
1/14	2	2	0	2	5	6	0
1/16	2	2	0	2	5	6	0
1/17	2	2	0	2	5	6	0
1/18	2	2	0	2	5	6	0
1/19	?	?	0	?	5	6	0
1/20	3	3	0	3	5	6	0
1/22	?	?	0	?	5	6	0
1/23	3	3	0	3	5	6	0
1/24	?	?	0	?	5	6	0
1/25	?	?	0	?	5	6	0
1/26	2	2	0	2	5	6	0

The following table "[Diagnostics tab fields](#)" (page 221) describes the **Diagnostics** tab fields.

Diagnostics tab fields

Field	Description
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.

Field	Description
NonQosMasksConsumed	Displays the number of classification masks in use <i>not</i> from policy and filter data by that interface.
NonQosFiltersConsumed	Displays the number of rules (filters) in use <i>not</i> from policy and filter data by that interface.
NonQosMetersConsumed	Displays the number of meters in use <i>not</i> from policy data by that interface. These are meter resources used by other applications besides QoS; none of these are currently supported on the BayStack 5500 switch.

—End—

See also

- ["Displaying QoS agent configuration" \(page 217\)](#)
 - ["Displaying policy class support" \(page 218\)](#)
- ["Displaying policy device identification" \(page 220\)](#)

Index

Symbols/Numerics

802.1p user priority 116
 802.1pPriority field 161, 162, 164, 165, 173

A

AbsBandwidth field 152
 Action extensions 134
 Action field 185
 add an Interface Application 206
 AddressType field 169
 aggregate flow 18
 ARP spoofing 41

B

Bandwidth Allocation field 152
 Bandwidth field 152
 BlockNumber field 185
 buffer allocation mode 61

C

Capabilities field 154
 class field 64
 classifier 208
 classifier blocks 25, 36, 66, 129
 classifier elements 23
 Classifier elements 25, 36
 ClassifierName field 200
 classifiers 36, 66
 ClassifierSetId field 185
 ClassifierType field 200
 CLI commands 51
 Command Line Interface (CLI) 45
 CommittedBurstSize field 195

CommittedRate field 195
 configuration
 QoS 155, 156
 contact Nortel Technical Support 15
 CoS priority value 38
 CoS queues 38, 38
 CoS-to-queue 38, 40
 CoS-to-queue assignments 62
 CountersConsumed field 221
 CurrentInstances field 219

D

DCOM 42
 default queue configuration 60
 delete an Interface Application 207
 Device Manager 220
 DHCP Snooping 41
 DHCP Spoofing 41
 Diagnostics 145
 Differentiated Services (DiffServ) 17, 17
 Differentiated services (DiffServ) 18
 DiffServ 93
 Discipline field 152
 Drop field 189
 drop precedence 32
 DropPrecedence field 166
 DSCP 32
 Dscp field 164, 165, 169
 DSCP mapping 117
 DSCP to 802.1p user priority/drop
 precedence mapping 118
 DSCP, IEEE 802.1p priority 65
 DstAddr field 169
 DstL4Port field 170

DstMacAddr field 173
 DstMacAddrMask field 173
 DstMaskLength field 169

E

EAP 22
 egress QoS interface 38, 38
 Elements 66
 end-to-end QoS 19
 EPM 22
 EtherType field 173
 Express Routing Code (ERC) 16
 Extension field 190

F

feedback 228
 FiltersConsumed field 221

G

Group Assignment dialog box 155

H

hardware policy configuration 142

I

ICMP Echo Requests (ping) 40
 Id feild 189
 Id field 195
 IEEE 802.1p priority 32
 IfClass field 154
 in-profile-action field 78
 InProfileAction field 195, 201
 Insert Action dialog box 190
 Insert Classifier Block dialog box 186, 186,
 186, 188
 Insert Classifier dialog box 181
 Insert Interface Group dialog box 156
 Insert IP Classifier Element dialog box 170
 Insert L2 Classifier Element dialog box 174
 Insert Meter dialog box 195
 Insert Policy dialog box 203
 Interface Action Ext dialog box 193
 Interface Action Extension 134
 interface action extensions 28
 Interface Assignment button 155

Interface Configurations 21
 interface group configuration 112
 Interface groups 21
 interface groups 153
 Interface ID Table 113
 interface IDs 157
 Interface queues 151
 interface queues 151
 Interface Shaper 199
 Interface shaping 22
 Interface Shaping 138
 InterfaceRoles field 200
 interfaces 64
 intradomain QoS 19
 IP classifier element 122
 IP filter tab
 IPv6FlowId field 170

L

Label field 192
 Layer 2 classifier elements 124
 layer 2 filter group tab

M

MasksConsumed field 221
 MaximumInstalledInstances field 219
 MaxMsg field 220
 Meter field 185, 201
 MetersConsumed field 221
 microflow 18

N

Name field 189, 195
 network access device 22
 NonMatchAction field 201
 NonQosFiltersConsumed field 222
 NonQosMasksConsumed field 222
 NonQosMetersConsumed field 222
 Nortel Ethernet Routing Switch 5510-24T 13
 Nortel Ethernet Routing Switch 5510-48T 13
 Nortel Ethernet Routing Switch
 5520-24T-PWR 13
 Nortel Ethernet Routing Switch
 5520-48T-PWR 13
 Nortel Ethernet Routing Switch
 5530-24TFD 13

Nortel service program 15
 Nortel SNA 22
 NVRamCommitDelay field 217

O

out-profile-action field 78
 OutOfProfileAction field 195

P

Packet classifiers 23
 per-hop behavior (PHB) 18
 Platinum, Gold, Silver, and Bronze
 classes 19
 Policy Class Support 218
 Policy-enabled networks 17
 PolicyClassName field 219
 port-based Quality of Service 18
 Ports 63
 Precedence field 201
 precedence range 34
 Premium class 19
 Protocol field 169

Q

QoS

action 191
 adding classifier blocks 186
 adding classifiers 181
 adding interface groups 156
 adding IP classifier elements 170
 adding policies 202
 classifier block 188
 classifier blocks 187
 classifier elements 181
 classifiers 171, 181, 182
 deleting classifier blocks 187
 deleting classifiers 182
 deleting interface groups 157
 deleting IP classifier elements 171
 deleting L2 classifier elements 174
 deleting meters 196
 deleting policies 203
 deleting ports from interface groups 155
 displaying DSCP mappings 164
 displaying L2 classifier elements 172,
 175, 176

displaying policies 197
 displaying policy device identification 220
 displaying priority mapping 163
 displaying priority queue assign-
 ments 161
 interface action extension 194
 interface group 156
 interface groups 153, 155, 156, 157
 interface IDs 157
 interface queues 151
 interfaces 64
 meter 191, 196
 policy precedence 201
 policy, enabling 200
 ports 155, 156
 queues 157
 role combinations 156, 157
 statistics 202
 trusted ports 64
 unrestricted ports 64
 untrusted ports 64

QoS action tab
 QoS actions 74
 QoS agent 91
 QoS agent configuration tab ,
 QoS agents 216
 QoS classes 35
 QoS Classifier tab
 QoS Configuration Wizard 105
 QoS diagnostics 221
 QoS DSCP mapping tab
 QoS egress port 37
 qos if-shaper 78
 QoS interface 37
 QoS interface action 76
 QoS Interface Applications 204
 QoS Interface Applications wizard 110
 QoS Interface group tab
 QoS interface ID tab
 QoS Interface Queue tab
 QoS Interface Shaper wizard 109
 QoS interfaces 40
 QoS IP Classifier Element tab
 QoS Management Wizard 105
 qos meter 77
 QoS metering 29
 QoS meters 136

- QoS meters tab ,
 - QoS policies 34, 79, 140, 199
 - QoS policies tab
 - QoS policy class tab
 - QoS policy device identification tab
 - QoS priority assign tab
 - QoS priority mapping tab
 - QoS queue 37
 - QoS Resource Allocation Table field 147
 - QoS security settings 56
 - qos system-element 72
 - QoS Wizards 93
 - QPA operational parameters 144
 - Quality of Service (QoS) 17, 17, 18, 93, 151
 - Queue bandwidth allocation 37
 - Queue count 37
 - Queue field 162
 - Queue service discipline 37
 - Queue service order 37
 - Queue size 37
 - queue weights 38
 - QueueId field 152
 - QueueSet field 158
- R**
- ResetToDefaults field 217
 - role-based policies 18
 - RoleCombination field 158
 - Roles field 154
 - RPC 42
- S**
- service disciplines 38
 - ServiceClass field 166
 - ServiceOrder field 153
 - SetDropPrecedence field 190
 - SetEgressNonUnicastPort field 192
 - SetEgressUnicastPort field 192
 - SetId field 152, 180
 - single policy 35
 - SLA 19
 - SNMP 40
 - Specific field 180
 - SQLSlam 42
 - SrcAddr field 169
 - SrcL4Port field 170
 - SrcMacAddr field 173
 - SrcMacAddrMask field 173
 - SrcMaskLength field 169
 - Standard class 19
 - Statistics 35
 - StatsType field 202
 - Status field 200
 - Storage field 170, 173, 190, 193, 195, 202
 - StorageType field 154
 - system classifier 24
 - System Classifier Element 125
- T**
- traffic stream 18
 - troubleshooting
 - QoS 155, 157, 171, 181, 182, 187, 188, 191, 194, 196
 - trusted 30
- U**
- UDP packets 42
 - UDP port 42
 - unrestricted 30
 - untrusted 30
 - Update Dscp field 190
 - UpdateUserPriority field 190
 - user based policies 22
 - User Based Policies 87, 208, 215
 - User Policy Table 22
- V**
- video stream 18, 18
 - VlanId field 173
 - VlanTag field 173
- W**
- W32/Blaster-A 42
 - W32/Nachi 42
 - W32/Nachi-A 42
 - W32/Nachi-B 42
 - worm 42
 - worms 42
 - WRR queues 38

Nortel Ethernet Routing Switch 5500 Series

Configuration - Quality of Service

Copyright © 2005 - 2007, Nortel Networks
All Rights Reserved.

Publication: NN47200-504
Document status: Standard
Document version: 03.01
Document date: 27 August 2007

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.

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

