Part No. 217106-A
June 2005

4655 Great America Parkway
Santa Clara, CA 95054

Configuring Quality of Service and IP Filtering

Nortel Ethernet Switches 460 and 470
Software Release 3.6

217106-A

NORTEL

Copyright © Nortel Networks Limited 2005. 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 NA 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.

Trademarks

Autotopology, BayStack, BaySecure, Business Policy Switch 2000, Nortel Networks, the Nortel Networks logo, Optivity, Optivity Policy Services, Preside, and Quick2Config are trademarks of Nortel Networks.

Microsoft, MS, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Java is a trademark of Sun Microsystems, Inc.

Acrobat and Adobe are trademarks of Adobe Systems, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

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 Inc. reserves the right to make changes to the products described in this document without notice.

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

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

International regulatory statements of conformity

This is to certify that the Nortel Ethernet Switches 460 and 470 were evaluated to the international regulatory standards for electromagnetic compliance (EMC) and safety and were found to have met the requirements for the following international standards:

- EMC - Electromagnetic Emissions – CISPR 22, Class A
- EMC - Electromagnetic Immunity – CISPR 24
- Electrical Safety – IEC 60950, with CB member national deviations

Further, the equipment has been certified as compliant with the national standards as detailed below.

National electromagnetic compliance (EMC) statements of compliance

FCC statement (USA only)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission (FCC) rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to take whatever measures may be necessary to correct the interference at their own expense.

ICES statement (Canada only)

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Nortel Ethernet Switches 460 and 470) do not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (Nortel Ethernet Switches 460 and 470) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

CE marking statement (Europe only)

EN 55 022 statements

This is to certify that the Nortel Ethernet Switches 460 and 470 are shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC. Conformity is declared by the application of EN 55 022 Class A (CISPR 22).

Caution: This device is a Class A product. In a domestic environment, this device can cause radio interference, in which case the user may be required to take appropriate measures.

EN 55 024 statement

This is to certify that the Nortel Ethernet Switches 460 and 470 are shielded against the susceptibility to radio interference in accordance with the application of Council Directive 89/336/EEC. Conformity is declared by the application of
EN 55 024 (CISPR 24).

CE Declaration of Conformity

This product conforms to the provisions of the R&TTE Directive 1999/5/EC.

VCCI statement (Japan/Nippon only)

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI) for information technology equipment. If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

BSMI statement for Ethernet Switches 460 and 470 (Taiwan only)

This is a Class A product based on the standard of the Bureau of Standards, Metrology and Inspection (BSMI) CNS 13438, Class A.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻
干擾，在這種情況下，使用者 會被要求採取某些適當的對策。

MIC notice for Ethernet Switches 460 and 470 (Republic of Korea only)

This device has been approved for use in Business applications only per the Class A requirements of the Republic of Korea Ministry of Information and Communications (MIC). This device may not be sold for use in a non-business application.

Observe the Regulatory Marking label on the bottom surface of the chassis for specific certification information pertaining to this model. Each model in the Ethernet Switch Series which is approved for shipment to/usage in Korea is labeled as such, with all appropriate text and the appropriate MIC reference number.

National safety statements of compliance

CE marking statement (Europe only)

EN 60 950 statement

This is to certify that the Nortel Ethernet Switches 460 and 470 are in compliance with the requirements of EN 60 950 in accordance with the Low Voltage Directive. Additional national differences for all European Union countries have been evaluated for compliance.

NOM statement Ethernet Switches 460 and 470 (Mexico only)

The following information is provided on the devices described in this document in compliance with the safety requirements of the Norma Oficial Méxicana (NOM):

Exporter:	Nortel Networks, Inc. 4655 Great America Parkway Santa Clara CA 95054 USA
Importer:	Nortel Networks de México, S.A. de C.V. Avenida Insurgentes Sur #1605 Piso 30, Oficina Col. San Jose Insurgentes Deleg-Benito Juarez México D.F. 03900
Tel:	52 5 480 2100
Fax:	52 5 480 2199
Input:	Ethernet Switch 460, Ethernet Switch 470
	100 - 120 VAC 16A 50 to 60 Hz
	200 - 240 VAC 12 A 50 to 60 Hz

Información NOM (unicamente para México)

La información siguiente se proporciona en el dispositivo o en los dispositivos descritos en este documento, en cumplimiento con los requisitos de la Norma Oficial Méxicana (NOM):

Exportador:	Nortel Networks, Inc. 4655 Great America Parkway Santa Clara, CA 95054 USA
Importador:	Nortel Networks de México, S.A. de C.V. Avenida Insurgentes Sur #1605 Piso 30, Oficina Col. San Jose Insurgentes Deleg-Benito Juarez México D.F. 03900
Tel:	52 5 480 2100
Fax:	52 5 480 2199
Embarcar a:	Ethernet Switch 460, Ethernet Switch 470
	100 - 120 VAC 16A 50 to 60 Hz
	200 - 240 VAC 12 A 50 to 60 Hz

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 MERCHANTABLITITY 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 forgoing 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-Odd entities) and 48 C.F.R. 227.7202 (for Odd 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
June 2005	1.0	Created new document structure and incorporated new features for Ethernet Switch Release 3.6 software.

Contents

Figures

Tables

Preface

About this guide

This guide provides information about configuring and managing Quality of Service and IP Filtering features on the Nortel Ethernet Switch 460 and Nortel Ethernet Switch 470.

Network management tools and interfaces

The following are the management tools and interfaces available with the switch (for basic instructions on these tools, refer to the *System Configuration Guide* (217105-A)):

- Console interface

  The console interface (CI) allows you to configure and manage the switch locally or remotely. Access the CI menu and screens locally through a console terminal attached to your Ethernet Switch, remotely through a dial-up modem connection, or in-band through a Telnet session.

- Web-based management

  You can manage the network from the World Wide Web and can access the Web-based Graphical User Interface (GUI) through the HTML-based browser located on your network. The GUI allows you to configure, monitor, and maintain your network through web browsers. You can also download software using the web.

- Java-based Device Manager

  The Device Manager is a set of Java-based graphical network management applications that is used to configure and manage Ethernet Switches 460 and 470.

- Command Line Interface (CLI)

  The CLI is used to automate general management and configuration of the Ethernet Switches 460 and 470. Use the CLI through a Telnet connection or through the serial port on the console.

- Any generic SNMP-based network management software

  You can use any generic SNMP-based network management software to configure and manage Ethernet Switches 460 and 470.

- Telnet

  Telnet allows you to access the CLI and CI menu and screens locally using an in-band Telnet session.

- SSH

  Secure Shell (SSH) is a client/server protocol that can provide a secure remote login with encryption of data, username, and password. For details on SSH connections, refer to *Configuring and managing Security* (217104-A).

- Nortel Enterprise Policy Manager

  The Nortel Enterprise Policy Manager (formerly Optivity Policy Services) allows you to configure the Ethernet Switches 460 and 470 with a single system.

Before you begin

This guide is intended for network administrators with the following background:

- Basic knowledge of networks, bridging, and IP
- Familiarity with networking concepts and terminology
- Basic knowledge of network topologies

Before using this guide, you must complete the installation procedures discussed in *Installing the Nortel Ethernet Switch 460-24T-PWR* (213318-C) or *Installing the Nortel Ethernet Switch 470* (217108-A).

Text conventions

angle brackets (< >)

Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command.

Example: If the command syntax is

```
ip default-gateway <XXX.XXX.XXX.XXX>,
```

you enter

```
ip default-gateway 192.32.10.12
```

braces ({})

Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command.

Example: If the command syntax is

```
http-server {enable|disable}
```

the options for are `enable` or `disable`.

brackets ([ ])

Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.

Example: If the command syntax is

```
show ip [bootp],
```

you can enter either:

`show ip` or `show ip bootp`.

`plain Courier text`

Indicates command syntax and system output.

Example:

```
TFTP Server IP Address:  192.168.100.15
```

vertical line |

Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command.

Example: If the command syntax is

```
cli password <serial|telnet>,
```

you must enter either `cli password serial` or `cli password telnet`, but not both.

H.H.H.

Enter a MAC address in this format (XXXX.XXXX.XXXX).

Related publications

For more information about managing or using the switches, refer to the following publications:

- *Release Notes for the Ethernet Switch 460 and 470 Switch Software Version 3.6* (217103)
- *Installing the Nortel Ethernet Switch 460-24T-PWR* (213318-C)
- *Installing the Nortel Ethernet Switch 470* (217108-A)
- *System Configuration Guide* (217105-A)
- *Configuring and managing Security* (217104-A)
- *System Monitoring Guide* (217107-A)
- *Configuring IP Multicast Routing Protocols* (217459-A)
- *Configuring VLANs, Spanning Tree, and MultiLink Trunking* (217460-A)
- *Installing Gigabit Interface Converters and Small Form Factor Pluggable Interface Converters* (312865-B)

You can print selected technical manuals and release notes free, directly from the Internet. Go to www.nortel.com/support. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to the Adobe Systems web site to download a free copy of the Adobe Acrobat Reader.

Obtaining technical assistance

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel service program, contact one of the following Nortel Technical Solutions Centers:

Technical Solutions Center	Telephone
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 4NORTEL or (800) 466-7835
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

Additional information about the Nortel Technical Solutions Centers is available from www.nortel.com/callus.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to www.nortel.com/erc.

Chapter 1 About QoS

This chapter provides an overview of Differentiated Services Quality of Service (QoS) network architecture. The Ethernet Switches 460 and 470 provide a Web-based management interface, a Command Line Interface (CLI), and the graphical user interface Device Manager (DM) to configure QoS. Refer to the following for detailed information:

- Chapter 2, “Configuring QoS using the CLI,” on page 95
- Chapter 3, “Configuring QoS using Device Manager,” on page 137
- Chapter 4, “Implementing QoS Using QoS Wizard and QoS Quick Config,” on page 187
- Chapter 5, “Implementing QoS using QoS Advanced,” on page 233

In addition to these management systems, policies can be configured using SNMP and Common Open Policy Services (COPS). (See Chapter 6, “Implementing Common Open Policy Services using Web-based management” for details.)

The complexities of QoS are discussed in this chapter as listed below:

- “Summary” on page 34
- “Differentiated Services (DiffServ) overview” on page 36
- “QoS classes” on page 37
- “Packet classifiers or filters” on page 39
- “Ports” on page 43
- “Interface groups” on page 48
- “Metering overview” on page 49
- “Shaping overview” on page 50
- “Policy overview” on page 52
- “Packet flow using QoS” on page 53
- “Default QoS settings” on page 55

- “QoS configuration guidelines” on page 55
- “COPS overview” on page 55

Summary

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

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

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

Briefly, with DiffServ, you use policies to direct traffic by assigning packets to certain queues. The system marks the DiffServ (DS) field of IP packets to define how the packet is treated as it moves through the network. You classify traffic so that, together, the policies and the DS fields direct the traffic prioritization. You can specify a number of policies, and each policy can match one or many flows—supporting complex classification scenarios.

Summary of packet classifiers

The Ethernet Switches 460 and 470 classify packets based on various parameters:

- IP packets
  - source address/mask

  - destination address/mask
  - IP protocol type (such as TCP/UDP)
  - DSCP value
  - Layer 4 source port number
  - Layer 4 destination port number
  - Ingress port number
- Layer 2 packets
  - VLAN ID number
  - IEEE 802.1q tag presence
  - EtherType, which is the Layer 3 protocol type (such as AppleTalk)
  - IEEE 802.1p user priority values
  - Ingress port number
  - For EtherType IP:
    - DSCP value
    - IP protocol type (such as TCP/UDP)
    - TCP/UDP source port range
    - TCP/UDP destination port range

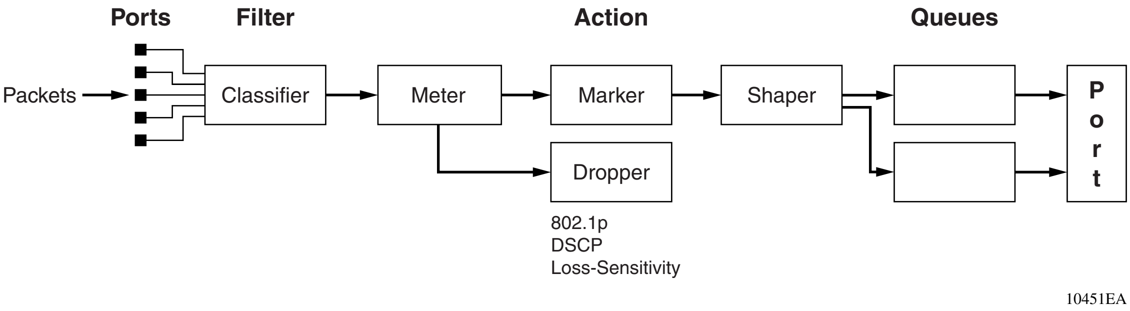
Summary of actions

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

- Pass or Drop.
- Re-mark the packet when Pass is selected:
  - Re-mark a new DiffServ Codepoint (DSCP).
  - Re-mark the 802.1p field.
  - Assign a drop precedence.

Figure 1 provides a schematic overview of QoS policies.

Figure 1 Schematic of QoS policy



Differentiated Services (DiffServ) overview

DiffServ is a QoS network architecture that offers varied levels of service for different types of data traffic. DiffServ lets you designate a specific level of performance on a packet-by-packet basis instead of using the best-effort model for your data delivery. You can give preferential treatment (prioritization) to applications that require high performance and reliable service, such as voice and video over IP.

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

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. Traffic shaping can also be used to temporarily delay traffic to ensure that the flows conform to downstream bandwidth limits.

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, marking, and shaping

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 six bits in the DSCP are marked to identify how the packet is to be treated at each subsequent network node. This mapping of DS codepoints to per-hop behavior (PHB) is configurable, and the DSCP can be re-marked as it passes through a DiffServ network. Re-marking the DSCP allows for the treatment of packets to be reset based on new network specifications or desired levels of service.

DiffServ assumes the existence of a Service Level Agreement (SLA) between DS domains that share a border. The SLA defines the profile for the aggregate traffic flowing from one network to the other based on policy criteria. In a given traffic direction, the traffic is expected to be shaped at the egress point of the upstream network and 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. Traffic metering and shaping ensures that the traffic flow conforms to an SLA to provide certain levels of service in terms of bandwidth for different types of network traffic.

QoS classes

The Ethernet Switches 460 and 470 support the following Nortel 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. Shape traffic requiring this service at the network boundary in order to undergo a negligible delay and delay variance. This service class is suitable for real-time applications like 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 in-profile packets (packets that do not break the service agreements between the user and the service provider).

Table 1 describes the service classes and the required treatment.

Table 1 Service classes

Traffic category	Service class	Application type	Required treatment
Critical network control	Critical	Critical network control traffic	Highest priority over all other traffic. Guaranteed minimum bandwidth.
Standard network control	Network	Standard network control traffic	Priority over user traffic. Guaranteed minimum bandwidth.
Real-time, delay-intolerant, fixed bandwidth	Premium	Inter-human 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	Inter-human 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.

Table 1 Service classes (Continued)

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

Packet classifiers or filters

Packet classifiers, or filters, select packets according to a particular content in the packet header, such as the source address, destination address, source port number, destination port number, and others. Packet classifiers identify flows for more processing.

You can create the following two types of filter groups:

- Layer 2 filters
- IP filters

A filter group is an ordered list of filters. Filters can be added to or deleted from an existing group.

Note: Layer 2 and IP filters cannot coexist in the same group.

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

Each group of filters is associated with actions that are executed when the packet matches the filters in the group. The filter group and the associated actions, meters, shaping criteria, and interface groups are referenced by a policy, which dictates the overall traffic treatment.

Filters are associated with an interface group, action, metering, and shaping criteria, through a policy. There are two levels of precedence that both work from the lowest order to the highest:

- order of filters in a filter group
- order of policies

Note: Among policies, any policy with a Layer 2 filter group must have a lower precedence (higher order) than any policy with an IP filter group.

Layer 2 filters

The Layer 2 filters are used to classify traffic based on the following criteria:

- Layer 2 information, including VLAN ID, IEEE 802.1p priority, and etherType
- Layer 3 information, including DSCP and IP protocol such as TCP/UDP
- Layer 4 information, including TCP/UDP port ranges

There are up to 24 global Layer 2 filters available per unit. The number of available Layer 2 filters varies according to the category of interface class you configure.

- If the supported interface class is untrusted (the default value), 24 Layer 2 filters are available.
- If the supported interface class is trusted, 23 Layer 2 filters are available.
- If the supported interface class is unrestricted, 24 Layer 2 filters are available per unit.

For more information, see "Setting up filters and filter groups" on page 62. Refer to "Ports" on page 43 for information on configuring interface classes.

You can filter multiple VLANs with a single Layer 2 filter. You can filter up to 32 VLANs with a single Layer 2 filter.

Note: If a Layer 2 filter specifies Layer 3 or Layer 4 information, that filter must match IP traffic only.

Layer 2 classifiers can be associated with the following actions:

- Drop matching packets.
- Change DSCP of matching IP packets. If you request changing the DSCP for non-IP traffic, the request is ignored.
- Change IEEE 802.1p and drop precedence of matching packets.

If a Layer 2 filter is installed on a trusted port, then it cannot change the DSCP of the matching IP traffic or the IEEE 802.1p for all types of traffic. If a Layer 2 filter is installed on an untrusted port, then the associated action must change the DSCP (if matching IP traffic), IEEE 802.1p, and drop precedence of all matching traffic. If a Layer 2 filter is installed on an unrestricted port, you can specify an action to change or ignore either the DSCP (if matching IP traffic), IEEE 802.1p, and drop precedence of the matching traffic.

Refer to Table 2 on page 43 and Table 3 on page 44 for more information on Layer 2 traffic, either IP or non-IP, and trusted, untrusted, or unrestricted ports.

IP filters

IP filters are used to classify IP traffic based on the following criteria:

- Layer 3 information, including IP source and subnet addresses, IP destination and subnet addresses, DSCP, and IP protocols such as TCP/UDP
- Layer 4 information, including TCP/UDP port numbers (port ranges are not supported by Layer 3 filters)

IP filters have the same actions as Layer 2 filters. If an IP filter is installed on a trusted port, then it cannot change the DSCP of the matching IP traffic or 802.1p user priority. If an IP filter is installed on an untrusted port, then it must change the DSCP, IEEE 802.1p, and drop precedence of the matching IP traffic. If an IP filter is installed on an unrestricted port, you configure that interface to change or not either the DSCP, IEEE 802.1p, and drop precedence of the matching IP traffic, as you want.

Refer to Table 2 on page 43 and Table 3 on page 44 for more information on Layer 2 traffic, either IP or non-IP, and trusted, untrusted, or unrestricted ports.

Changing IEEE 802.1p priority and drop precedence

You can change the IEEE 802.1p priority and drop precedence for IP traffic by using either IP or Layer 2 filters. To change IEEE 802.1p priority and drop precedence for non-IP traffic, you must use Layer 2 filters.

For example, to configure a policy that changes the IEEE 802.1p priority and the drop precedence of traffic belonging to VLAN 100 received on untrusted ports that are associated with a specific role combination (or interface group), you need the following two filters:

- A Layer 2 filter that changes the DSCP, the IEEE 802.1p priority, and the drop precedence of IP traffic in VLAN 100
- A Layer 2 filter that changes the IEEE 802.1p priority and the drop precedence of all types of traffic (both IP and non-IP) in VLAN 100

The Layer 2 filter can match against multiple Layer 3 protocols. Otherwise, numerous Layer 2 filters would be necessary to match against all non-IP traffic. The first filter identifies IP traffic, and the second filter matches everything else for VLAN 100. Because the first filter is installed on an untrusted port, it must change the DSCP, IEEE 802.1p priority, and drop precedence of the matching IP traffic.

For trusted ports, you also need two Layer 2 filters. However, the actions do not re-mark the fields. Layer 2 filters that do not match IP traffic pass the traffic through untouched. With Layer 2 filters that match IP traffic, the hardware matches the fields using mapping tables you configure (or uses the preset default tables, which Nortel recommends).

Refer to Table 2 and Table 3 on page 44 for more information on Layer 2 traffic, either IP or non-IP, and trusted, untrusted, or unrestricted ports.

➡ **Note:** Layer 2 filters should have the same evaluation order (or precedence order) as shown in this example to ensure that IP traffic is treated properly.

Ports

The ports on Ethernet Switches 460 and 470 are classified into three categories: trusted, untrusted, and unrestricted ports. 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.

The classifications of trusted, untrusted, and unrestricted actually apply to *groups* of ports (interface groups). 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. The three classes of interface groups are: trusted, untrusted, and unrestricted. By default, all ports are untrusted.

Table 2 shows the configurations available to the user for each class of interface for IP traffic (including Layer 2 traffic matching IP) and Layer 2, non-IP traffic.

Table 2 Possible user re-marking of QoS fields by class of interface

Type of filter	Action	Trusted	Untrusted	Unrestricted
IP filter or Layer 2 filter matching IP	DSCP	Cannot re-mark	Must re-mark	Re-mark or not
	IEEE 802.1p	Cannot re-mark	Must re-mark	Re-mark or not
	Drop precedence	Cannot re-mark	Must re-mark	Re-mark or not
Layer 2 filter (non-IP)	DSCP	Cannot re-mark	Cannot re-mark	Cannot re-mark

Table 2 Possible user re-marking of QoS fields by class of interface (Continued)

Type of filter	Action	Trusted	Untrusted	Unrestricted
	IEEE 802.1p	Cannot re-mark	• Tagged—Must re-mark • Untagged—Cannot re-mark	Re-mark or not
	Drop precedence	Cannot re-mark	• Tagged—Must re-mark • Untagged—Cannot re-mark	Re-mark or not

Table 3 shows the default guidelines the switch uses to re-mark various fields of IP traffic (and Layer 2 traffic matching IP) based on the class of the interface. These actions occur if the user does not intervene at all; they are the default actions of the switch.

Table 3 Default with no user action re-marking of QoS fields by class of interface—IP only

Type of filter	Action	Trusted	Untrusted	Unrestricted
IP filter or Layer 2 filter matching IP	DSCP	Does not change	• Tagged—Updates to 0 (Standard) • Untagged—Updates using mapping table and port's default value	Does not change
	IEEE 802.1p	Internally updates	• Tagged—Updates to 0 • Untagged—Updates to port's default value	Does not change
	Drop precedence	Internally updates	Updates to high drop precedence	Does not change

Table 4 describes how to select the proper policy settings.

Table 4 Description of proper policy settings

Interface type	Filter type	Update DSCP	Precedence	Priority
Untrusted	IP, or Global IP	0-63	LS, NLS, Default	0-7 Default
Untrusted	Global Non IP-tagged	Ignore	LS, NLS	0-7
Untrusted	Global Non IP-untagged	Ignore	Ignore	Ignore
Trusted	IP, or Global IP	Ignore	Use egress	Use egress

Table 4 Description of proper policy settings (Continued)

Interface type	Filter type	Update DSCP	Precedence	Priority
Trusted	Global Non IP VLAN classified	Ignore	Ignore	Ignore
Unrestricted	IP, or Global IP	0-63	Default	Default
Unrestricted	IP, or Global IP	Ignore	Use egress LS	Use Egress 1-7
Unrestricted	Global Non IP	Ignore	LS Ignore	1-7 Ignore

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

Ethernet Switches 460 and 470 do not trust the DSCP of IP traffic received from an untrusted port, but they trust the DSCP of IP traffic received from a trusted port. Filters installed on trusted ports cannot change the DSCP of the IP packets received on these ports. These filters specify an action that must change the IEEE 802.1p and drop precedence of the matching packets based on the incoming DSCP, using a table that matches each one of the 64 DSCP values to the corresponding IEEE 802.1p priority. The values can be modified by a policy server or by the user.

If a packet is received from a trusted port and either does not match any filters installed on this port or does match a filter but is not dropped, the Ethernet Switches 460 and 470 use a default Layer 2 filter to change the packet IEEE 802.1p and drop precedence based on the DSCP of the packet.

Filters that you install on untrusted ports must specify an action to change the DSCP, IEEE 802.1p priority, and drop precedence of IP traffic received from these ports. For non-IP traffic, the filters must specify an action to update the IEEE 802.1p priority and drop precedence, but not update the DSCP.

If an IP packet is received from an untrusted port, and it does not match any one of the filters installed on the port, the Ethernet Switches 460 and 470 use default Layer 2 filters to change the packet DSCP, IEEE 802.1p priority, and drop precedence as follows:

- If the packet is tagged, the Ethernet Switch uses a Layer 2 filter to change the DSCP, IEEE 802.1p to 0, and drops precedence to 1 so that the packet receives best-effort treatment.
- If an IP packet is untagged, the Ethernet Switch uses 8 default Layer 2 filters to change the DSCP based on the default IEEE 802.1p priority of the ingress untrusted port. The Ethernet Switch changes the packet DSCP using the 802.1p priority mapping table that matches each one of the eight IEEE 802.1p priorities to the corresponding DSCP. The values can be modified by you or a policy server.

The unrestricted ports, or the unrestricted class of interface groups, have no restrictions. That is, you can re-mark the DSCP or not, depending on your configuration. Using unrestricted ports allows you to manipulate the DSCP value based on the filter criteria.

Table 5 describes the default DSCP, QoS class, IEEE 802.1p, and egress queue assignment for packets in each traffic class.

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

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

As displayed in Table 5, 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.

When the power is turned on, all ports are considered untrusted. You can change the power-up defaults using the Web-based management interface. See the *System Configuration Guide* (217105-A).

Note: You must reboot the unit after making any changes to the interface class of a port.

Queue sets

You can change the default IEEE 802.1p to queue mapping and the default DSCP to IEEE 802.1p mapping using the Web-based management interface, SNMP, the CLI, or DM. Note that the IEEE 802.1p to queue mapping for an interface (port) depends on the number of queues available at that interface. This number depends on the queue set associated with the interface.

The cascade port has a set of two queues that are serviced using an absolute priority discipline.

Ethernet Switch 460 and 470 ports are associated with three types of queue sets:

- Queue set 1 has four queues. The first queue is serviced in an absolute priority fashion. The other three queues are serviced in a WRR fashion.
- Queue set 2 has two queues that are serviced in an absolute priority fashion.
- Queue set 3 has eight queues. The first queue is serviced in an absolute priority fashion. The other seven queues are serviced in a WRR fashion.

Three sets of external ports correspond to the queue sets. The first set of external ports contains the 10/100 Mb/s ports; these interfaces are associated with queue set 1. Each port in this set has a set of 4 queues. The first queue holds the highest priority and is serviced in an absolute priority fashion, meaning that this queue is serviced first until all the queued packets are transmitted. The other three queues are serviced using a WRR scheduler.

The second set of external ports contains the cascade ports; these interfaces are associated with queue set 2, which has 2 queues that are serviced in an absolute priority fashion.

The third set of external ports contains the GBIC ports; these interfaces are associated with queue set 3. Each port in this set has a set of eight queues. The first queue holds the highest priority and is serviced in an absolute priority fashion, meaning that this queue is serviced first until all the queued packets are transmitted. The other seven queues are serviced using a WRR scheduler.

You cannot change the characteristics of these queue sets (such as the service discipline, packet or buffer thresholds, and queue weights for WRR scheduler).

Interface groups

Assign every port to an interface group. The interface group is used to apply policies to traffic received by a port. Each port can belong to only *one* interface group. The Web-based interface for Advanced QoS uses the term “Interface Configurations” for this function. One policy references only one interface group, but you can configure several policies to reference the same interface group.

All ports that have the same interface group (role combination) have the same set of filters installed on them. When you move a port to another interface group (role combination), the filters associated with the previous interface group are removed, and the filters associated with the new interface group are installed on the port.

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

When the power is turned on, ports are assigned to the default interface group (role combination), which is named allBPSIfcs. When you create a filter, you must create or specify an interface group. Ports that are not assigned to an interface group and are detected on initialization are assigned to the default interface group named allBPSIfcs.

Note: You must remove all ports from an interface group in order to delete it.You cannot delete an interface group that is referenced by a policy.

Metering overview

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.

You no longer need to configure a meter if you are not metering data.

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

Note: The maximum committed rate that can be specified is limited to 8500 Kb/s. Requests for a committed rate greater than this limit are rejected.

An example of traffic policing is limiting traffic entering a port to a specified bandwidth, such as 25 Kb/s (Committed Rate). Instead of dropping all traffic that exceeds this threshold, you can configure a Maximum Burst Rate 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.

Note: Meter definitions where the committed burst size is too small based on the requested committed rate are rejected. (The determination of "too small" is made by multiplying the committed rate by the token fill interval. If the fill rate in bytes exceeds the maximum committed burst size (token bucket size), the request is rejected.) The committed burst size can only be one of the following discrete values (in bytes): 2047, 4095, 8191, 16383, 32767, 65535 or 131071.

You can also configure policies without metering. In this case, using the Web-based management system, you choose No Meter Data in the Data Specification field of the Meter page. Refer to Chapter 4, "Implementing QoS Using QoS Wizard and QoS Quick Config," on page 187 and Chapter 5, "Implementing QoS using QoS Advanced," on page 233 for more information on how to use the Web-based management system to configure QoS parameters on the Ethernet Switches 460 and 470.

Shaping overview

Shaping, or traffic shaping, which operates at egress, smooths the traffic on the uplink connection to the network core to provide efficient bandwidth utilization. Shaping is available only on the GBIC ports.

Note: You must install the Ethernet Switch 470-24T GBIC in order to use shaping.

You can shape the traffic to fit the profile specified in the Service Level Agreement (SLA). Shaping specifies the maximum rate at which traffic is transmitted over a given time. Traffic is allowed to exceed this rate in short bursts. You specify a burst size to indicate the maximum burst size of traffic allowed to egress without a shaping delay.

Traffic that is being shaped can be buffered temporarily to conform to the specified flows. You can choose whether 1, 2, 4, 8, or 16 packets can be held in the shaping queue. Some packets can be dropped if buffers are completely used.

Traffic flows can be metered and shaped, or only shaped (or only metered). Shaped packets lose the loss-sensitivity property.

Shaping is accomplished using QoS Policies (refer to "Policy overview" on page 52 for more information on Policies). Shaping is applied to a traffic flow by configuring a Policy to reference that particular Shaper. When you delete a Policy, the shaping on that Policy is also deleted. You can also configure aggregate shaping, which is shaping a group of policies as a single policy.

As with Meters and Policies, Shapers and Policies work together. First, you configure a Shaper. When you configure a policy, you reference a particular Shaper. Additionally, the system assigns each Policy a unique Shaping Group value, from 2 to 63, if you do not assign that Policy a specific Shaping Group value. Thus, the Shaping Group value for the Policy is user-configurable; otherwise, the system assigns the value.

Once you configure one Policy with a Shaping Group, you can configure additional Policies that reference existing Shaping Group numbers—this is aggregate shaping. All Policies with the same Shaping Group number are shaped at egress as if they were a single Policy.

To define shaping criteria, you set a Shaping Rate in Kbps (1000 bits per second in each Kb/s) and a Shaping Burst Rate that specifies an allowed data burst larger than the Shaping Rate for a brief period. After you specify the Shaping Burst Rate, you choose among up to six possible Shaping Burst Rate Durations. Finally, you set the shaping queue size, which is used to configure the size of the shaping queue.

Note: You must enter a multiple of 64 Kbps as the shaping rate.

An example of rate shaping is limiting traffic egressing a port to a specified transmission rate, such as 64 Kbps (Shaping Rate). Instead of dropping all traffic that exceeds this threshold, you can configure a Shaping Burst Size that allows the switch to exceed the designated Shaping Rate for a brief period without delaying the traffic. Traffic that exceeds the threshold (Shaping Rate) for longer periods is delayed. This combination of actions shapes the traffic to conform to the designated maximum transmission rate. The switch temporarily buffers the delayed traffic. You choose the number of packets you want buffered when you configure the Queue Size. If traffic is received at a rate greater than it can be transmitted, based on the configured maximum transmission rate, for an extended period, the switch buffering resources are exhausted, and that traffic is dropped.

You can shape only those traffic flows that have an IEEE 802.1p value that is known at egress. Table 6 shows the type of traffic that can be shaped on trusted, untrusted, and unrestricted interface classes.

Table 6 Shaping possibilities by class of interface

Action	Trusted	Untrusted	Unrestricted
Shaping	Traffic flow must be IP or Layer 2 packets (matching IP) with a specific DSCP value **Note:** If a filter group has multiple filters, all filters must match the identical DSCP value.	Yes	• Traffic flow must be associated with policies that have actions that update the 802.1p value at egress. • Traffic flow must be IP or Layer 2 packets (matching IP) with a specific DSCP value plus a specified action of “useEgressMap.” **Note:** If a filter group has multiple filters, all filters must match the identical DSCP value

For more information, see “Configuring shapers” on page 79.

Policy overview

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 the device.

Among policies, the policy with the lowest order (and highest precedence) is evaluated first, then the policy with the next-lowest order, and so on. For example, with an order of 1 to 20, the system begins the evaluation with 1, moves onto 2, and so forth. This is important to remember when you configure policies.

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
- Shapers
- Filter groups
- Interface groups

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

Ports are assigned to interface groups that are linked to policies. 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.

You can enable or disable policies; you do not have to delete a policy to disable it. However, you must still delete a policy to modify it. For more information, see “Configuring policies” on page 81.

Packet flow using QoS

Using DiffServ and QoS, you can designate a specific performance level for packets. This system allows you to prioritize network traffic. You can specify a number of policies, and each policy can match one or many flows—supporting complex classification scenarios.

This section contains an 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 Premium, Platinum, Gold, Silver, Bronze, and Standard. The level of service for each packet is determined by the configurable DSCP.

Filters and filter groups basically sort the packets by various configurable parameters. These parameters include VLAN IDs, IP source and subnet address, IP protocol, and many others.

The filter groups are associated with policies, and policies are organized into a hierarchy. The policy with the highest precedence is evaluated first. The filters and filter groups are associated with interface groups, in that packets from a specific port have the same filters as all others in the particular interface group (role combination).

Meters, operating at ingress, keep the sorted packets within certain parameters. You configure a committed rate of traffic, 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.

Shaping specifies a maximum transmission rate over a given period, as well as a burst size that allows a traffic flow to briefly exceed the shaping rate. You can also specify, within a specified range, the number of packets that can be held prior to transmission until the necessary bandwidth is available at egress. Some packets are dropped if buffers are completely used. If you choose not to shape the flow, you do not configure shapers.

Actions determine how the traffic is treated.

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

Default QoS settings

The Ethernet Switches 460 and 470 are shipped with limited default QoS information. Defaults include a default interface group, default user priority-to-queue mappings for each queue set, and default DSCP-to-user priority mappings.

QoS configuration guidelines

You can install filters that act on traffic destined for the switch itself, such as ICMP Echo Requests (ping) and SNMP messages. If the associated action is to drop the traffic, you can lock yourself out of the switch.

However, traffic destined for the switch and received through a port on the base unit of a stack is not dropped even if filters targeting the traffic are installed and drop has been specified. This behavior prevents you from completely isolating yourself from the switch. Consider this behavior when you configure filters and when you allocate ports for the purposes of configuring or monitoring the switch.

COPS overview

Common Open Policy Services (COPS) is important as a stateful protocol between a policy server and a network device such as the Ethernet Switches 460 and 470. COPS is implemented by using the Optivity Policy Services* (OPS), Version 1.2 or later, which is a comprehensive network management application. OPS provides a centralized management point for DiffServ policies. The policy server distributes policies to edge devices and border routers. These edge devices police traffic flows by marking packets and applying forwarding behaviors to the packets at the network node.

Information is transferred using the Common Open Policy Services (COPS) protocol, a query and response protocol that exchanges policy information messages using the Transmission Control Protocol (TCP). COPS ensures redundancy for devices to contact an alternate policy server if the primary server fails. Specifically, COPS for Provisioning (COPS-PR) is used to download information.

COPS is used to communicate with edge devices on the network. Some of the benefits of the COPS protocol are:

- It uses a client/server model for communication between the policy server and the policy clients.
- It uses TCP for messaging, reducing the resources it requires.
- The policy server can send configuration information to the policy client, as well as remove unneeded configuration information.

For information about OPS, and specific Ethernet Switch implementation notes, go to www.nortel.com/support. Then locate the specific software product (in this case, Optivity Policy Services).

Sample QoS configuration

You can configure QoS using the Common Open Policy Services (COPS), the CLI, the Web-based management system, SNMP, or Device Manager. This section presents a sample QoS configuration using the Web-based management system using the QoS Advanced pages.

For more information on configuring QoS with the Web-based management system, see Chapter 4, “Implementing QoS Using QoS Wizard and QoS Quick Config,” on page 187 and Chapter 5, “Implementing QoS using QoS Advanced,” on page 233.

You can configure QoS using the embedded Web-based QoS Wizard in the Web-based management system. The QoS Wizard allows you to configure simplified policies and common filters, in order to control the behavior of network traffic in your stand-alone or stack switch configuration. In addition, you can prioritize a VLAN to receive better service than others.

⚠ **Warning:** Nortel recommends that you use the QoS Wizard for your *initial* configuration only. Each time the QoS Wizard is initiated, all existing configurations are reset to the default values. After you complete the *initial* QoS Wizard configuration method, you can customize traffic treatment using the QoS Quick Config or QoS Advanced configuration process.

With Release 3.0 software and higher, you can configure QoS parameters using the QoS Quick Config Web pages. QoS Quick Config allows you to configure multiple QoS components using only two Web pages. Although QoS Quick config does not provide the full range of options as the QoS Advanced Pages, Quick Config is suitable for many QoS applications.

Ensure that you refer to the *System Configuration Guide* (217105-A) for details to access the Web-based management interface, directory and page navigation information, and field descriptions.

➡ **Note:** Nortel recommends that you configure filter and interface parameters in the order in which the screens are presented in this example.

This section provides a sample configuration using the Web-based management interface QoS > QoS Advanced Web pages. You must define filters before you define filter groups, and you must define actions before you define the meters. The policy must be defined last, after the other parameters are configured. This section covers the following topics, using the QoS Advanced Web pages:

- "Creating interface groups" on page 58
- "Accepting default mapping values" on page 62
- "Setting up filters and filter groups" on page 62
- "Configuring actions" on page 75

- "Configuring meters" on page 77
- "Configuring shapers" on page 79
- "Configuring policies" on page 81
- "Assigning mapping values" on page 85

➡ **Note:** You cannot modify many configured items, including interfaces, interface groups, filters, filter groups, actions, meters, and shapers. You must first delete the current item and then enter a new one with the modifications.

Creating interface groups

To create an interface group:

1 In the Web-based management interface, click the Application > QoS > QoS Advanced menu option.

The QoS Advanced menu option expands to display:

- Devices
- Rules
- Actions
- Meters
- Shapers
- Policies
- Agent

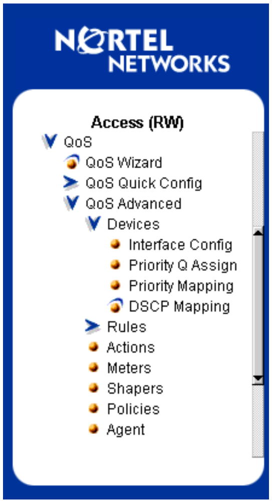
2 Click Devices.

The Devices menu option expands (Figure 2 on page 59) to display:

- Interface Config
- Priority Q Assign
- Priority Mapping
- DSCP Q Assign

- DSCP Mapping

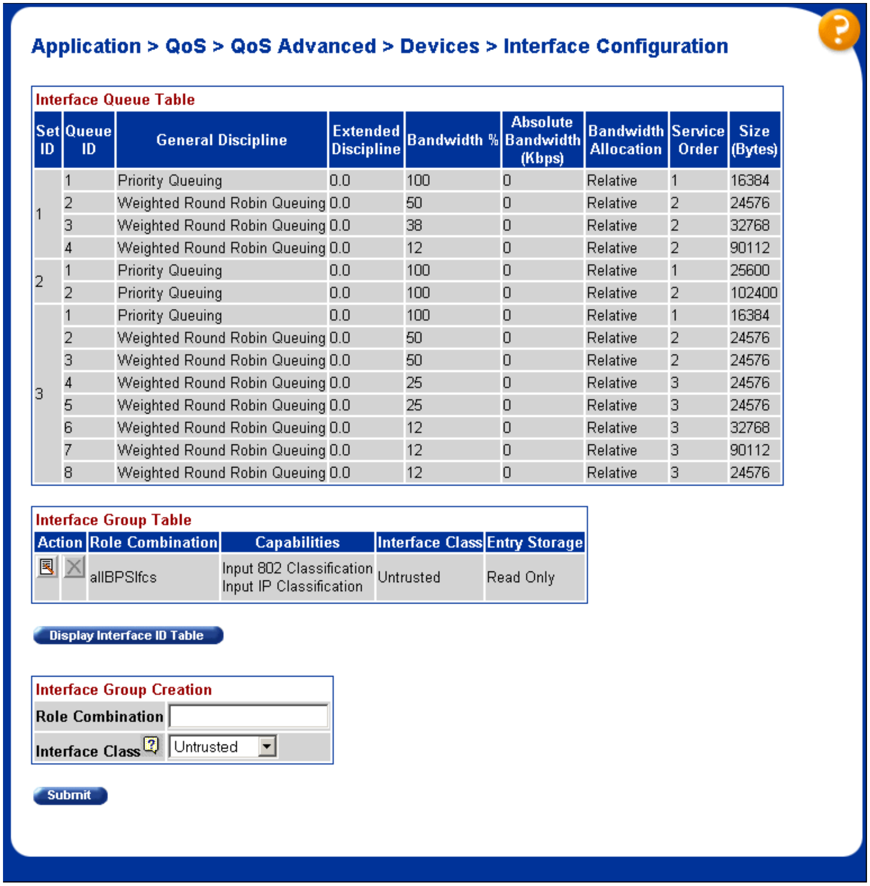
Figure 2 Web-based management menu page



3 Click Interface Config.

The Interface Configuration page opens (Figure 3).

Figure 3 Interface Configuration page



Application > QoS > QoS Advanced > Devices > Interface Configuration

Interface Queue Table

Set ID	Queue ID	General Discipline	Extended Discipline	Bandwidth %	Absolute Bandwidth (Kbps)	Bandwidth Allocation	Service Order	Size (Bytes)
1	1	Priority Queuing	0.0	100	0	Relative	1	16384
	2	Weighted Round Robin Queuing	0.0	50	0	Relative	2	24576
	3	Weighted Round Robin Queuing	0.0	38	0	Relative	2	32768
	4	Weighted Round Robin Queuing	0.0	12	0	Relative	2	90112
2	1	Priority Queuing	0.0	100	0	Relative	1	25600
	2	Priority Queuing	0.0	100	0	Relative	2	102400
3	1	Priority Queuing	0.0	100	0	Relative	1	16384
	2	Weighted Round Robin Queuing	0.0	50	0	Relative	2	24576
	3	Weighted Round Robin Queuing	0.0	50	0	Relative	2	24576
	4	Weighted Round Robin Queuing	0.0	25	0	Relative	3	24576
	5	Weighted Round Robin Queuing	0.0	25	0	Relative	3	24576
	6	Weighted Round Robin Queuing	0.0	12	0	Relative	3	32768
	7	Weighted Round Robin Queuing	0.0	12	0	Relative	3	90112
	8	Weighted Round Robin Queuing	0.0	12	0	Relative	3	24576

Interface Group Table

Action		Role Combination	Capabilities	Interface Class	Entry Storage
✎	✕	allBPSIfcs	Input 802 Classification Input IP Classification	Untrusted	Read Only

Interface Group Creation

Role Combination	
Interface Class ?	Untrusted ▼

The Interface Group Creation section of this page allows you to define groups of interfaces. You can view your interface configurations in the read-only Interface Queue Table and the Interface Group Table.

4 Use the Interface Group Creation section to create a new Role Combination. In the Role Combination field, enter `Webbrowsing`. (Because this is an example, you can enter any string in this field.)

➡ **Note:** Do not use spaces in the naming field.

5 In the Interface Class field, choose `untrusted`.

By selecting untrusted, incoming DSCP values are changed.

By using system defaults or manual configurations, you can configure whether the DSCP value is changed.

Note: Nortel recommends that you use the default configurations. By choosing “Use Defaults” in the Set Drop Precedence and Update Priority fields in the QoS Advanced > Action page, the DSCP value is used to update IEEE 802.1p user priority and drop precedence based on values in the DSCP mapping table.

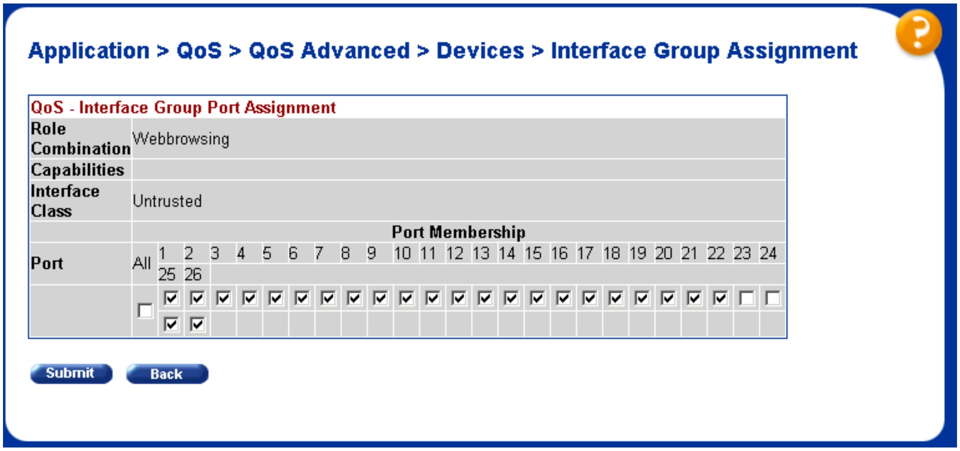
6 Click Submit.

The new entry appears in the Interface Group Table.

7 Click the modify icon of the new role combination to assign interfaces.

The Interface Group Assignment page opens (Figure 4).

Figure 4 Interface Group Assignment page



Application > QoS > QoS Advanced > Devices > Interface Group Assignment
Submit
Back

QoS - Interface Group Port Assignment

Role Combination	Webbrowsing
Capabilities	
Interface Class	Untrusted

Port Membership

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																						
	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☐
		☑	☑																						

The Interface Group Assignment page displays the name of the interface group (role combination), the capabilities, and the interface class (or type of interface) in the group.

a Click the ports you want to add to the specified interface group, or click All to add all ports on the unit.

b Click Submit.

Note: If you delete a role combination, you must remove all ports in the Interface Group Assignment page first. A role combination cannot be deleted if it is referenced by an installed meter.

Accepting default mapping values

If you choose to accept the default values for IEEE 802.1p priority and DSCP values, skip this section and go to "Setting up filters and filter groups".

Note: Nortel recommends that you use the default mapping values to ensure end-to-end QoS connectivity across Nortel Network products.

To manually configure mapping values, refer to "Assigning mapping values" on page 85.

Setting up filters and filter groups

Filters allow you to classify packets by various parameters. Filters are combined into filter groups. Filter groups are then associated with an interface group.

You configure filter specifications. The QoS Advanced > Rules > IP Classification page or the QoS Advanced > Rules > Layer 2 Classification page allows you to enter matching conditions for an individual filter. You set up special conditions for packet processing. In order to process packets, a packet must match all the fields you specify.

➡ **Note:** When you choose the value Ignore, the system matches all fields for that parameter.

Defining an IP filter

You can create IP filters for IP packets that are to be forwarded through the Ethernet Switch 460 or 470 on specific ingress ports. In each IP packet, there is a differentiated services (DiffServ) field in the packet header that you can mark for specific treatment. This field is called the DiffServ code point (DSCP). The DSCP has a specific value that determines how the packet is treated as it travels through the network. As each packet is examined, it is forwarded or dropped, depending on whether the filter criteria is matched.

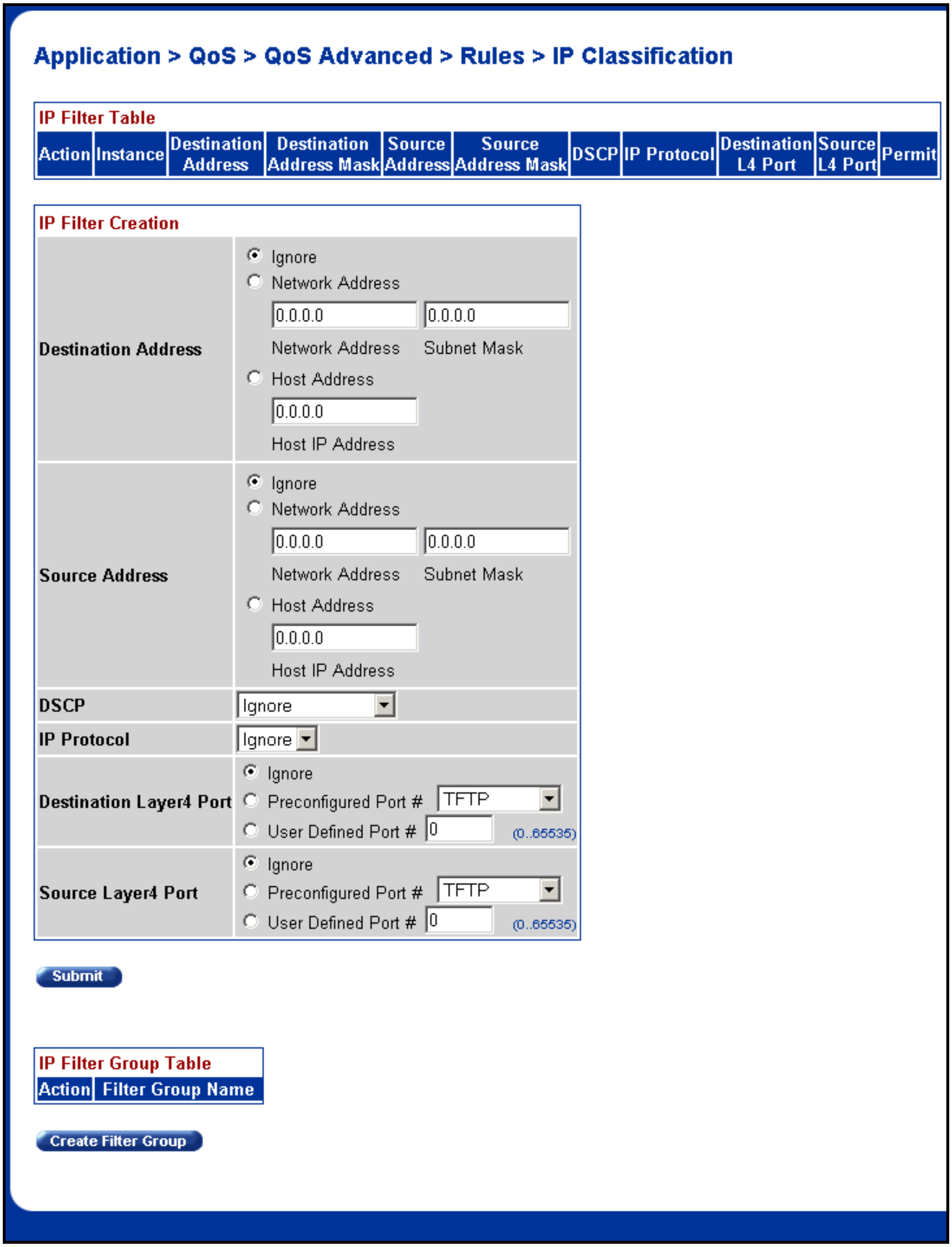
You can use the IP Filter Creation section of the Rules > IP Classification page when defining your IP filters.

To define an IP filter:

1 Click the Application > QoS > QoS Advanced > Rules > IP Classification menu option.

The IP Classification page opens (Figure 5 on page 64).

Figure 5 IP Classification page



Application > QoS > QoS Advanced > Rules > IP Classification

IP Filter Table

Action	Instance	Destination Address	Destination Address Mask	Source Address	Source Address Mask	DSCP	IP Protocol	Destination L4 Port	Source L4 Port	Permit

IP Filter Creation

Destination Address	● Ignore ○ Network Address 0.0.0.0 0.0.0.0 Network Address Subnet Mask ○ Host Address 0.0.0.0 Host IP Address
Source Address	● Ignore ○ Network Address 0.0.0.0 0.0.0.0 Network Address Subnet Mask ○ Host Address 0.0.0.0 Host IP Address
DSCP	Ignore
IP Protocol	Ignore
Destination Layer4 Port	● Ignore ○ Preconfigured Port # TFTP ○ User Defined Port # 0 (0..65535)
Source Layer4 Port	● Ignore ○ Preconfigured Port # TFTP ○ User Defined Port # 0 (0..65535)

IP Filter Group Table

Action	Filter Group Name

2 In the Destination Address box, click **`Network Address`**.

a In the Network Address field, enter **`134.177.69.0.`**

This address is used to match the destination IP address in the packet IP header.

b In the Subnet Mask field, enter **`255.255.255.0`**.

3 In the Source Address box, click **`Network Address`**.

a In the Network Address field, enter **`134.177.0.0`**.

This is the IP address to match against the packet source IP address.

b In the Subnet Mask field, enter **`255.255.0.0`**.

4 In the DSCP field, choose **`0x20`** from the list.

This value matches packets with a DSCP of 0x20 (32 decimal value).

If you choose Ignore, the DSCP value in the packet is ignored.

5 In the Protocol field, choose **`TCP`** from the list.

When you select TCP, you must specify that only TCP packets can be matched. If you select Ignore, all IP protocols are matched.

6 In the Destination Layer 4 Port field, click **`Ignore`**.

7 In the Source Layer 4 Port field, click **`Ignore`**.

8 Click Submit.

The new entry appears in the IP Filter Table.

Creating an IP Filter Group Table entry

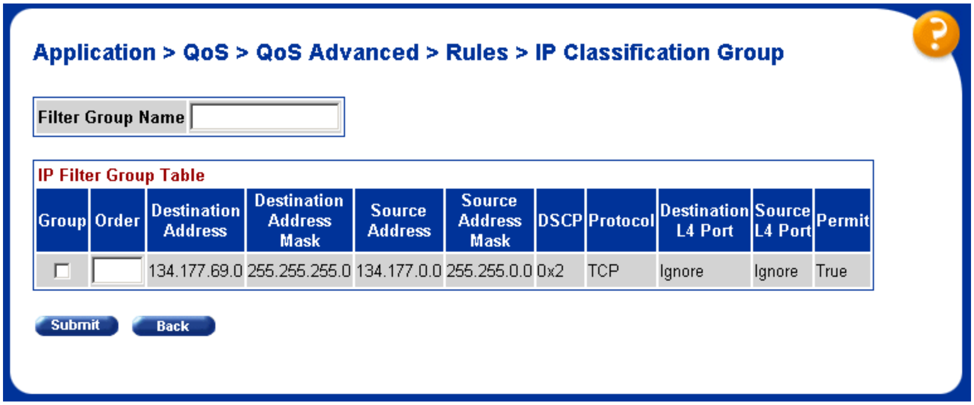
Now you can create an IP filter group in the IP Filter Group Table section of the IP Classification page.

To create an IP filter group entry:

1 Click Create Filter Group in the IP Filter Group Table section of the IP Classification page.

The IP Classification Group page opens (Figure 6).

Figure 6 IP Classification Group page



Application > QoS > QoS Advanced > Rules > IP Classification Group

Filter Group Name

IP Filter Group Table

Group	Order	Destination Address	Destination Address Mask	Source Address	Source Address Mask	DSCP	Protocol	Destination L4 Port	Source L4 Port	Permit
□		134.177.69.0	255.255.255.0	134.177.0.0	255.255.0.0	0x2	TCP	Ignore	Ignore	True

2 In the Filter Group Name field, enter **IPacket**.

This unique identification label distinguishes this filter group from other filter groups.

Note: Do not leave spaces in your naming entry.

3 Click the Group check box in the Filter Group Table to include the entry in the filter group.

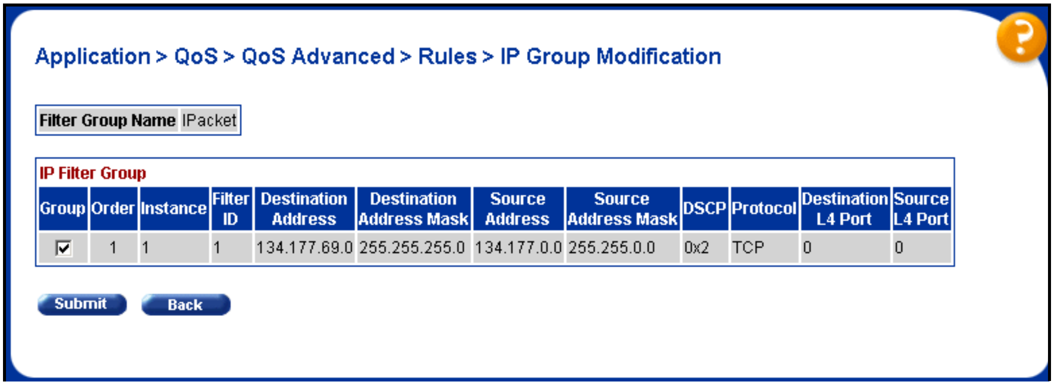
4 Enter the Order number **1**.

This step establishes the evaluation order of filters in the group.

5 Click Submit.

The new entry is displayed on the IP Group Modification page (Figure 7).

Figure 7 IP Group Modification page



Application > QoS > QoS Advanced > Rules > IP Group Modification

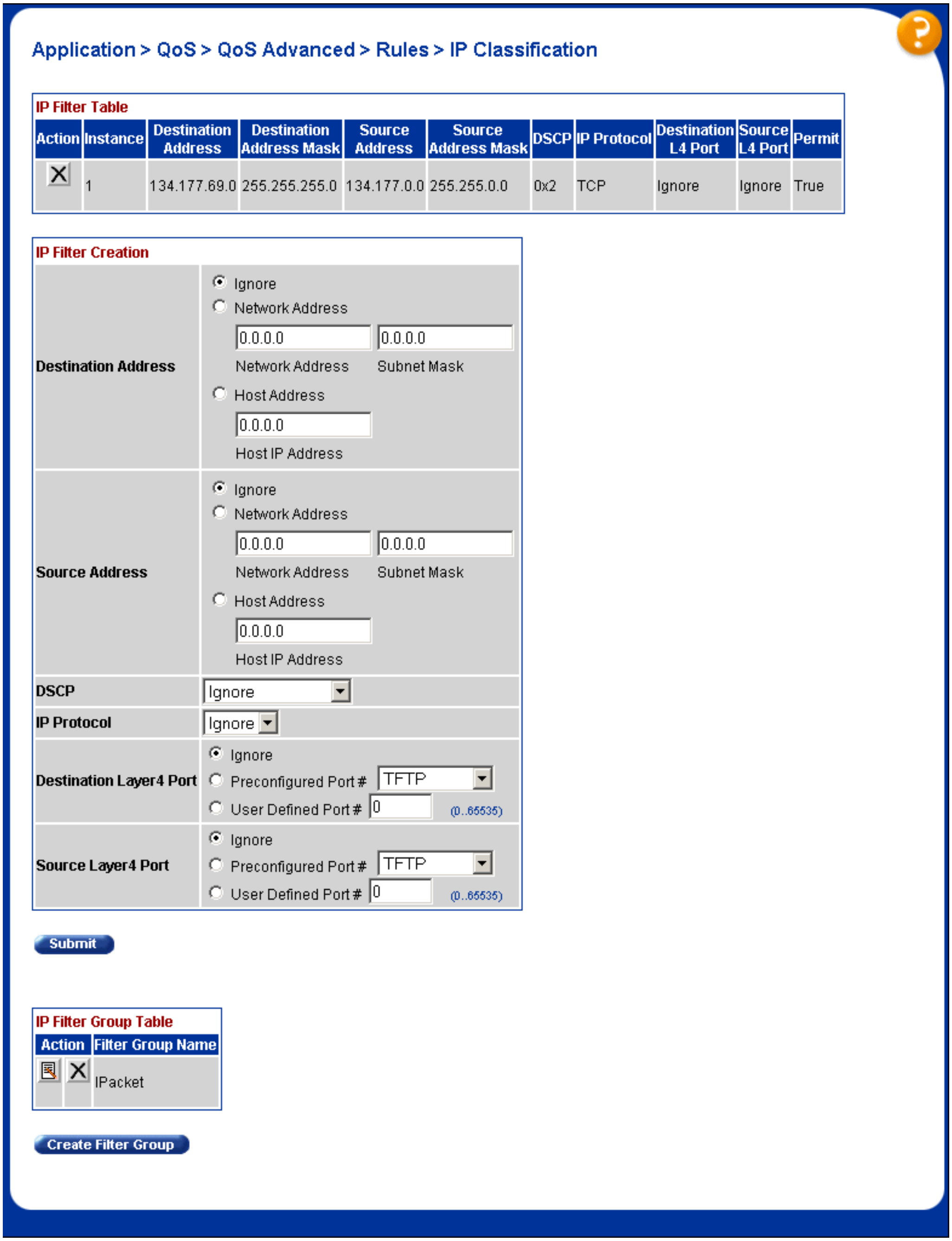
Filter Group Name	IPacket

IP Filter Group

Group	Order	Instance	Filter ID	Destination Address	Destination Address Mask	Source Address	Source Address Mask	DSCP	Protocol	Destination L4 Port	Source L4 Port
☑	1	1	1	134.177.69.0	255.255.255.0	134.177.0.0	255.255.0.0	0x2	TCP	0	0

The system returns you to the IP Classification page. The new filter appears in the IP Filter Table, and the new filter group appears in the IP Filter Group Table (Figure 8 on page 68).

Figure 8 IP Classification page



Application > QoS > QoS Advanced > Rules > IP Classification

IP Filter Table

Action	Instance	Destination Address	Destination Address Mask	Source Address	Source Address Mask	DSCP	IP Protocol	Destination L4 Port	Source L4 Port	Permit
☒	1	134.177.69.0	255.255.255.0	134.177.0.0	255.255.0.0	0x2	TCP	Ignore	Ignore	True

IP Filter Creation

Destination Address	● Ignore ○ Network Address 0.0.0.0 Network Address, 0.0.0.0 Subnet Mask ○ Host Address 0.0.0.0 Host IP Address
Source Address	● Ignore ○ Network Address 0.0.0.0 Network Address, 0.0.0.0 Subnet Mask ○ Host Address 0.0.0.0 Host IP Address
DSCP	Ignore
IP Protocol	Ignore
Destination Layer4 Port	● Ignore ○ Preconfigured Port # TFTP ○ User Defined Port # 0 (0..65535)
Source Layer4 Port	● Ignore ○ Preconfigured Port # TFTP ○ User Defined Port # 0 (0..65535)

IP Filter Group Table

Action	Filter Group Name
☒	IPacket

Layer 2 restricted filters

The Layer 2 restricted filters feature allows you to configure up to 23 metered policies. Release 3.6 software supports both restricted and unrestricted meters.

Defining a Layer 2 filter

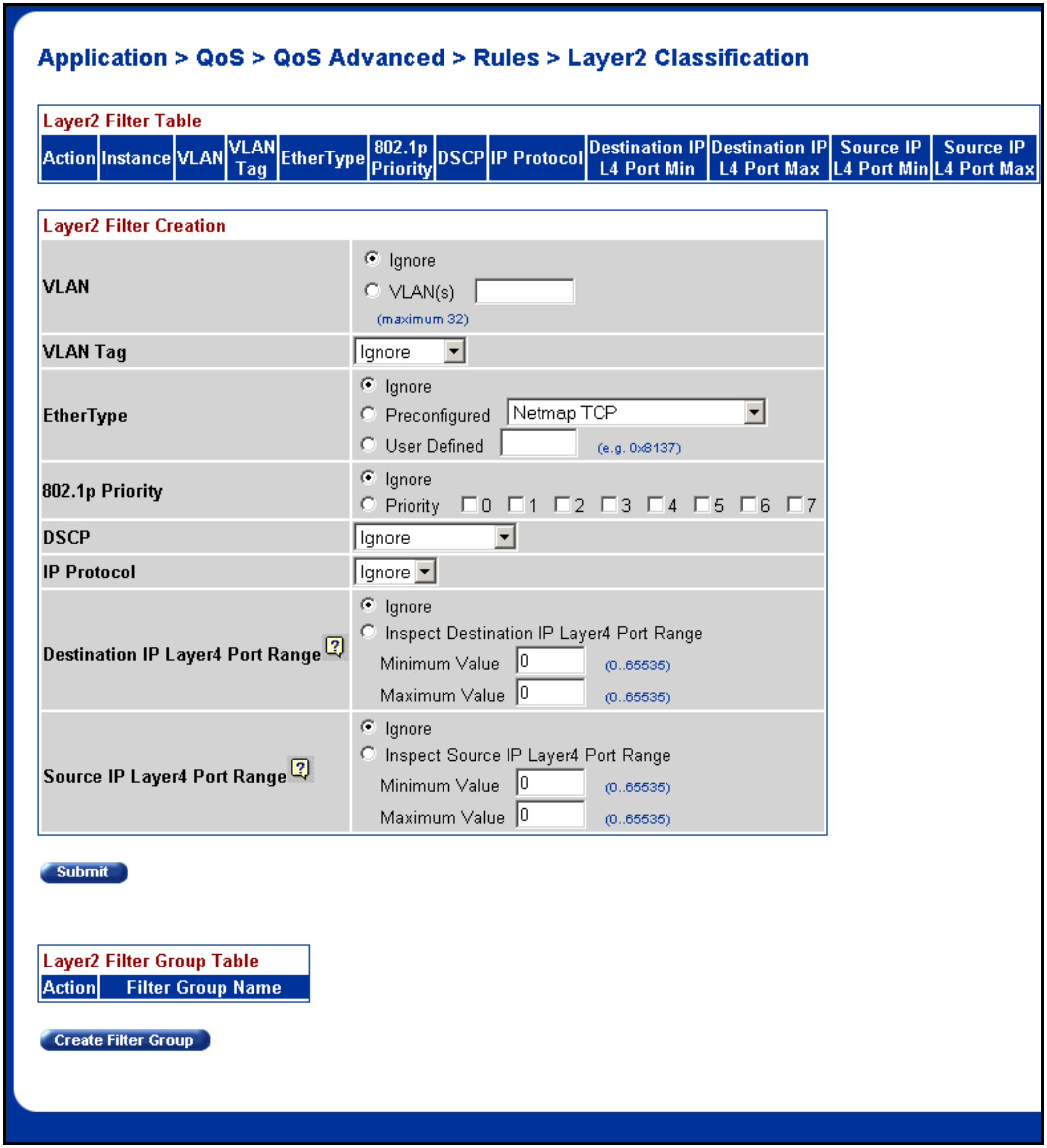
You can configure Layer 2 filters by defining IEEE 802-based parameters and selective Layer 3 and Layer 4 parameters. To define Layer 2 filter groups, specify the Layer 2 filter to be included in the given filter group.

To configure a Layer 2 filter:

1 Click the Application > QoS > QoS Advanced > Rules > Layer 2 Classification menu option.

The Layer2 Classification page opens. (Figure 9).

Figure 9 Layer 2 Classification page



Application > QoS > QoS Advanced > Rules > Layer2 Classification

Layer2 Filter Table

Action	Instance	VLAN	VLAN Tag	EtherType	802.1p Priority	DSCP	IP Protocol	Destination IP L4 Port Min	Destination IP L4 Port Max	Source IP L4 Port Min	Source IP L4 Port Max

Layer2 Filter Creation

VLAN	● Ignore ○ VLAN(s) (maximum 32)
VLAN Tag	Ignore
EtherType	● Ignore ○ Preconfigured Netmap TCP ○ User Defined (e.g. 0x8137)
802.1p Priority	● Ignore ○ Priority □ 0 □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7
DSCP	Ignore
IP Protocol	Ignore
Destination IP Layer4 Port Range	● Ignore ○ Inspect Destination IP Layer4 Port Range Minimum Value 0 (0..65535) Maximum Value 0 (0..65535)
Source IP Layer4 Port Range	● Ignore ○ Inspect Source IP Layer4 Port Range Minimum Value 0 (0..65535) Maximum Value 0 (0..65535)

Layer2 Filter Group Table

Action	Filter Group Name

2 In the VLAN field, click **VLAN** and choose **VLAN # 1**.

This filter matches packets in VLAN 1.

3 In the VLAN Tag field, choose **`Tagged`**.

Only packets with an IEEE 802.1p tag match this Layer 2 filter.

4 In the EtherType field, click **`Ignore`**.

All EtherTypes are ignored.

5 In the 802.1p Priority field, click **`Priority`** and **`0, 1, 2`**.

Only packets with IEEE 802.1p user priority 0, 1, 2 match this filter.

6 In the DSCP field, accept the default **`Ignore`**.

Any values in the DSCP field are ignored.

7 In the Protocol field, select **`Ignore`**.

All IP protocols are matched against the packet IP protocol field.

8 In the Destination IP Layer4 Port Range field, click **`Ignore`**.

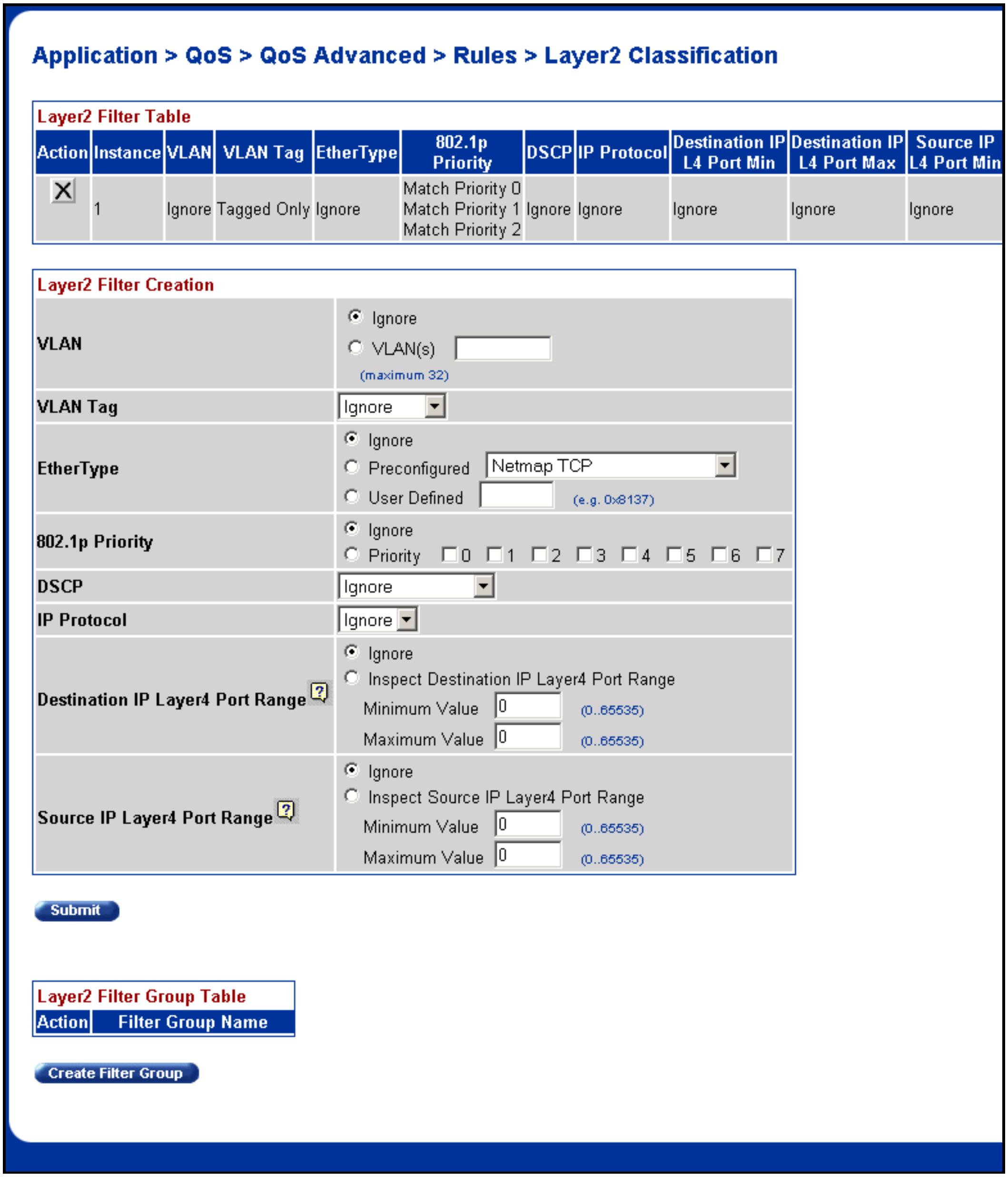
9 In the Source IP Layer4 Port Range field, click **`Ignore`**.

Any values for the packet Layer 4 source port are ignored.

10 Click Submit.

The new entry is displayed in the Layer2 Filter Table (Figure 10 on page 72).

Figure 10 Layer 2 Classification page with new entry



Application > QoS > QoS Advanced > Rules > Layer2 Classification

Layer2 Filter Table

Action	Instance	VLAN	VLAN Tag	EtherType	802.1p Priority	DSCP	IP Protocol	Destination IP L4 Port Min	Destination IP L4 Port Max	Source IP L4 Port Min
☒	1	Ignore	Tagged Only	Ignore	Match Priority 0 Match Priority 1 Match Priority 2	Ignore	Ignore	Ignore	Ignore	Ignore

Layer2 Filter Creation

VLAN	● Ignore ○ VLAN(s) [ ] (maximum 32)
VLAN Tag	Ignore ▾
EtherType	● Ignore ○ Preconfigured Netmap TCP ▾ ○ User Defined [ ] (e.g. 0x8137)
802.1p Priority	● Ignore ○ Priority □0 □1 □2 □3 □4 □5 □6 □7
DSCP	Ignore ▾
IP Protocol	Ignore ▾
Destination IP Layer4 Port Range ?	● Ignore ○ Inspect Destination IP Layer4 Port Range Minimum Value 0 (0..65535) Maximum Value 0 (0..65535)
Source IP Layer4 Port Range ?	● Ignore ○ Inspect Source IP Layer4 Port Range Minimum Value 0 (0..65535) Maximum Value 0 (0..65535)

Layer2 Filter Group Table

Action	Filter Group Name

Creating a Layer2 Filter Group Table entry

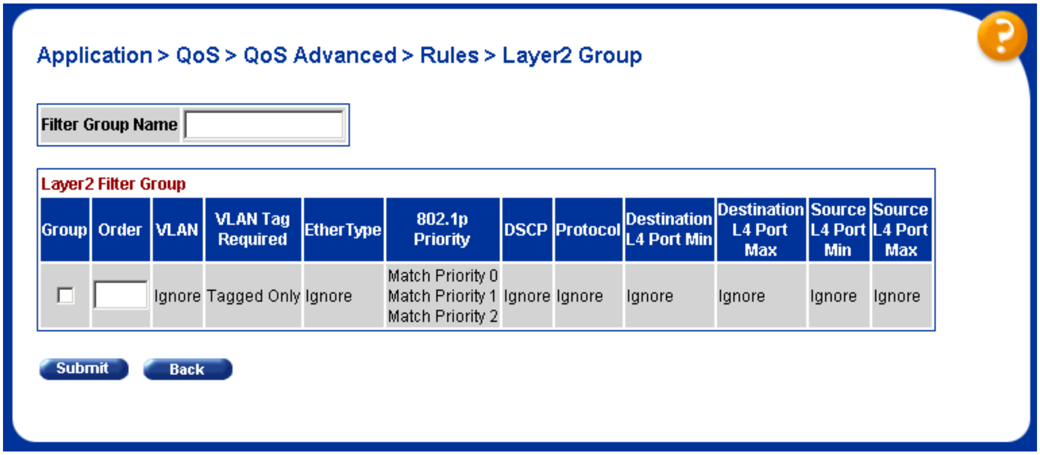
Now you can create a Layer 2 filter group in the Layer2 Filter Group Table section of the Layer2 Classification page.

To create a Layer 2 filter group entry:

1 Click Create Filter Group in the Layer2 Filter Group Table section of the Layer 2 Classification page (Figure 9 on page 70).

The Layer2 Group page opens (Figure 11).

Figure 11 Layer2 Group page



Filter Group Name

Layer2 Filter Group

Group	Order	VLAN	VLAN Tag Required	EtherType	802.1p Priority	DSCP	Protocol	Destination L4 Port Min	Destination L4 Port Max	Source L4 Port Min	Source L4 Port Max
☐		Ignore	Tagged Only	Ignore	Match Priority 0 Match Priority 1 Match Priority 2	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore

2 In the Filter Group Name field, enter `layer2filter`.

This entry is a unique identification label to distinguish this filter group from other filter groups.

Note: Do not leave spaces in your naming entry.

3 Click the Group check box in the Filter Group Table to include the entry in the filter group.

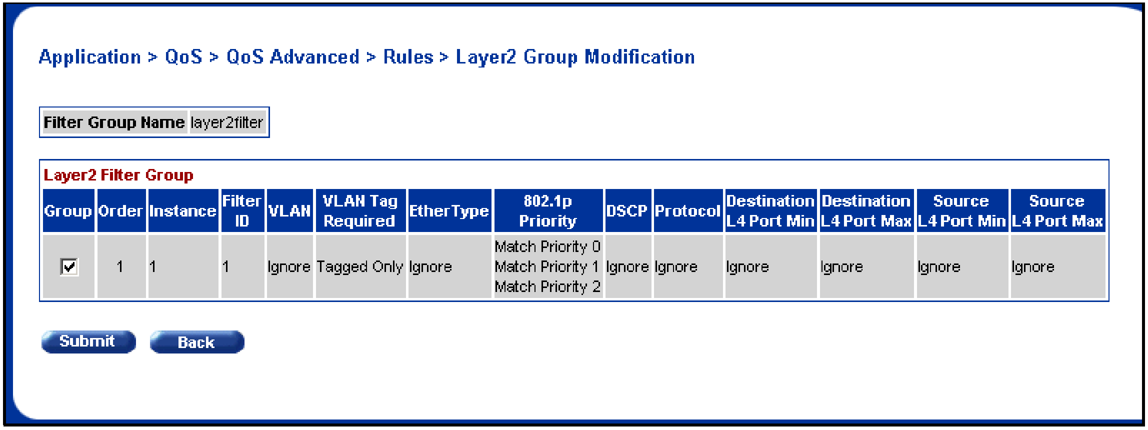
4 Enter the Order number `1`.

This entry establishes the evaluation order of filters in the group.

5 Click Submit.

The new entry is displayed on the Layer 2 Group Modification page (Figure 12).

Figure 12 Layer 2 Group Modification page



Application > QoS > QoS Advanced > Rules > Layer2 Group Modification

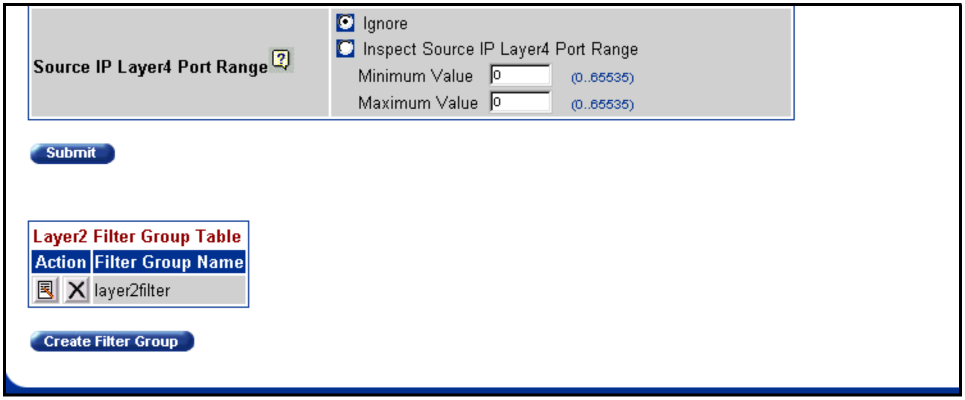
Filter Group Name	layer2filter

Layer2 Filter Group

Group	Order	Instance	Filter ID	VLAN	VLAN Tag Required	EtherType	802.1p Priority	DSCP	Protocol	Destination L4 Port Min	Destination L4 Port Max	Source L4 Port Min	Source L4 Port Max
☑	1	1	1	Ignore	Tagged Only	Ignore	Match Priority 0 Match Priority 1 Match Priority 2	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore

The system returns you to Layer 2 Classification page. The new filter group appears in the Layer2 Filter Group Table (Figure 13).

Figure 13 Layer 2 Classification page



Source IP Layer4 Port Range

● Ignore
○ Inspect Source IP Layer4 Port Range
Minimum Value 0 (0..65535)
Maximum Value 0 (0..65535)

Layer2 Filter Group Table

Action	Filter Group Name
✎ ✕	layer2filter

Configuring actions

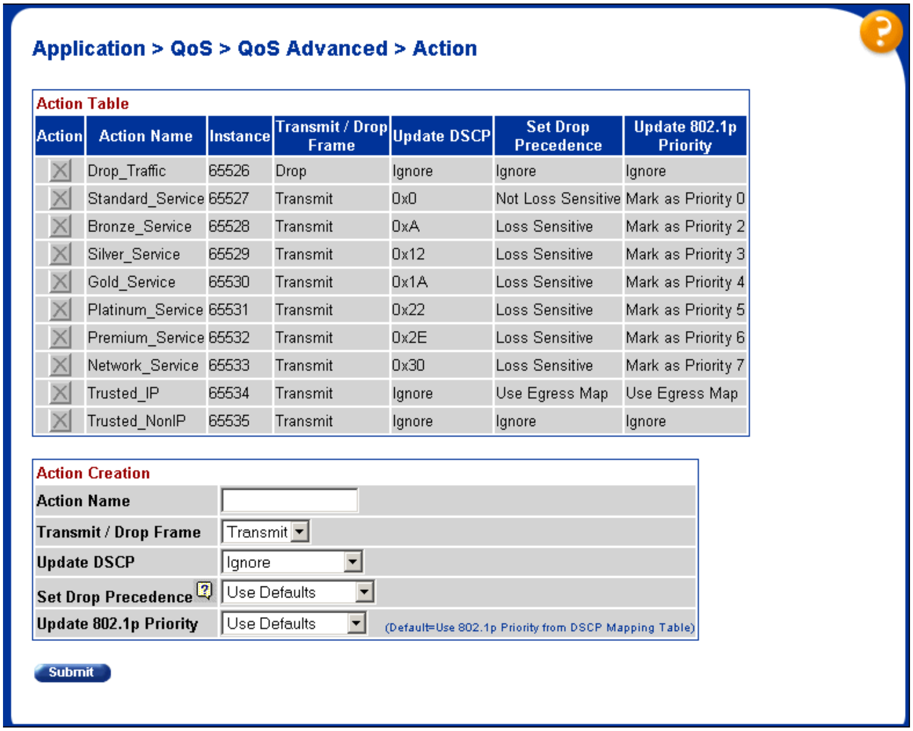
When you assign actions to filters, you must specify the type of behavior you want a policy to apply to a flow of IP and IEEE 802 packets. Actions applied to filters establish packet-specific criteria that determine how a packet is processed. You must specify the actions associated with specific IP and Layer 2 filter groups. When filters match incoming packets, the actions are performed on those packets. Actions can be configured to re-mark packets, to change priorities and loss-sensitivity (drop precedence), or to drop packets. In order to use a particular action, that action must be assigned to a meter (refer to "Configuring meters" on page 77).

To configure an action:

1 Click the Application > QoS > QoS Advanced > Actions menu option.

The Actions page opens (Figure 14).

Figure 14 Actions page



Application > QoS > QoS Advanced > Action

Action Table

Action	Action Name	Instance	Transmit / Drop Frame	Update DSCP	Set Drop Precedence	Update 802.1p Priority
☒	Drop_Traffic	65526	Drop	Ignore	Ignore	Ignore
☒	Standard_Service	65527	Transmit	0x0	Not Loss Sensitive	Mark as Priority 0
☒	Bronze_Service	65528	Transmit	0xA	Loss Sensitive	Mark as Priority 2
☒	Silver_Service	65529	Transmit	0x12	Loss Sensitive	Mark as Priority 3
☒	Gold_Service	65530	Transmit	0x1A	Loss Sensitive	Mark as Priority 4
☒	Platinum_Service	65531	Transmit	0x22	Loss Sensitive	Mark as Priority 5
☒	Premium_Service	65532	Transmit	0x2E	Loss Sensitive	Mark as Priority 6
☒	Network_Service	65533	Transmit	0x30	Loss Sensitive	Mark as Priority 7
☒	Trusted_IP	65534	Transmit	Ignore	Use Egress Map	Use Egress Map
☒	Trusted_NonIP	65535	Transmit	Ignore	Ignore	Ignore

Action Creation

Action Name		
Transmit / Drop Frame	Transmit	
Update DSCP	Ignore	
Set Drop Precedence	Use Defaults	
Update 802.1p Priority	Use Defaults	(Default=Use 802.1p Priority from DSCP Mapping Table)

2 In the Action Name field of the Action Creation section, enter **`Generic`**.

3 In the Transmit/Drop Frame field, choose **`Transmit`**.

4 In the Update DSCP field, choose **`47,0x2F`**.

This entry changes the DSCP value to the decimal value 47 in the match packet.

5 In the Set Drop Precedence field, choose **`Not Loss Sensitive`**.

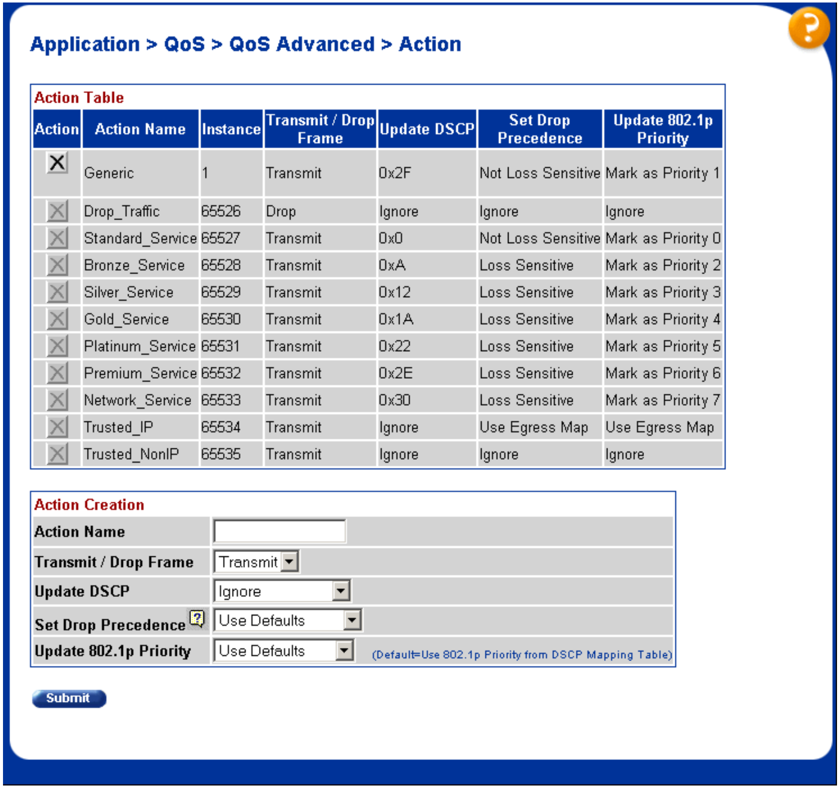
6 In the Update 802.1p Priority field, select **`Priority 1`**.

Priority 1 specifies a low priority.

7 Click Submit.

The entry is displayed in the Action Table (Figure 15).

Figure 15 Action page with entry in Action Table



Action Table

Action	Action Name	Instance	Transmit / Drop Frame	Update DSCP	Set Drop Precedence	Update 802.1p Priority
☒	Generic	1	Transmit	0x2F	Not Loss Sensitive	Mark as Priority 1
☒	Drop_Traffic	65526	Drop	Ignore	Ignore	Ignore
☒	Standard_Service	65527	Transmit	0x0	Not Loss Sensitive	Mark as Priority 0
☒	Bronze_Service	65528	Transmit	0xA	Loss Sensitive	Mark as Priority 2
☒	Silver_Service	65529	Transmit	0x12	Loss Sensitive	Mark as Priority 3
☒	Gold_Service	65530	Transmit	0x1A	Loss Sensitive	Mark as Priority 4
☒	Platinum_Service	65531	Transmit	0x22	Loss Sensitive	Mark as Priority 5
☒	Premium_Service	65532	Transmit	0x2E	Loss Sensitive	Mark as Priority 6
☒	Network_Service	65533	Transmit	0x30	Loss Sensitive	Mark as Priority 7
☒	Trusted_IP	65534	Transmit	Ignore	Use Egress Map	Use Egress Map
☒	Trusted_NonIP	65535	Transmit	Ignore	Ignore	Ignore

Action Creation

Action Name		
Transmit / Drop Frame	Transmit ▾	
Update DSCP	Ignore ▾	
Set Drop Precedence ?	Use Defaults ▾	
Update 802.1p Priority	Use Defaults ▾	(Default=Use 802.1p Priority from DSCP Mapping Table)

In summary, you have configured a new action named Generic. This action specifies a high drop precedence, a low user priority, and a DSCP value of 0x2F for packets that match a filter associated with this action.

Unrestricted meters

In software versions prior to Release 3.5, only unrestricted meters were supported. When using unrestricted meters, you can configure a maximum of 12 Layer 2 metered policies. This is because each metered policy requires a filter for in-profile actions, and another filter for out-of-profile actions. With 24 Layer 2 filters available, and two filters for each metered policy, you have12 Layer 2 metered policies.

Unrestricted meters can be applied to any group of interfaces: Trusted, Untrusted, and Restricted.

Configuring meters

Metering operates at ingress and provides different levels of service to data streams through user-configurable parameters. An example is to limit traffic entering a port to a specified bandwidth, such as 25 Kb/s (Committed Rate). Instead of dropping all traffic that exceeds this threshold, traffic policing allows you to configure a Committed Burst Rate to exceed the threshold (Committed Rate), for a brief period of time, without being dropped.

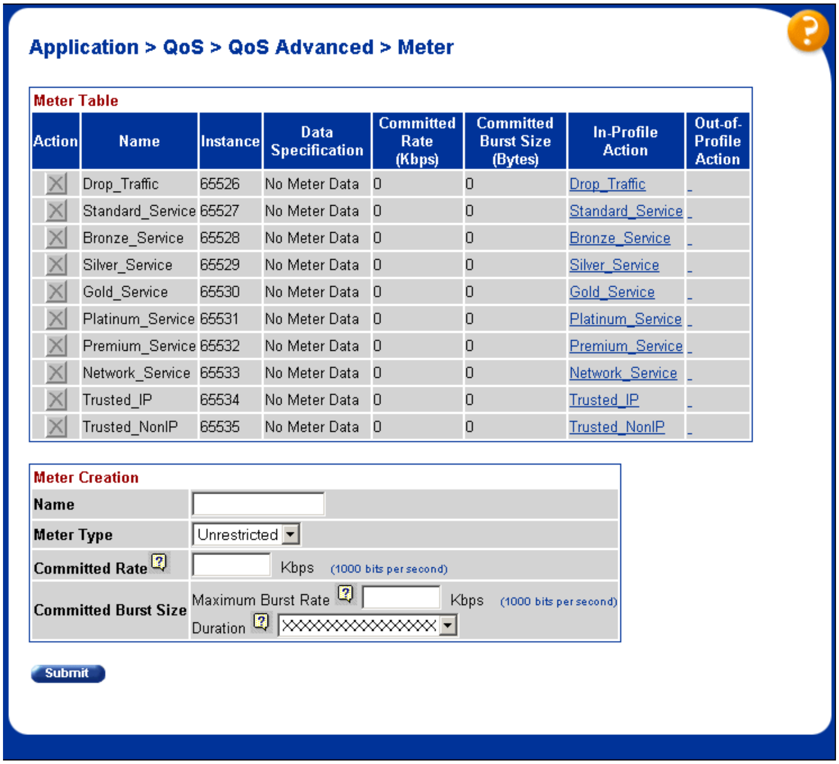
➡ **Note:** If you are not metering data, go to “Configuring shapers” on page 79.

To configure a meter:

1 Click the Application > QoS > QoS Advanced > Meters menu option.

The Meters page opens (Figure 16).

Figure 16 Meters page



Application > QoS > QoS Advanced > Meter

Meter Table

Action	Name	Instance	Data Specification	Committed Rate (Kbps)	Committed Burst Size (Bytes)	In-Profile Action	Out-of-Profile Action
☒	Drop_Traffic	65526	No Meter Data	0	0	Drop_Traffic	_
☒	Standard_Service	65527	No Meter Data	0	0	Standard_Service	_
☒	Bronze_Service	65528	No Meter Data	0	0	Bronze_Service	_
☒	Silver_Service	65529	No Meter Data	0	0	Silver_Service	_
☒	Gold_Service	65530	No Meter Data	0	0	Gold_Service	_
☒	Platinum_Service	65531	No Meter Data	0	0	Platinum_Service	_
☒	Premium_Service	65532	No Meter Data	0	0	Premium_Service	_
☒	Network_Service	65533	No Meter Data	0	0	Network_Service	_
☒	Trusted_IP	65534	No Meter Data	0	0	Trusted_IP	_
☒	Trusted_NonIP	65535	No Meter Data	0	0	Trusted_NonIP	_

Meter Creation

Name	
Meter Type	Unrestricted
Committed Rate	Kbps (1000 bits per second)
Committed Burst Size	Maximum Burst Rate Kbps (1000 bits per second) Duration XXXXXXXXXXXXXXXXX

2 In the Name field of the Meter Creation section, enter **`Practice`**.

3 In the Committed Rate field, enter **`3000`**.

4 In the Maximum Burst Rate field of the Committed Burst Size section, enter **`3500`**.

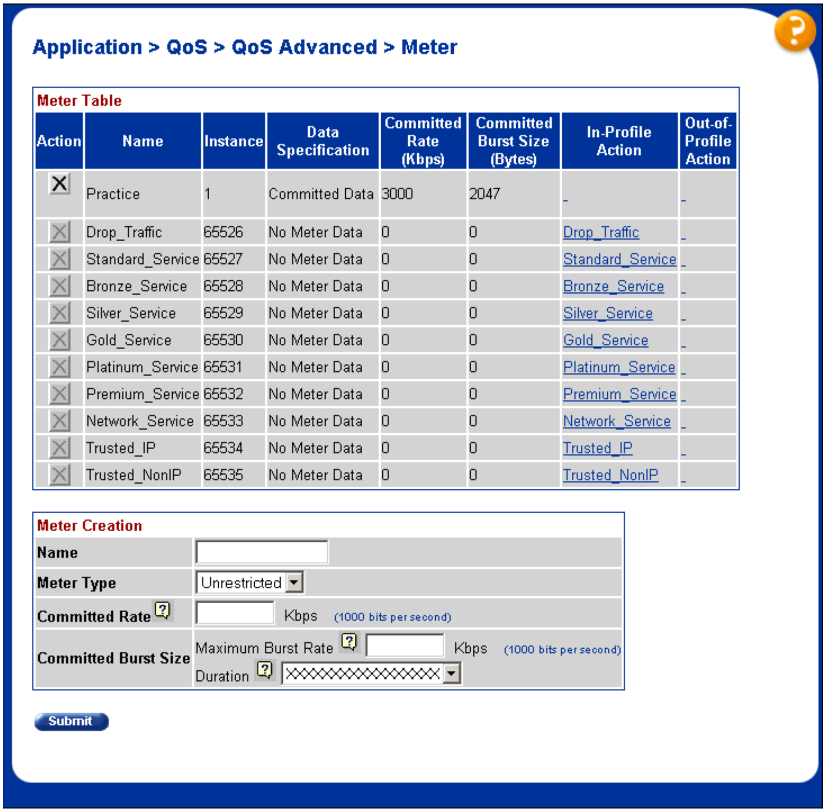
5 In the Duration field of the Committed Burst Size section, select **`33 milliseconds`** from the drop-down list.

The switch calculates from 1 to 7 durations and presents the results to you in a drop-down list. Choose the duration you want.

6 Click Submit.

The new entry is displayed in the Meter Table (Figure 17).

Figure 17 Meter page with new entry in Meter Table



Application > QoS > QoS Advanced > Meter

Meter Table

Action	Name	Instance	Data Specification	Committed Rate (Kbps)	Committed Burst Size (Bytes)	In-Profile Action	Out-of-Profile Action
☒	Practice	1	Committed Data	3000	2047	_	_
☒	Drop_Traffic	65526	No Meter Data	0	0	Drop_Traffic	_
☒	Standard_Service	65527	No Meter Data	0	0	Standard_Service	_
☒	Bronze_Service	65528	No Meter Data	0	0	Bronze_Service	_
☒	Silver_Service	65529	No Meter Data	0	0	Silver_Service	_
☒	Gold_Service	65530	No Meter Data	0	0	Gold_Service	_
☒	Platinum_Service	65531	No Meter Data	0	0	Platinum_Service	_
☒	Premium_Service	65532	No Meter Data	0	0	Premium_Service	_
☒	Network_Service	65533	No Meter Data	0	0	Network_Service	_
☒	Trusted_IP	65534	No Meter Data	0	0	Trusted_IP	_
☒	Trusted_NonIP	65535	No Meter Data	0	0	Trusted_NonIP	_

Meter Creation

Name	
Meter Type	Unrestricted
Committed Rate	Kbps (1000 bits per second)
Committed Burst Size	Maximum Burst Rate Kbps (1000 bits per second) Duration XXXXXXXXXXXXXXXX

In summary, you have configured a new meter named Practice. This meter specifies committed data, with a committed rate of 3000 Kbps and a committed burst size of 2047 bytes, for packets that match a filter associated with this meter.

Configuring shapers

Shaping operates at egress and specifies the maximum rate at which traffic is transmitted over a given time. Traffic is allowed to exceed this rate in short bursts. You must specify a burst size to indicate the maximum burst size of traffic allowed to egress without a shaping delay.

Traffic that is being shaped can be buffered temporarily to conform to the specified flows. You can choose whether 1, 2, 4, 8, or 16 packets can be held in the shaping queue for each policy. Some packets can be dropped if buffers are completely used.

You can shape either metered data or no metered data. Also, you do not have to shape the traffic.

Shapers are not modifiable. If you want to change a shaper, you must delete the entry in the Shaper Table and reenter the information.

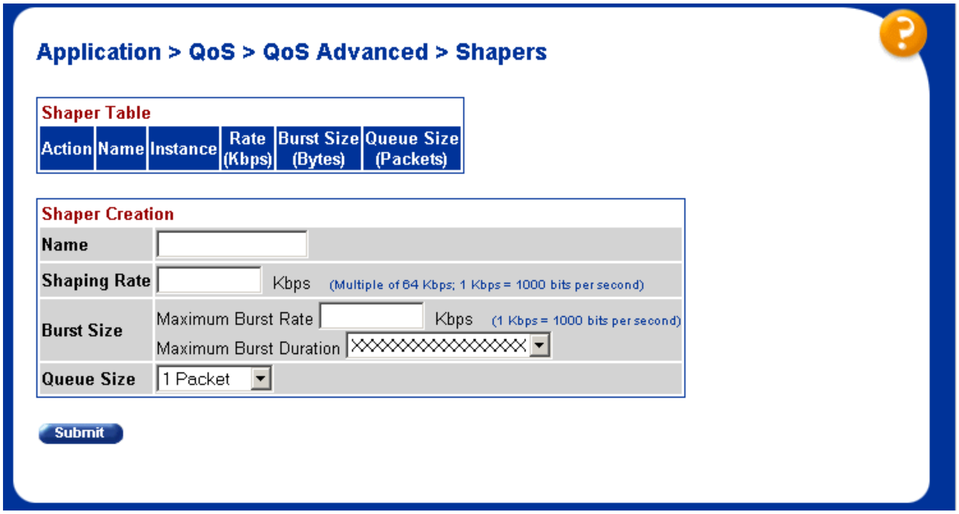
Note: If you do not want to shape the traffic, skip to "Configuring policies" on page 81.

To configure a shaper:

1 Click the Application > QoS > QoS Advanced > Shapers menu option.

The Shapers page opens (Figure 18).

Figure 18 Shapers page



Application > QoS > QoS Advanced > Shapers

Shaper Table

Action	Name	Instance	Rate (Kbps)	Burst Size (Bytes)	Queue Size (Packets)

Shaper Creation

Name	
Shaping Rate	Kbps (Multiple of 64 Kbps; 1 Kbps = 1000 bits per second)
Burst Size	Maximum Burst Rate Kbps (1 Kbps = 1000 bits per second) Maximum Burst Duration XXXXXXXXXXXXXXXX
Queue Size	1 Packet

2 In the Name field of the Shaper Creation section, enter **`Shape1`**.

3 In the Shaping Rate field, enter **`64`**.

You must enter a multiple of 64 Kbps in this field.

4 In the Maximum Burst Rate field, enter `70`.

5 Choose **`2729 milliseconds`** from the drop-down list for Maximum Burst Duration.

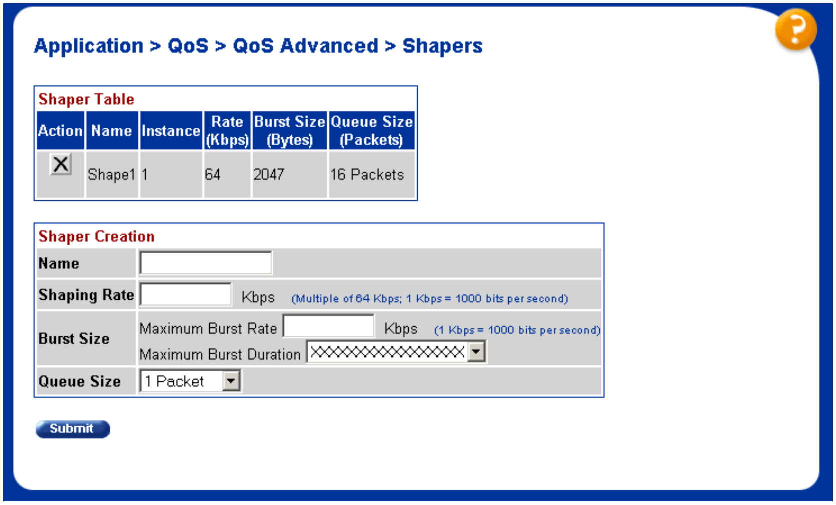
The switch calculates from 1 to 6 durations and presents the results to you in a drop-down list. Choose the one you want.

6 Choose **16 Packets** from the drop-down list for Queue Size.

7 Click Submit.

The new entry is displayed in the Shaper Table (Figure 19).

Figure 19 Shapers page with new entry in Shaper Table



Application > QoS > QoS Advanced > Shapers

Shaper Table

Action	Name	Instance	Rate (Kbps)	Burst Size (Bytes)	Queue Size (Packets)
☒	Shape1	1	64	2047	16 Packets

Shaper Creation

Name	
Shaping Rate	Kbps (Multiple of 64 Kbps; 1 Kbps = 1000 bits per second)
Burst Size	Maximum Burst Rate Kbps (1 Kbps = 1000 bits per second) Maximum Burst Duration XXXXXXXXXXXXXXXX
Queue Size	1 Packet

You configured a shaper named Shape1, with a 64-Kb/s rate, a maximum burst size of 2,047 bytes, and a queue depth of 16 packets.

Configuring policies

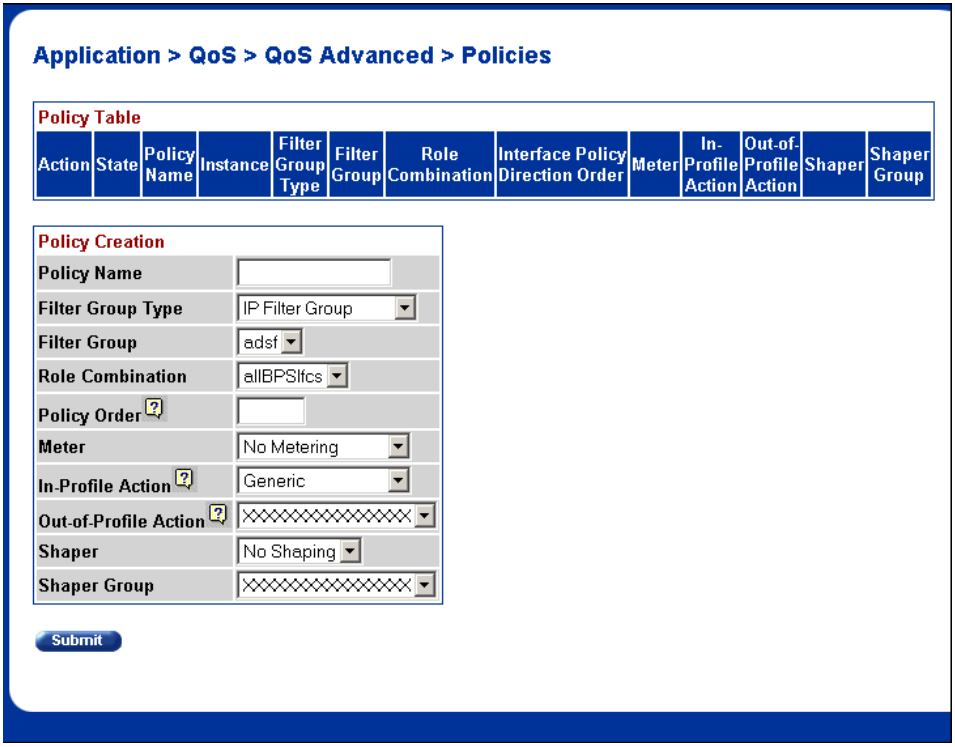
A policy is an interface group, a group of filters (filter set) and the associated meter, shaper or shaper group, and action. Policies are applied according to the precedence order that you assign in the QoS Advanced > Policies page.

To configure a policy:

1 Click the Application > QoS > QoS Advanced > Policies menu option.

The Policies page opens (Figure 20).

Figure 20 Policies page



Application > QoS > QoS Advanced > Policies

Policy Table

Action	State	Policy Name	Instance	Filter Group Type	Filter Group	Role Combination	Interface Policy Direction Order	Meter	In-Profile Action	Out-of-Profile Action	Shaper	Shaper Group

Policy Creation

Policy Name	
Filter Group Type	IP Filter Group
Filter Group	adsf
Role Combination	allBPSIfcs
Policy Order	
Meter	No Metering
In-Profile Action	Generic
Out-of-Profile Action	XXXXXXXXXXXXXXX
Shaper	No Shaping
Shaper Group	XXXXXXXXXXXXXXX

2 In the Policy Name field of the Policy Creation area, enter **`IPpolicy`**.

This entry is a unique name to identify this target.

Note: You cannot have spaces in the naming field.

3 In the Filter Group Type, choose **`IP Filter Group`**.

This entry is the filter group that is associated with this policy.

4 In the Filter Group field, choose **`IPacket`**.

This entry is the filter group you created in the IP Classification Group page, IP Filter Group Table.

5 In the Role Combination field, choose **`Webbrowsing`**.

This entry is the unique Role Combination that you created.

6 In the Policy Order field, enter **`1`**.

Note: Nortel recommends that you consider an order numbering strategy (for the values in the Order field) as you configure policies. The policies in the Policy Table are arranged in ascending order according to value in the Order column. By establishing a policy ordering scheme in multiples of, for example, 10 (Order 10, Order 20, Order 30, Order 40, and so on), you are able to insert policies in the appropriate filter precedence location and still retain the precedence of the remaining policies.

7 In the Meter field, choose **`Practice`**.

8 In the In-Profile Action field, choose **`Generic.`**

9 In the Out-of-Profile Action field, choose **`Drop Traffic.`**

10 In the Shaper field, choose **`Shape1`**.

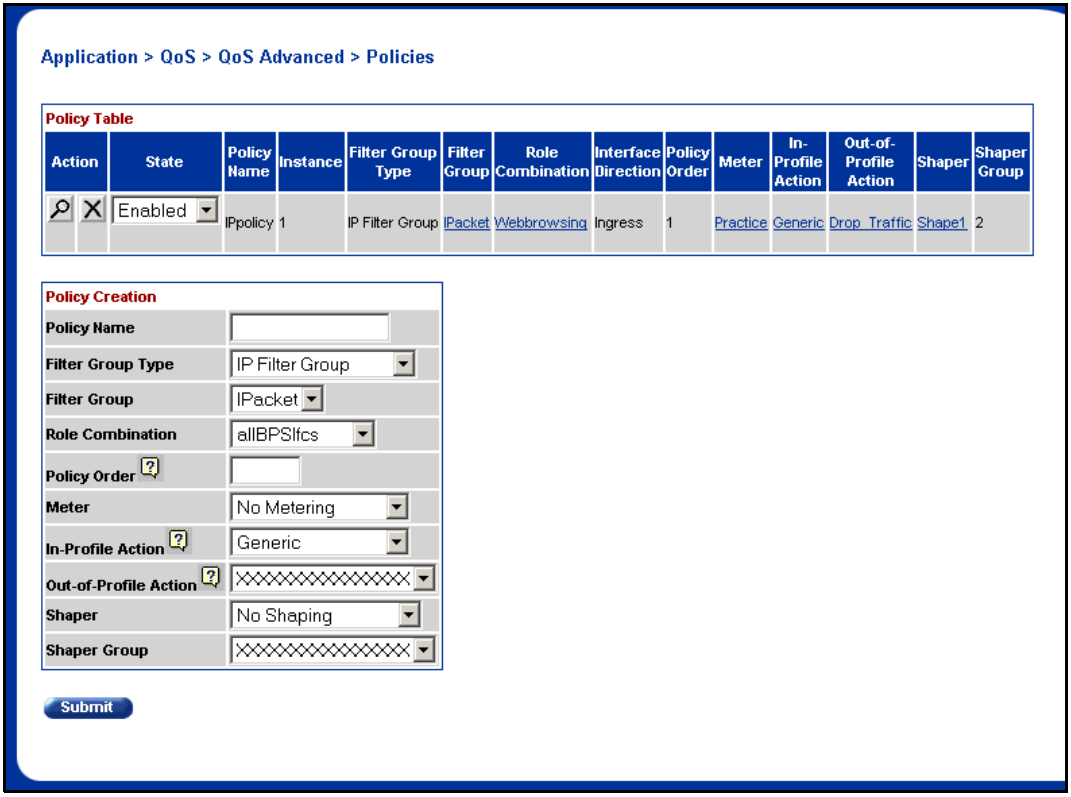
11 Leave the Shaper Group field as is.

You can associated the traffic with the policy you are creating shaped as a group (or aggregate) with the traffic associated with other installed policies. To do so, choose the Shaping Group identified in the Policy Table with the policy or policies you want to group with this traffic, rather than using the Shaper field.

12 Click Submit.

The new entry is displayed in the Policy Table (Figure 21).

Figure 21 Policies page with new entry



Application > QoS > QoS Advanced > Policies

Policy Table

Action	State	Policy Name	Instance	Filter Group Type	Filter Group	Role Combination	Interface Direction	Policy Order	Meter	In-Profile Action	Out-of-Profile Action	Shaper	Shaper Group
	Enabled	IPpolicy	1	IP Filter Group	IPacket	Webbrowsing	Ingress	1	Practice	Generic	Drop Traffic	Shape1	2

Policy Creation

Policy Name	
Filter Group Type	IP Filter Group
Filter Group	IPacket
Role Combination	allBPSIfcs
Policy Order	
Meter	No Metering
In-Profile Action	Generic
Out-of-Profile Action	XXXXXXXXXXXXXXXX
Shaper	No Shaping
Shaper Group	XXXXXXXXXXXXXXXX

In summary, you configured a QoS policy called IPpolicy. This policy applies a combination of packet filtering (matching) criteria and actions to individual interfaces (ports) in the hardware. You specified that this policy will use the IPacket filter group with the elements that you specified. IPpolicy will use the Role Combination Webbrowsing, the Practice meter, and the Shape1 shaper. The system assigned the IPpolicy the Shaper Group number 2, and the policy will track statistics. IPpolicy specifies the type of behavior you want to apply to a flow of packets.

You can enable or disable each policy using the drop-down list under the Status heading. The default value is Enabled.

Assigning mapping values

> **Note:** Nortel recommends that you use the default mapping values to ensure end-to-end QoS connectivity across Nortel Network products.

To manually configure the mapping among 802.1p priority values, priority, and DSCP mapping, you must refer to the following QoS Advanced pages:

- "Assigning 802.1p priority queue assignment" on page 85
- "Verifying DSCP mapping" on page 87
- "Assigning 802.1p user priority mapping" on page 89
- "Verifying DSCP queue assignments" on page 90

Assigning 802.1p priority queue assignment

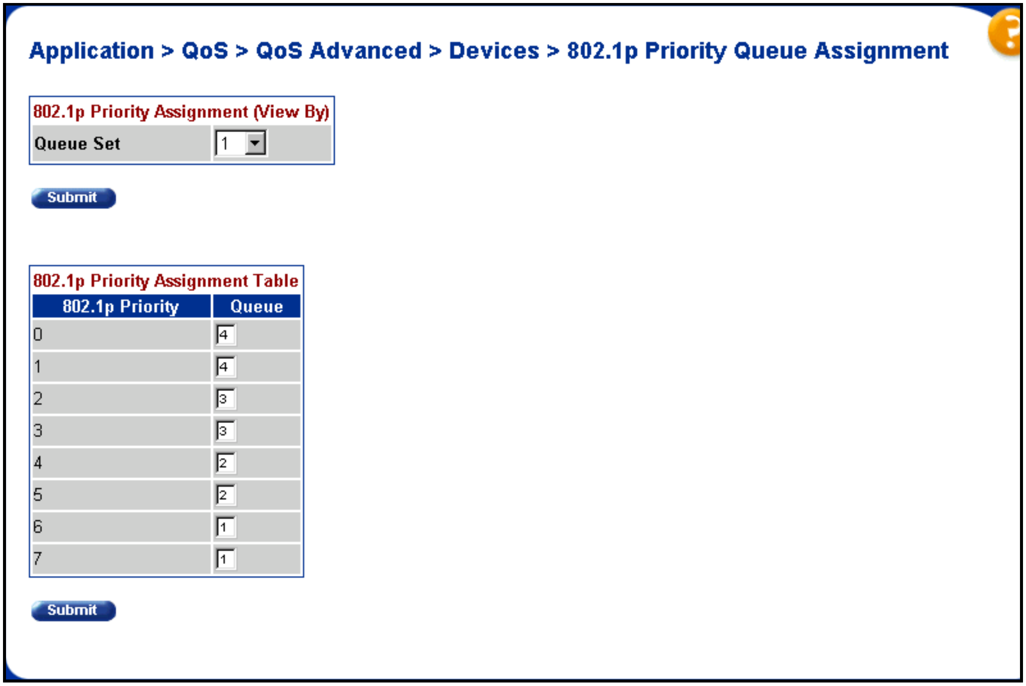
You must assign IEEE 802.1p priority values to a queue for specific queue set. This information is used for assigning egress traffic to outbound queues.

To configure 802.1p priority:

1 Click the Application > QoS > QoS Advanced > Devices > Priority Q Assign menu option.

The 802.1p Priority Queue Assignment page opens (Figure 22).

Figure 22 802.1p Priority Queue Assignment page



Application > QoS > QoS Advanced > Devices > 802.1p Priority Queue Assignment

802.1p Priority Assignment (View By)

Queue Set	1

802.1p Priority Assignment Table

802.1p Priority	Queue
0	4
1	4
2	3
3	3
4	2
5	2
6	1
7	1

2 In the Queue Set field in the 802.1p Priority Assignment (View By) section, select 1.

This value is the queue set you want to modify.

3 Click Submit.

The 802.1p Priority Assignment Table is updated with the queue set you requested.

4 Change the value of Priority 5 from 2 to 1.

➡ **Note:** Clicking Submit in the 802.1p Priority Assignment Table section results in a system reset.

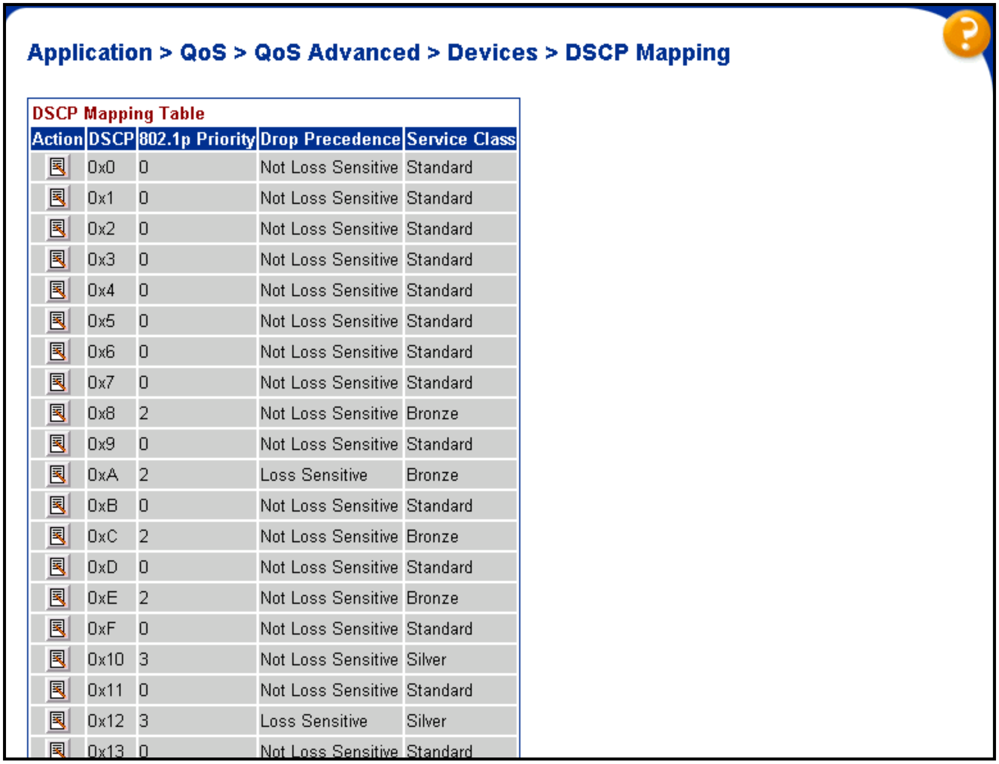
Verifying DSCP mapping

Next, verify the mapping of the DSCP to an IEEE 802.1p priority, drop precedence, and service class.

➨ Click the Application > QoS > QoS Advanced > Devices > DSCP Mapping menu option.

The DSCP Mapping page opens (Figure 23).

Figure 23 DSCP Mapping page



Application > QoS > QoS Advanced > Devices > DSCP Mapping

DSCP Mapping Table

Action	DSCP	802.1p Priority	Drop Precedence	Service Class
✎	0x0	0	Not Loss Sensitive	Standard
✎	0x1	0	Not Loss Sensitive	Standard
✎	0x2	0	Not Loss Sensitive	Standard
✎	0x3	0	Not Loss Sensitive	Standard
✎	0x4	0	Not Loss Sensitive	Standard
✎	0x5	0	Not Loss Sensitive	Standard
✎	0x6	0	Not Loss Sensitive	Standard
✎	0x7	0	Not Loss Sensitive	Standard
✎	0x8	2	Not Loss Sensitive	Bronze
✎	0x9	0	Not Loss Sensitive	Standard
✎	0xA	2	Loss Sensitive	Bronze
✎	0xB	0	Not Loss Sensitive	Standard
✎	0xC	2	Not Loss Sensitive	Bronze
✎	0xD	0	Not Loss Sensitive	Standard
✎	0xE	2	Not Loss Sensitive	Bronze
✎	0xF	0	Not Loss Sensitive	Standard
✎	0x10	3	Not Loss Sensitive	Silver
✎	0x11	0	Not Loss Sensitive	Standard
✎	0x12	3	Loss Sensitive	Silver
✎	0x13	0	Not Loss Sensitive	Standard

To change the DSCP to an 802.1p priority:

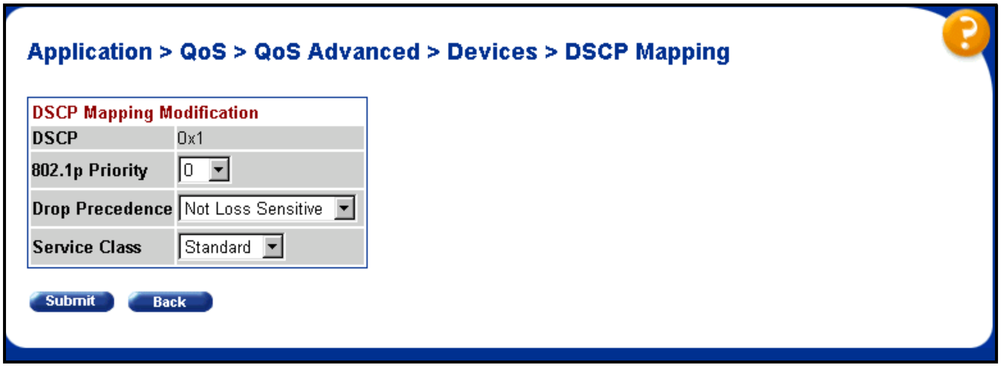
1 Click the Application > QoS > QoS Advanced > Devices > DSCP Mapping menu option.

The DSCP Mapping page opens (Figure 23).

2 Click the Modify icon of DSCP 0x1.

The DSCP Mapping page opens (Figure 24) for DSCP 0x1.

Figure 24 DSCP Mapping page



DSCP Mapping Modification

DSCP	0x1
802.1p Priority	0
Drop Precedence	Not Loss Sensitive
Service Class	Standard

3 In the 802.1 User Priority field, choose `1`.

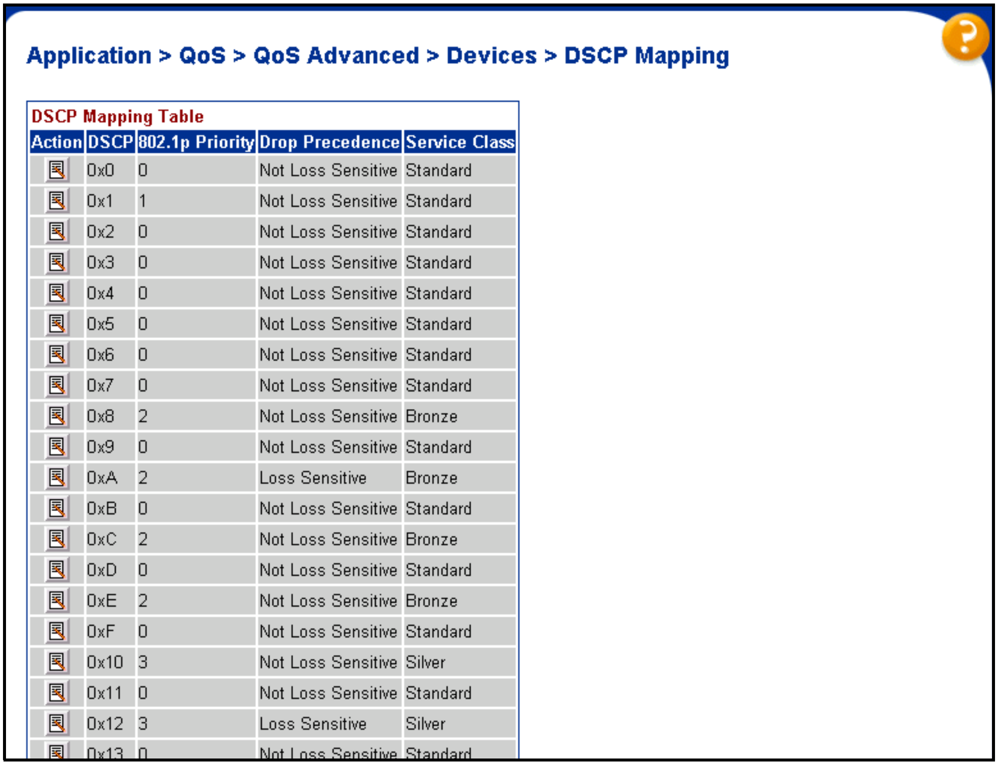
4 In the Drop Precedence field, choose **`Not Loss Sensitive`**.

5 In the Service Class field, choose **`Standard`**.

6 Click Submit.

The DSCP Mapping page opens with the updated information (Figure 25).

Figure 25 DSCP Mapping page



Application > QoS > QoS Advanced > Devices > DSCP Mapping

DSCP Mapping Table

Action	DSCP	802.1p Priority	Drop Precedence	Service Class
✎	0x0	0	Not Loss Sensitive	Standard
✎	0x1	1	Not Loss Sensitive	Standard
✎	0x2	0	Not Loss Sensitive	Standard
✎	0x3	0	Not Loss Sensitive	Standard
✎	0x4	0	Not Loss Sensitive	Standard
✎	0x5	0	Not Loss Sensitive	Standard
✎	0x6	0	Not Loss Sensitive	Standard
✎	0x7	0	Not Loss Sensitive	Standard
✎	0x8	2	Not Loss Sensitive	Bronze
✎	0x9	0	Not Loss Sensitive	Standard
✎	0xA	2	Loss Sensitive	Bronze
✎	0xB	0	Not Loss Sensitive	Standard
✎	0xC	2	Not Loss Sensitive	Bronze
✎	0xD	0	Not Loss Sensitive	Standard
✎	0xE	2	Not Loss Sensitive	Bronze
✎	0xF	0	Not Loss Sensitive	Standard
✎	0x10	3	Not Loss Sensitive	Silver
✎	0x11	0	Not Loss Sensitive	Standard
✎	0x12	3	Loss Sensitive	Silver
✎	0x13	0	Not Loss Sensitive	Standard

Assigning 802.1p user priority mapping

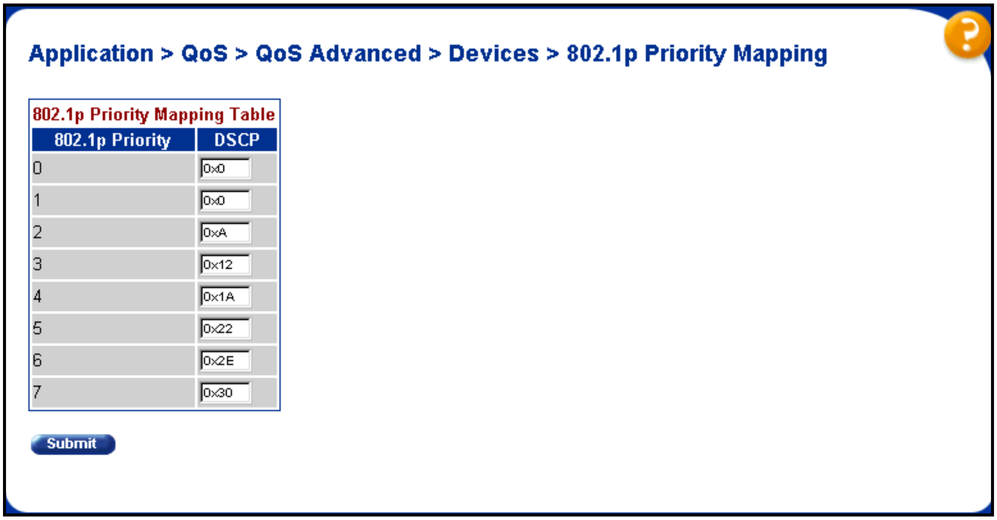
To map the 802.1p priority to a specific DSCP.

To configure IEEE 802.1p user priority to DSCP mapping:

1 Click the Application > QoS > QoS Advanced > Devices > Priority Mapping menu option.

The 802.1p Priority Mapping page opens (Figure 26).

Figure 26 802.1p Priority Mapping page



Application > QoS > QoS Advanced > Devices > 802.1p Priority Mapping

802.1p Priority Mapping Table

802.1p Priority	DSCP
0	0x0
1	0x0
2	0xA
3	0x12
4	0x1A
5	0x22
6	0x2E
7	0x30

2 Change the DSCP value for 802.1. Priority 2 to `0x0`.

3 Click Submit.

Verifying DSCP queue assignments

Next, view the DSCP queue assignments.

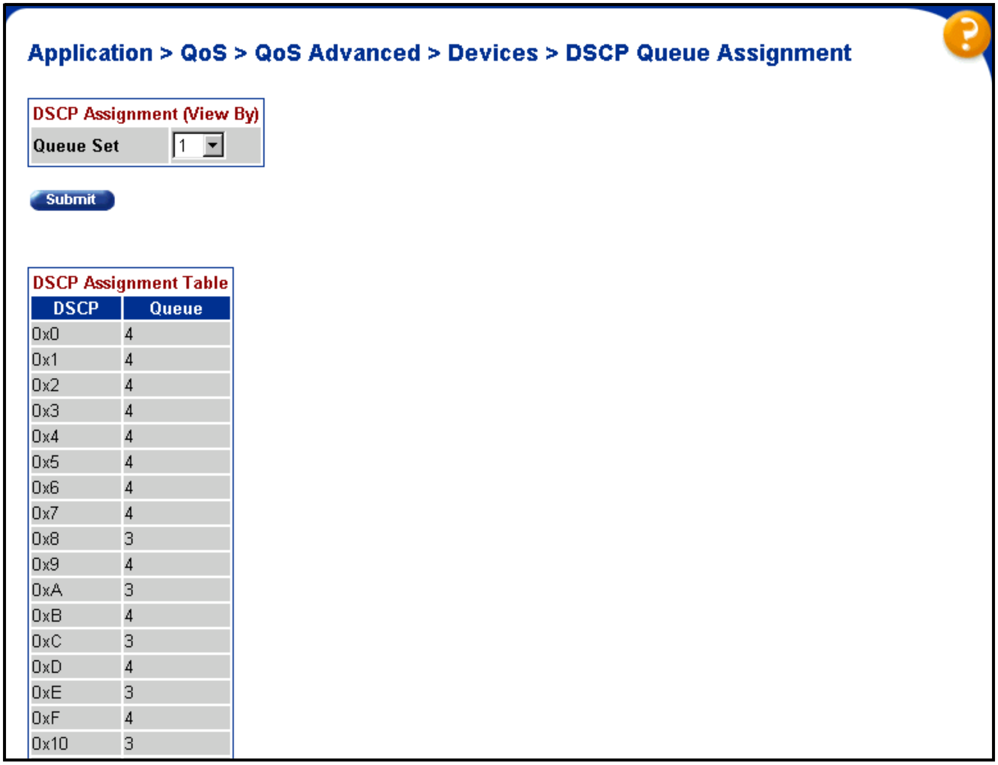
Note: When you want to map DSCP to a queue, you must map DSCP to 802.1p, and then map 802.1p to a queue.

To view DSCP queue assignments:

1 Click the Application > QoS > QoS Advanced > Devices > DSCP Q Assign menu option.

The DSCP Queue Assignment page opens (Figure 27).

Figure 27 DSCP Queue Assignment page


Application > QoS > QoS Advanced > Devices > DSCP Queue Assignment
Submit

DSCP Assignment (View By)

Queue Set	1

DSCP Assignment Table

DSCP	Queue
0x0	4
0x1	4
0x2	4
0x3	4
0x4	4
0x5	4
0x6	4
0x7	4
0x8	3
0x9	4
0xA	3
0xB	4
0xC	3
0xD	4
0xE	3
0xF	4
0x10	3

2 Choose Queue Set `1.`

3 Click Submit.

4 View the queue assignment.

Layer 2 restricted QoS meters

With restricted meters, you are allowed a maximum of 23 Layer 2 metered policies. All 23 metered policies can have a different in-profile-action, but they all share the same out-of-profile action. The first policy created consumes two filters; one filter is consumed for the in-profile action, and another filter is consumed for the out-of-profile action. Subsequent restricted Layer 2 metered policies use only one filter for the in-profile-action and they share the out-of-profile action defined by the first filter. Since only one filter is used for each policy, statistics count only in-profile traffic.

Restricted meters can be used only when the Interface Class Restriction is set to Unrestricted Only.

Configuration

To configure the device to use restricted meters, the following steps must be performed:

1 Ensure that the current Interface Class Restriction is set to Unrestricted Only by entering the following CLI command.

```
460-24T(config)# show qos agent
```

2 If the current Interface Class Restriction is not set to Unrestricted Only, you can enable the Unrestricted Only mode by entering the following command:

```
460-24T(config)# designate class-restrictions
unrestricted-only
```

3 Reboot the switch for this mode to take effect:

```
460-24T(config)#boot
```

```
Reboot the unit(s) (y/n)? y
```

4 Assign a default action or use the default “Drop_Traffic”:

```
460-24T(config)# qosagent default-out-of-profile-action
name no-flow
```

5 Create the restricted meter:

```
qos meter 1 create name myMeter committed-rate 5000
max-burst-rate 6000 restricted
```

Restricted meters are created when the “restricted” command argument is appended to the “`qos meter <meter_id> create`” command.

Apply the new restricted meter to a policy in the same manner used for an unrestricted meter.

User-based policies

This feature allows user-specific QoS policy information to be manipulated based on the presence, or lack thereof, of a specific network user. User information is retrieved from the RADIUS Server during EAP authentication and passed to the QoS Agent. The QoS Agent, in turn, notifies OPS of the user's presence if the policy server is currently in charge of policy configuration. OPS can then download policy components to the device associated with the user. The User Based Policies (UBP) components are automatically deleted when the user logs off or is no longer authenticated.

This feature adds an ON/OFF attribute to the console interface to enable/disable UBP support. For SNMP support, an Enterprise-specific MIB is added. CLI support is similar to other EAP configurations. This feature is presently not supported from the Web interface.

Chapter 2 Configuring QoS using the CLI

This chapter describes how to configure DiffServ and Quality of Service (QoS) parameters for policy-enabled networks. This chapter covers the following topics:

- "Displaying QoS parameters"
- "Resetting" on page 106
- "Configuring COPS" on page 107
- "Configuring QoS interface groups" on page 114
- "Configuring DSCP and 802.1p and queue associations" on page 117
- "Configuring QoS filters and filter groups" on page 119
- "Configuring QoS actions" on page 125
- "Configuring QoS meters" on page 126
- "Configuring QoS shapers" on page 128
- "Configuring QoS policies" on page 130
- "Reordering packets" on page 133
- "Interface Class Restrictions" on page 134
- "User-based policies" on page 134

.

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

Displaying QoS parameters

You can display QoS parameters using the CLI show qos command

The show qos command displays the current QoS policy configuration The syntax for the show qos command is:

```
show qos [interface-groups|interface-assignments|
if-assign-list|egressmap|ingressmap|
ip-filters|ip-filter-sets|
l2-filters|l2-filter-sets|
actions|meters|shapers|policies|
queue-sets|queue-set-assignments|
agent|statistics]
```

The show qos command is in the privExec command mode.

Table 7 describes the parameters and variables for the show qos command.

Table 7 show qos command parameters and variables

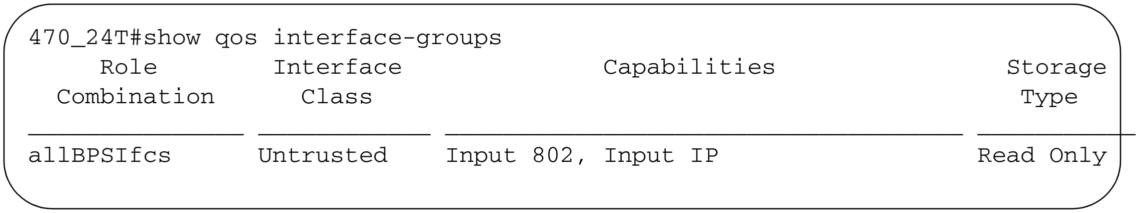
Parameters and variables	Description
interface-groups	Displays configured interface groups.
interface-assignments	Displays interface-to-interface group assignments.
if-assign-list	Displays interface-to-interface group assignments.
egressmap	Displays DSCP-to-802.1p priority and loss-sensitivity mapping.
ingressmap	Displays 802.1p priority-to-DSCP mapping.
ip-filters	Displays defined IP filters.
ip-filter-sets	Displays defined IP filter sets.
l2-filters	Displays defined Layer 2 filters.
l2-filter-sets	Displays defined Layer 2 filter sets.
actions	Displays defined QoS action entries.
meters	Displays defined traffic metering entries.
shapers	Displays defined traffic shaping entries.
policies	Displays configured QoS policies.
queue-sets	Displays current queue set information.
queue-set-assignments	Displays 802.1p priority-to-queue assignments by queue set.

Table 7 `show qos` command parameters and variables (Continued)

Parameters and variables	Description
`agent`	Displays QoS agent configuration parameters.
`statistics`	Displays QoS policy statistics.

Figure 28 displays sample output from the `show qos interface-groups` command.

Figure 28 `show qos interface-groups` command output



```
470_24T#show qos interface-groups
     Role          Interface               Capabilities                  Storage
  Combination        Class                                                 Type
_______________  ____________  ____________________________________  ___________
allBPSIfcs       Untrusted     Input 802, Input IP                   Read Only
```

Figure 29 displays sample output from the `show qos interface-assignments` command.

Figure 29 `show qos interface-assignments` command output

```
470_24T#show qos interface-assignments
Unit Port IfIndex Role Combination

____ ____ _______ _________________
1    1       1     allBPSIfcs
1    2       2     Webbrowsing
1    3       3     Test1
1    4       4     allBPSIfcs
1    5       5     allBPSIfcs
1    6       6     allBPSIfcs
1    7       7     Test1
1    8       8     allBPSIfcs
1    9       9     allBPSIfcs
1    10      10    allBPSIfcs
1    11      11    Webbrowsing
1    12      12    allBPSIfcs
1    13      13    allBPSIfcs
1    14      14    allBPSIfcs
1    15      15    Test1
1    16      16    allBPSIfcs
1    17      17    Webbrowsing
1    18      18    allBPSIfcs
1    19      19    allBPSIfcs
1    20      20    allBPSIfcs
1    21      21    allBPSIfcs
1    22      22    allBPSIfcs
```

Figure 30 displays sample output from the `show qos if-assign-list` command.

Figure 30 `show qos if-assign-list` command output

```
470_24T#show qos interface-assignments
Unit  Port  IfIndex  Role Combination
_____ _____ ________ ___________________
1     1       1       allBPSIfcs
1     2       2       Webbrowsing
1     3       3       Test1
1     4       4       allBPSIfcs
1     5       5       allBPSIfcs
1     6       6       allBPSIfcs
1     7       7       Test1
1     8       8       allBPSIfcs
1     9       9       allBPSIfcs
1     10      10      allBPSIfcs
1     11      11      Webbrowsing
1     12      12      allBPSIfcs
1     13      13      allBPSIfcs
1     14      14      allBPSIfcs
1     15      15      Test1
1     16      16      allBPSIfcs
1     17      17      Webbrowsing
1     18      18      allBPSIfcs
1     19      19      allBPSIfcs
1     20      20      allBPSIfcs
1     21      21      allBPSIfcs
1     22      22      allBPSIfcs
```

Figure 31 displays sample output from the `show qos egressmap` command.

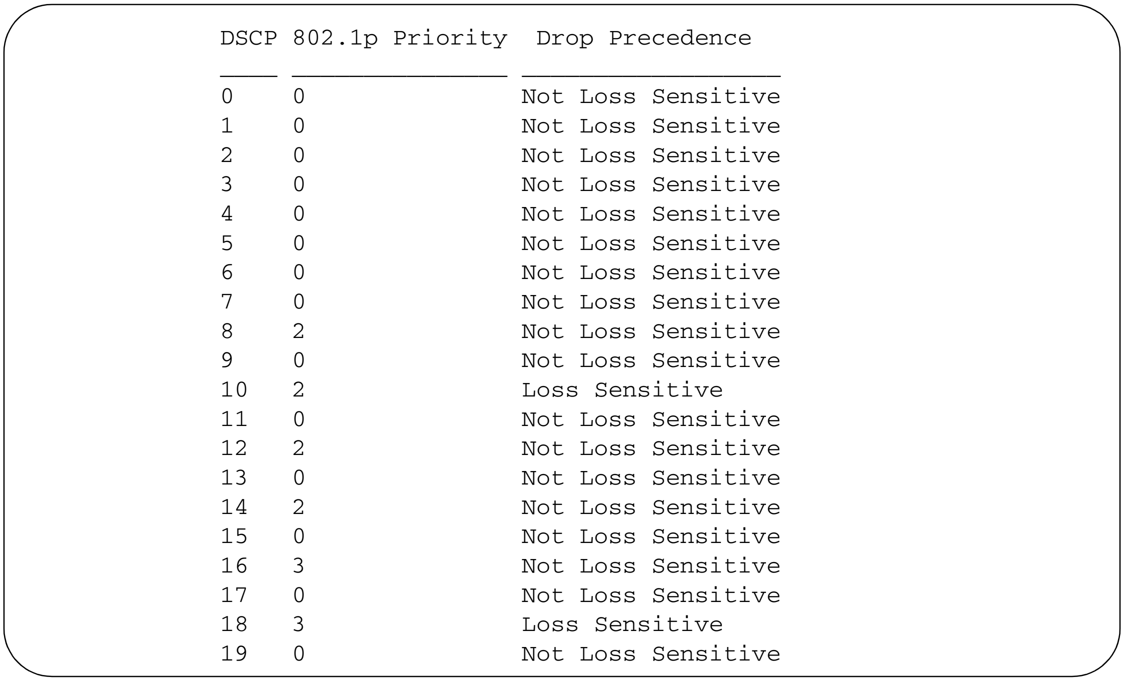


Figure 31 `show qos egressmap` command output

```
DSCP 802.1p Priority  Drop Precedence
____ _______________ __________________
0    0               Not Loss Sensitive
1    0               Not Loss Sensitive
2    0               Not Loss Sensitive
3    0               Not Loss Sensitive
4    0               Not Loss Sensitive
5    0               Not Loss Sensitive
6    0               Not Loss Sensitive
7    0               Not Loss Sensitive
8    2               Not Loss Sensitive
9    0               Not Loss Sensitive
10   2               Loss Sensitive
11   0               Not Loss Sensitive
12   2               Not Loss Sensitive
13   0               Not Loss Sensitive
14   2               Not Loss Sensitive
15   0               Not Loss Sensitive
16   3               Not Loss Sensitive
17   0               Not Loss Sensitive
18   3               Loss Sensitive
19   0               Not Loss Sensitive
```

Figure 32 displays sample output from the `show qos ingressmap` command.

Figure 32 `show qos ingressmap` command output

```
470_24T#show qos ingressmap
802.1p Priority DSCP

_______________ ____
0               0
1               0
2               10
3               18
4               26
5               34
6               46
7               48
```

Figure 33 displays sample output from the `show qos ip-filters` command.

Figure 33 `show qos ip-filters` command output

```
470_24T#show qos ip-filters
Id    Destination       Source       DSCP  Protocol  Dest     Src
      Addr / Mask     Addr / Mask                   L4 Port L4 Port

___ _______________ _______________ ______ ________ _______ _______
1   Ignore          Ignore          Ignore Ignore   0       0
    Ignore          Ignore
2   10.10.1.102     Ignore          Ignore Ignore   0       0
    255.255.255.255 Ignore
```

Figure 34 displays sample output from the `show qos ip-filter-sets` command.

Figure 34 `show qos ip-filter-sets` command output

```
470_24T#show qos ip-filter-sets
IP Filter Sets

Id        Name       Acl Id Ace Id Ace Order

___ ________________ ______ ______ _________
2   G1-ip            1      2      2
```

Figure 35 displays sample output from the `show qos l2-filters` command.

Figure 35 `show qos l2-filters` command output

```
470_24T#show qos l2-filters
Id  VLAN  VLAN Tag Ether   802.1p   DSCP  Protocol    Dest IP       Src IP
                   Type   Priority                    L4 Port       L4 Port
                                                     Min   Max     Min   Max

__ ______ ________ ______ ________ ______ ________ ______ ______ ______ ______
1  Ignore Ignore   Ignore          Ignore Ignore   Ignore Ignore Ignore Ignore
2  Ignore Ignore   0x800  Ignore   63     Ignore   Ignore Ignore Ignore Ignore
3  Ignore Ignore   Ignore          Ignore Ignore   Ignore Ignore Ignore Ignore
4  Ignore Ignore   Ignore 0,1,2,3, Ignore Ignore   Ignore Ignore Ignore Ignore
5  Ignore Ignore   0x800           1      Ignore   Ignore Ignore Ignore Ignore
470_24T#
```

Figure 36 displays sample output from the `show qos l2-filter-sets` command.

Figure 36 `show qos l2-filter-sets` command output

```
470_24T#show qos l2-filter-sets
Layer2 Filter Sets

Id        Name         Acl Id Ace Id Ace Order

___ ________________ ______ ______ _________
1   fGrp1            1      1      1
2   fGrp2            2      1      1
```

Figure 37 displays sample output from the `show qos actions` command. Each service class has a default action that uses default mappings.

Figure 37 `show qos actions` command output

```
470_24T#show qos actions
 Id          Name        Drop  Update      Set Drop      802.1p Priority
                               DSCP      Precedence

_____ ________________ _____ ______ __________________ _______________
65526 Drop_Traffic     True  Ignore Ignore             Ignore
65527 Standard_Service False 0x0    Not Loss Sensitive Priority 0
65528 Bronze_Service   False 0xA    Loss Sensitive     Priority 2
65529 Silver_Service   False 0x12   Loss Sensitive     Priority 3
65530 Gold_Service     False 0x1A   Loss Sensitive     Priority 4
65531 Platinum_Service False 0x22   Loss Sensitive     Priority 5
65532 Premium_Service  False 0x2E   Loss Sensitive     Priority 6
65533 Network_Service  False 0x30   Loss Sensitive     Priority 7
65534 Trusted_IP        False Ignore Use Egress Map     Use Egress Map
65535 Trusted_NonIP    False Ignore Ignore             Ignore
```

Figure 38 displays sample output from the `show qos meters` command. Each service class has a default meter that uses default actions and mappings.

Figure 38 `show qos meters` command output

```
470_48T#show qos meters
 Id       Name           Data     Commit  Commit    In-Profile Out-Profile
                         Spec      Rate    Burst    Action          Action
                                  (Kbps)  (Bytes)

_____ ________________ ______________________________________________
65526 Drop_Traffic     No Meter 0          0      Drop_Traffic
65527 Standard_Service No Meter 0          0      Standard_Servi
65528 Bronze_Service   No Meter 0          0      Bronze_Service
65529 Silver_Service   No Meter 0          0      Silver_Service
65530 Gold_Service     No Meter 0          0      Gold_Service
65531 Platinum_Service No Meter 0          0      Platinum_Servi
65532 Premium_Service  No Meter 0          0      Premium_Servic
65533 Network_Service  No Meter 0          0      Network_Servic
65534 Trusted_IP       No Meter 0          0      Trusted_IP
```

Figure 39 displays sample output from the `show qos shapers` command.

Figure 39 `show qos shapers` command output

```
470_24T#show qos shapers
Id         Name                Rate           Burst          Queue
                                              Size            Size
                              (Kbps)         (Bytes)        (Packets)

___  ____________________________  ___________ _______________
1          shaper1             64000          5555              2
```

Figure 40 displays sample output from the `show qos policies` command.

Figure 40 `show qos policies` command output

```
470_24T#show qos policies
Id     Name        Filter Set     Filter      Role         Order Type   Combination

___ ___________ ________________ ______ ______
1   wizardIP     wizardIP_FLTR     IP     allBPSIfcs     1
2   wizardL2     wizardL2_FLTR     L2     allBPSIfcs       2
Id Meter In-Profile   Out-of-Profile  Shaper Shaper  User Group
```

Figure 41 displays sample output from the `show qos queue-sets` command.

Figure 41 `show qos queue-sets` command output

```
470_24T#show qos queue-sets
Set Queue  General     Extended   Bandwidth Absolute   Bandwith  Service  Size
ID   ID   Discipline  Discipline    (%)     Bandwidth Allocation  Order  (Bytes)
                                            (Kbps)

___ _____ ___________ __________ _________ _________ __________ _______ _______
1   1     Priority     0.0        100       0          Relative   1       16384
1   2     Weight Round 0.0        50        0          Relative   2       24576
1   3     Weight Round 0.0        30        0          Relative   2       32768
1   4     Weight Round 0.0        20        0          Relative   2       32768
2   1     Priority     0.0        100       0          Relative   1       16384
2   2     Priority     0.0        100       0          Relative   2       16384
```

Figure 42 displays sample output from the `show qos queue-set-assignments` command.

Figure 42 `show qos queue-set-assignments` command output

```
470_24T#show qos queue-set-assignment
Queue Set 1

802.1p Priority Queue
_______________ _____
0               4
1               4
2               3
3               3
4               2
5               2
6               1
7               1
Queue Set 2

802.1p Priority Queue
_______________ _____
0               2
1               2
2               2
3               2
4               2
5               2
6               1
7               1
```

Figure 43 displays sample output from the `show qos agent` command.

Figure 43 `show qos agent` command output

```
470_24T#show qos agent
QoS Policy Server Control: Enabled
QoS Policy Agent Retry Timer: 5 seconds
Allow Packet Reordering: Enabled
Maintain Policing Statistics: Enabled
Interface Class Restrictions: Allow All Classes
```

Figure 44 displays sample output from the `show qos statistics` command.

Figure 44 `show qos statistics` command output

```
470_24T#show qos statistics
Id        Name          Packet    Overflow    Total      Total    InProfile
                       Hits      Packet     Octets     Overflow    Octets
                                 Hits                  Octets

___ ________________  __________ __________ __________ __________ __________
1   VLAN1_IP          85         0          9776       0          0
2   VLAN1             137        0          13178      0          0

Id    Overflow  OutProfile  Overflow   Shaping    Overflow   Percent
     InProfile    Octets   OutProfile  Q Drops    Shaping   OutProfile
       Octets                Octets               Q Drops     Octets

___  __________ __________ __________ __________ __________ __________
1    0          0          0          0          0          0 %
2    0          0          0          0          0          0 %
```

Resetting

You can reset the system to the factory defaults.

qosagent reset-default command

The `qosagent reset-default` command deletes all installed states and resets the system to factory default values. The syntax for the `qosagent reset-default` command is:

```
qosagent reset-default
```

The `qosagent reset-default` command is in the config mode.

The `qosagent reset-default` command has no parameters or variables.

Configuring COPS

You can enable COPS-PR, the dynamic management system, using the CLI. This section covers:

- "qosagent server-control command"
- "show cops retry command" on page 108
- "show cops server command" on page 108
- "show cops stats command" on page 109
- "cops retry command" on page 112
- "cops server command" on page 112
- "default cops retry command" on page 113
- "no cops server command" on page 114

qosagent server-control command

The `qosagent server-control` command enables COPS. The syntax for the `qosagent server-control` command is:

```
qosagent server-control {enable|disable} [retry-timer
<no-retry|1-86400>]
```

The `qosagent server-control` command is in the config mode.

Table 8 describes the parameters and variables for the `qosagent server-control` command.

Table 8 `qosagent server-control` command parameters and variables

Parameters and variables	Description
`enable|disable`	Enables COPS.

`retry-timer`
`<no-retry|1-86400>`
	Sets the value for the retry timer:
	• no retry—connection retry not attempted after a failed attempt
	• 1-86400—specifies the seconds between receipt of a connection termination/rejection notification and initiation of a new connection request

show cops retry command

The show cops retry command displays COPS TCP retry settings. The syntax for the show cops retry command is:

```
show cops retry
```

The show cops retry command is in the privExec mode.

The show cops retry command has no variables or parameters.

Figure 45 displays sample output from the show cops retry command.

Figure 45 show cops retry command output

```
470_24T#show cops retry
Retry Algorithm:  Sequential
Retry Count     :  1
Retry Interval :  100 seconds
```

show cops server command

The show cops server command displays configured COPS servers. The syntax for the show cops server command is:

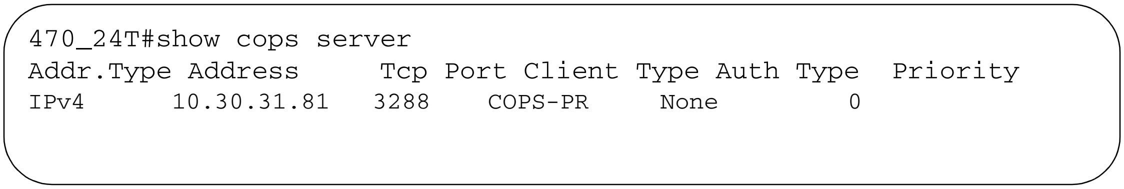
```
show cops server
```

The show cops server command is in the privExec mode.

The show cops server command has no variables or parameters.

Figure 46 displays sample output from the `show cops server` command.

Figure 46 `show cops server` command output



```
470_24T#show cops server
Addr.Type Address      Tcp Port Client Type Auth Type  Priority
IPv4      10.30.31.81   3288     COPS-PR     None          0
```

show cops stats command

The `show cops stats` command displays COPS statistics. The syntax for the `show cops stats` command is:

```
show cops stats
```

The `show cops stats` command is in the privExec mode.

The `show cops stats` command has no variables or parameters.

Figure 47 on page 110 and Figure 48 on page 111 display sample output from the `show cops stats` command.

Figure 47 `show cops stats` command output (1 of 2)

```
470_24T#show cops stats
---------------------------------------------
PDP IPv4 Address:             47.130.100.42
    TCP Port:                 3288
    Configuration Source:     Static
    Authentication Type:      None
    Last Connection Attempt:  5745
    TCP Connect Attempts:     12
    TCP Connect Failures:     12
    Connection State:            Invalid
    Keep-Alive Time:             0
    Accounting Time:             0
    Messages Received:           0
    Messages Sent:               0
    Messages Syntax Errors:      0
    Last Protocol Error:         <unknown>
    Open Attempts:               0
    Open Failures:               0
    Unsupported Client Types:    0
    Unsupported Versions:        0
    Length Mismatches:           0
    Unknown Opcodes:             0
    Unknown C-NUMs:              0
    Bad C-TYPEs:                 0
    Bad Sends:                   0
    Wrong Objects:               0
    Wrong Opcodes:               0
    Client Keep-Alive Timeouts:  0
    Authentication Failures:     0
    Authentication Missings:     0
---------------------------------------------
PDP IPv4 Address:             47.130.101.81
    TCP Port:                 3288
    Configuration Source:     Static
    Authentication Type:      None
    Last Connection Attempt:  6343
TCP Connect Attempts:     12
    TCP Connect Failures:     11
    Connection State:            Connected
    Keep-Alive Time:             120
    Accounting Time:             0
```

Figure 48 `show cops stats` command output (2 of 2)

```
Accounting Time:             0
   Messages Received:           21
   Messages Sent:               3
   Messages Syntax Errors:      0
   Last Protocol Error:         <unknown>
   Open Attempts:               0
   Open Failures:               0
   Unsupported Client Types:    0
   Unsupported Versions:        0
   Length Mismatches:           0
   Unknown Opcodes:             0
   Unknown C-NUMs:              0
   Bad C-TYPEs:                 0
   Bad Sends:                   0
   Wrong Objects:               0
   Wrong Opcodes:               0
   Client Keep-Alive Timeouts:  0
   Authentication Failures:     0
   Authentication Missings:     0
                Client Type:  COPS-PR
                        Connection State:            Accepted
                        Keep-Alive Time:             120
                        Accounting Time:             0
                        Messages Received:           15
                        Messages Sent:               16
                        Messages Syntax Errors:      0
                        Last Protocol Error:         <unknown>
                        Open Attempts:               1
                        Open Failures:               0
                        Unsupported Client Types:    0
                        Unsupported Versions:        0
                        Length Mismatches:           0
                        Unknown Opcodes:             0
                        Unknown C-NUMs:              0
                        Bad C-TYPEs:                 0
                        Bad Sends:                   0
                        Wrong Objects:               0
                        Wrong Opcodes:               0
                        Client Keep-Alive Timeouts:  0
                        Authentication Failures:     0
                        Authentication Missings:     0
```

cops retry command

The `cops retry` command sets the COPS TCP retry settings. The syntax for the `cops retry` command is:

```
cops retry <0-32> <1-600>
```

The `cops retry` command is in the config command mode.

Table 9 describes the parameters and variables for the `cops retry` command.

Table 9 `cops retry` command parameters and variables

Parameters and variables	Description
`retry` *<0-32> <1-500>*	Enter the number of retries and the retry interval (in seconds). Default is 10 seconds.

cops server command

The `cops server` command creates or modifies a COPS server configuration. The syntax for the `cops server` command is:

```
cops server <A.B.C.D> [tcp-port <0-65535>] [priority
<0-65535>]
```

The `cops server` command is in the config command mode.

Table 10 describes the parameters and variables for the `cops server` command.

Table 10 `cops server` command parameters and variables

Parameters and variables	Description
<A.B.C.D>	Enter the IP address of the COPS server you want to use.
`tcp-port` *<0-65535>*	Enter the number of the TCP port you want to use. The default port is 3288.
`priority` *<0-65535>*	Enter the priority you want this server to have. The default priority is 0.

default cops retry command

The `default cops retry` command restores the default COPS TCP retry settings. The syntax for the `default cops retry` command is:

```
default cops retry
```

The `default cops retry` command is in the config command mode.

The `default cops retry` command has no variables or parameters.

default cops server command

The `default cops server` command restores COPS TCP port and priority settings for a COPS server configuration. The syntax for the `default cops server` command is:

```
default cops server <A.B.C.D> [tcp-port] [priority]
```

The `default cops server` command is in the config command mode.

Table 11 describes the parameters and variables for the `default cops server` command.

Table 11 `default cops server` command parameters and variables

Parameters and variables	Description
<A.B.C.D>	Enter the IP address of the COPS server you want to use.
`tcp-port`	Restores the default TCP port. The default TCP port is 3288
`priority` *<0-65535>*	Restores the default priority. The default priority is 0.

no cops server command

The `no cops server` command removes a COPS server configuration. The syntax for the `no cops server` command is:

```
no cops server <A.B.C.D>
```

The `no cops server` command is in the config command mode.

Table 12 describes the parameters and variables for the `no cops server` command.

Table 12 `no cops server` command parameters and variables

Parameters and variables	Description
<A.B.C.D>	Enter the IP address of the COPS server you want to clear. Omitting this variable clears the entire COPS server table.

Configuring QoS interface groups

You can add or delete ports to or from an interface group, or add or delete the interface groups themselves. This section covers:

- "qos if-assign command"
- "qos if-group command" on page 115
- "qos if-assign-list command" on page 116

qos if-assign command

The `qos if-assign` command adds or deletes ports to or from a defined interface group. The syntax for the `qos if-assign` command is:

```
qos if-assign {del [portlist <portlist>]|add [port
<portlist>] name <tag>}
```

The `qos if-assign` command is in the config-if command mode.

Table 13 describes the parameters and variables for the `qos if-assign` command.

qos if-group command

Table 13 `qos if-assign` command parameters and variables

Parameters and variables	**Description**
`add|del`	Adds or deletes the port to or from the interface group.
`port <portlist>`	Enter the port(s) the port to add or delete to interface group. Note: If you omit this parameter, the system uses the port number specified when you issued the `interface` command.
`name <tag>`	Enter the name of the defined interface group.

The `qos if-group` command adds or deletes interface groups. The syntax for the `qos if-group` command is:

```
qos if-group name <tag> {create class <ifclass>|delete}
```

The `qos if-group` command is in the config command mode.

Table 14 describes the parameters and variables for the `qos if-group` command.

Table 14 `qos if-group` command parameters and variables

Parameters and variables	**Description**
`name <tag>`	Enter the name of the interface group with which you are working; maximum of 32 alphanumeric characters.
`create class <ifclass>`	Defines a new interface group and specifies the class of traffic received on interfaces associated with this interface group: • `trusted` • `untrusted` • `unrestricted`
`delete`	Deletes an existing interface group.

qos if-assign-list command

The `qos if-assign-list` command adds or deletes a list of ports to or from a defined interface group. The syntax for the `qos if-assign-list` command is:

```
qos if-assign-list {del portlist <portlist>|add portlist
<portlist> name <tag>}
```

The `qos if-assign-list` command is in the config-if command mode.

Table 15 describes the parameters and variables for the `qos if-assign-list` command.

Table 15 `qos if-assign-list` command parameters and variables

Parameters and variables	Description
`add|del`	Adds or deletes the port to or from the interface group.
`portlist <portlist>`	Enter the list of ports to add or delete to interface group. Note: If you omit this parameter, the system uses the port number specified when you issued the `interface` command.
`name <tag>`	Enter the name of the defined interface group.

Note: Before adding an interface to an interface group, you must delete the interface from its current interface group.

Note: You cannot delete interface groups that are referenced by an installed policy or associated with device interfaces.

qosagent class-restrictions command

The `qosagent class-restrictions` command restricts interfaces classes to all classes, trusted and unrestricted, or unrestricted-only. The syntax for the `qosagent class-restrictions` command is:

```
qosagent class-restrictions
{all-classes|trusted-and-unrestricted|unrestricted-only}
```

The `qosagent class-restrictions` command is in the config mode.

Table 16 describes the parameters and variables for the `qosagent class-restrictions` command.

Table 16 `qosagent class-restrictions` command parameters and variables

Parameters and variables	Description
<all-classes|trusted-and-unrestricted|unrestricted-only>	Sets the allowed interface class or classes.

Configuring DSCP and 802.1p and queue associations

You can configure the DSCP, IEEE 802.1p priority, and queue set association using the CLI. This section covers:

- "qos egressmap command"
- "qos ingressmap command" on page 118
- "qos queue-set-assignment command" on page 119

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 ds <dscp> 1p <ieee1p> dp <dropprec>
```

The `qos egressmap` command is in the config command mode.

Table 17 describes the parameters and variables for the `qos egressmap` command.

Table 17 `qos egressmap` command parameters and variables

Parameters and variables	Description
`ds <dscp>`	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 <ieee1p>`	Enter the 802.1p priority value associated with the DSCP; range is between 0 and 7.
`dp <dropprec>`	Enter the drop precedence values associated with the DSCP: • loss-sensitive • not-loss-sensitive

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 priority value in the received packet. The syntax for the `qos ingressmap` command is:

```
qos ingressmap 1p <ieee1p> ds <dscp>
```

The `qos ingressmap` command is in the config command mode.

Table 18 describes the parameters and variables for the `qos ingressmap` command.

Table 18 `qos ingressmap` command parameters and variables

Parameters and variables	Description
`1p <ieee1p>`	Enter the 802.1p priority value used as a lookup key for DSCP assignment at ingress when appropriate; range is between 0 and 7.
`ds <dscp>`	Enter the DSCP value associated with the 802.1p priority value; range is between 0 and 63.

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 <setid> 1p <ieee1p>
queue <qid>
```

The `qos queue-set-assignment` command is in the config command mode.

Table 19 describes the parameters and variables for the `qos queue-set-assignment` command.

Table 19 `qos queue-set-assignment` command parameters and variables

Parameters and variables	**Description**
`queue-set <setid>`	Enter the queue set ID.
`1p <ieee1p>`	Enter the 802.1p priority value for which the queue association is being modified; range is between 0 and 7.
`queue <qid>`	Enter the queue **within** the identified queue set to assign the 802.1p priority traffic at egress.

Configuring QoS filters and filter groups

You can configure filters and filter sets using the CLI. This section covers:

- "qos ip-filter command" on page 120
- "qos ip-filter-set command" on page 121
- "qos l2-filter command" on page 122
- "qos l2-filter-set command" on page 123

qos ip-filter command

The `qos ip-filter` command adds or deletes IP filters. The syntax for the `qos ip-filter` command is:

```
qos ip-filter <fid> {create [src-ip <src-ip-info>] [dst-ip
<dst-ip-info>] [ds-field <dscp>] [protocol <protocoltype>]
[src-port <port>] [dst-port <port>]|delete}
```

The `qos ip-filter` command is in the config command mode.

Table 20 describes the parameters and variables for the `qos ip-filter` command.

Table 20 `qos ip-filter` command parameters and variables

Parameters and variables	Description
`<fid>`	Enter an integer to specify the filter ID.
`create`	Defines a new IP filter with the specified filter ID.
`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. Default is 0.0.0.0.
`dst-ip <dst-ip-info>`	Enter the destination IP address and mask in the form of a.b.c.d/x or a.b.c.d x.x.x.x. Default is 0.0.0.0.
`ds-field <dscp>`	Enter 6-bit DSCP value; range is 0 to 63. Default is ignore.
`protocol <protocoltype>`	Enter the protocol type: • ignore • icmp • tcp • udp Default is ignore.
`src-port <port>`	Enter TCP/UDP source port value. Default is ignore.
`dst-port <port>`	Enter TCP/UDP destination port value. Default is ignore.
`delete`	Deletes the IP filter with the specified filter ID.

Note: If you omit any parameter, the default value is used..

qos ip-filter-set command

The `qos ip-filter-set` command adds or deletes currently defined IP filters into an IP filter set. The syntax for the `qos ip-filter-set` command is:

```
qos ip-filter-set <fgid> {create set <setid> [name
<setname>] filter <fid> filter-prec <prec>|delete}
```

The `qos ip-filter-set` command is in the config command mode.

Table 21 describes the parameters and variables for the `qos ip-filter-set` command.

Table 21 `qos ip-filter-set` command parameters and variables

Parameters and variables	Description
`<fgid>`	Enter an integer to specify the filter group ID; range is 1 to 65535.
`create set <setid>`	Initiates creation of an IP filter set with the designated filter set ID. Enter the IP filter set ID; range is 1 to 65535
`name <setname>`	Assigns a name to the designated filter set ID. Enter the name for the filter set; maximum is 16 alphanumeric characters
`filter <fid>`	Adds an IP filter to the filter set; range is 1 to 65535.
`filter-prec <prec>`	Specifies the precedence, or filter evaluation order, within the set. Enter the precedence value you want for this filter; range is 1 to 65535.
`delete`	Deletes the IP filter set.

Note: You must define the filter before adding it to a filter set.
You cannot delete an IP filter set that is referenced in an installed policy.
You cannot delete the last IP filter in an IP filter set that is referenced in an installed policy.

qos l2-filter command

The `qos l2-filter` command adds and deletes Layer 2 (L2) filters. The syntax for the `qos l2-filter` command is:

```
qos l2-filter <fid> {create [ethertype <etype>]
[vlan <vidlist>] [vlan-tag <vtag>] [priority <ieee1p-seq>]
[ds-field <dscp>] [protocol <protocoltype>] [src-port-min
<port> src-port-max <port>] [dst-port-min <port>
dst-port-max <port>]|delete}
```

The `qos l2-filter` command is in the config mode.

Table 22 describes the parameters and variables for the `qos l2-filter` command.

Table 22 `qos l2-filter command` parameters and variables

Parameters and variables	Description
`<fid>`	Enter an integer to specify the filter ID; range is 1 to 65535.
`create`	Defines a new L2 filter with the specified filter ID.
`ethertype <etype>`	Enter the Ethernet type in the form of 0xXXXX, for example, 0x0801. Default is ignore.
`vlan <vidlist>`	Enter the number of the VLAN IDs, separated by commas. (Format: VLAN x-x, x, x) Default is ignore.
`vlan-tag <vtag>`	Enter the type of VLAN tagging filter you want: • tagged • untagged • ignore Default is ignore.
`priority <ieee1p-seq>`	Enter the 802.1p priority values; range from 0 to 7. Enter in the form of [a(,b)*(c-d)*], for example, 0, 3-4, 7. Default is ignore.
`ds-field <dscp>`	Enter a 6-bit value for the DS field; range is from 0 to 63. Default is ignore.

Table 22 `qos l2-filter command` parameters and variables (Continued)

Parameters and variables	Description
`protocol <protocoltype>`	Enter the protocol type: • ignore • icmp • tcp • udp Default is ignore.
`src-port-min <port>`	Enter the TCP/UDP minimum source port value; range is 0 to 65535. Default is 0 = ignore.
`src-port-max <port>`	Enter the TCP/UDP maximum source port value; range is 0 to 65535. Default is 65535 = ignore.
`dst-port-min <port>`	Enter the TCP/UDP minimum destination port value; range is 0 to 65535. Default is 0 = ignore.
`dst-port-max <port>`	Enter the TCP/UDP maximum destination port value; range is 0 to 65535. Default is 65535 = ignore.
`delete <fid>`	Enter the filter ID you want to delete.

Note: If you omit any parameter, the default value is used. You cannot delete a filter that is referenced by an L2 filter set.

qos l2-filter-set command

The `qos l2-filter-set` command adds and deletes Layer 2 filters into an L2 filter set. The syntax for the `qos l2-filter-set` command is:

```
qos l2-filter-set <fgid> {create set <setid> [name
<setname>] filter <fid> filter-prec <prec>|delete}
```

The `qos l2-filter-set` command is in the config command mode.

Table 23 describes the parameters and variables for the `qos l2-filter-set` command.

Table 23 `qos l2-filter-set` command parameters and variables

Parameters and variables	Description
`<fgid>`	Enter an integer to specify the filter group ID with which you want to work; range is 1 to 65535.
`create set <setid>`	Initiates creation of an L2 filter set with the designated filter set ID. Enter the IP filter set ID; range is 1 to 65535.
`name <setname>`	Assigns a name to the designated filter set ID. Enter the name for the filter set; maximum is 16 alphanumeric characters.
`filter <fid>`	Adds an L2 filter to the filter set; range is 1 to 65535.
`filter-prec <prec>`	Specifies the precedence, or filter evaluation order, within the set. Enter the precedence value you want for this filter; range is 1 to 65535.
`delete`	Deletes the L2 filter set.

→ You must define the filter before adding it to a filter set. You cannot delete an L2 filter set that is referenced in an installed policy. You cannot delete the last L2 filter in an L2 filter set that is referenced in an installed policy.

Layer 2 restricted QoS meters

With restricted meters, you are allowed a maximum of 23 Layer 2 metered policies. All 23 metered policies can have a different in-profile-action, but they all share the same out-of-profile action. The first policy created consumes two filters; one filter is consumed for the in-profile action, and another filter is consumed for the out-of-profile action. Subsequent restricted Layer 2 metered policies use only one filter for the in-profile-action and they share the out-of-profile action defined by the first filter. Since only one filter is used for each policy, statistics count only in-profile traffic.

Restricted meters can be used only when the Interface Class Restriction is set to Unrestricted Only.

Configuring QoS actions

You can configure QoS actions, which directs the Ethernet Switch 470 to take specific action on each packet, using the CLI.

qos action command

The `qos action` command creates or deletes a QoS action. The syntax for the `qos action` command is:

```
qos action <actid> [name <actname>] [drop-action
{enable|disable}] [update-dscp <dscp>] [update-1p
{<ieee1p>|default|use-egress-map}] [set-drop-prec
{loss-sensitive|not-loss-sensitive|default|use-egress-map}]
```

The `qos action` command is in the config mode.

Table 24 describes the parameters and variables for the `qos action` command.

Table 24 `qos action` command parameters and variables

Parameters and variables	Description
`<actid>`	Enter an integer to specify the QoS action; range is 1 to 65535.
`name <actname>`	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}`	Specifies whether packets are dropped or not; the drop action equals enable. Default is disable.
`update-dscp <dscp>`	Specifies whether DSCP value is updated or left unchanged; unchanged equals ignore. Enter the 6-bit DSCP value you want; range is 0 to 63. Default is ignore.

Table 24 `qos action` command parameters and variables (Continued)

Parameters and variables	Description
`update-1p`	Specifies whether 802.1p priority value is updated or left unchanged; unchanged equals ignore: • ieee1p—enter the value you want; range is 0 to 7 • default—allows the value to be derived based on assignment of other action parameters • use-egress-map—uses the egress map to assign value Default is ignore.
`set-drop-prec {loss-sensitive| not-loss-sensitive| default| use-egress-map}`	Enter the loss-sensitivity value you want: • loss-sensitive • not-loss-sensitive • default • use-egress-map Default is ignore.

Note: Certain options can be restricted based on the policy associated with the specific action.
You cannot delete an action that is referenced in an installed policy.

Configuring QoS meters

Using the CLI, you set meters. If you want to meter, or police, the traffic, configure the committed rate, burst rate, and burst duration. If you are not metering data, skip this page.

qos meter command

The `qos meter` command creates or deletes a QoS meter. The syntax for the `qos meter` command is:

```
qos meter <metid> {create [name <metname>] committed-rate
<rate> max-burst-rate <burstrate> [max-burst-duration
<burstdur>]|delete}
```

The `qos meter` command is in the config command mode.

Table 25 describes the parameters and variables for the `qos meter` command.

Table 25 `qos meter` command parameters and variables

Parameters and variables	Description
`<metid>`	Enter an integer to specify the QoS meter; range is 1 to 65535.
`name <metname>`	Assigns a name to the QoS meter with the designated meter ID. Enter name for meter; maximum is 16 alphanumeric characters.
`committed-rate <rate>`	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; range is 1 to 65535 Kb/s.
`max-burst-rate <burstrate>`	Specifies the largest burst of traffic that can be received at a given time for the traffic to be considered in-profile. Used in calculating the committed burst size. Enter the burst rate in Kb/s for in-profile traffic; range is 1 to 65535 Kb/s.
`max-burst-duration <burstdur>`	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 65535 ms.
`delete`	Deletes the specified meter.

The formula for the Committed Burst Size (in bytes) is:

Committed Burst Size = [(max-burst-duration) * (max-burst-rate - committed rate)]/8

Where:

Committed Burst Size is rounded up to one of the following values:

2047, 4095, 8191, 16383, 32767, 65535, 131071

Note: You cannot delete a meter that is referenced in an installed policy.

Configuring QoS shapers

Note: You must be using the Ethernet Switch 470-24T GBIC in order to implement the QoS shaping features.

Using the CLI, you set shapers. If you want to shape traffic at the egress point, configure the committed rate, burst rate, burst duration, and queue depth for each shaper.

qos shaper command

The `qos shaper` command creates or deletes a QoS shaper. The syntax for the `qos shaper` command is:

```
qos shaper <shapeid> {create [name <shapername>] shape-rate
<rate> max-burst-rate <burstrate> [max-burst-duration
<burstdur>] queue-size <1|2|4|8|16>|delete}
```

The `qos shaper` command is in the config command mode.

Table 26 describes the parameters and variables for the `qos shaper` command.

Table 26 `qos shaper` command parameters and variables

Parameters and variables	Description
<shapeid>	Enter an integer to specify the QoS shaper; range is 1 to 65535.
name *<shapername>*	Assigns a name to the QoS shaper with the designated shaper ID. Enter name for shaper; maximum is 16 alphanumeric characters.
shape-rate *<rate>*	Specifies maximum rate that traffic is transmitted over a given duration Enter the rate in Kbps; range is 1 to 42949672955 Kbps. Note: You must specify a value that is a multiple of 64 Kbps; 0 is invalid.
max-burst-rate *<burstrate>*	Specifies the largest burst of traffic that can be transmitted without a shaping delay. Used in calculating the committed burst size. Enter the burst rate in Kbps; range is 0 to 42949672955 kbps.
max-burst-duration *<burstdur>*	Specifies the amount of time that the largest burst of traffic can be transmitted without a shaping delay. Enter the burst duration in ms; range is 0 to 42949672955 ms.

Table 26 `qos shaper` command parameters and variables (Continued)

Parameters and variables	Description
`queue-size <1|2|4|8|16>`	Specifies the number of packets that can exceed the largest burst of traffic allowed and still be queued for transmission.
`delete`	Deletes the specified shaper.

The formula for the Committed Burst Size (in bytes) is:

Committed Burst Size = (max-burst-duration * (max-burst-rate - shape rate))/8

Where:

Committed Burst Size is rounded up to one of the following values:

2047, 4095, 8191, 16383, 32767, 65535

➡ You cannot delete a shaper that is referenced in an installed policy.

Gathering QoS statistics

You can gather statistics on QoS, such as the number of in-profile octets and out-of-profile octets. These statistics can serve as an important method to evaluate the effectiveness of the installed policies. However, tracking these statistics requires additional system resources, which limits the number of filters for classification.

qosagent police-statistics command

The `qosagent police-statistics` command gathers traffic policing, or metering, statistics. The syntax for the `qosagent police-statistics` command is:

```
qosagent police-statistics {enable|disable}
```

The `qosagent police-statistics` command is in the config command mode.

Table 27 describes the parameters and variables for the `qosagent police-statistics` command.

Table 27 `qosagent police-statistics` command parameters and variables

Parameters and variables	Description
`enable|disable`	Set policing statistics to: • Enable—statistics are tracked by default for all policies defined after this command is issued. • Disable—disables tracking statistics for policies defined after this command is issued.

Configuring QoS policies

You configure QoS policies using the CLI.

qos policy command

The `qos policy` command creates or deletes a QoS policy. The syntax for the `qos policy` command is:

```
qos policy <polid> {create [name <polname>]
if-group <ifgroup> filter-set-type {ip|l2}
{filter-set <setid>|filter-set-name <setname>}
{{in-profile-action <actid>|in-profile-action-name
<actname>}|
{{meter <metid>|meter-name <metname>}
{in-profile-action <actid>|in-profile-action-name <actname>}
{out-profile-action <actid>|out-profile-action-name
<actname>}}}
[shaper <shapeid>|shaper-name <shapename>]
[shaper-group <shapegroup>]
order <order>|delete|enable|disable}
```

The `qos policy` command is in the config command mode.

Table 28 describes the parameters and variables for the `qos policy` command.

Table 28 `qos policy` command parameters and variables

Parameters and variables	Description
`<polid>`	Enter an integer to specify the QoS policy; range is 1 to 65535.
`create`	Creates the QoS policy.
`name <polname>`	Assigns a name to the QoS policy with the designated policy ID. Enter the name for the policy; maximum is 16 alphanumeric characters.
`if-group <ifgroup>`	Enter the interface group name to which this policy applies.
`filter-set-type {ip|l2}`	Enter the type of filter set associated with this policy: • ip—specifies IP filter set • l2—specifies Layer 2 filter set
`filter-set <setid>`	Enter the filter set ID associated with this policy; range is 1 to 65535.
`filter-set-name <setname>`	Enter the name of the filter set associated with this policy.
`in-profile-action <actid>`	Enter the action ID for in-profile traffic; range is 1 to 65535.
`in-profile-action-name <actname>`	Enter the action name for in-profile traffic; maximum is 16 alphanumeric characters.
`meter <metid>`	Enter meter ID associated with this policy; range is 1 to 65535.
`meter-name <metname>`	Enter the meter name associated with this policy; maximum of 16 alphanumeric characters.
`in-profile-action <actid>`	Enter the action ID for in-profile traffic; range is 1 to 65535.
`in-profile-action-name <actname>`	Enter the action name for in-profile traffic; maximum is 16 alphanumeric characters.
`out-profile-action <actid>`	Enter the action ID for out-of-profile traffic; range is 1 to 65535.
`out-profile-action -name <actname>`	Enter the action name for in-profile traffic; maximum is 16 alphanumeric characters.
`shaper <shapeid>`	Enter shaper ID associated with this policy; range is 1 to 65535.
`shaper-name <shapername>`	Enter the shaper name associated with this policy; maximum of 16 alphanumeric characters.
`shaper-group <shapegroup>`	Enter shaper group ID associated with this policy; range is 2 to 63.

Table 28 `qos policy` command parameters and variables (Continued)

Parameters and variables	Description
`order <order>`	Specifies the evaluation order of this policy in relation to other policies associated with the same interface group. Enter order number; range is 1 to 65535. Note: Policies with a lower order value are evaluated before policies with a higher order number. Evaluation goes from lowest value to highest.
`delete`	Deletes the specified QoS policy.
`enable|disable`	Enables or disables the specified QoS policy.

You must define all components associated with a policy, including the interface group, filter set, meter, and shaper before referencing those components with a policy.

Displaying QoS user roles

You can display QoS user roles using the CLI.

show qos user-role command

The `show qos user-role` command displays defined QoS user roles.

The syntax for the `show qos user-role` command is:

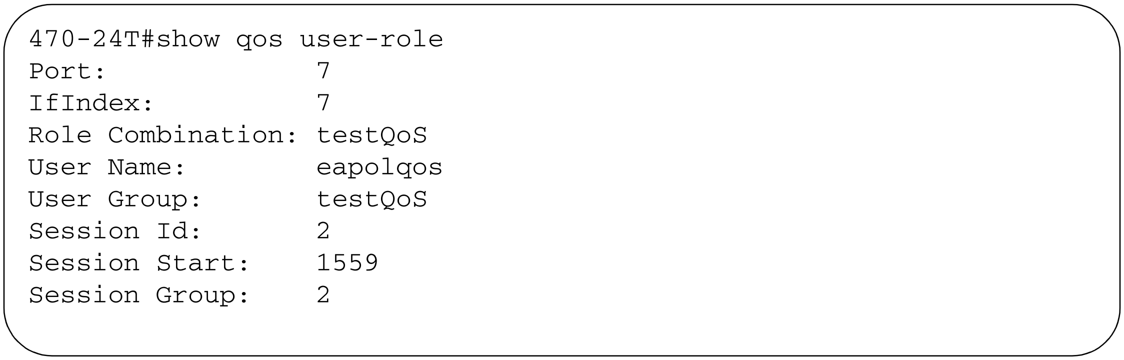
```
show qos user-role
```

The `show qos user-role` command is in the privExec command mode.

The `show qos user-role` command has no variables or parameters.

Figure 49 displays a sample output from the `show qos user-role` command.

Figure 49 `show qos user-role` command output



```
470-24T#show qos user-role
Port:              7
IfIndex:           7
Role Combination:  testQoS
User Name:         eapolqos
User Group:        testQoS
Session Id:        2
Session Start:     1559
Session Group:     2
```

Reordering packets

Support for certain per-hop behaviors (PHBs) requires packets within a flow be reordered upon transmission. Using the CLI, you can assign packets to specified egress queues.

qosagent packet-reordering command

The `qosagent packet-reordering` command allows you to reorder packets for transmission. The syntax for the `qosagent packet-reordering` command is:

```
qosagent packet-reordering {enable|disable}
```

The `qosagent packet-reordering` command is in the config command mode.

Table 29 describes the parameters and variables for the `qosagent packet-reordering` command.

Table 29 `qosagent packet-reordering` command parameters and variables

Parameters and variables	Description
`enable|disable`	Set packet-reordering to: • Enable—allows full flexibility in terms of the egress queue to which a packet is assigned. • Disable—the system verifies that in-profile and out-of-profile actions associated with a flow will not cause packets from the same flow to be assigned to different egress queues.

Interface Class Restrictions

qosagent class restrictions command

The `qosagent class restrictions` command allows you to set restrictions for each type of qosagent. The syntax for the `qosagent class restrictions` command is:

```
qosagent class-restrictions {all
classes|trusted-and-untrusted| unrestricted only}
```

User-based policies

This feature allows user-specific QoS policy information to be manipulated based on the presence, or lack thereof, of a specific network user. User information is retrieved from the RADIUS Server during EAP authentication and passed to the QoS Agent. The QoS Agent, in turn, notifies OPS of the user's presence if the policy server is currently in-charge of policy configuration. OPS can then download policy components to the device that is associated with the user. The User Based Policies (UBP) components are automatically deleted when the user logs off or is no longer authenticated.

This feature adds an ON/OFF attribute to the console interface to enable/disable UBP support. For SNMP support, an Enterprise-specific MIB is added. CLI support is similar to other EAP configuration. This attribute is presently not supported from the Web-based management interface.

eapol user-based-policies enable command

The `eapol user-based-policies enable` command enables user-based-policies. RADIUS must be configured prior to enabling user-based-policies. The syntax for user-based-policies is:

```
eapol user-based-policies enable
```

no eapol user-based-policies enable command

The `no eapol user-based-policies enable` command disables user-based-policies. The syntax for no eapol user-based-policies enable is:

```
no eapol user-based-policies enable
```

default eapol user-based-policies enable command

The `default eapol user-based-policies enable` command sets user-based-policies to the default setting. The default setting for user-based-policies is disabled. The syntax for the default `eapol user-based-policies enable` command is:

```
default eapol user-based-policies enable
```

show eapol command

The `show eapol` command shows whether user-based-policies are enabled or disabled. The syntax for `show eapol` is:

```
show eapol
```

The `show eapol` command is in the privExec mode.

The show eapol command has no variables or parameters.

Figure 50 displays sample output from the show eapol command.

Figure 50 show eapol command output

```
460_24T_PWR#show eapol
EAPOL Administrative State:  Disabled
EAPOL User-Based Policies :  Disabled
     Admin         Admin Oper ReAuth ReAuth Quiet  Xmit   Supplic Server  Max
Port Status   Auth Dir   Dir  Enable Period Period Period Timeout Timeout Req
---- -------- ---- ----- ---- ------ ------ ------ ------ ------- ------- ---
1    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
2    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
3    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
4    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
5    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
6    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
7    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
8    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
9    F Auth   Yes  Both  Both No     3600   60     30     30      30      2
10   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
11   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
12   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
13   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
14   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
15   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
16   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
17   F Auth   Yes  Both  Both No     3600   60     30     30      30      2
----More ----
```

Chapter 3
Configuring QoS using Device Manager

This chapter describes using Device Manager to manage Quality of Service (QoS) parameters on your Ethernet Switches 460 and 470. Additionally, this chapter describes using Common Open Policy Services (COPS). It includes the following sections:

- "Managing interface groups"
- "Managing QoS rules" on page 150
- "Managing QoS actions, meters, shapers, policies, and user roles" on page 160
- "QoS agent" on page 175
- "COPS" on page 178

Managing interface groups

You can display interface queues and groups.

This section contains the following topics:

- "Displaying interface queues" on page 138
- "Displaying interface groups" on page 139
- "Assigning ports to an interface group" on page 140
- "Deleting ports from an interface group" on page 141
- "Adding interface groups" on page 142
- "Deleting interface groups" on page 143
- "Displaying interface IDs" on page 143
- "Displaying priority queue assignments" on page 145
- "Displaying priority queue assignments" on page 145

- "Displaying priority mapping" on page 147
- "Displaying DSCP mappings" on page 148

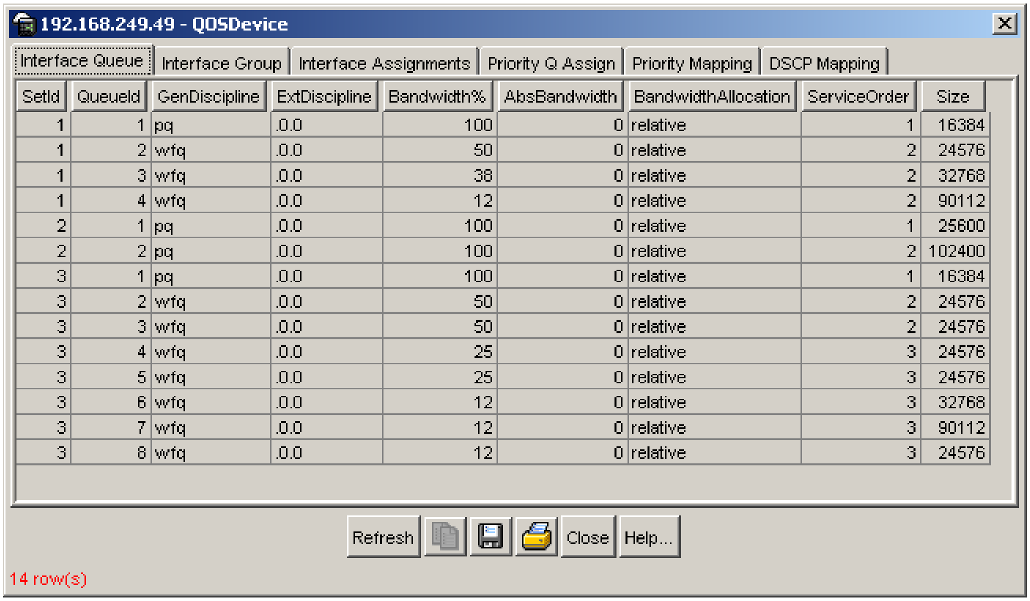
Displaying interface queues

To display interface queues:

➨ From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 51).

Figure 51 Interface Queue tab



SetId	QueueId	GenDiscipline	ExtDiscipline	Bandwidth%	AbsBandwidth	BandwidthAllocation	ServiceOrder	Size
1	1	pq	.0.0	100	0	relative	1	16384
1	2	wfq	.0.0	50	0	relative	2	24576
1	3	wfq	.0.0	38	0	relative	2	32768
1	4	wfq	.0.0	12	0	relative	2	90112
2	1	pq	.0.0	100	0	relative	1	25600
2	2	pq	.0.0	100	0	relative	2	102400
3	1	pq	.0.0	100	0	relative	1	16384
3	2	wfq	.0.0	50	0	relative	2	24576
3	3	wfq	.0.0	50	0	relative	2	24576
3	4	wfq	.0.0	25	0	relative	3	24576
3	5	wfq	.0.0	25	0	relative	3	24576
3	6	wfq	.0.0	12	0	relative	3	32768
3	7	wfq	.0.0	12	0	relative	3	90112
3	8	wfq	.0.0	12	0	relative	3	24576

14 row(s)

Table 30 describes the Interface Queue tab fields.

Table 30 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.
GenDiscipline	Displays the paradigm used to empty the queue: • other-Refer to ExtDiscipline • fifo-first in, first out queuing • pq-priority queuing • fq-fair queuing (round-robin) • wfq-weighted fair queuing
ExtDiscipline	Displays the queuing discipline that is associated with the specified queue. This attribute provides a means to add more queuing mechanisms.
Bandwidth%	Displays relative bandwidth available to a given queue with respect to other associated queues.
AbsBandwidth	Displays absolute bandwidth available to this queue, in Kb/s.
BandwidthAllocation	Displays bandwidth allocation: relative or absolute.
ServiceOrder	Displays the order in which a queue is serviced based on the defined discipline.
Size	Displays the size of the queue in bytes.

Displaying interface groups

To display interface groups:

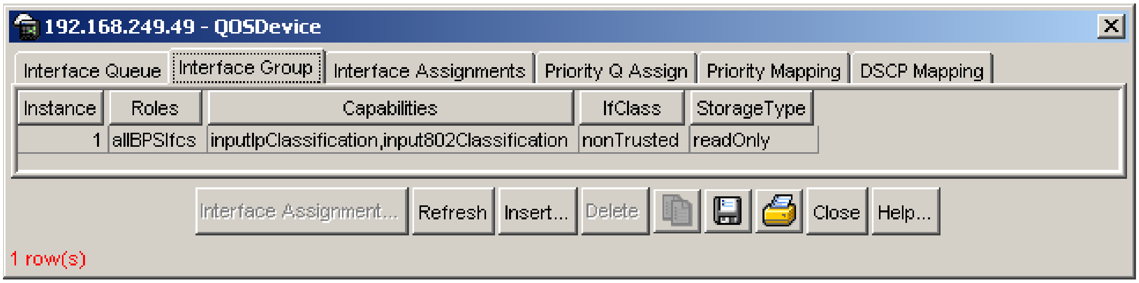
1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 51 on page 138).

2 Click the Interface Group tab.

The Interface Group tab opens (Figure 52).

Figure 52 Interface Group tab



Instance	Roles	Capabilities	IfClass	StorageType
1	allBPSIfcs	inputIpClassification,input802Classification	nonTrusted	readOnly

1 row(s)

Table 31 describes the Interface Group tab fields.

Table 31 Interface Group tab fields

Field	Description
Id	Displays a unique identifier of an interface group.
Roles	Displays 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	Displays 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	Displays the type of traffic received on interfaces associated with the specified role combination.
StorageType	Displays storage type for this interface group: • Volatile • nonVolatile (default) • readOnly

Assigning ports to an interface group

To assign ports to an interface group:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 51).

2 Click the Interface Group tab.

The Interface Group tab opens (Figure 52 on page 140).

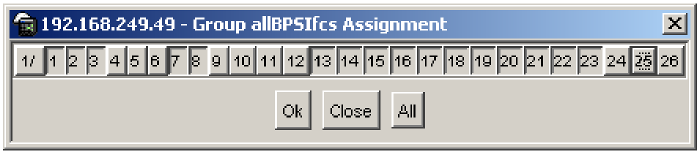
3 Highlight the interface group to which you want to add ports.

The Interface Assignment button appears on the bottom of the tab.

4 Click Interface Assignment.

The Group Assignment dialog box opens (Figure 53).

Figure 53 Group Assignment dialog box



5 Click the port numbers you want to add to the interface group.

6 Click OK.

Note: Adding or deleting a number of ports can take a long time, and can cause the Device Manager to time out.

Deleting ports from an interface group

To remove ports from an interface group:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 51 on page 138).

2 Click the Interface Group tab.

The Interface Group tab opens (Figure 52 on page 140).

3 Highlight the interface group from which you want to delete ports.

The Interface Assignment button appears on the bottom of the tab.

4 Click Interface Assignment.

The Group Assignment dialog box opens (Figure 53 on page 141).

5 Click the port numbers you want to delete from the interface group.

6 Click OK.

Adding interface groups

To add an interface group:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 51 on page 138).

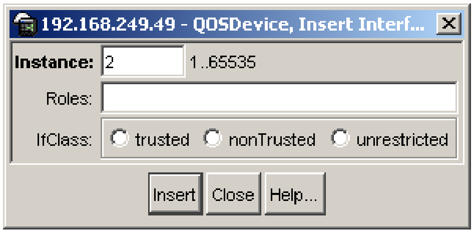
2 Click the Interface Group tab.

The Interface Group tab opens (Figure 52 on page 140).

3 Click Insert.

The Insert Interface Group dialog box opens (Figure 54).

Figure 54 Insert Interface Group dialog box



192.168.249.49 - QOSDevice, Insert Interf...

Instance: 2 1..65535

Roles:

IfClass: ○ trusted ○ nonTrusted ○ unrestricted

4 Enter the unique identifier you want for this Interface Group; range is 1 to 65535.

5 Enter the Role combination tag you want for this Interface Group.

6 Choose the interface class you want for this interface group: trusted, nonTrusted, or unrestricted.

7 Click Insert.

Deleting interface groups

To delete an interface group:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 51 on page 138).

2 Click the Interface Group tab.

The Interface Group tab opens (Figure 52 on page 140).

3 Highlight the interface group you want to delete.

4 Click Delete.

➡ **Note:** You cannot delete an interface group that is referenced by a policy. You must first delete the policy. You also cannot delete an interface group that has ports assigned to it.

You can display the association between interfaces, role combinations, and queue sets. A role combination is a unique label that identifies a group of interfaces.

Displaying interface IDs

To display the interface ID:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

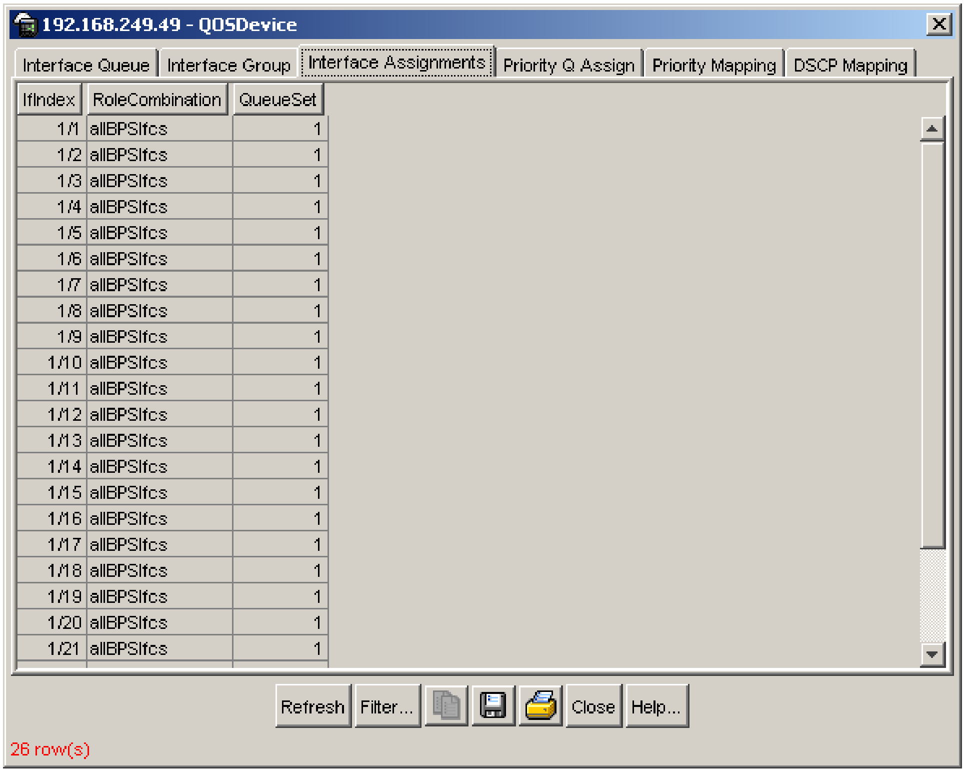
The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 51 on page 138).

2 Click the Interface Assignments tab.

The Interface Assignments tab opens (Figure 55 on page 144).

The table can take some time to fill; you can interrupt the process by clicking the Stop button. The Stop button disappears when the table is complete.

Figure 55 Interface Assignments tab



IfIndex	RoleCombination	QueueSet
1/1	allBPSIfcs	1
1/2	allBPSIfcs	1
1/3	allBPSIfcs	1
1/4	allBPSIfcs	1
1/5	allBPSIfcs	1
1/6	allBPSIfcs	1
1/7	allBPSIfcs	1
1/8	allBPSIfcs	1
1/9	allBPSIfcs	1
1/10	allBPSIfcs	1
1/11	allBPSIfcs	1
1/12	allBPSIfcs	1
1/13	allBPSIfcs	1
1/14	allBPSIfcs	1
1/15	allBPSIfcs	1
1/16	allBPSIfcs	1
1/17	allBPSIfcs	1
1/18	allBPSIfcs	1
1/19	allBPSIfcs	1
1/20	allBPSIfcs	1
1/21	allBPSIfcs	1

26 row(s)

Table 32 describes the Interface Assignments tab fields.

Table 32 Interface Assignments tab fields

Field	Description
IfIndex	Displays ports numbers.
RoleCombination	Displays the role combination associated with the interface.
QueueSet	Displays the queue set associated with this interface.

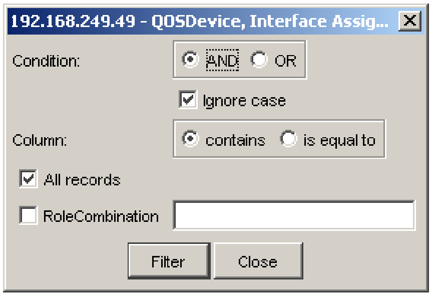
Displaying selected portions of the Interface Assignments table

To display only selected portions of the Interface Assignments table:

1 From the Interface Assignments tab, click Filter.

The QOSDevice, Interface Assignment Filter dialog box opens (Figure 56).

Figure 56 QOSDevice, Interface Assignment Filter dialog box



192.168.249.49 - QOSDevice, Interface Assig...

Condition: ● AND ○ OR

☑ Ignore case

Column: ● contains ○ is equal to

☑ All records

□ RoleCombination

2 Enter the information you want to use for this filter.

3 Click Filter.

Displaying priority queue assignments

To display priority queue assignments:

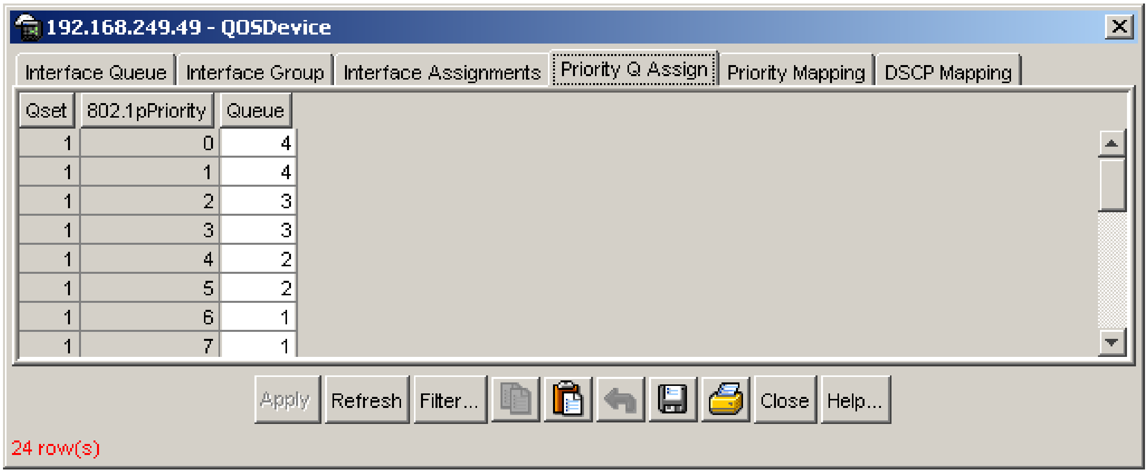
1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 51 on page 138).

2 Click the Priority Q Assign tab.

The Priority Q Assign tab opens (Figure 57 on page 146).

Figure 57 Priority Q Assign tab



Qset	802.1pPriority	Queue
1	0	4
1	1	4
1	2	3
1	3	3
1	4	2
1	5	2
1	6	1
1	7	1

24 row(s)

Table 33 describes the Priority Q Assign tab fields.

Table 33 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 eight instances of this class for each supported queue set.
802.1pPriority	A 802.1 user priority value.
Queue	A queue in a specified queue set that is assigned a priority value. To change a Queue assignment, click in the cell and type a new value.

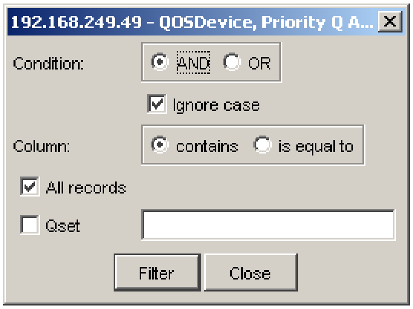
Displaying selected portions of table

To add display only selected portions of the Priority Q Assign table:

1 From the Priority Q Assign tab, click Filter.

The QOSDevice, Priority Q Assignment Filter dialog box opens (Figure 58 on page 147).

Figure 58 QOSDevice, Priority Q Assignment Filter dialog box



192.168.249.49 - QOSDevice, Priority Q A...

Condition: ● AND ○ OR

☑ Ignore case

Column: ● contains ○ is equal to

☑ All records

□ Qset

2 Enter the information you want to use for this filter.

3 Click Filter.

Displaying priority mapping

To display priority mapping:

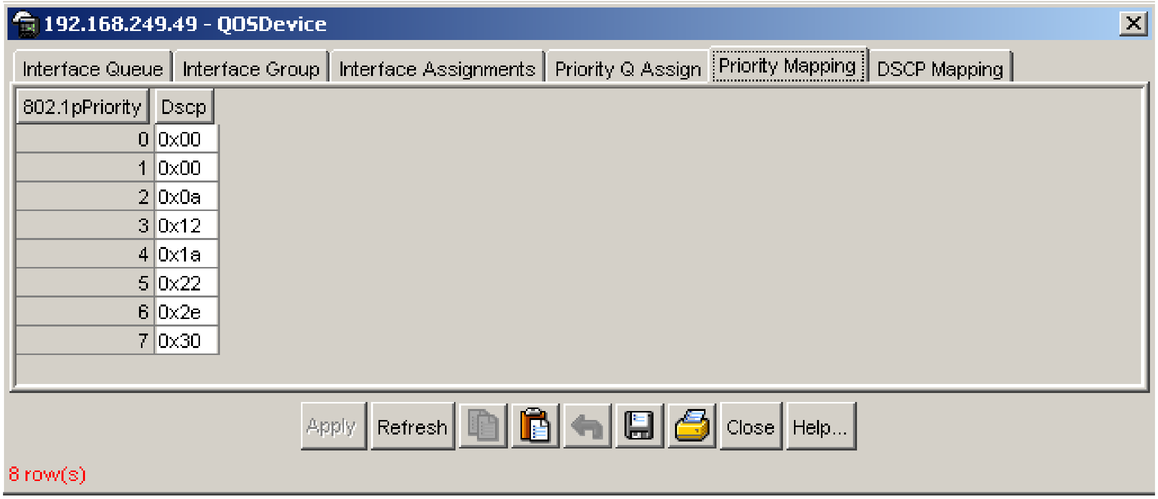
1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 51 on page 138).

2 Click the Priority Mapping tab.

The Priority Mapping tab opens (Figure 59 on page 148).

Figure 59 Priority Mapping tab



802.1pPriority	Dscp
0	0x00
1	0x00
2	0x0a
3	0x12
4	0x1a
5	0x22
6	0x2e
7	0x30

8 row(s)

Table 34 describes the Priority Mapping tab fields.

Table 34 Priority Mapping tab fields

Field	Description
802.1pPriority	A 802.1 user priority value to map to a DSCP value at ingress.
Dscp	A 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.

Displaying DSCP mappings

To display DSCP mappings:

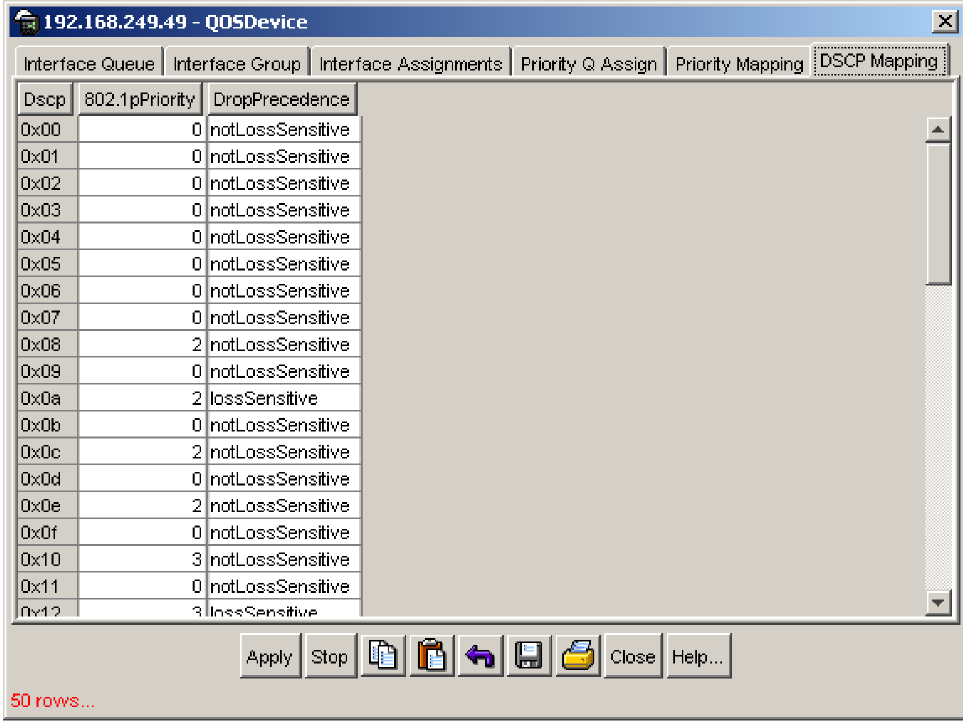
1 From the Device Manager menu bar, choose QoS/COPS > QoS Devices.

The QoSDevice dialog box opens with the Interface Queue tab displayed (Figure 51 on page 138).

2 Click the DSCP Mapping tab.

The DSCP Mapping tab opens (Figure 60 on page 149).

Figure 60 DSCP Mapping tab



Dscp	802.1pPriority	DropPrecedence
0x00	0	notLossSensitive
0x01	0	notLossSensitive
0x02	0	notLossSensitive
0x03	0	notLossSensitive
0x04	0	notLossSensitive
0x05	0	notLossSensitive
0x06	0	notLossSensitive
0x07	0	notLossSensitive
0x08	2	notLossSensitive
0x09	0	notLossSensitive
0x0a	2	lossSensitive
0x0b	0	notLossSensitive
0x0c	2	notLossSensitive
0x0d	0	notLossSensitive
0x0e	2	notLossSensitive
0x0f	0	notLossSensitive
0x10	3	notLossSensitive
0x11	0	notLossSensitive
0x12	3	lossSensitive

50 rows...

Table 35 describes the DSCP Mapping tab fields.

Table 35 DSCP Mapping tab fields

Field	**Description**
Dscp	Shows the DSCP value. This field is read-only.
802.1pPriority	A user priority value associated with the DSCP. To change a value, double-click in the cell and edit the value. The valid range is 0 - 7.
DropPrecedence	The drop precedence setting. The available settings are: • lossSensitive • notLossSensitive Traffic associated with lossSensitive drop precedence is generally given priority over traffic with notLossSensitive precedence during resource allocation. To change the setting, click in a cell and choose the setting.

Managing QoS rules

This section contains the following topics:

- "Displaying IP filters"
- "Adding IP filters" on page 151
- "Deleting IP filters" on page 152
- "Displaying IP filter groups" on page 152
- "Adding IP filter groups" on page 153
- "Deleting IP filter groups" on page 154
- "Displaying Layer 2 filters" on page 155
- "Adding Layer 2 filters" on page 156
- "Deleting Layer 2 filters" on page 157
- "Displaying Layer 2 filter groups" on page 158
- "Adding Layer 2 filter groups" on page 159
- "Deleting Layer 2 filter groups" on page 160

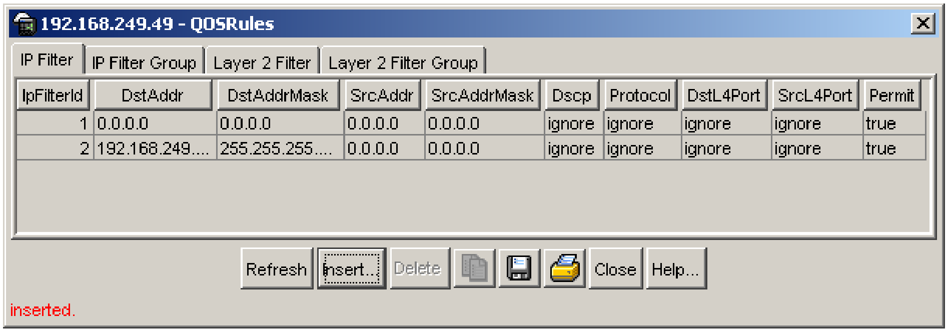
Displaying IP filters

To display IP filters:

➨ From the Device Manager menu bar, choose QoS/COPS > QoSRules.

The QoSRules dialog box opens with the IP Filter tab displayed (Figure 61).

Figure 61 IP Filter tab



IpFilterId	DstAddr	DstAddrMask	SrcAddr	SrcAddrMask	Dscp	Protocol	DstL4Port	SrcL4Port	Permit
1	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	ignore	ignore	ignore	ignore	true
2	192.168.249....	255.255.255....	0.0.0.0	0.0.0.0	ignore	ignore	ignore	ignore	true

inserted.

Table 36 describes the IP Filter tab fields.

Table 36 IP Filter tab fields

Field	Description
Id	The filter identifier.
DstAddr	The IP address that matches the destination IP address of the packet.
DstAddrMask	The mask for matching the destination IP address.
SrcAddr	Specifies the source address to match against the source IP address of the packet.
SrcAddrMask	The mask for matching the source IP address.
Dscp	The value that the DSCP in the packet must have to match the filter.
Protocol	The protocol that is matched against the IP protocol field of the packet.
DstL4Port	The value the packet Layer 4 destination port must have to match this filter.
SrcL4Port	The value the packet Layer 4 source port must have to match this filter.
Permit	Specifies whether traffic with the above characteristics is considered a match (true) or not a match (false). If the frame matches the filter when this field is set to true, the matching process stops. True is the only value supported by Ethernet Switches 460 and 470.

Adding IP filters

To add an IP filter:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP Filter tab displayed (Figure 61 on page 150).

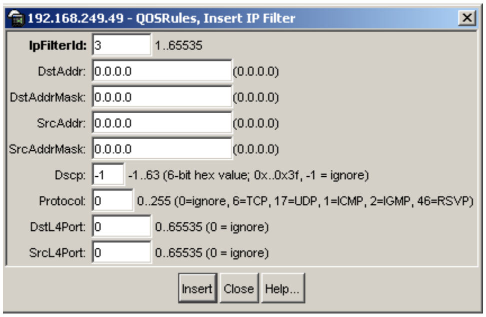
2 Click the IP Filter tab.

The IP Filter tab opens (Figure 61 on page 150).

3 Click Insert.

The Insert IP Filter dialog box opens (Figure 62 on page 152).

Figure 62 Insert IP Filter dialog box



192.168.249.49 - QOSRules, Insert IP Filter

IpFilterId: 3 1..65535

DstAddr: 0.0.0.0 (0.0.0.0)

DstAddrMask: 0.0.0.0 (0.0.0.0)

SrcAddr: 0.0.0.0 (0.0.0.0)

SrcAddrMask: 0.0.0.0 (0.0.0.0)

Dscp: -1 -1..63 (6-bit hex value; 0x..0x3f, -1 = ignore)

Protocol: 0 0..255 (0=ignore, 6=TCP, 17=UDP, 1=ICMP, 2=IGMP, 46=RSVP)

DstL4Port: 0 0..65535 (0 = ignore)

SrcL4Port: 0 0..65535 (0 = ignore)

4 Enter the information you want to use for this IP filter.

5 Click Insert.

Deleting IP filters

To delete an IP filter:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP Filter tab displayed (Figure 61 on page 150).

2 Highlight the IP filter you want to delete.

3 Click Delete.

Note: You cannot delete an IP filter if it is referenced by a filter group.

Displaying IP filter groups

To display IP filter groups:

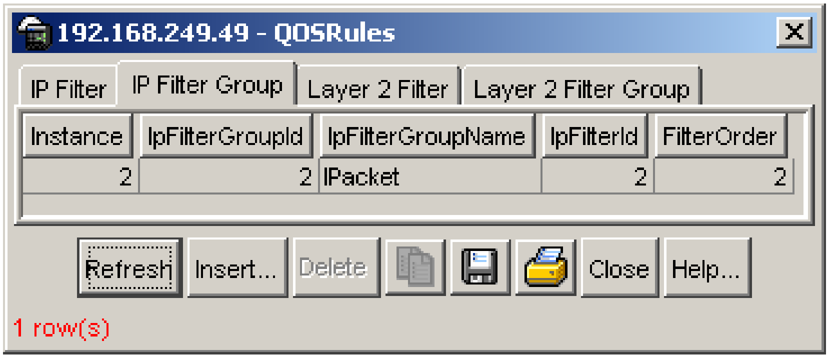
1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP Filter tab displayed (Figure 61).

2 Click the IP Filter Group tab.

The IP Filter Group tab opens (Figure 63).

Figure 63 IP Filter Group tab



Instance	IpFilterGroupId	IpFilterGroupName	IpFilterId	FilterOrder
2	2	IPacket	2	2

Table 37 describes the IP Filter Group tab fields.

Table 37 IP Filter Group tab fields

Field	**Description**
Instance	Specifies the unique identifier for this entry.
IpFilterGroupId	Specifies the identifier for an IP filter group.
IpFilterGroupName	Specifies the name for an IP filter group.
IpFilterId	Specifies the identifier for an IP filter.
FilterOrder	Specifies the evaluation order of filters in a group.

Adding IP filter groups

To add IP filter groups:

1. From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

   The QoSRules dialog box opens with the IP Filter tab displayed (Figure 61 on page 150).

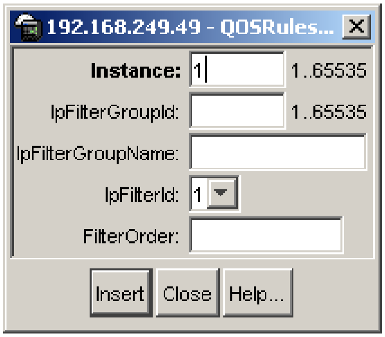
2. Click the IP Filter Group tab.

   The IP Filter Group tab opens (Figure 63 on page 153).

3 Click Insert.

The Insert IP Filter Group dialog box opens (Figure 64).

Figure 64 Insert IP Filter Group dialog box



192.168.249.49 - QOSRules...

Instance: 1 1..65535

IpFilterGroupId: 1..65535

IpFilterGroupName:

IpFilterId: 1

FilterOrder:

4 Enter the information you want to use for this IP filter group.

5 Click Insert.

Deleting IP filter groups

To delete an IP filter groups:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP Filter tab displayed (Figure 61 on page 150).

2 Click the IP Filter Group tab.

The IP Filter Group tab opens (Figure 63 on page 153).

3 Highlight any table cell of the IP filter group you want to delete.

4 Click Delete.

Device Manager deletes the entire filter group.

Note: You cannot delete an IP filter group if it is the last entry for a given filter group and the group is referenced by a policy. You must first delete the policy.

Displaying Layer 2 filters

Device Manager lets you display Layer 2 filters.

To display Layer 2 filters:

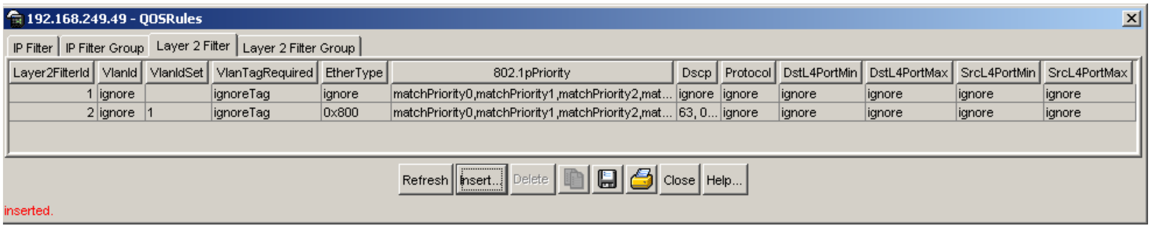
1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP Filter tab displayed (Figure 61 on page 150).

2 Click the Layer 2 Filter tab.

The Layer 2 Filter tab opens (Figure 65).

Figure 65 Layer 2 Filter tab



192.168.249.49 - QOSRules

Layer2FilterId	VlanId	VlanIdSet	VlanTagRequired	EtherType	802.1pPriority	Dscp	Protocol	DstL4PortMin	DstL4PortMax	SrcL4PortMin	SrcL4PortMax
1	ignore		ignoreTag	ignore	matchPriority0,matchPriority1,matchPriority2,mat...	ignore	ignore	ignore	ignore	ignore	ignore
2	ignore	1	ignoreTag	0x800	matchPriority0,matchPriority1,matchPriority2,mat...	63, 0...	ignore	ignore	ignore	ignore	ignore

inserted.

Table 38 describes the Layer 2 Filter tab fields.

Table 38 Layer 2 Filter tab fields

Field	Description
Layer2FilterId	The Layer 2 filter identifier.
VlanId	The VLAN number. A value of -1 indicates that the VLAN ID is ignored.
VlanIdSet	Shows the VLANs referenced by the filter. The filter can reference up to 32 VLANs.
VlanTagRequired	Specifies whether or not to check the VLAN tagging.
EtherType	The etherType to match.
802.1pPriority	Specifies the 802.1 priority.
Dscp	The value that the DSCP in the packet must have to match the filter.
Protocol	The protocol that is matched against the IP protocol field of the packet.

Table 38 Layer 2 Filter tab fields (Continued)

Field	Description
DstL4PortMin	The minimum value that the packet Layer 4 destination port number must have to match the filter.
DstL4PortMax	The maximum value that the packet Layer 4 destination port number must have to match the filter.
SrcL4PortMin	The minimum value that the packet Layer 4 source port number must have to match the filter.
SrcL4PortMax	The maximum value that the packet Layer 4 source port number must have to match the filter.

Adding Layer 2 filters

To add a Layer 2 filter:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP Filter tab displayed (Figure 61 on page 150).

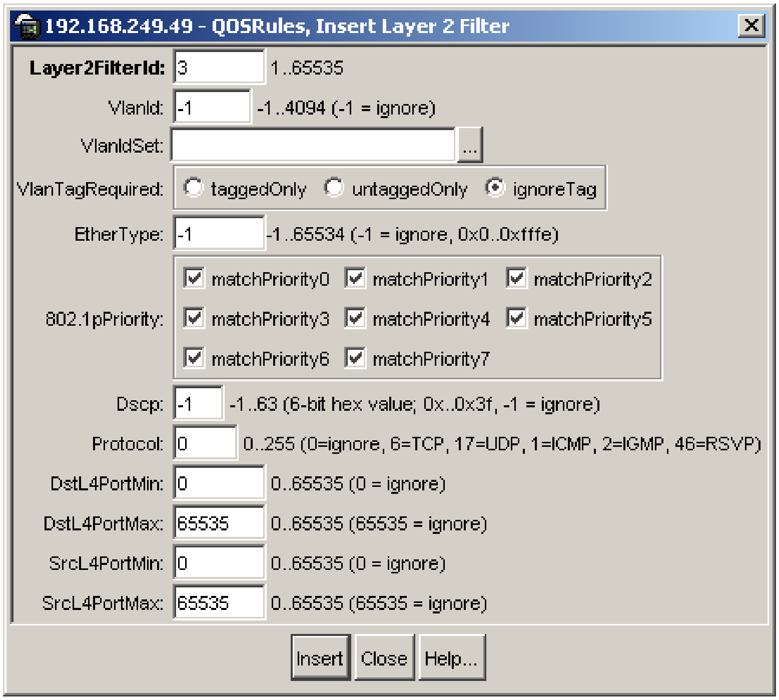
2 Click the Layer 2 Filter tab.

The Layer 2 Filter tab opens (Figure 65 on page 155).

3 Click Insert.

The Insert Layer 2 Filter dialog box opens (Figure 66 on page 157).

Figure 66 Insert Layer 2 Filter dialog box



192.168.249.49 - QOSRules, Insert Layer 2 Filter

Layer2FilterId: 3 1..65535

VlanId: -1 -1..4094 (-1 = ignore)

VlanIdSet:

VlanTagRequired: ○ taggedOnly ○ untaggedOnly ● ignoreTag

EtherType: -1 -1..65534 (-1 = ignore, 0x0..0xfffe)

802.1pPriority: ☑ matchPriority0 ☑ matchPriority1 ☑ matchPriority2 ☑ matchPriority3 ☑ matchPriority4 ☑ matchPriority5 ☑ matchPriority6 ☑ matchPriority7

Dscp: -1 -1..63 (6-bit hex value; 0x..0x3f, -1 = ignore)

Protocol: 0 0..255 (0=ignore, 6=TCP, 17=UDP, 1=ICMP, 2=IGMP, 46=RSVP)

DstL4PortMin: 0 0..65535 (0 = ignore)

DstL4PortMax: 65535 0..65535 (65535 = ignore)

SrcL4PortMin: 0 0..65535 (0 = ignore)

SrcL4PortMax: 65535 0..65535 (65535 = ignore)

4 Enter the information you want to use for this Layer 2 filter.

5 Click Insert.

Deleting Layer 2 filters

To delete a Layer 2 filter:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP Filter tab displayed (Figure 61 on page 150).

2 Click the Layer 2 Filter tab.

The Layer 2 Filter tab opens (Figure 65 on page 155).

3 Highlight the Layer 2 filter you want to delete.

4 Click Delete.

Note: You cannot delete an Layer 2 filter that is referenced in a filter group.

Displaying Layer 2 filter groups

To display Layer 2 filter groups:

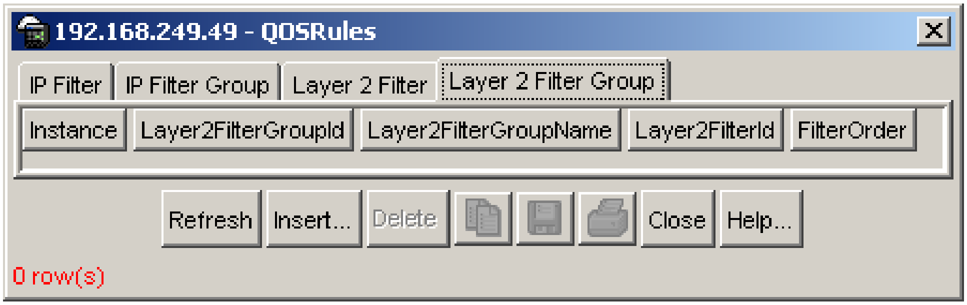
1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP Filter tab displayed (Figure 61 on page 150).

2 Click the Layer 2 Filter Group tab.

The Layer 2 Filter Group tab opens (Figure 67).

Figure 67 Layer 2 Filter Group tab



0 row(s)

Table 39 describes the Layer 2 Filter Group tab fields.

Table 39 Layer 2 Filter Group tab fields

Field	Description
Instance	Specifies the unique identifier for this entry.
Layer2FilterGroupId	Specifies the identifier for a Layer 2 filter group.
Layer2FilterGroupName	Specifies the name for a Layer 2 filter group.

Table 39 Layer 2 Filter Group tab fields (Continued)

Field	Description
Layer2FilterId	Specifies the identifier for a Layer 2 filter.
Layer2FilterOrder	The evaluation order of filters in a group.

Adding Layer 2 filter groups

To add a Layer 2 filter group:

1 From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

The QoSRules dialog box opens with the IP Filter tab displayed (Figure 61 on page 150).

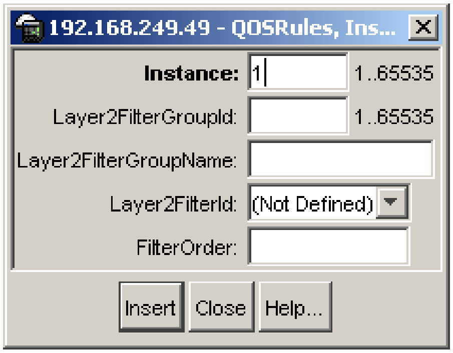
2 Click the Layer 2 Filter Group tab.

The Layer 2 Filter Group tab opens (Figure 67 on page 158).

3 Click Insert.

The Insert Layer 2 Filter Group dialog box opens (Figure 68).

Figure 68 Insert Layer 2 Filter Group dialog box



192.168.249.49 - QOSRules, Ins...

Instance: 1 1..65535

Layer2FilterGroupId: 1..65535

Layer2FilterGroupName:

Layer2FilterId: (Not Defined)

FilterOrder:

4 Enter the information you want to use for this Layer 2 filter group.

5 Click Insert.

Deleting Layer 2 filter groups

To delete a Layer 2 filter group:

1. From the Device Manager menu bar, choose QoS/COPS > QoS Rules.

   The QoSRules dialog box opens with the IP Filter tab displayed (Figure 61 on page 150).

2. Click the Layer 2 Filter Group tab.

   The Layer 2 Filter Group tab opens (Figure 67 on page 158).

3. Highlight the Layer 2 filter group you want to delete.
4. Click Delete.

Note: You cannot delete the last group entry in a Layer 2 filter group if it is referenced by a policy. You must first delete the policy.

Managing QoS actions, meters, shapers, policies, and user roles

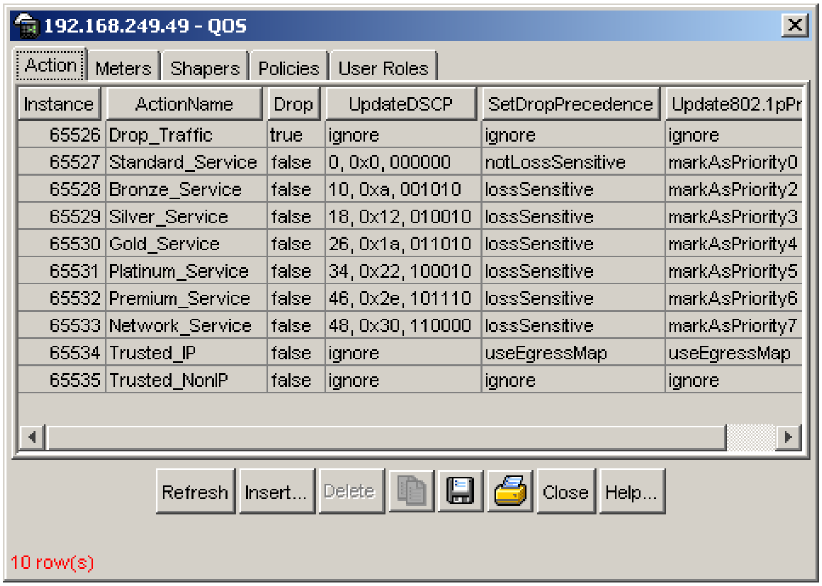
Displaying QoS actions

To display a QoS action:

➨ From the Device Manager menu bar, choose QoS/COPS > QoS...

The QoS dialog box opens with the QoS Action tab displayed (Figure 69 on page 161).

Figure 69 QoS Action tab



Instance	ActionName	Drop	UpdateDSCP	SetDropPrecedence	Update802.1pPr
65526	Drop_Traffic	true	ignore	ignore	ignore
65527	Standard_Service	false	0, 0x0, 000000	notLossSensitive	markAsPriority0
65528	Bronze_Service	false	10, 0xa, 001010	lossSensitive	markAsPriority2
65529	Silver_Service	false	18, 0x12, 010010	lossSensitive	markAsPriority3
65530	Gold_Service	false	26, 0x1a, 011010	lossSensitive	markAsPriority4
65531	Platinum_Service	false	34, 0x22, 100010	lossSensitive	markAsPriority5
65532	Premium_Service	false	46, 0x2e, 101110	lossSensitive	markAsPriority6
65533	Network_Service	false	48, 0x30, 110000	lossSensitive	markAsPriority7
65534	Trusted_IP	false	ignore	useEgressMap	useEgressMap
65535	Trusted_NonIP	false	ignore	ignore	ignore

10 row(s)

Table 40 describes the QoS Action tab fields.

Table 40 QoS Action tab fields

Field	Description
Instance	Specifies a unique identifier for the entry.
Action Name	Specifies a name for the entry.
Drop	Specifies whether the frame being evaluated is dropped (true) or not dropped (false).
UpdateDSCP	An integer that causes the value contained in the differentiated services field of an associated IP datagram to be updated with the value of the object.
SetDropPrecedence	Sets a precedence value.
Update802.11p Priority	A value that updates the value in the user priority field in the 802.1. The values range from 0 to 7, from lowest to highest priority. Other choices include: UseDefault, Ignore, and UseEgressMap.

Adding QoS actions

To add a QoS action:

1. From the Device Manager menu bar, choose QoS/COPS > QoS...

   The QoS dialog box opens with the QoS Action tab displayed (Figure 69 on page 161).

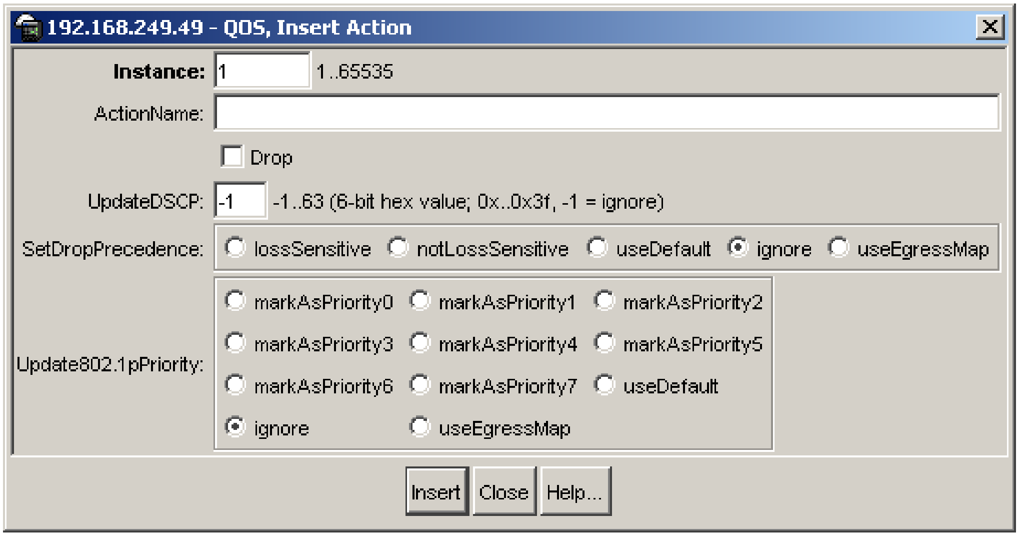
2. Click the QoS Action tab.

   The QoS Action tab opens (Figure 69 on page 161).

3. Click Insert.

   The Insert QoS Action dialog box opens (Figure 70).

Figure 70 Insert QoS Action dialog box



192.168.249.49 - QOS, Insert Action

Instance: 1 1..65535

ActionName:

□ Drop

UpdateDSCP: -1 -1..63 (6-bit hex value; 0x..0x3f, -1 = ignore)

SetDropPrecedence: ○ lossSensitive ○ notLossSensitive ○ useDefault ● ignore ○ useEgressMap

Update802.1pPriority: ○ markAsPriority0 ○ markAsPriority1 ○ markAsPriority2 ○ markAsPriority3 ○ markAsPriority4 ○ markAsPriority5 ○ markAsPriority6 ○ markAsPriority7 ○ useDefault ● ignore ○ useEgressMap

4. Enter the information and make the selections you want to use for this QoS action.

5. Click Insert.

Deleting QoS actions

To delete a QoS action:

1. From the Device Manager menu bar, choose QoS/COPS > QoS...

   The QoS dialog box opens with the QoS Action tab displayed (Figure 69 on page 161).

2. Click the QoS Action tab.

   The QoS Action tab opens (Figure 69 on page 161).

3. Highlight the QoS action you want to delete.
4. Click Delete.

➡ **Note:** You cannot delete a QoS action that is referenced by a meter entry. You must first delete the meter.

Displaying QoS meters

To display a QoS meter:

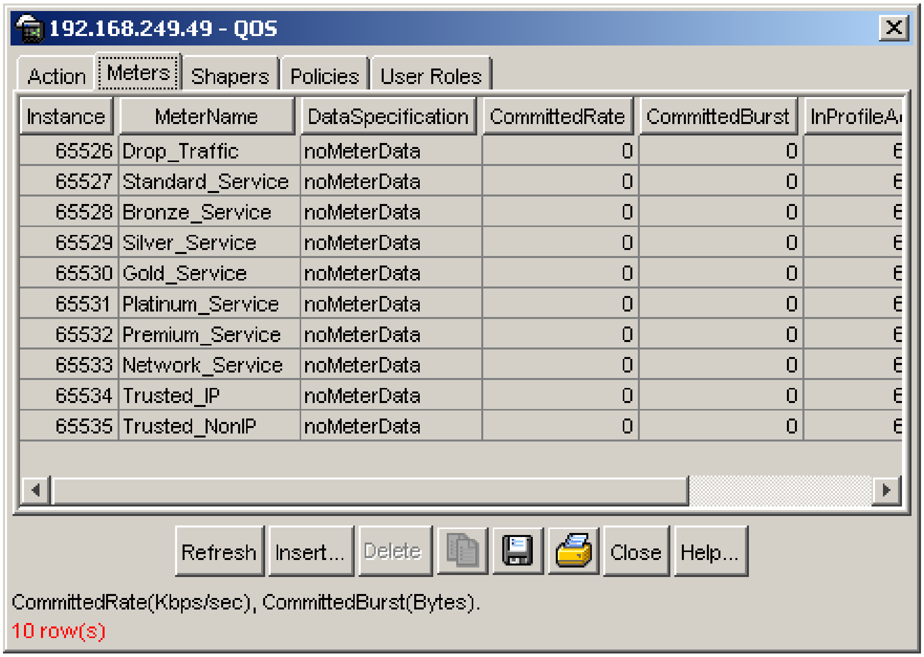
1. From the Device Manager menu bar, choose QoS/COPS > QoS...

   The QoS dialog box opens with the QoS Action tab displayed (Figure 69 on page 161).

2. Click the QoS Meters tab.

The QoS Meters tab opens (Figure 71).

Figure 71 QoS Meters tab



Instance	MeterName	DataSpecification	CommittedRate	CommittedBurst	InProfileA
65526	Drop_Traffic	noMeterData	0	0	6
65527	Standard_Service	noMeterData	0	0	6
65528	Bronze_Service	noMeterData	0	0	6
65529	Silver_Service	noMeterData	0	0	6
65530	Gold_Service	noMeterData	0	0	6
65531	Platinum_Service	noMeterData	0	0	6
65532	Premium_Service	noMeterData	0	0	6
65533	Network_Service	noMeterData	0	0	6
65534	Trusted_IP	noMeterData	0	0	6
65535	Trusted_NonIP	noMeterData	0	0	6

CommittedRate(Kbps/sec), CommittedBurst(Bytes).

10 row(s)

Table 41 describes the QoS Meters tab fields.

Table 41 QoS Meters tab fields

Field	Description
Instance	Specifies the unique identifier for this entry.
MeterName	Specifies a name for this entry.
DataSpecification	Specifies whether to meter the data or not. If you choose to not meter the data, the CommittedRate, CommittedBurst, and OutOfProfileAction fields are not applicable.
CommittedRate	Specifies the committed rate.
CommittedBurst	Specifies the committed burst.
InProfileAction	Specifies in-profile action.
OutOfProfileAction	Specifies out-of-profile action.

Adding QoS meters

To add a QoS meter:

1 From the Device Manager menu bar, choose QoS/COPS > QoS...

The QoS dialog box opens with the QoS Action tab displayed (Figure 69 on page 161).

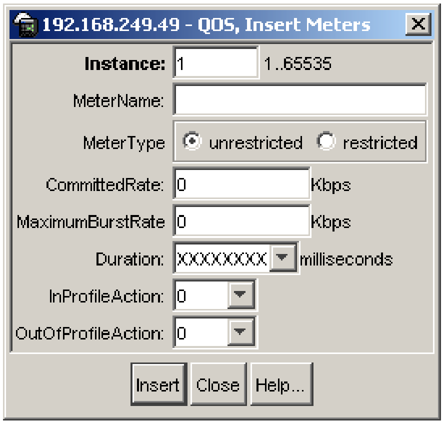
2 Click the QoS Meters tab.

The QoS Meters tab opens (Figure 71 on page 164).

3 Click Insert.

The Insert QoS Meters dialog box opens (Figure 72).

Figure 72 Insert QoS Meters dialog box



192.168.249.49 - QOS, Insert Meters

Instance: 1 1..65535

MeterName:

MeterType ● unrestricted ○ restricted

CommittedRate: 0 Kbps

MaximumBurstRate 0 Kbps

Duration: XXXXXXXX milliseconds

InProfileAction: 0

OutOfProfileAction: 0

4 Specify an Instance and Name for the meter.

5 Specify whether the meter is restricted or unrestricted.

6 Enter the committed rate you want for the meter.

7 Enter the maximum burst rate you want for the meter.

The system calculates a series of 7 or fewer possible durations for the committed and expected burst rates you set.

8 Choose a Duration in milliseconds from the drop-down list.

9 Choose an in-profile and out-of-profile action from the drop-down lists.

10 Click Insert.

Deleting QoS meters

To delete a QoS meter:

1 From the Device Manager menu bar, choose QoS/COPS > QoS...

The QoS dialog box opens with the QoS Action tab displayed (Figure 69 on page 161).

2 Click the QoS Meters tab.

The QoS Meters tab opens (Figure 71 on page 164).

3 Highlight the QoS meter(s) you want to delete.

4 Click Delete.

Note: You cannot delete a QoS meter that is referenced by a policy. You must first delete the policy.

Displaying QoS shapers

To display QoS shapers:

1 From the Device Manager menu bar, choose QoS/COPS > QoS...

The QoS dialog box opens with the QoS Action tab displayed (Figure 69 on page 161).

2 Click the Shapers tab.

The QoS Shapers tab opens (Figure 73 on page 167).

Figure 73 QoS Shapers tab

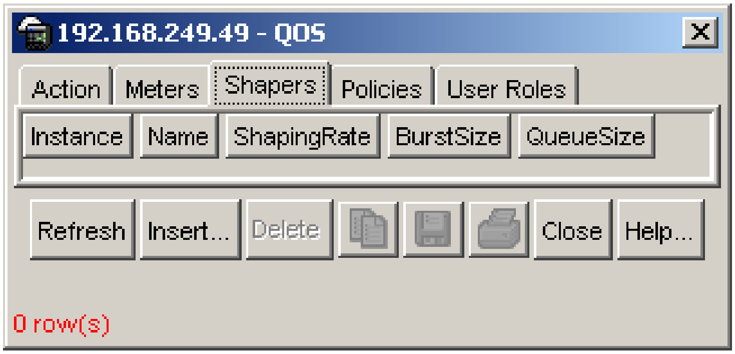


Table 42 describes the QoS Shapers tab fields.

Table 42 QoS Shapers tab fields

Field	Description
Instance	Specifies the unique identifier for this entry.
Name	Specifies the name for this entry.
ShapingRate	The maximum rate (in Kbps) at which traffic shaped using this shaper is transmitted over a given duration. When you insert Shaper entries, you must enter a rate that is a multiple of 64 Kbps.
BurstSize	The maximum traffic burst size (in bytes) that can be transmitted without a shaping delay. The available values are: • 2047 • 4095 • 8191 • 16383 • 32767 • 65535
QueueSize	The number of packets that can exceed the traffic burst size and still be queued for transmission.

Adding QoS shapers

To add a QoS shaper:

1 From the Device Manager menu bar, choose QoS/COPS > QoS.

The QoS dialog box opens with the QoS Action tab displayed (Figure 69 on page 161).

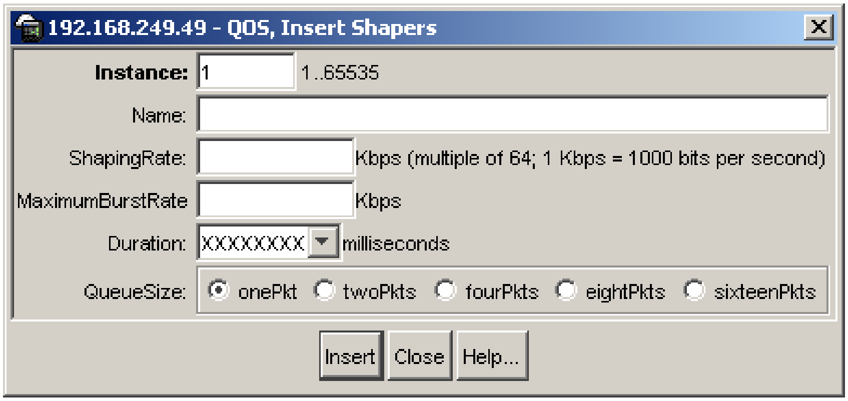
2 Click the QoS Shapers tab.

The QoS shapers tab opens (Figure 71 on page 164).

3 Click Insert.

The Insert QoS Shapers dialog box opens (Figure 74).

Figure 74 Insert QoS shaper dialog box



192.168.249.49 - QOS, Insert Shapers

Instance: 1 1..65535

Name:

ShapingRate: Kbps (multiple of 64; 1 Kbps = 1000 bits per second)

MaximumBurstRate Kbps

Duration: XXXXXXXX milliseconds

QueueSize: ● onePkt ○ twoPkts ○ fourPkts ○ eightPkts ○ sixteenPkts

4 Enter the instance and name for the shaper you are creating.

5 Enter the Shaping Rate in Kbps

6 Enter the Maximum Burst Rate in Kbps.

7 From the drop-down list, choose a duration for the period that the Maximum Burst Rate is allowed.

8 Choose a queue size from the options displayed.

9 Click Insert.

Deleting QoS shapers

To delete a QoS shaper:

1 From the Device Manager menu bar, choose QoS/COPS > QoS.

The QoS dialog box opens with the QoS Action tab displayed (Figure 69 on page 161).

2 Click the QoS Shapers tab.

The QoS Shapers tab opens (Figure 71 on page 164).

3 Highlight the QoS shaper you want to delete.

4 Click Delete.

Note: You cannot delete a QoS shaper that is referenced by a policy. You must first delete the policy.

Displaying QoS policies

To display QoS policies:

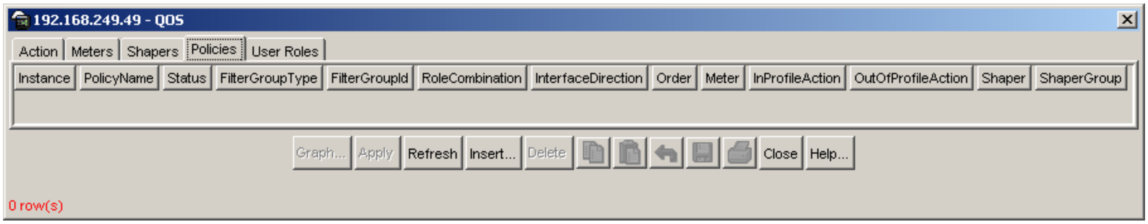
1 From the Device Manager menu bar, choose QoS/COPS > QoS...

The QoS dialog box opens with the QoS Action tab displayed (Figure 69 on page 161).

2 Click the QoS Policies tab.

The QoS Policies tab opens (Figure 75).

Figure 75 QoS Policies tab



Instance	PolicyName	Status	FilterGroupType	FilterGroupId	RoleCombination	InterfaceDirection	Order	Meter	InProfileAction	OutOfProfileAction	Shaper	ShaperGroup

0 row(s)

Table 43 describes the QoS Policies tab fields.

Table 43 QoS Policies tab fields

Field	Description
Instance	The unique identifier for this policy entry.
PolicyName	The name for this policy entry.
Status	Specifies the status of the policy.
FilterGroupType	Specifies the type of filter group.
FilterGroupId	The filter group associated with a policy.
RoleCombination	A tag that identifies the interfaces to which a policy specification applies.
InterfaceDirection	Specifies direction of packet flow at the specified interface. Note: The Ethernet Switch 460-24T-PWR only supports ingress.
Order	The number used to determine the order of precedence for a policy specification.
Meter	Specifies the meter associated with a policy.
InProfileAction	The identifier of the in-profile action associated with the policy.
OutOfProfileAction	The identifier of the out-of-profile action associated with the policy.
Shaper	Specifies the shaper associated with a policy.
ShaperGroup	Specifies the shaper group associated with a policy.

Adding QoS policies

To add a QoS policy:

1 From the Device Manager menu bar, choose QoS/COPS > QoS...

The QoS dialog box opens with the QoS Action tab displayed (Figure 69 on page 161).

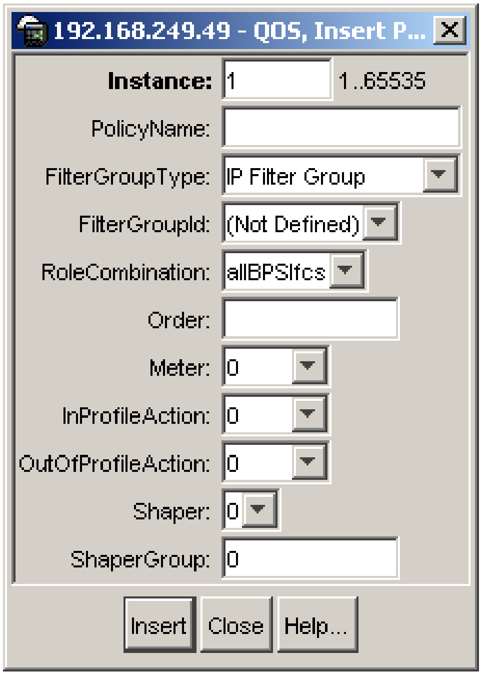
2 Click the QoS Policies tab.

The QoS Policies tab opens (Figure 75 on page 169).

3 Click Insert.

The Insert QoS Policies dialog box opens (Figure 76 on page 171).

Figure 76 Insert QoS Policies dialog box



192.168.249.49 - QOS, Insert P...

Instance:	1	1..65535
PolicyName:		
FilterGroupType:	IP Filter Group	
FilterGroupId:	(Not Defined)	
RoleCombination:	allBPSIfcs	
Order:		
Meter:	0	
InProfileAction:	0	
OutOfProfileAction:	0	
Shaper:	0	
ShaperGroup:	0	

4 Enter the information you want to use for this QoS policies.

5 Click Insert.

Deleting QoS policies

To delete a QoS policy:

1 From the Device Manager menu bar, choose QoS/COPS > QoS...

The QoS dialog box opens with the QoS Action tab displayed (Figure 69 on page 161).

2 Click the QoS Policies tab.

The QoS Policies tab opens (Figure 75 on page 169).

3 Highlight the QoS policies you want to delete.

4 Click Delete.

Displaying QoS policy statistics

To display QoS policy statistics:

1 From the Device Manager menu bar, choose QoS/COPS > QoS.

The QoS dialog box opens with the QoS Action tab displayed (Figure 69 on page 161).

2 Click the QoS Policies tab.

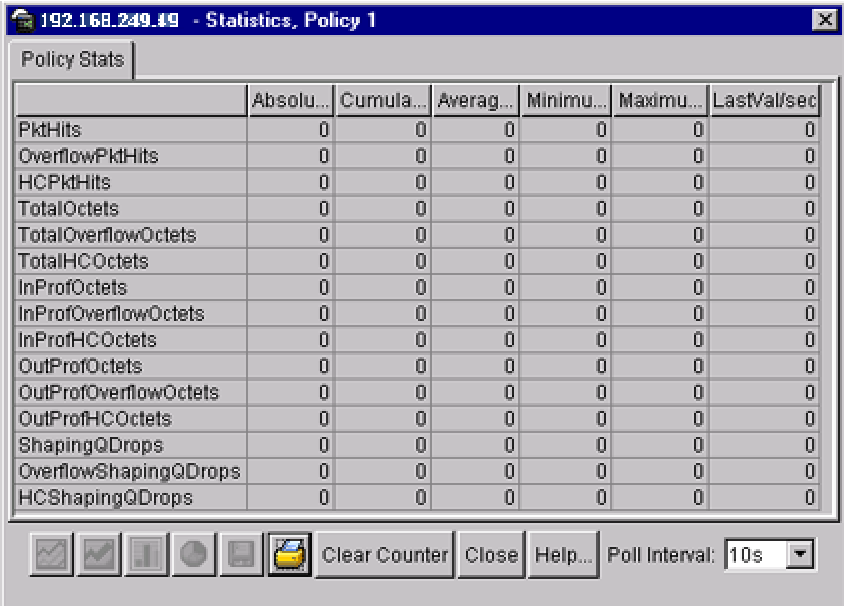
The QoS Policies tab opens (Figure 75 on page 169).

3 Highlight an entry in the QoS Policies tab. This activates the Graph button.

4 Click the Graph button.

The QoS policy statistics tab opens (Figure 77).

Figure 77 QoS policy statistics tab



	Absolu...	Cumula...	Averag...	Minimu...	Maximu...	LastVal/sec
PktHits	0	0	0	0	0	0
OverflowPktHits	0	0	0	0	0	0
HCPktHits	0	0	0	0	0	0
TotalOctets	0	0	0	0	0	0
TotalOverflowOctets	0	0	0	0	0	0
TotalHCOctets	0	0	0	0	0	0
InProfOctets	0	0	0	0	0	0
InProfOverflowOctets	0	0	0	0	0	0
InProfHCOctets	0	0	0	0	0	0
OutProfOctets	0	0	0	0	0	0
OutProfOverflowOctets	0	0	0	0	0	0
OutProfHCOctets	0	0	0	0	0	0
ShapingQDrops	0	0	0	0	0	0
OverflowShapingQDrops	0	0	0	0	0	0
HCShapingQDrops	0	0	0	0	0	0

Table 44 describes the QoS policy statistics tab fields.

Table 44 QoS policy statistics tab fields

Field	Description
PktHits	The packets selected for additional processing. The action taken is based on a match with a specified filter or threshold information.
OverflowPktHits	The number of times that the associated PkHits counter overflowed.
TotalOctets	The total number of octets associated with the packet hits for this policy.
TotalOverflowOctets	The total number of times that the associated TotalOctets counter overflowed.
InProfOctets	The total number of in-profile octets associated with packet hits for this policy.
InProfOverflowOctets	The total number of times that the associated InProfOctets counter overflowed.
OutProfOctets	The total number of out-of-profile octets associated with packet hits for this policy.
OutProfOverflowOctets	The total number of times the associated OutProfOctets counter overflowed.
ShapingQDrops	The number of packets dropped during shaping due to insufficient shaping queue resources.
OverflowShapingQDrops	The number of times that the ShapingQDrops counter has overflowed.
HCShapingQDrops	A 64-bit counter that represents the combination of the ShapingQDrops and OverflowShapingQDrops counters.

Displaying QoS User Roles

To display QoS user roles:

1 From the Device Manager menu bar, choose QoS/COPS > QoS.

The QoS dialog box opens with the QoS Action tab displayed (Figure 69 on page 161).

2 Click the QoS User Roles tab.

The QoS User Roles tab opens (Figure 78).

Figure 78 QoS User Roles tab

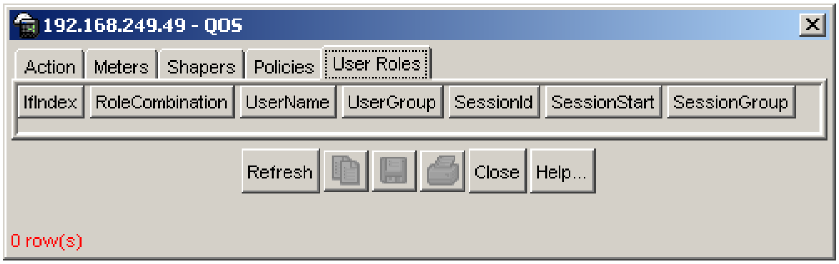


Table 45 describes the QoS User Roles tab fields.

Table 45 QoS user Roles tab fields

Field	Description
IfIndex	Specifies the interface index number.
UserRole Combination	Specifies a physical interface to which policy rules and actions can be applied.
UserRoleName	Specifies the user currently associated with the user role.
UserRoleGroup	Specifies the user group with which the user is associated.
SessionId	Specifies the system-assigned session identifier used to track instances of a user role entry.
SessionStart	Specifies the system-assigned session start timestamp.
SessionGroup	Specifies the system-assigned session group identifier.

QoS agent

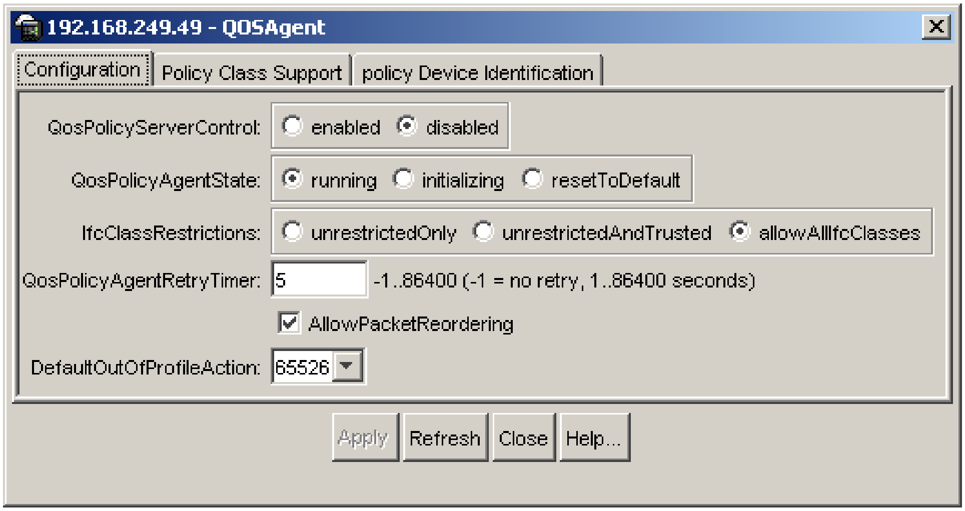
Displaying QoS agent configuration

To display QoS agent configuration:

➨ From the Device Manager menu bar, choose QoS/COPS > QoS Agent.

The QoSAgent dialog box opens with the Configuration tab displayed (Figure 79).

Figure 79 Configuration tab



QosPolicyServerControl: ○ enabled ● disabled

QosPolicyAgentState: ● running ○ initializing ○ resetToDefault

IfcClassRestrictions: ○ unrestrictedOnly ○ unrestrictedAndTrusted ● allowAllIfcClasses

QosPolicyAgentRetryTimer: 5 -1..86400 (-1 = no retry, 1..86400 seconds)

☑ AllowPacketReordering

DefaultOutOfProfileAction: 65526

Table 46 describes the QoS Agent Configuration tab fields.

Table 46 Configuration tab fields

Field	Description
QosPolicyServerControl	Specifies whether policy server control is enabled or disabled.
QosPolicyAgentState	The current state of the policy agent.
QosPolicyAgentRetryTimer	The amount of time between each policy server retry.
AllowPacketReordering	Specifies whether packet reordering is acceptable.

Table 46 Configuration tab fields (Continued)

Field	Description
MaintainPolicingStats	Specifies whether policy statistics are maintained.
DefaultOutOfProfileAction	Specifies out-of-profile action for flows that are being metered using the committedRestricted QoS meter. The value of this attribute cannot be changed while meters of this type are currently associated with a policy.

Displaying policy class support

To display policy class support:

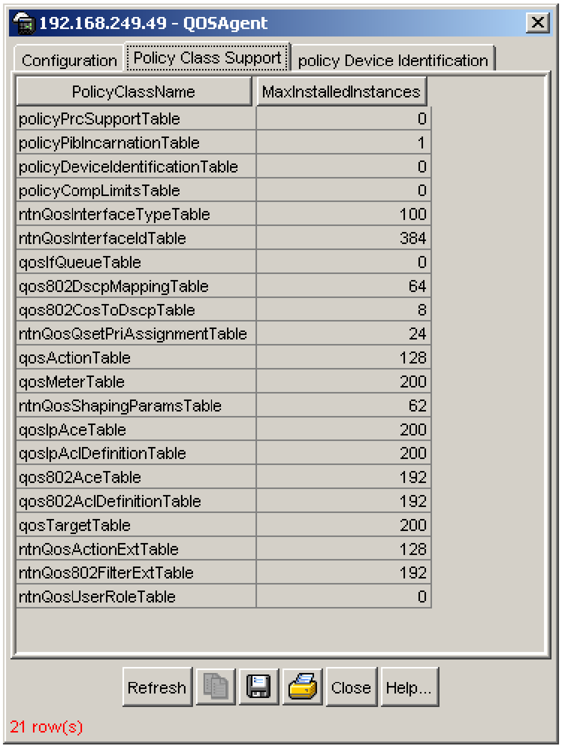
1 From the Device Manager menu bar, choose QoS/COPS > QoS Agent.

The QoSAgent dialog box opens with the Configuration tab displayed (Figure 79 on page 175).

2 Click the Policy Class Support tab.

The Policy Class Support tab opens (Figure 80 on page 177).

Figure 80 Policy Class Support tab



PolicyClassName	MaxInstalledInstances
policyPrcSupportTable	0
policyPibIncarnationTable	1
policyDeviceIdentificationTable	0
policyCompLimitsTable	0
ntnQosInterfaceTypeTable	100
ntnQosInterfaceIdTable	384
qosIfQueueTable	0
qos802DscpMappingTable	64
qos802CosToDscpTable	8
ntnQosQsetPriAssignmentTable	24
qosActionTable	128
qosMeterTable	200
ntnQosShapingParamsTable	62
qosIpAceTable	200
qosIpAclDefinitionTable	200
qos802AceTable	192
qos802AclDefinitionTable	192
qosTargetTable	200
ntnQosActionExtTable	128
ntnQos802FilterExtTable	192
ntnQosUserRoleTable	0

21 row(s)

Table 47 describes the Policy Class Support tab fields.

Table 47 policy Class Support tab fields

Field	Description
PolicyClassName	The name of the policy class.
MaximumInstalledInstances	The maximum number of installed instances of the policy class.

Displaying policy device identification

To display policy device identification data:

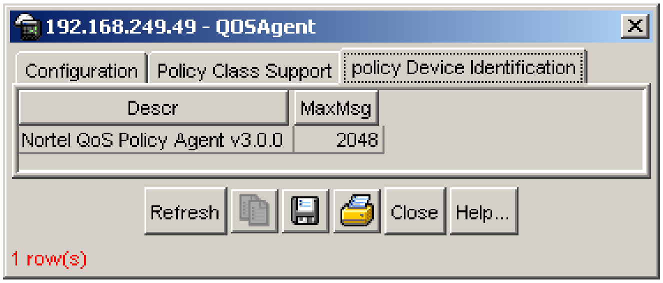
1 From the Device Manager menu bar, choose QoS/COPS > QoS Agent.

The QoSAgent dialog box opens with the Configuration tab displayed (Figure 79 on page 175).

2 Click the policy Device Identification tab.

The policy Device Identification tab opens (Figure 81).

Figure 81 policy Device Identification tab



Descr	MaxMsg
Nortel QoS Policy Agent v3.0.0	2048

Table 48 describes the policy Device Identification tab fields.

Table 48 policy Device Identification tab fields

Field	Description
Descr	A description of the policy device.
MaxMsg	The maximum message size in bytes that the device can support.

COPS

COPS is a comprehensive network management application for policy-based network traffic control. The policy server distributes policies to edge devices and border routers.COPS is used to communicate with edge devices on the network. Some of the benefits of the COPS protocol are:

- It uses a client/server model for communication between the policy server and the policy clients.
- It uses TCP for messaging, reducing the resources it requires.
- The policy server can send configuration information to the policy client, as well as removing unneeded configuration information.

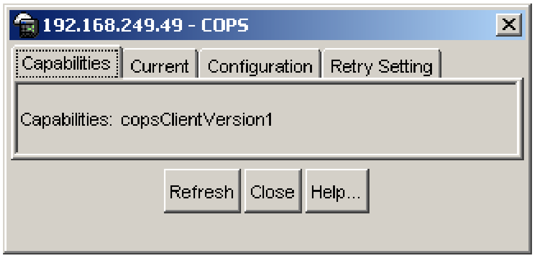
Displaying COPS capabilities

To display COPS capabilities:

➨ From the Device Manager menu bar, choose QoS/COPS > QoS COPS.

The COPS dialog box opens with the Capabilities tab displayed (Figure 82).

Figure 82 Capabilities



Capabilities: copsClientVersion1

Table 49 describes the Capabilities tab fields.

Table 49 Capabilities tab fields

Field	Description
Capabilities	A list of COPS protocols supported by Ethernet Switches 460 and 470.

Displaying COPS current service configuration

To display current service configuration data:

1 From the Device Manager menu bar, choose QoS/COPS > COPS.

The COPS dialog box opens with the Capabilities tab displayed (Figure 82).

2 Click the Current tab.

The Current tab opens (Figure 83 on page 180).

Figure 83 Current tab

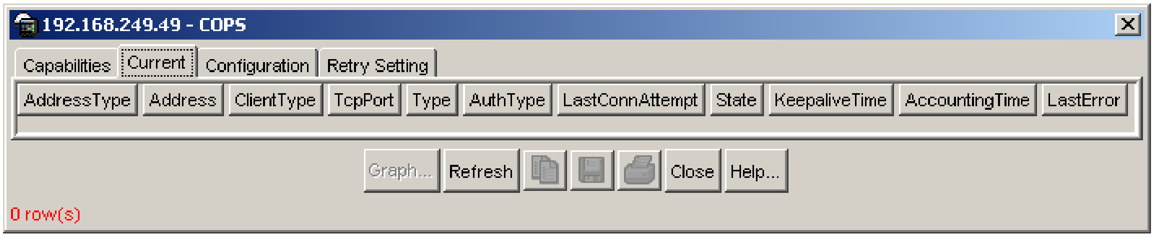


Table 50 describes the Current tab fields.

Table 50 Current tab fields

Field	Description
AddressType	The type of address in the copsClientServerAddress.
Address	The IPv4 address of a COPS server.
ClientType	The protocol client type for an entry.
TcpPort	The TCP port number on the COPS server to which the client is connected.
Type	The source of COPS server information.
AuthType	The security mode being used between the client and the COPS server.
LastConnAttempt	The timestamp of the last time that the client attempted to connect to the COPS server.
State	The operational state of a connection between a client and the COPS server.
KeepaliveTime	The value of the keepalive timeout, in centiseconds, that is currently in use by a client. The COPS server specifies this value in the Client-Accept operation.
AccountingTime	The value of the COPS protocol Accounting timeout, in centiseconds, that is currently in use by a client. The COPS server specifies this value in the Client-Accept operation.
LastError	The code contained in the last protocol Error Object received from the COPS server.

Displaying COPS local configuration

To display COPS configuration data:

1 From the Device Manager menu bar, choose QoS/COPS > COPS.

The COPS dialog box opens with the Capabilities tab displayed.

2 Click the Configuration tab.

The Configuration tab opens (Figure 84).

Figure 84 Configuration tab

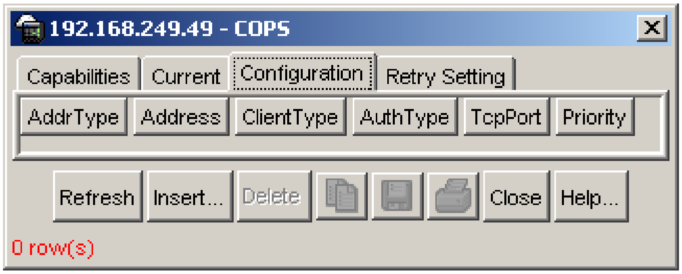


Table 51 describes the Configuration tab fields.

Table 51 Configuration tab fields

Field	**Description**
AddrType	The type of address.
Address	The address identifier.
ClientType	The type of client
AuthType	The security mode used between the client and the COPS server.
TcpPort	The TCP port number on the COPS server to which the client is connected.
Priority	The level of priority.

Adding COPS local configuration data

To add COPS local configuration data:

1 From the Device Manager menu bar, choose QoS/COPS > COPS.

The COPS dialog box opens with the Capabilities tab displayed.

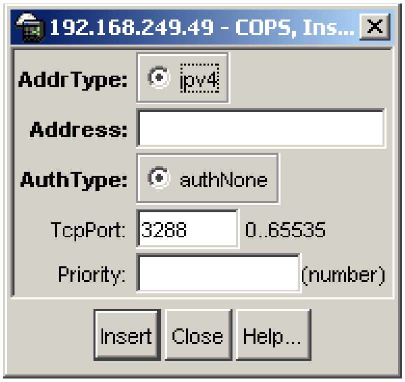
2 Click the Configuration tab.

The Configuration tab opens (Figure 84).

3 Click Insert.

The Insert COPS Configuration dialog box opens (Figure 85).

Figure 85 Insert COPS Configuration dialog box


192.168.249.49 - COPS, Ins...

AddrType: ● ipv4

Address:

AuthType: ● authNone

TcpPort: 3288 0..65535

Priority: (number)

4 Enter the information you want to use for this COPS configuration.

5 Click Insert.

Deleting COPS local configuration data

To delete COPS local configuration data:

1 From the Device Manager menu bar, choose QoS/COPS > COPS.

The COPS dialog box opens with the Capabilities tab displayed.

2 Click the Configuration tab.

The Configuration tab opens (Figure 84 on page 181).

3 Highlight the COPS configuration you want to delete.

4 Click Delete.

Displaying COPS retry setting

To display COPS retry setting:

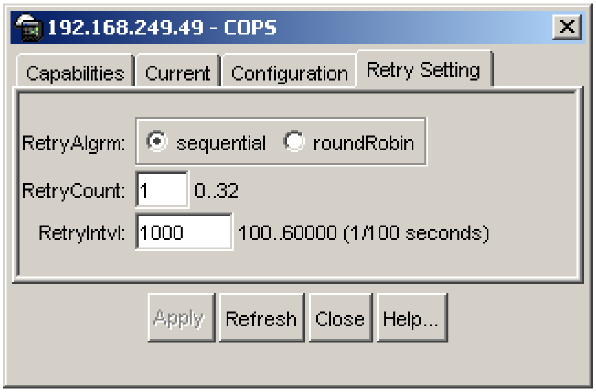
1 From the Device Manager menu bar, choose QoS/COPS > COPS.

The COPS dialog box opens with the Capabilities tab displayed.

2 Click the Retry Setting tab.

The Retry Setting tab opens (Figure 86).

Figure 86 Retry Setting tab



RetryAlgrm: ● sequential ○ roundRobin

RetryCount: 1 0..32

RetryIntvl: 1000 100..60000 (1/100 seconds)

Table 52 describes the tab fields.

Table 52 COPS Retry Setting tab fields

Field	Description
RetryAlgrm	The type of algorithm.
RetryCount	The number of retry attempts. Valid range is 0 to 32.
RetryIntvl	The retry interval in 1/100 seconds. Valid range is 100 to 60000 (1 to 600 seconds).

To make changes to the information in the Retry Setting tab:

1 Make the changes you want in the Retry Setting tab.

2 Click on the Apply button to confirm the changes.

Displaying COPS statistics

To display COPS statistics:

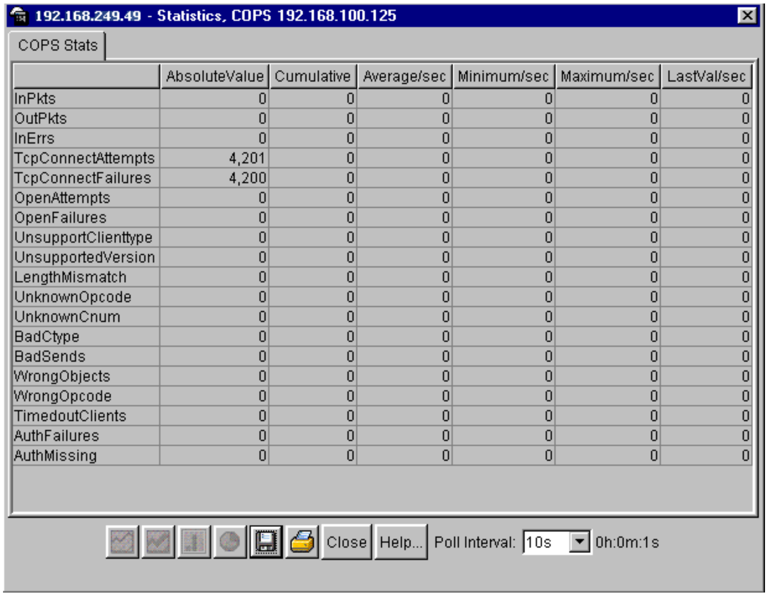
1. In the Current tab, highlight an entry and click on the Graph button.

   The COPS Stats dialog box opens.

2. Click the COPS Stats tab.

   The COPS Stats tab is active (Figure 87).

Figure 87 COPS Stats tab



192.168.249.49 - Statistics, COPS 192.168.100.125

COPS Stats

	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
InPkts	0	0	0	0	0	0
OutPkts	0	0	0	0	0	0
InErrs	0	0	0	0	0	0
TcpConnectAttempts	4,201	0	0	0	0	0
TcpConnectFailures	4,200	0	0	0	0	0
OpenAttempts	0	0	0	0	0	0
OpenFailures	0	0	0	0	0	0
UnsupportClienttype	0	0	0	0	0	0
UnsupportedVersion	0	0	0	0	0	0
LengthMismatch	0	0	0	0	0	0
UnknownOpcode	0	0	0	0	0	0
UnknownCnum	0	0	0	0	0	0
BadCtype	0	0	0	0	0	0
BadSends	0	0	0	0	0	0
WrongObjects	0	0	0	0	0	0
WrongOpcode	0	0	0	0	0	0
TimedoutClients	0	0	0	0	0	0
AuthFailures	0	0	0	0	0	0
AuthMissing	0	0	0	0	0	0

Poll Interval: 10s 0h:0m:1s

Table 53 describes the COPS Stats tab fields.

Table 53 COPS Stats tab fields

Field	Description
InPkts	The total number of COPS messages received for this client type.
OutPkts	The total number of COPS messages sent for this client type.

Table 53 COPS Stats tab fields (Continued)

Field	Description
InErrs	The total number of COPS messages received for this client type that contained an error in syntax.
TcpConnectAttempts	The total number of TCP connections attempted to this COPS server for this client type.
TcpConnectFailures	The total number of TCP connections to this COPS server for this client type that failed.
OpenAttempts	The total number of attempts to perform a COPS Client-Open to this COPS server for this client type.
OpenFailures	The total number of failed attempts to perform a COPS Client -Open to this COPS server for this client type.
UnsupportClientType	The total number of COPS messages received from this COPS server containing unsupported client types.
UnsupportedVersion	The total number of COPS messages received from this COPS server containing an unsupported protocol version.
LengthMismatch	The total number of COPS messages received from this COPS server for this client type where the COPS protocol message length did not match the actual message length.
UnknownOpcode	The total number of COPS messages received from this COPS server for this client type that contained an unrecognized COPS protocol op code.
UnknownCnum	The total number of COPS messages received from this COPS server for this client type that contained an unrecognized COPS object C-Num.
BadCtype	The total number of COPS messages received from this COPS server for this client type that contained a COPS protocol object C-type that was not defined for the C-Nums known by the COPS client.
BadSends	The total number of COPS messages the client attempted to send to the COPS server for which a transit error occurred.
WrongObjects	The total number of COPS messages received from this COPS server for this client type that contained a set of un-permitted COPS protocol objects.
WrongOpcode	The total number of COPS messages received from this COPS server for this client type containing a COPS protocol op code that should not be sent to a COPS client.
TimeoutClients	The total number of times this client has been shut down for this client type by COPS servers that detected a COPS protocol keepalive timeout.

Table 53 COPS Stats tab fields (Continued)

Field	Description
AuthFailures	The total number of COPS messages received from this COPS server for this client type that could not be authenticated with the authentication method used by the client.
AuthMissing	The total number of COPS messages received from this COPS server for this client type that did not contain required authentication information.

Chapter 4
Implementing QoS Using QoS Wizard and QoS Quick Config

You can configure Quality of Service (QoS) features in your network by using the Web-based QoS Wizard, using the QoS Quick Config pages, or using the Advanced QoS configuration pages available in the Web-based management user interface.

This chapter shows how to use the QoS Wizard and QoS Quick Config pages to configure QoS parameters for the Ethernet Switches 460 and 470.

This chapter covers the following topics:

- "Using QoS Wizard"
- "Using QoS Quick Config" on page 216

Using QoS Wizard

The QoS Wizard provides a set of Web pages that allows you to specify common QoS settings for the Ethernet Switches 460 and 470.

⚠ **Warning:** Nortel recommends that you use the QoS Wizard for your *initial* configuration only. Each time the QoS Wizard is initiated, all existing configurations are reset to the default values. After you complete the *initial* QoS Wizard configuration method, you can then customize traffic treatment using the QoS Advanced configuration process.

This section discusses the following topics:

- "Configuring Standard traffic with the QoS Wizard"
- "Prioritizing traffic with the QoS Wizard" on page 190
- "Prioritizing VLANs with the QoS Wizard" on page 193
- "Prioritizing IP applications with the QoS Wizard" on page 200
- "Prioritizing user defined flows with the QoS Wizard" on page 206

Note: All the settings you configure with QoS Wizard are actually set when you click the final Finish and see the Session Confirmation page.

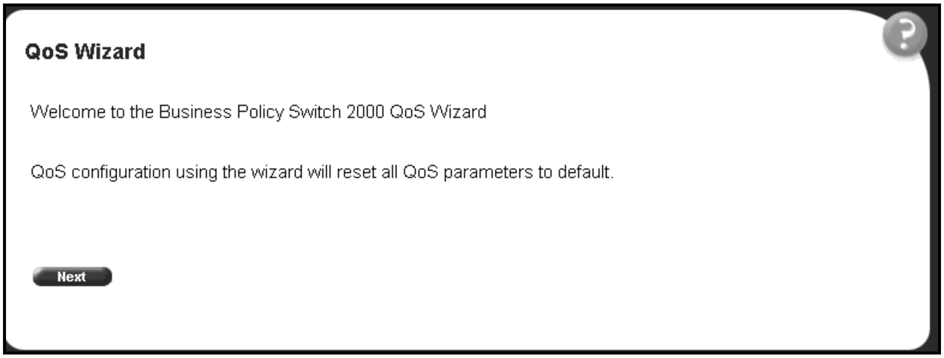
Configuring Standard traffic with the QoS Wizard

To use the QoS Wizard to configure Standard traffic:

1 From the main menu, choose Application > QoS > QoS Wizard.

The QoS Wizard opens (Figure 88).

Figure 88 QoS Wizard opening page



QoS Wizard

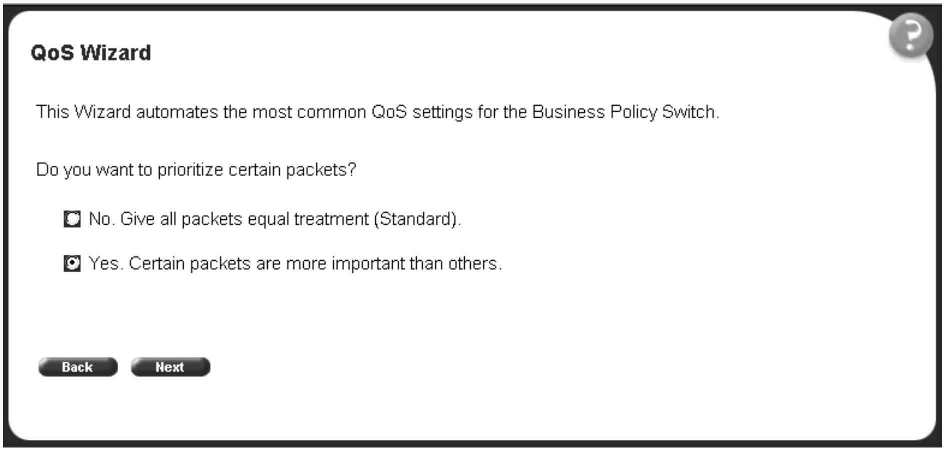
Welcome to the Business Policy Switch 2000 QoS Wizard

QoS configuration using the wizard will reset all QoS parameters to default.

2 To continue the configuration process, click Next.

A packet prioritization selection page opens (Figure 89).

Figure 89 Packet prioritization selection page



QoS Wizard

This Wizard automates the most common QoS settings for the Business Policy Switch.

Do you want to prioritize certain packets?

○ No. Give all packets equal treatment (Standard).

● Yes. Certain packets are more important than others.

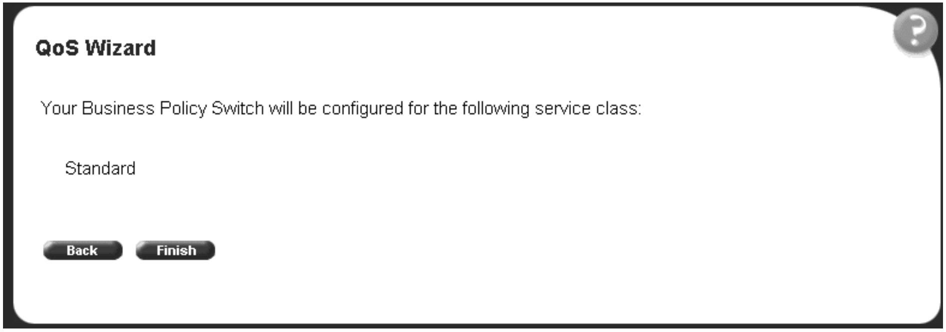
3 Select No.

4 Click Next.

A Standard prioritization page opens (Figure 90).

Note: If you want to prioritize traffic, skip this step and continue the steps outlined in "Prioritizing traffic with the QoS Wizard".

Figure 90 Standard prioritization page



QoS Wizard

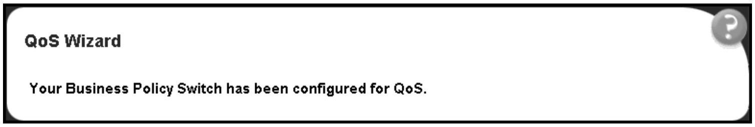
Your Business Policy Switch will be configured for the following service class:

Standard

5 To complete the configuration process, click Finish.

The session confirmation page appears (Figure 91).

Figure 91 Session confirmation page



QoS Wizard

Your Business Policy Switch has been configured for QoS.

Prioritizing traffic with the QoS Wizard

You can specify that different types of traffic in your network configuration be marked with different priority levels.

The QoS Wizard allows you to prioritize traffic flows by:

- VLAN
- IP application
- User defined flow

Using the QoS Wizard, you can prioritize traffic by one of these categories, by two categories, or by all three. Also, you can define more than one flow in each category. The QoS Wizard leads you through the following four general steps in defining each flow you want to prioritize:

- Step 1 is setting the category of prioritized traffic flow—VLAN, IP Application, or User Defined Flow.

  The User Defined Flow has two steps in classifying the flow:

  — Policy Label

  — Policy Definition
- Step 2/3 is setting a Meter for the flow, if required.
- Step 3/4 is choosing the Service Class or Drop for the flow.

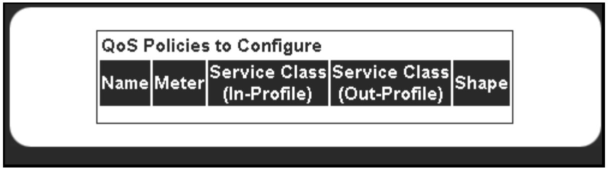
  If you are metering traffic within the flow, you choose two separate Service Classes: one for In-Profile traffic, and one for Out-of-Profile traffic. If you are not metering traffic within the flow, you choose only one Service Class.
- Step 4/5 is setting a Shaper, or shaping criteria, for the flow, if required.

The QoS Wizard automatically steps you through each of these four steps for each flow you want to prioritize. You can prioritize flows within three different categories and more than one flow per category. When you fill the resources of one category, you are not prompted again. You see a check mark next to that category if there are some flows to be configured, or an X mark next to that category if there are no flows to be configured in the packet prioritization screen (Figure 93 on page 193). You cannot configure more flows for that category. When you fill the QoS Wizard resources, are not prompted again.The QoS Wizard automatically presents screens to configure each prioritized traffic flow.

Additionally, the packet prioritization screen has a Status button that displays a QoS Policies to Configure in a pop-up window (Figure 92). As you finish configuring each type of flow, this pop-up window displays the flows you configure using the QoS Wizard listed. When you finish the QoS Wizard, the policies are implemented.

Note: The system configures the QoS parameters that you configure using the QoS Wizard only when you click Finish.

Figure 92 QoS Policies to Configure window



QoS Policies to Configure

Name	Meter	Service Class (In-Profile)	Service Class (Out-Profile)	Shape

The QoS Policies to Configure table has the following fields:

— Name—Displays the name of the policy.

— Meter—Displays whether you are metering the data in the flow associated with the policy.

— Service Class (In-Profile)—Displays the service class of the flow associated with the policy. If you are metering the data, this is the service class for the data that fits the metered profile.

— Service Class (Out-Profile)—Displays the service class of metered data that falls outside the profile.

— Shape—Displays whether you are shaping the data in the flow associated with the policy.

To assign priority levels to different types of network traffic:

1 From the main menu, choose Application > QoS > QoS Wizard.

The QoS Wizard opens (Figure 88 on page 188).

2 To continue the configuration process, click Next.

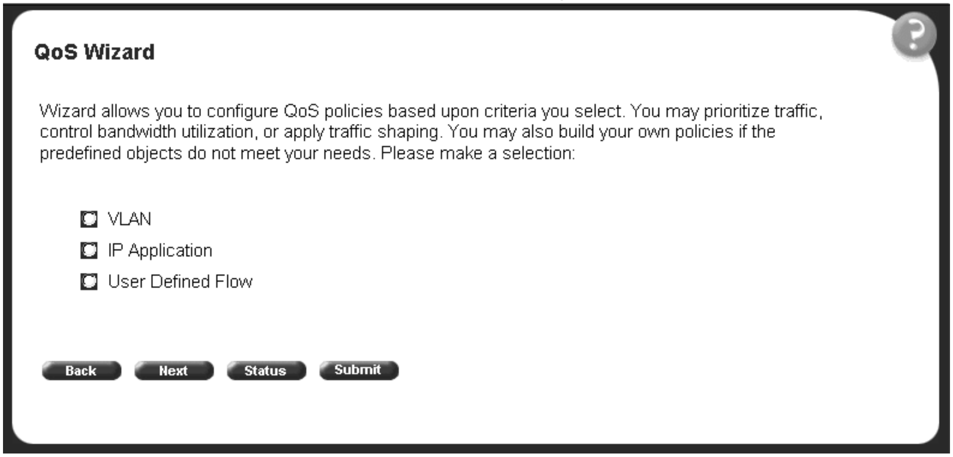
A packet prioritization selection page opens (Figure 89 on page 189).

3 Select Yes.

4 Click Next.

A packet prioritization explanation page opens (Figure 93).

Figure 93 Packet prioritization explanation page



QoS Wizard

Wizard allows you to configure QoS policies based upon criteria you select. You may prioritize traffic, control bandwidth utilization, or apply traffic shaping. You may also build your own policies if the predefined objects do not meet your needs. Please make a selection:

- ☐ VLAN
- ☐ IP Application
- ☐ User Defined Flow

a To see the policies you have configured, click Status.

The QoS Policies to Configure table opens in a pop-up window (Figure 92 on page 192).

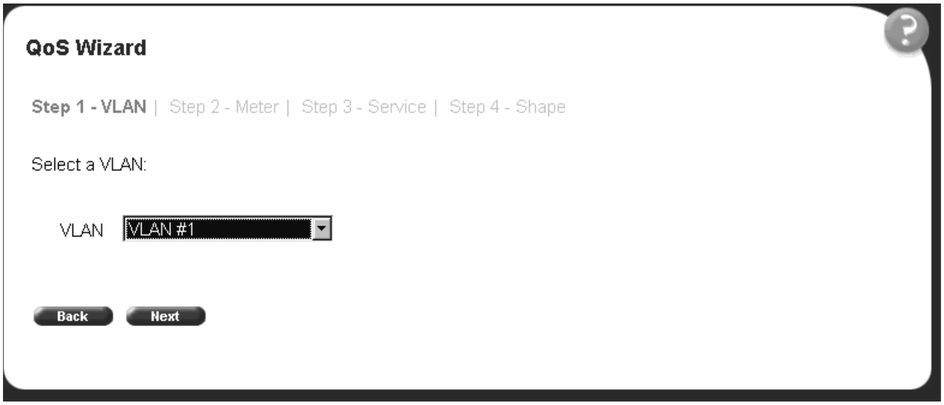
Prioritizing VLANs with the QoS Wizard

You can specify that different VLANs in your network configuration be marked with different priority levels.

1 In the packet prioritization window (Figure 93), click VLAN, and click Next.

A VLAN prioritization selection page opens (Figure 94).

Figure 94 VLAN prioritization selection page


Step 1 - VLAN | Step 2 - Meter | Step 3 - Service | Step 4 - Shape
Back
Next

QoS Wizard

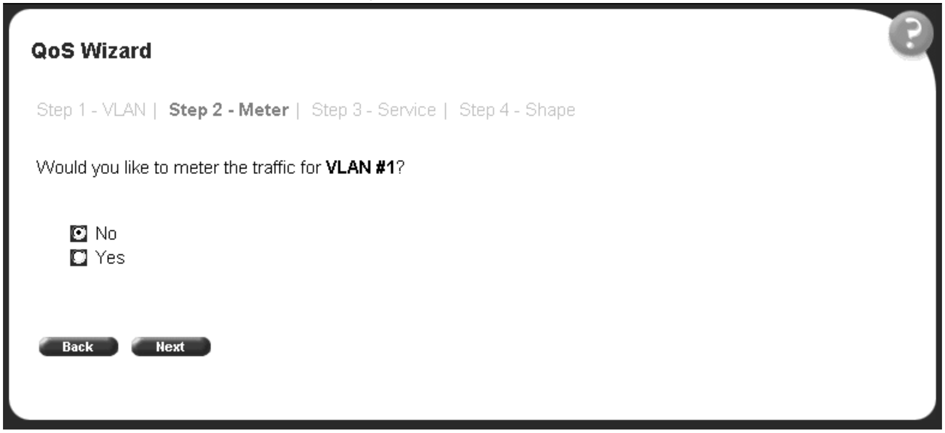
Select a VLAN:

VLAN: VLAN #1

2 Choose the VLAN and click Next.

A page opens (Figure 95) that asks if you want to set a Meter for the specified VLAN.

Figure 95 Meter for VLAN page


Step 1 - VLAN | Step 2 - Meter | Step 3 - Service | Step 4 - Shape
Back
Next

QoS Wizard

Would you like to meter the traffic for **VLAN #1**?

● No
○ Yes

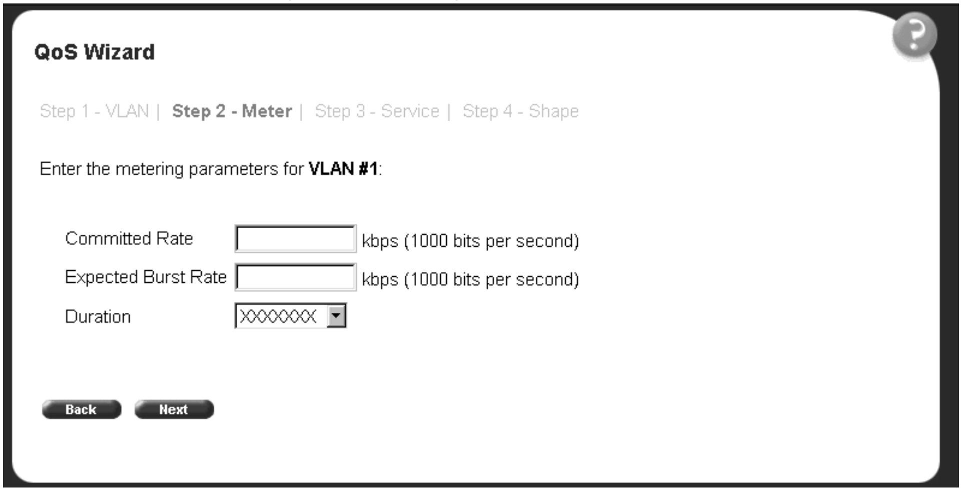
3 If you do not want to set a Meter, click No.

The system opens to the Service Class selection page (Figure 97 on page 196), which appears with only one Service Class to set. You cannot have In-Profile and Out-of-Profile without metering data.

4 If you want to set a Meter, click Yes.

A page opens (Figure 96) that allows you to set a Meter for the specified VLAN.

Figure 96 Meter setting for VLAN page



QoS Wizard

Step 1 - VLAN | **Step 2 - Meter** | Step 3 - Service | Step 4 - Shape

Enter the metering parameters for **VLAN #1**:

Committed Rate kbps (1000 bits per second)

Expected Burst Rate kbps (1000 bits per second)

Duration XXXXXXX

5 Enter the committed rate you want for this Meter.

6 Enter the expected burst rate you want for this Meter.

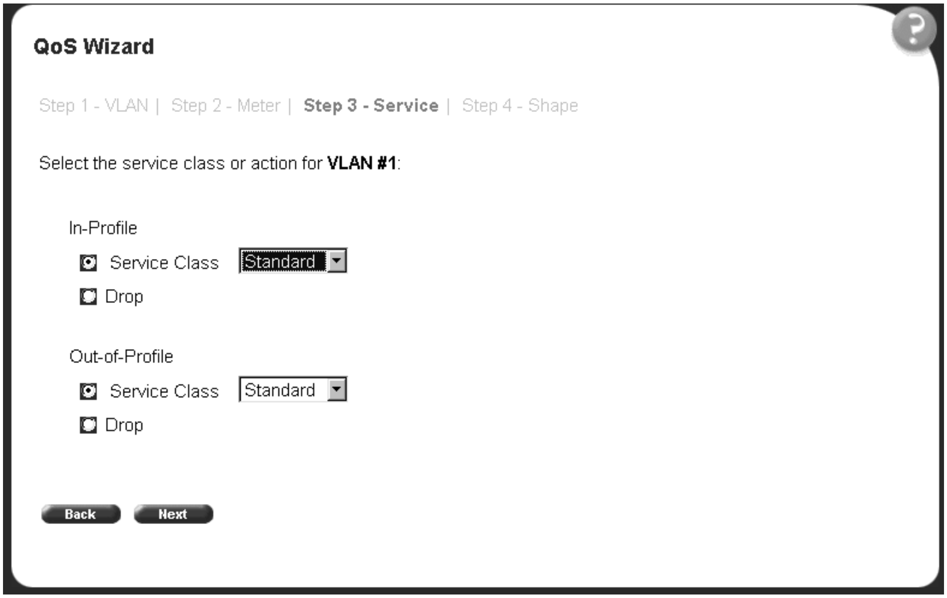
The system calculates a series of 7 or fewer possible durations for the committed and expected burst rates you set.

7 Choose the Duration you want.

8 Click Next.

A page opens (Figure 97) that allows you to select a Service Class separately for both the In-Profile and Out-of-Profile Action for the specified VLAN.

Figure 97 Service Class selection for VLAN page



QoS Wizard

Step 1 - VLAN | Step 2 - Meter | **Step 3 - Service** | Step 4 - Shape

Select the service class or action for **VLAN #1**:

In-Profile

● Service Class: Standard

○ Drop

Out-of-Profile

● Service Class: Standard

○ Drop

9 Click either Service Class or Drop.

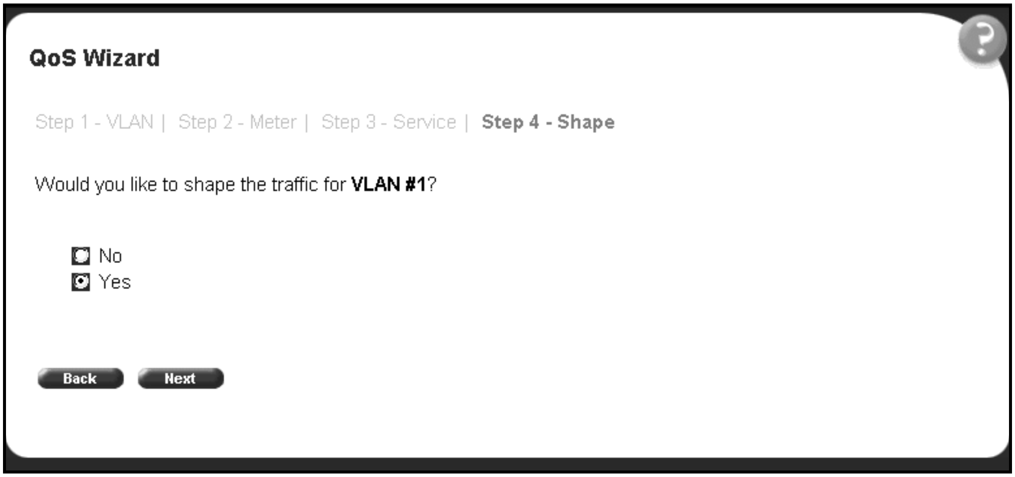
If you click Service Class, choose the Service Class you want from the drop-down list.

If you click Drop, the traffic in the specified VLAN is dropped.

10 Click Next.

A page opens (Figure 98 on page 197) that allows you to set shaping criteria for the specified VLAN.

Figure 98 Shaper for VLAN page



QoS Wizard

Step 1 - VLAN | Step 2 - Meter | Step 3 - Service | Step 4 - Shape

Would you like to shape the traffic for **VLAN #1**?

○ No
● Yes

11 If you do not want to shape traffic for the specified VLAN, click No.

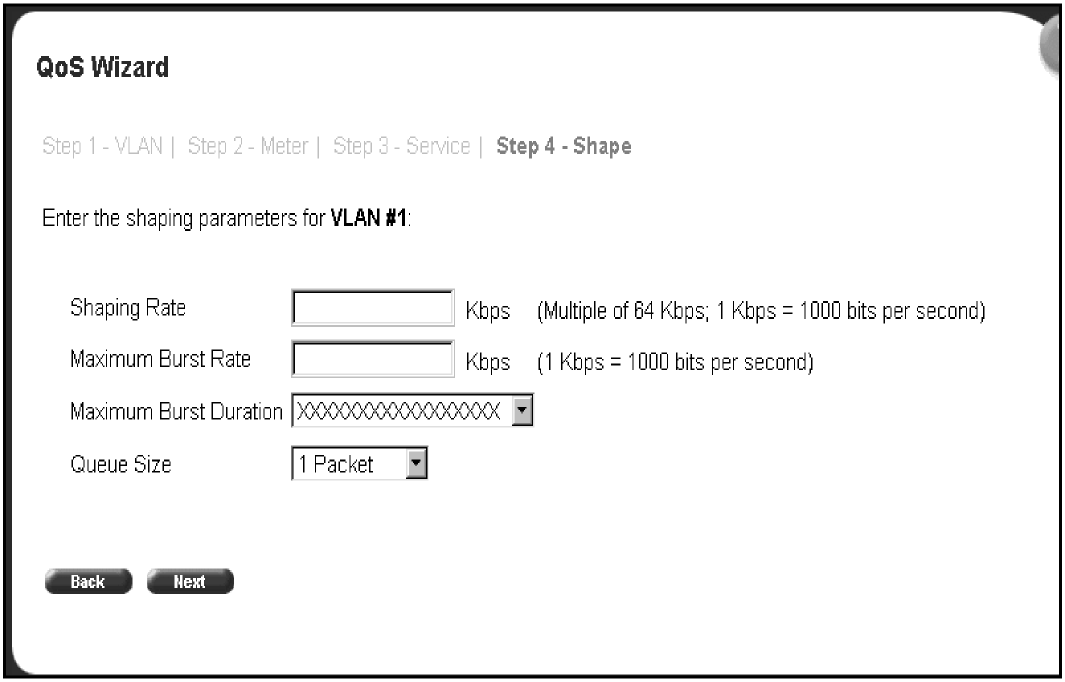
The system opens to a page (Figure 100 on page 199) that prompts you if you want to prioritize traffic for another VLAN.

If you fill the resources of the QoS Wizard, you are not prompted for another VLAN.

12 If you want to shape traffic for the specified VLAN, click Yes.

A page opens (Figure 99 on page 198) that allows you to set shaping parameters for the specified VLAN.

Figure 99 Setting shaping parameters for VLAN page



QoS Wizard

Step 1 - VLAN | Step 2 - Meter | Step 3 - Service | Step 4 - Shape

Enter the shaping parameters for **VLAN #1**:

Shaping Rate [ ] Kbps (Multiple of 64 Kbps; 1 Kbps = 1000 bits per second)

Maximum Burst Rate [ ] Kbps (1 Kbps = 1000 bits per second)

Maximum Burst Duration XXXXXXXXXXXXXXXXX

Queue Size 1 Packet

13 Enter the shaping rate you want for this Shaper.

The system rounds up shaping rates you enter, including 0, to multiples of 64 Kbps.

14 Enter the maximum burst rate you want for this Shaper.

The system calculates a series of 6 or fewer possible durations for the shaping and maximum burst rates you set.

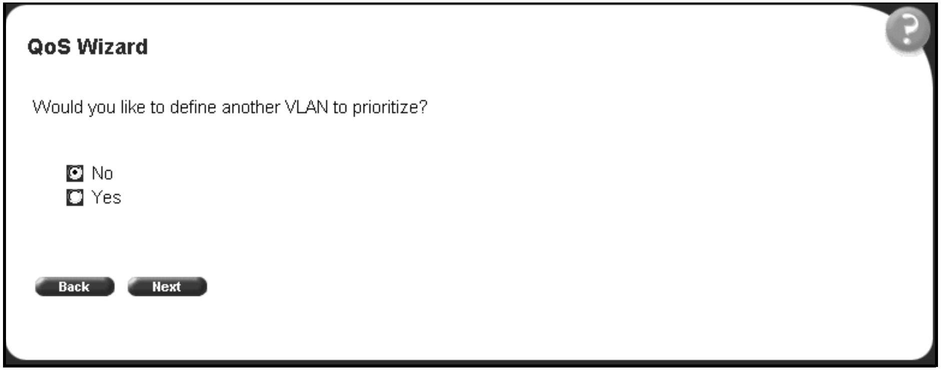
15 Choose the Maximum Burst Duration from the drop-down list.

16 Choose the queue size you want for this Shaper.

17 Click Next.

A page opens (Figure 100) that asks you if you want to prioritize traffic for another VLAN. If you fill the resources of the QoS Wizard, you will not be prompted for another VLAN.

Figure 100 Additional VLANs page



QoS Wizard

Would you like to define another VLAN to prioritize?

● No
○ Yes

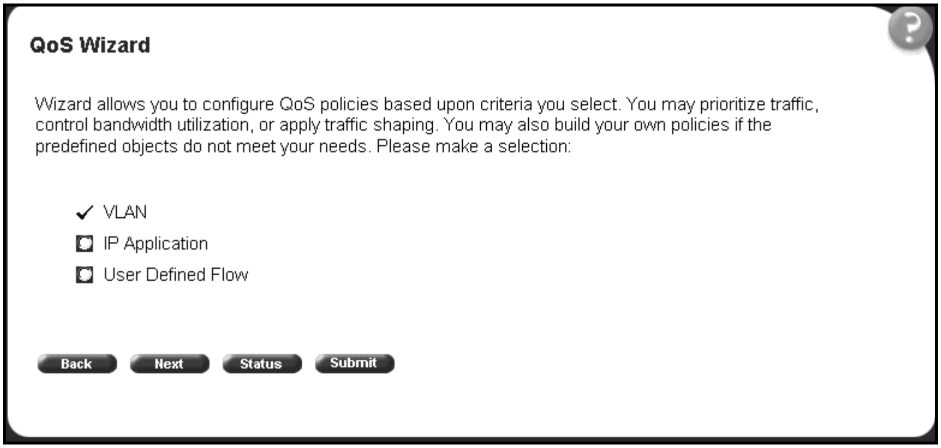
18 If you want to prioritize traffic for another VLAN, click Yes and Next.

The system returns you to the VLAN prioritization page (Figure 94 on page 194), and you continue through steps 1 to 17 for the next VLAN.

19 If you do not want to prioritize traffic for another VLAN, click No and Next.

The system returns you to the packet prioritization page (Figure 101), with a check mark next to VLAN. If you click Status, the QoS Policies to Configure table listing your new entry simultaneously appears in a pop-up window (Figure 102).

Figure 101 Packet prioritization page with prioritized VLANs

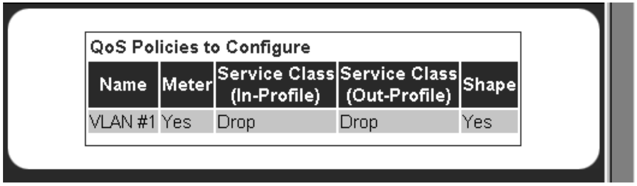


QoS Wizard

Wizard allows you to configure QoS policies based upon criteria you select. You may prioritize traffic, control bandwidth utilization, or apply traffic shaping. You may also build your own policies if the predefined objects do not meet your needs. Please make a selection:

✓ VLAN
☐ IP Application
☐ User Defined Flow

Figure 102 QoS Policies to Configure window with VLAN entry



QoS Policies to Configure

Name	Meter	Service Class (In-Profile)	Service Class (Out-Profile)	Shape
VLAN #1	Yes	Drop	Drop	Yes

20 When you finish with the table, click Back, then click Submit.

You see a session confirmation page.

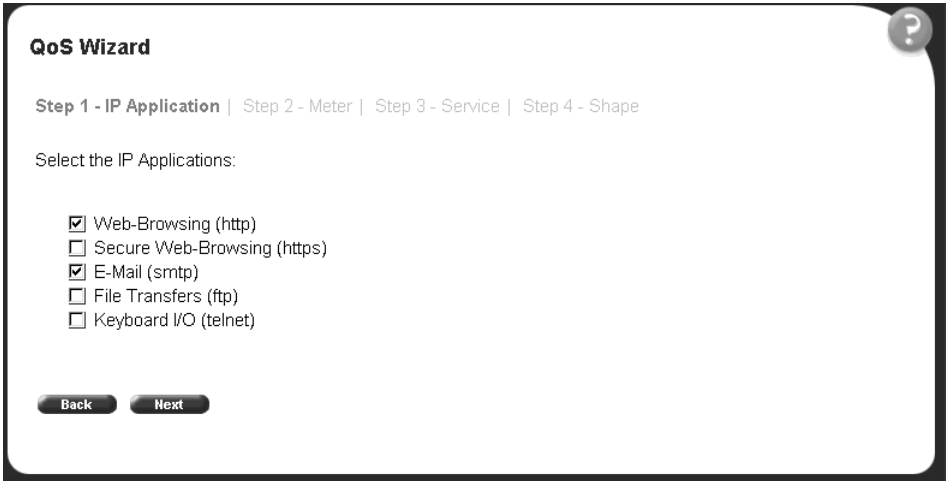
Prioritizing IP applications with the QoS Wizard

You can specify that different IP applications in your network configuration are marked with different priority levels.

1 In the packet prioritization window (Figure 93 on page 193), click IP Application, and click Next.

An IP Application prioritization selection page opens (Figure 103).

Figure 103 IP Application prioritization page



QoS Wizard

Step 1 - IP Application | Step 2 - Meter | Step 3 - Service | Step 4 - Shape

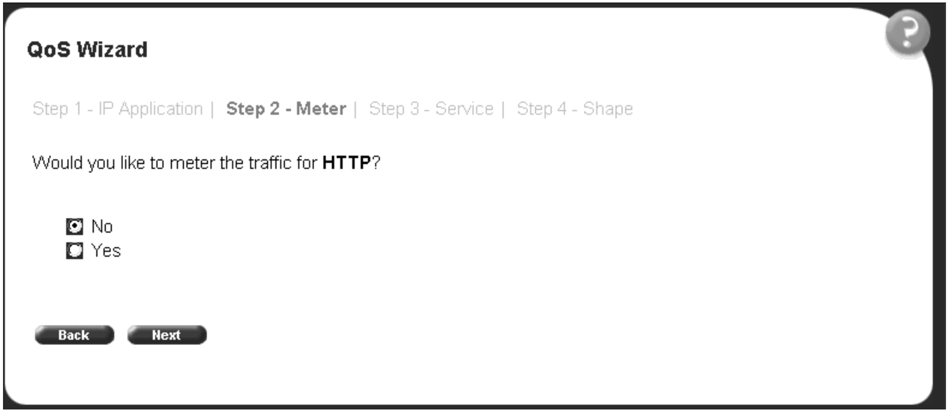
Select the IP Applications:

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

2 Click the applications you want to prioritize and click Next.

A page opens (Figure 104) that asks if you want to set a Meter for the specified IP Application.

Figure 104 Meter for IP Application page



QoS Wizard

Step 1 - IP Application | Step 2 - Meter | Step 3 - Service | Step 4 - Shape

Would you like to meter the traffic for **HTTP**?

● No
○ Yes

3 If you do not want to set a Meter, click No.

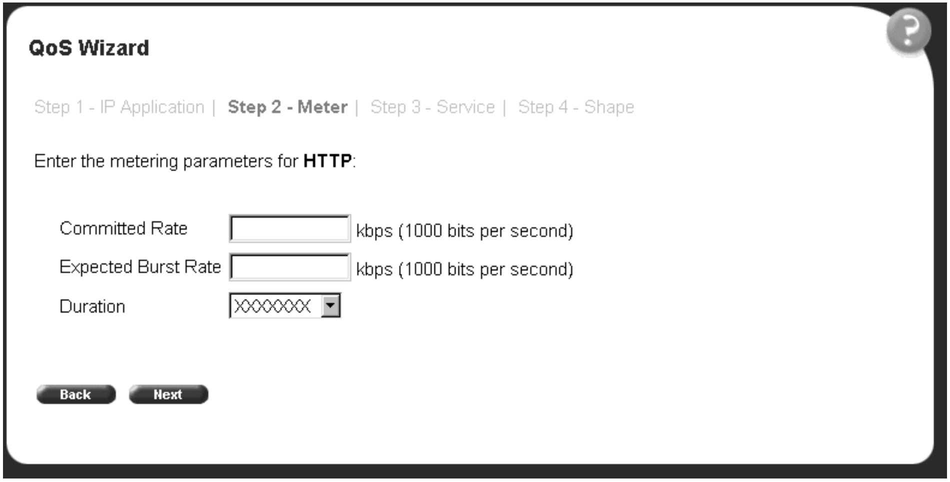
The system opens to the Service Class selection page (Figure 106 on page 203), which appears with only one Service Class to set. You cannot have In-Profile and Out-of-Profile without metering data.

4 If you want to set a Meter, click Yes.

A page opens (Figure 105) that allows you to set a Meter for the specified IP Application.

None of the filters, filter group, meter, shaper, and policy are actually created until Steps 1-4 are completed and submitted.

Figure 105 Meter setting for IP Application page



QoS Wizard

Step 1 - IP Application | **Step 2 - Meter** | Step 3 - Service | Step 4 - Shape

Enter the metering parameters for **HTTP**:

Committed Rate [ ] kbps (1000 bits per second)

Expected Burst Rate [ ] kbps (1000 bits per second)

Duration XXXXXXX

5 Enter the committed rate you want for this Meter.

6 Enter the expected burst rate you want for this Meter.

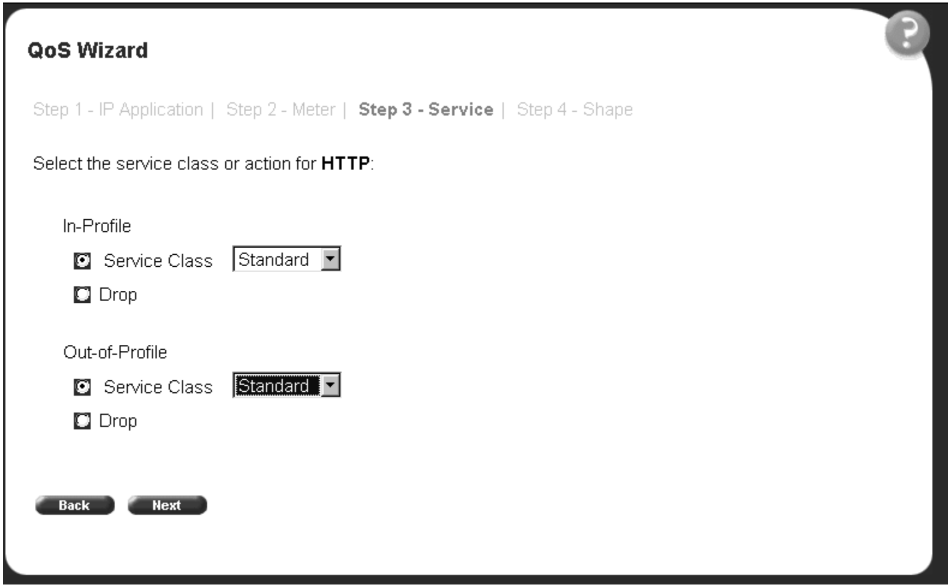
The system calculates a series of 7 or fewer possible durations for the committed and expected burst rates you set.

7 Choose the Duration you want.

8 Click Next.

A page opens (Figure 106) that allows you to select a Service Class separately for both the In-Profile and Out-of-Profile Action for the specified IP Application.

Figure 106 Service Class selection for IP Application page



QoS Wizard

Step 1 - IP Application | Step 2 - Meter | Step 3 - Service | Step 4 - Shape

Select the service class or action for **HTTP**:

In-Profile

● Service Class: Standard

○ Drop

Out-of-Profile

● Service Class: Standard

○ Drop

9 Click either Service Class or Drop.

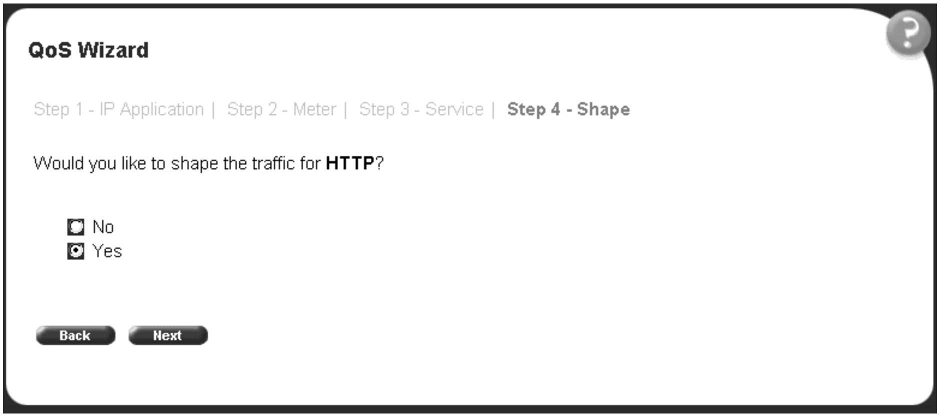
If you click Service Class, choose the Service Class you want from the drop-down list.

If you click Drop, the traffic in the specified IP Application is dropped.

10 Click Next.

A page opens (Figure 107) that allows you to set shaping criteria for the specified IP Application.

Figure 107 Shaper for IP Application page



QoS Wizard

Step 1 - IP Application | Step 2 - Meter | Step 3 - Service | Step 4 - Shape
Back
Next

Would you like to shape the traffic for **HTTP**?

○ No
● Yes

11 If you do not want to shape traffic for the specified IP Application, click No.

a If you choose more than one IP Application to prioritize, a page opens that asks if you want to set a Meter for the next specified IP Application (Figure 104 on page 201). Repeat steps 3 through 17 for each IP Application you chose.

b If you chose only one IP Application, you have completed the QoS Wizard prioritization process for that flow. The system returns you to the packet prioritization page (Figure 109 on page 206), with a check mark next to IP Application,

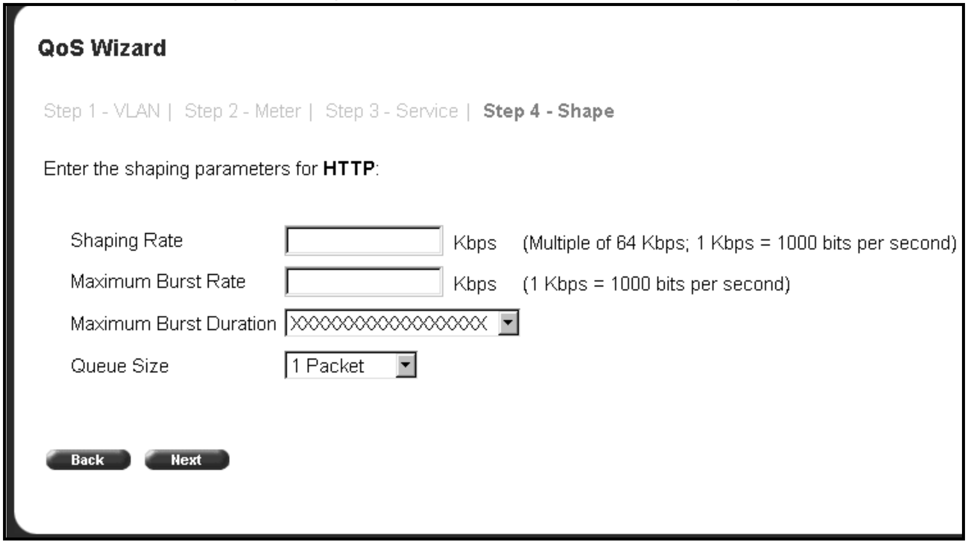
If you fill the resources of the QoS Wizard, you are not prompted for another IP Application.

If you click Status, the QoS Policies to Configure table listing your new entry simultaneously appears in a pop-up window (Figure 110 on page 206).

12 If you want to shape traffic for the specified IP Application, click Yes.

A page opens (Figure 108) that allows you to set shaping parameters for the specified IP Application.

Figure 108 Setting shaping parameters for IP Application page



QoS Wizard

Step 1 - VLAN | Step 2 - Meter | Step 3 - Service | **Step 4 - Shape**

Enter the shaping parameters for **HTTP**:

Shaping Rate Kbps (Multiple of 64 Kbps; 1 Kbps = 1000 bits per second)

Maximum Burst Rate Kbps (1 Kbps = 1000 bits per second)

Maximum Burst Duration XXXXXXXXXXXXXXXXX

Queue Size 1 Packet

13 Enter the shaping rate you want for this Shaper.

The system rounds up shaping rates you enter, including 0, to multiples of 64 Kbps.

14 Enter the maximum burst rate you want for this Shaper.

The system calculates a series of 6 or fewer possible durations for the shaping and maximum burst rates you set.

15 Choose the Maximum Burst Duration from the drop-down list.

16 Choose the queue size you want for this Shaper.

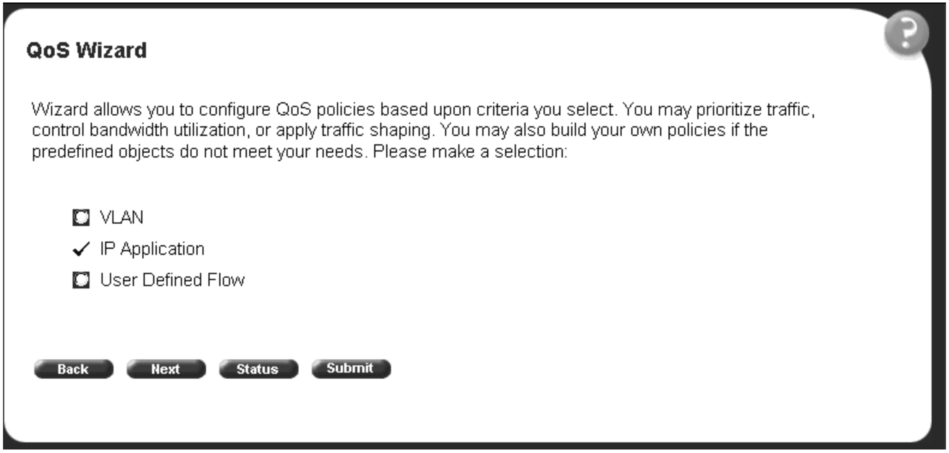
17 Click Next.

- **a** If you chose more than one IP Application to prioritize, a page opens that asks if you want to set a Meter for the next specified IP Application (Figure 104 on page 201). Repeat steps 3 through 17 for each IP Application you chose.
- **b** If you chose just one IP Application, you have completed the QoS Wizard prioritization process for that flow. The system returns you to the packet prioritization page (Figure 109 on page 206), with a check mark next to IP

Application. Press the Status button to view the QoS Policies to Configure table listing your new entry in a pop-up window (Figure 110).

If you fill the resources of the QoS Wizard, you are not prompted for another IP Application.

Figure 109 Packet prioritization page with prioritized IP Application(s)

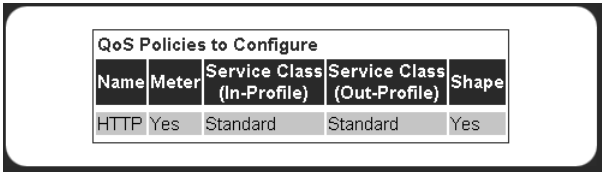


QoS Wizard

Wizard allows you to configure QoS policies based upon criteria you select. You may prioritize traffic, control bandwidth utilization, or apply traffic shaping. You may also build your own policies if the predefined objects do not meet your needs. Please make a selection:

□ VLAN
✓ IP Application
□ User Defined Flow

Figure 110 QoS Policies to Configure window with IP Application entry



QoS Policies to Configure

Name	Meter	Service Class (In-Profile)	Service Class (Out-Profile)	Shape
HTTP	Yes	Standard	Standard	Yes

18 When you are through viewing the table, click Back, then Submit.

You see a session confirmation page.

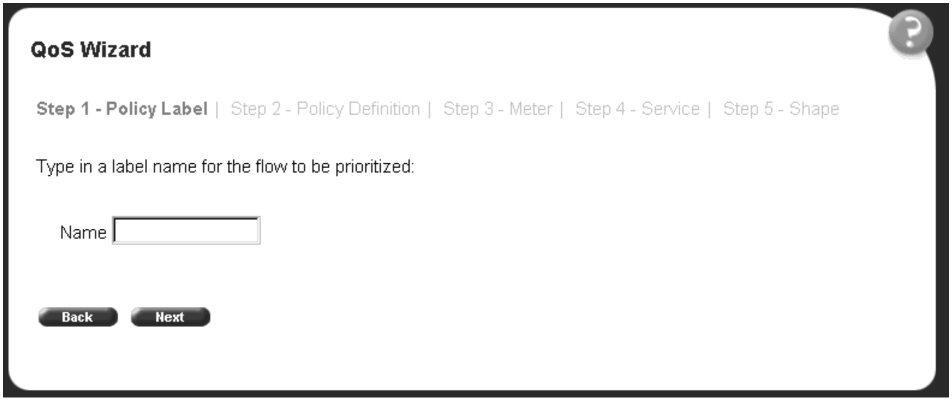
Prioritizing user defined flows with the QoS Wizard

You can specify that different user defined flows in your network configuration be marked with different priority levels.

1 In the packet prioritization window (Figure 93 on page 193), click User Defined Flow, and click Next.

A page opens (Figure 111) that asks the user to assign a name to the flow.

Figure 111 Policy label page



QoS Wizard

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

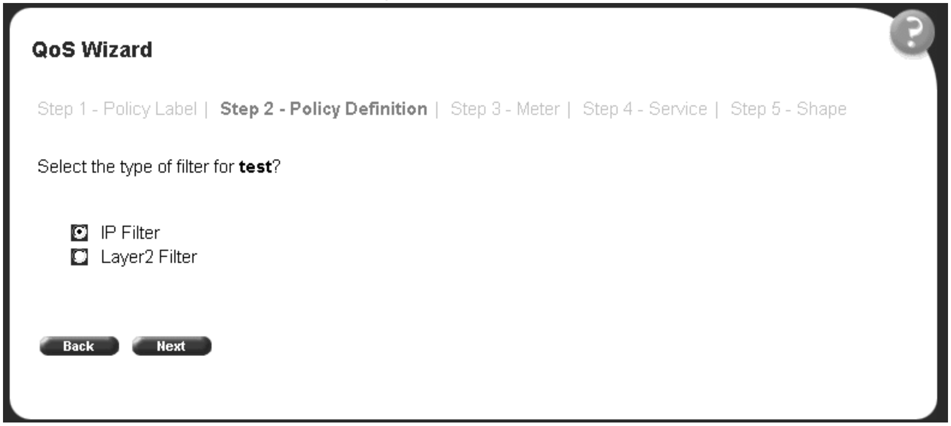
Type in a label name for the flow to be prioritized:

Name

2 Enter the name of the flow and click Next.

A page opens (Figure 112) that asks if you want to set an IP filter or a Layer 2 filter.

Figure 112 Policy definition page



QoS Wizard

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

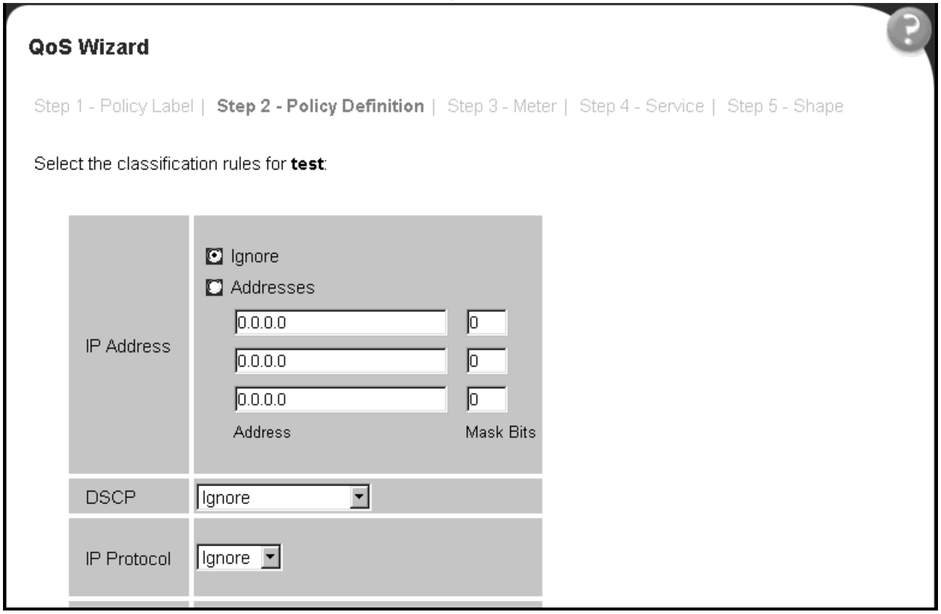
Select the type of filter for **test**?

● IP Filter
○ Layer2 Filter

a If you want an IP filter, click IP Filter and click Next.

A page opens that requests the customer to choose the IP filter criteria for the specified flow (Figure 113 and Figure 114).

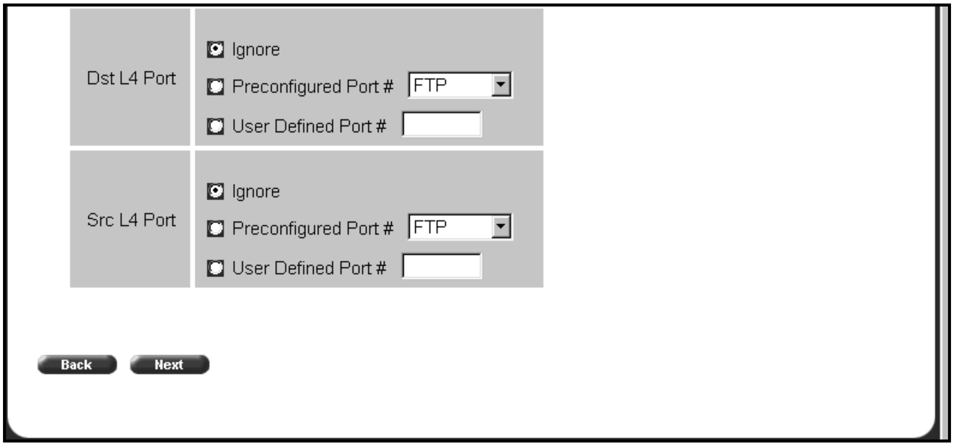
Figure 113 IP classification rules page (1 of 2)


QoS Wizard
Step 1 - Policy Label | Step 2 - Policy Definition | Step 3 - Meter | Step 4 - Service | Step 5 - Shape

Select the classification rules for **test**:

IP Address	● Ignore ○ Addresses 0.0.0.0 0 0.0.0.0 0 0.0.0.0 0 Address Mask Bits
DSCP	Ignore
IP Protocol	Ignore

Figure 114 IP classification rules page (2 of 2)



Dst L4 Port	● Ignore ○ Preconfigured Port # FTP ○ User Defined Port #
Src L4 Port	● Ignore ○ Preconfigured Port # FTP ○ User Defined Port #

— Choose the IP filter parameters you want the flow to have.

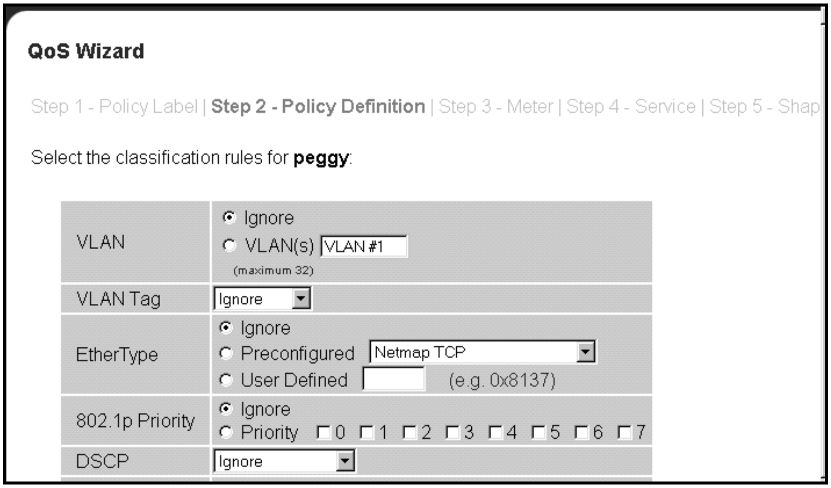
— Click Next.

A page opens (Figure 117 on page 210) that asks if you want to set a Meter for the specified flow.

b If you want a Layer 2 filter, click Layer2 Filter and click Next.

A page opens that requests the customer to choose the Layer 2 filter criteria for the specified flow (Figure 115 and Figure 116).

Figure 115 Layer 2 classification rules page (1 of 2)



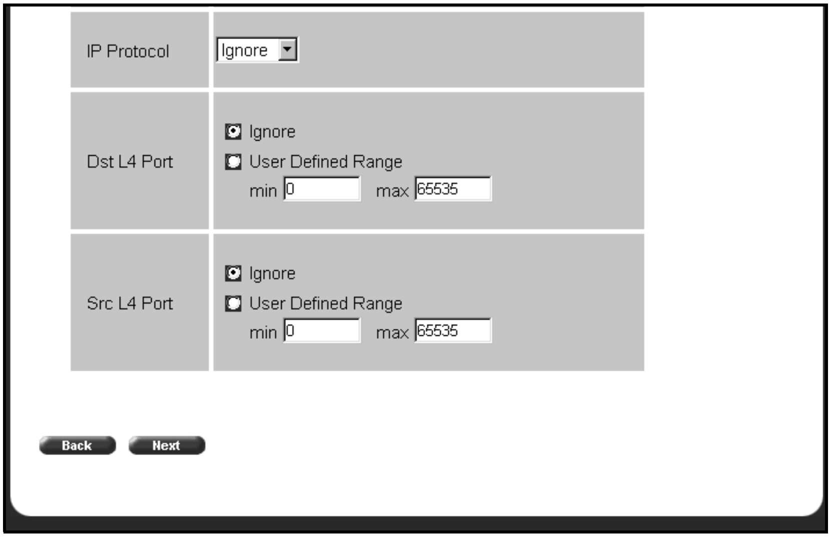
QoS Wizard

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

Select the classification rules for **peggy**:

VLAN	● Ignore ○ VLAN(s) VLAN #1 (maximum 32)
VLAN Tag	Ignore
EtherType	● Ignore ○ Preconfigured Netmap TCP ○ User Defined (e.g. 0x8137)
802.1p Priority	● Ignore ○ Priority □ 0 □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7
DSCP	Ignore

Figure 116 Layer 2 classification rules page (2 of 2)



IP Protocol	Ignore
Dst L4 Port	● Ignore ○ User Defined Range min 0 max 65535
Src L4 Port	● Ignore ○ User Defined Range min 0 max 65535

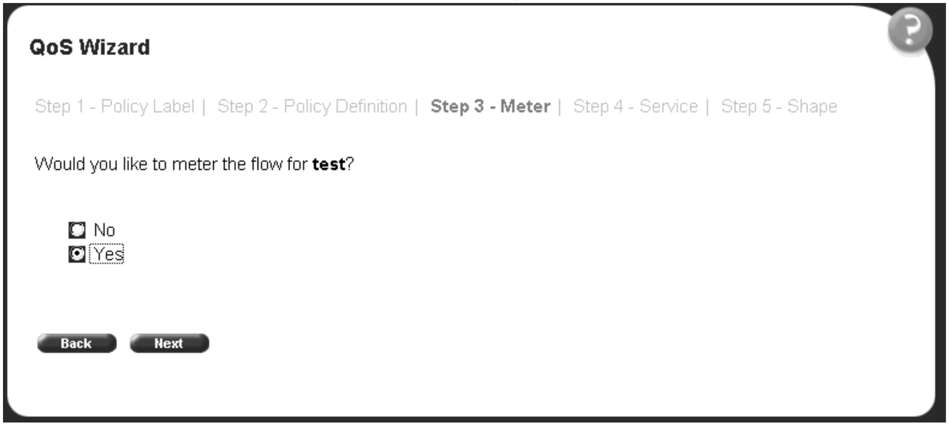
— Choose the Layer 2 filter parameters you want the flow to have.

You can reference up to 32 VLANs with a single Layer 2 filter.

— Click Next.

A page opens (Figure 117) that asks if you want to set a Meter for the specified flow.

Figure 117 Meter for user defined flow page



QoS Wizard

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

Would you like to meter the flow for **test**?

○ No
● Yes

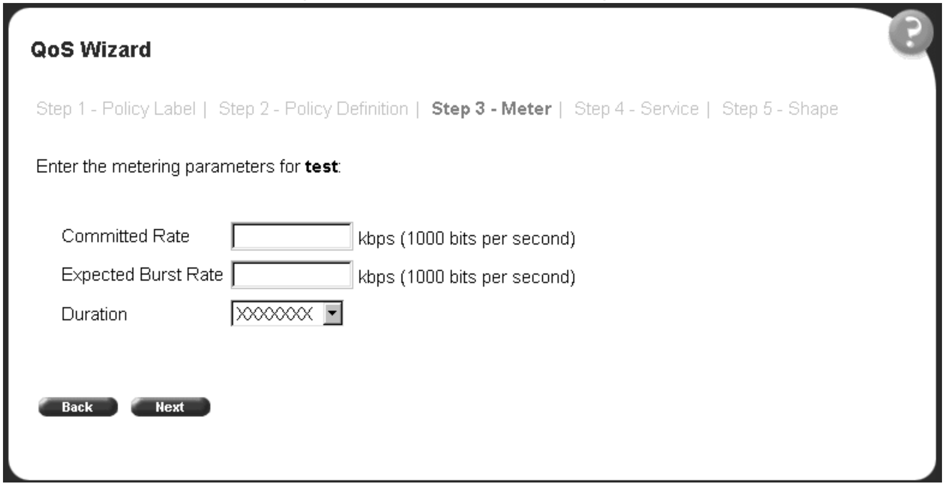
3 If you do not want to set a Meter, click No.

The system opens to the Service Class selection page (Figure 119 on page 212), which appears with only one Service Class to set. You cannot have In-Profile and Out-of-Profile without metering data.

4 If you want to set a Meter, click Yes.

A page opens (Figure 118) that allows you to set a Meter for the specified flow.

Figure 118 Meter setting for user-defined flow page



QoS Wizard

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

Enter the metering parameters for **test**:

Committed Rate [ ] kbps (1000 bits per second)

Expected Burst Rate [ ] kbps (1000 bits per second)

Duration XXXXXXX

5 Enter the committed rate you want for this Meter.

6 Enter the expected burst rate you want for this Meter.

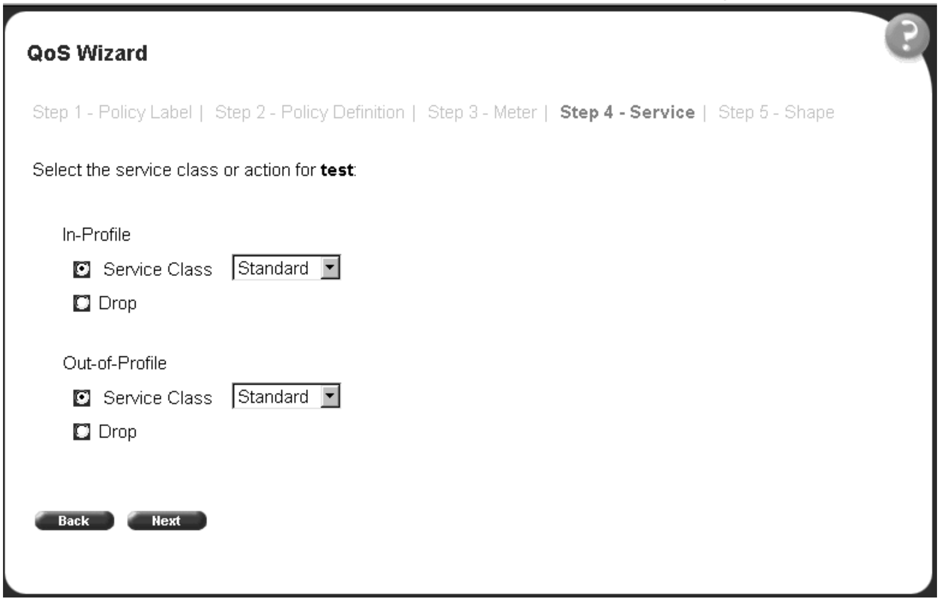
The system calculates a series of 7 or fewer possible durations for the committed and expected burst rates you set.

7 Choose the Duration you want.

8 Click Next.

A page opens (Figure 119) that allows you to select a Service Class separately for both the In-Profile and Out-of-Profile Action for the specified flow.

Figure 119 Service Class selection for user defined flow page



QoS Wizard

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

Select the service class or action for **test**:

In-Profile

● Service Class Standard

○ Drop

Out-of-Profile

● Service Class Standard

○ Drop

9 Click either Service Class or Drop.

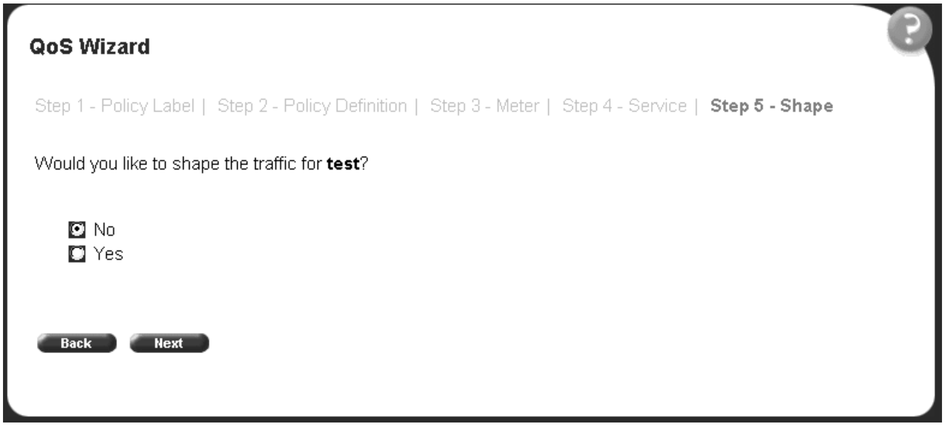
If you click Service Class, choose the Service Class you want from the drop-down list.

If you click Drop, the traffic in the specified flow is dropped.

10 Click Next.

A page opens (Figure 120) that allows you to set shaping criteria for the specified flow.

Figure 120 Shaper for user defined flow page



QoS Wizard

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

Would you like to shape the traffic for **test**?

● No
○ Yes

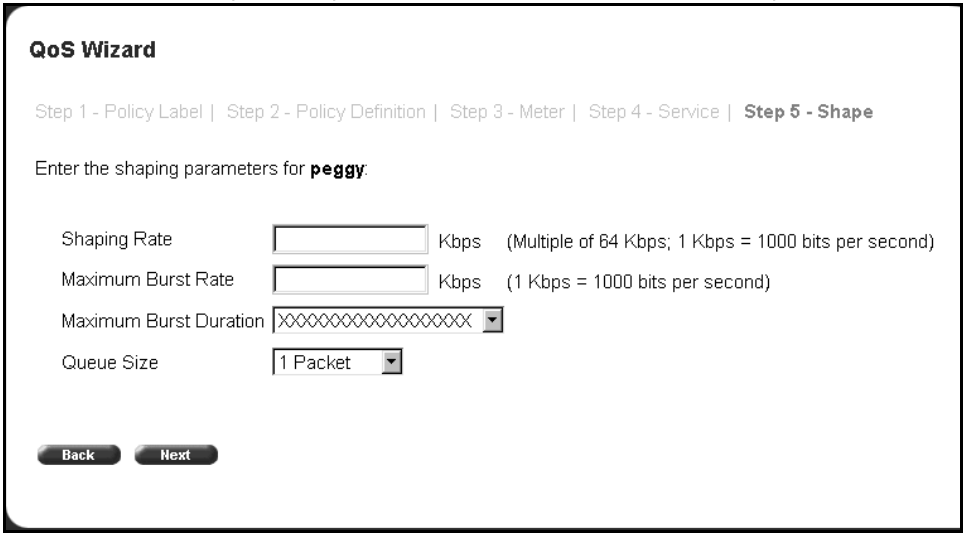
11 If you do not want to shape traffic for the specified flow, click No.

A page opens (Figure 122 on page 215) that asks if you want to prioritize traffic for another user defined flow.

12 If you want to shape traffic for the specified flow, click Yes.

A page opens (Figure 121) that allows you to set shaping parameters for the specified flow.

Figure 121 Setting shaping parameters for user defined flow page



QoS Wizard

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

Enter the shaping parameters for **peggy**:

Shaping Rate [ ] Kbps (Multiple of 64 Kbps; 1 Kbps = 1000 bits per second)

Maximum Burst Rate [ ] Kbps (1 Kbps = 1000 bits per second)

Maximum Burst Duration XXXXXXXXXXXXXXXXXX

Queue Size 1 Packet

13 Enter the shaping rate you want for this Shaper.

The system rounds up shaping rates you enter, including 0, to multiples of 64 Kbps.

14 Enter the maximum burst rate you want for this Shaper.

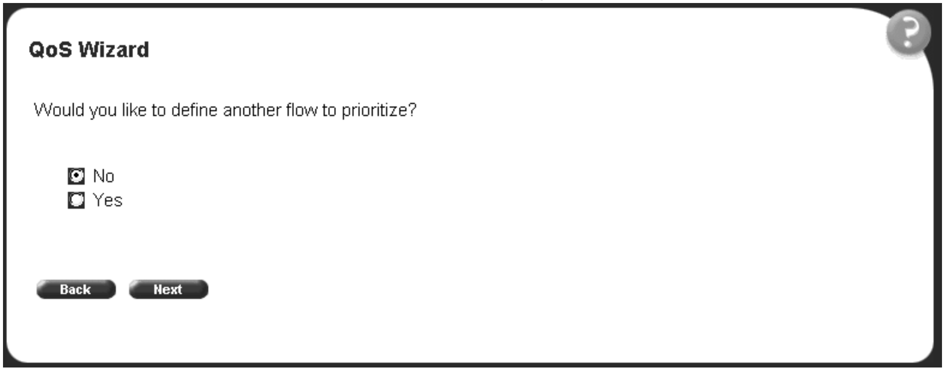
The system calculates a series of 6 or fewer possible durations for the shaping and maximum burst rates you set.

15 Choose the Maximum Burst Duration from the drop-down list.

16 Choose the queue size you want for this Shaper.

A page opens (Figure 122) that asks you if you want to prioritize traffic for another user defined flow.

Figure 122 Additional user defined flows page



QoS Wizard

Would you like to define another flow to prioritize?

● No
○ Yes

17 If you want to prioritize traffic for another user defined flow, click Yes and Next.

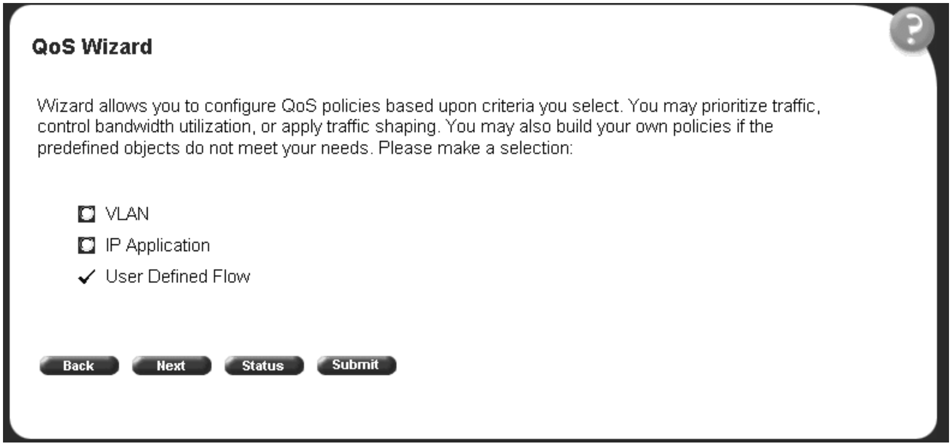
The system returns you to the policy label page (Figure 111 on page 207), and you continue through steps 1 to 17 for the next user defined flow.

If you fill the resources of the QoS Wizard, you are not be prompted for another user defined flow.

18 If you do not want to prioritize traffic for another user defined flow, click No and Next.

The system returns you to the packet prioritization page (Figure 123), with a check mark next to User Defined Flow. Press the Status button to view the QoS Policies to Configure table listing your new entry in a pop-up window (Figure 124).

Figure 123 Packet prioritization page with prioritized user defined flows

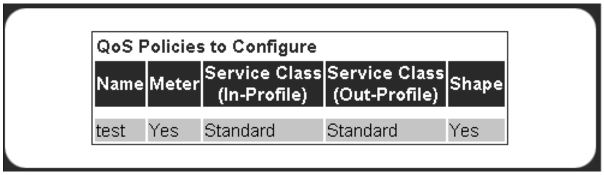


QoS Wizard

Wizard allows you to configure QoS policies based upon criteria you select. You may prioritize traffic, control bandwidth utilization, or apply traffic shaping. You may also build your own policies if the predefined objects do not meet your needs. Please make a selection:

□ VLAN
□ IP Application
✓ User Defined Flow

Figure 124 QoS Policies to Configure window with user defined flow entry



QoS Policies to Configure

Name	Meter	Service Class (In-Profile)	Service Class (Out-Profile)	Shape
test	Yes	Standard	Standard	Yes

19 When you finish viewing the table, click Back and then Submit.

You see a session confirmation page.

Using QoS Quick Config

This section describes how to use the QoS Quick Config option to configure QoS parameters for the Ethernet Switches 460 and 470. This section includes the following topics:

- "Using QoS Quick Config to configure interface groups" on page 217
- "Using QoS Quick Config to configure policies" on page 219

The QoS Quick Config option provides a set of web pages for configuring QoS parameters. Using the QoS Quick Config does not reset the QoS parameters to default values as the QoS Wizard does. The QoS Quick Config condenses the QoS Advanced pages to two pages and uses only default actions and mappings.

Using QoS Quick Config to configure interface groups

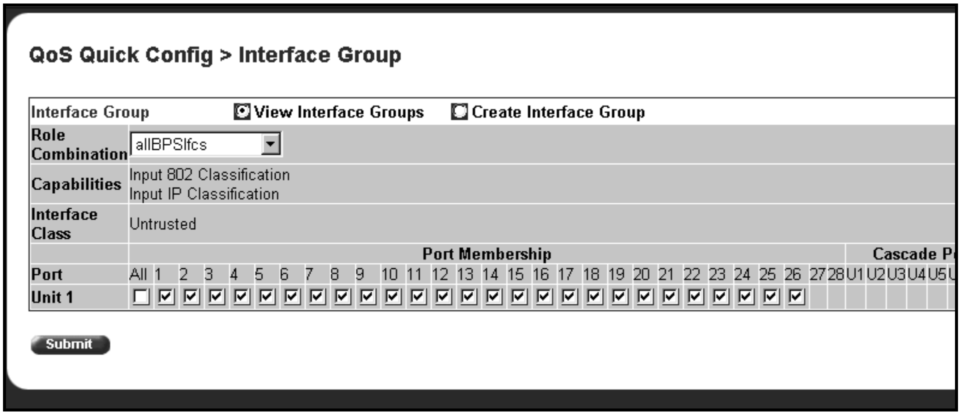
Note: If you do not need to define a new interface group (role combination), you can go directly to "Using QoS Quick Config to configure policies" on page 219.

To use the QoS Quick Config option:

1 From the main menu, choose Application > QoS > QoS Quick Config > Interface Group.

The QoS Quick Config Interface Group page opens (Figure 125) with the View Interface Groups option displaying.

Figure 125 QoS Quick Config Interface Group page—View Interface Group



QoS Quick Config > Interface Group

Interface Group ● View Interface Groups ○ Create Interface Group

Role Combination allBPSIfcs

Capabilities Input 802 Classification
Input IP Classification

Interface Class Untrusted

	Port Membership																													Cascade P					
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	U1	U2	U3	U4	U5	U
Unit 1	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑								

2 To view the parameters of a specified Interface group, choose the Role Combination (Interface Group) you want to view, and use the QoS Quick Config Interface Group page to view the following parameters:

— Capabilities

— Interface Class

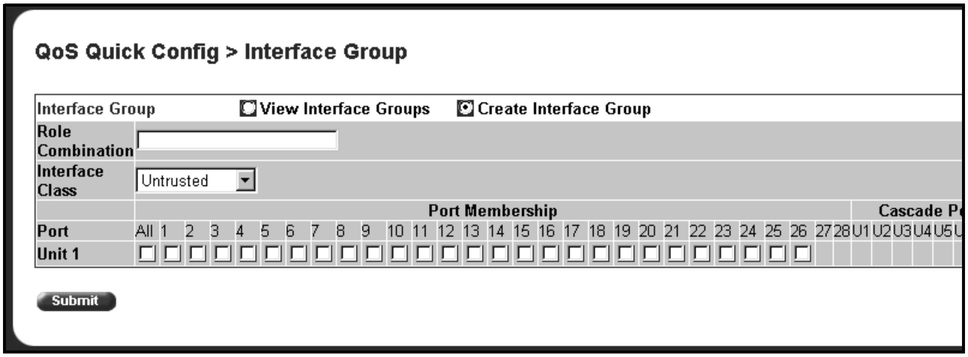
Refer to Chapter 1, “About QoS,” on page 33 for more information on interface classes.

— Port Membership

3 To create an Interface Group, click Create Interface Group.

The QoS Quick Config Interface Group page opens (Figure 126) with the Create Interface Groups option displaying.

Figure 126 QoS Quick Config Interface Group page—Create Interface Group



QoS Quick Config > Interface Group

Interface Group ○ View Interface Groups ● Create Interface Group

Role Combination

Interface Class: Untrusted

	Port Membership																													Cascade P					
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	U1	U2	U3	U4	U5	U
Unit 1	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□								

4 Enter the name you want for the new Role Combination (Interface Group).

5 Choose the Interface Class you want from Trusted, Untrusted, or Unrestricted.

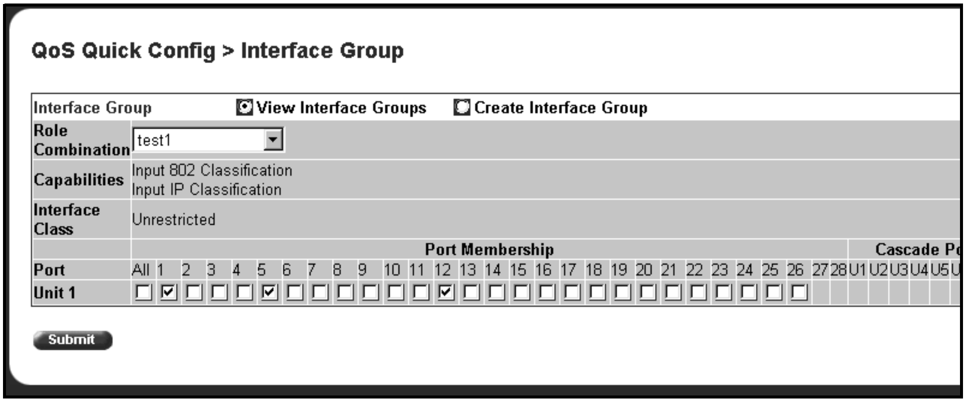
Refer to Chapter 1, “About QoS,” on page 33 for more information on interface classes.

6 Click the ports you want to belong to this Role Combination (Interface Group).

7 Click Submit.

The QoS Quick Config Interface Group page opens (Figure 127) with the View Interface Groups option displaying the new Role combination you created.

Figure 127 QoS Quick Config Interface Group page—View Interface Group



QoS Quick Config > Interface Group

Interface Group ● View Interface Groups ○ Create Interface Group

Role Combination: test1

Capabilities: Input 802 Classification
Input IP Classification

Interface Class: Unrestricted

	Port Membership																												Cascade P					
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	U1	U2	U3	U4	U5	U
Unit 1	□	☑	□	□	□	☑	□	□	□	□	□	□	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□								

8 Go to “Using QoS Quick Config to configure policies”.

Using QoS Quick Config to configure policies

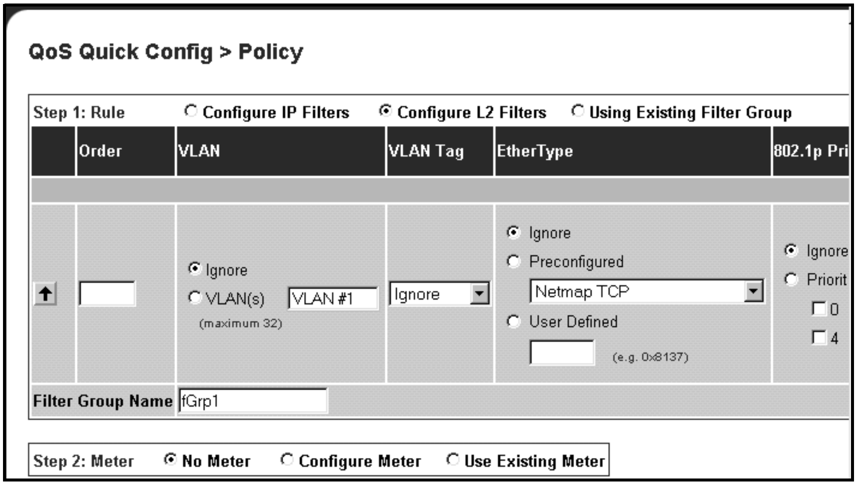
You use QoS Quick Config Web pages to configure the policies.

To configure QoS policies using QoS Quick Config:

➨ From the main menu, choose Application > QoS > QoS Quick Config > Policy.

The QoS Quick Config Policy page opens (Figure 128, Figure 129, and Figure 130 on page 221).

Figure 128 QoS Quick Config Policy page (1 of 3)



QoS Quick Config > Policy

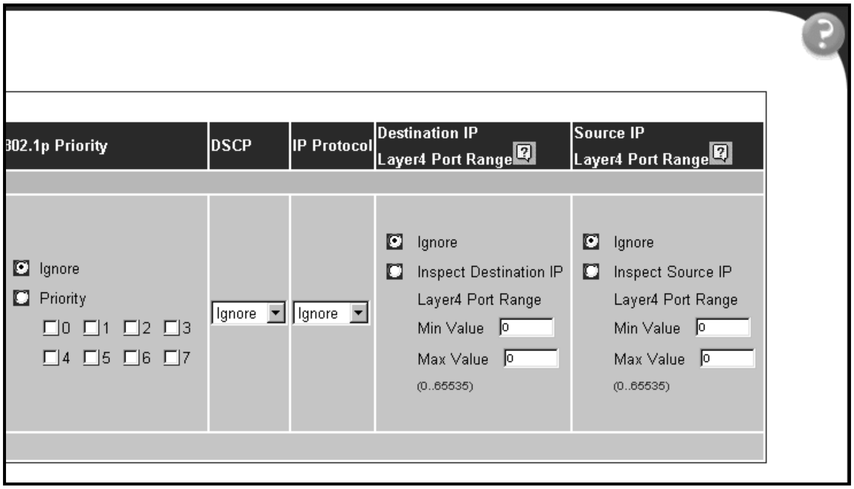
Step 1: Rule ○ Configure IP Filters ● Configure L2 Filters ○ Using Existing Filter Group

	Order	VLAN	VLAN Tag	EtherType	802.1p Pri
↑		● Ignore ○ VLAN(s) VLAN #1 (maximum 32)	Ignore ▾	● Ignore ○ Preconfigured Netmap TCP ▾ ○ User Defined (e.g. 0x8137)	● Ignore ○ Priorit □ 0 □ 4

Filter Group Name fGrp1

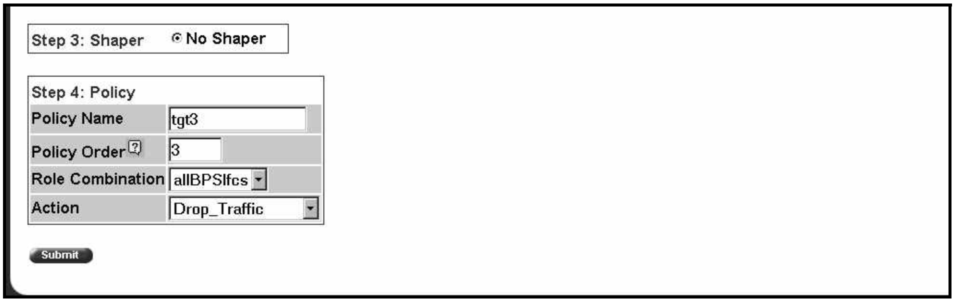
Step 2: Meter ● No Meter ○ Configure Meter ○ Use Existing Meter

Figure 129 QoS Quick Config Policy page (2 of 3)



302.1p Priority	DSCP	IP Protocol	Destination IP Layer4 Port Range	Source IP Layer4 Port Range
● Ignore ○ Priority □0 □1 □2 □3 □4 □5 □6 □7	Ignore ▾	Ignore ▾	● Ignore ○ Inspect Destination IP Layer4 Port Range Min Value 0 Max Value 0 (0..65535)	● Ignore ○ Inspect Source IP Layer4 Port Range Min Value 0 Max Value 0 (0..65535)

Figure 130 QoS Quick Config Policy page (3 of 3)



Step 3: Shaper ● No Shaper

Step 4: Policy	
Policy Name	tgt3
Policy Order	3
Role Combination	allBPSIfcs
Action	Drop_Traffic

The QoS Quick Config Policy page contains the following four steps:

- Step 1: Rule
- Step 2: Meter
- Step 3: Shaper
- Step 4: Policy

This section discusses the following areas:

- "Configuring QoS Quick Config filters"
- "Deleting Qos Quick Config filters from the filter group" on page 226
- "Configuring QoS Quick Config meters" on page 227
- "Configuring QoS Quick Config shapers" on page 228
- "Configuring QoS Quick Config policies" on page 230

Configuring QoS Quick Config filters

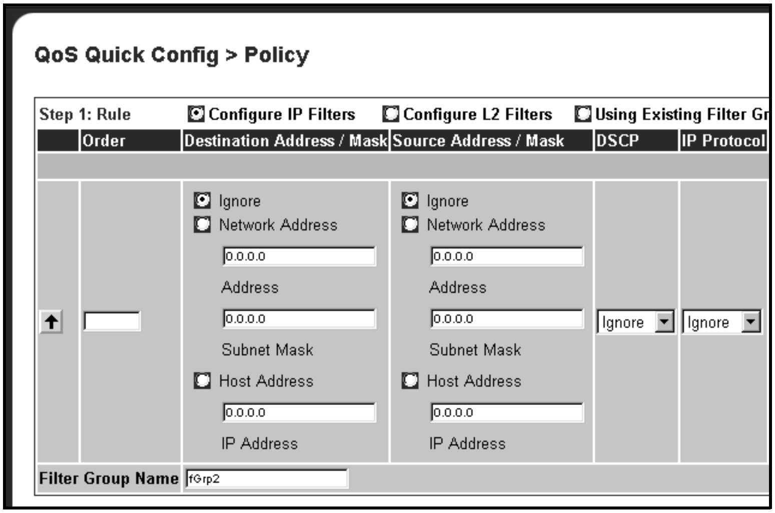
Using the Step 1: Rule section, you either configure a new filter group or use an existing group.

To configure a new IP filter group:

1 Click Configure IP Filters.

The QoS Quick Config Policy page for configuring IP filters opens (Figure 131 and Figure 132).

Figure 131 QoS Quick Config page for configuring IP filters page (1 of 2)



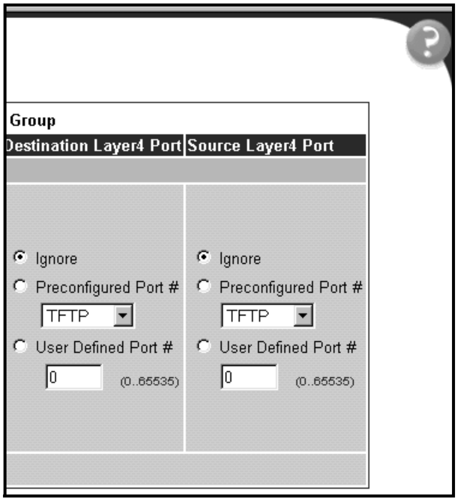
QoS Quick Config > Policy

Step 1: Rule ● Configure IP Filters ○ Configure L2 Filters ○ Using Existing Filter Gr

	Order	Destination Address / Mask	Source Address / Mask	DSCP	IP Protocol
↑		● Ignore ○ Network Address 0.0.0.0 Address 0.0.0.0 Subnet Mask ○ Host Address 0.0.0.0 IP Address	● Ignore ○ Network Address 0.0.0.0 Address 0.0.0.0 Subnet Mask ○ Host Address 0.0.0.0 IP Address	Ignore	Ignore

Filter Group Name fGrp2

Figure 132 QoS Quick Config page for configuring IP filters page (2 of 2)



Group

Destination Layer4 Port	Source Layer4 Port
● Ignore ○ Preconfigured Port # TFTP ○ User Defined Port # 0 (0..65535)	● Ignore ○ Preconfigured Port # TFTP ○ User Defined Port # 0 (0..65535)

2 Enter the number you want for the order of the IP filter you are configuring.

3 Complete the Destination Address/Mask area by either:

— choosing Ignore

- entering the Network Address, Subnet Mask, and Host Address

4 Complete the Source Address/Mask area by either:

- choosing Ignore
- entering the Network Address, Subnet Mask, and Host Address

5 In the DSCP field, choose either Ignore or a value from the drop-down list.

6 In the IP Protocol field, choose either Ignore or a protocol from the drop-down list.

7 Complete the Destination Layer4 Port area by performing one of the following:

- choosing Ignore
- choosing a preconfigured port number from the drop-down list
- entering a value for the User Defined Port Number

8 Complete the Source Layer4 Port area by performing one of the following:

- choosing Ignore
- choosing a preconfigured port number from the drop-down list
- entering a value for the User Defined Port Number

9 Enter the name you want to assign to the newly created IP filter group.

10 Click the arrow on the far left to add the newly created filter into the filter group.

11 Repeat steps 2 to 8 to add additional filters into the filter group.

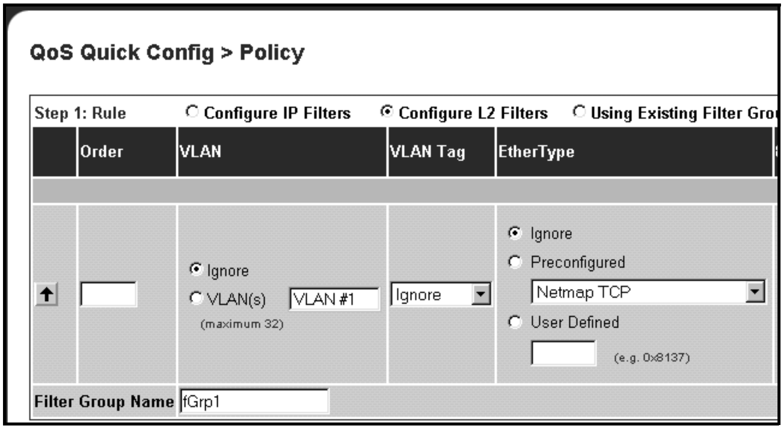
12 Go to “Configuring QoS Quick Config meters” on page 227.

To configure a new Layer 2 filter group:

1 Click Configure L2 Filters.

The QoS Quick Config Policy page for configuring Layer 2 filters opens (Figure 133 and Figure 134).

Figure 133 QoS Quick Config page for configuring Layer 2 filters page (1 of 2)



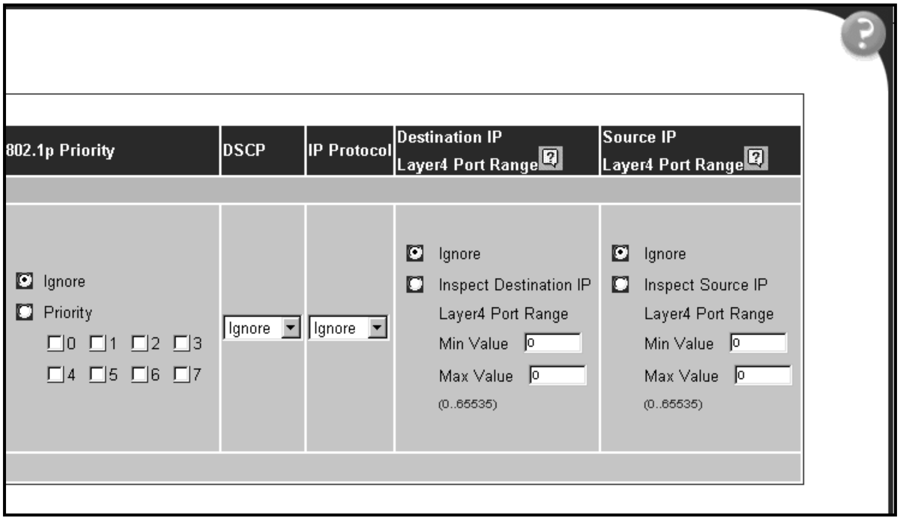
QoS Quick Config > Policy

Step 1: Rule ○ Configure IP Filters ● Configure L2 Filters ○ Using Existing Filter Gro

	Order	VLAN	VLAN Tag	EtherType
↑		● Ignore ○ VLAN(s) VLAN #1 (maximum 32)	Ignore	● Ignore ○ Preconfigured Netmap TCP ○ User Defined (e.g. 0x8137)

Filter Group Name fGrp1

Figure 134 QoS Quick Config page for configuring Layer 2 filters page (2 of 2)



802.1p Priority	DSCP	IP Protocol	Destination IP Layer4 Port Range	Source IP Layer4 Port Range
● Ignore ○ Priority □0 □1 □2 □3 □4 □5 □6 □7	Ignore	Ignore	● Ignore ○ Inspect Destination IP Layer4 Port Range Min Value 0 Max Value 0 (0..65535)	● Ignore ○ Inspect Source IP Layer4 Port Range Min Value 0 Max Value 0 (0..65535)

2 Enter the number you want for the order of the Layer 2 filter you are configuring.

3 In the VLAN area, choose the VLANs you want from the drop-down list.

Note: Beginning with software version 2.0, you can reference up to 32 VLANs with a Layer 2 filter.

4 In the VLAN Tag area, choose either Ignore, Tagged, or Untagged from the drop-down list.

5 Complete the EtherType area by performing one of the following:

- choosing Ignore
- choosing a preconfigured Ethernet type from the drop-down list
- entering a hex value for the User Defined Ethernet type

6 Complete the 802.1p Priority area by either:

- choosing Ignore
- clicking Priority and choosing one of the 0-7 boxes for the priority value

7 In the DSCP field, choose either Ignore or a value from the drop-down list.

8 In the IP Protocol field, choose either Ignore or a protocol from the drop-down list.

9 Complete the Destination IP Layer4 Port Range area by either:

- choosing Ignore
- clicking Inspect Destination Layer4 Range and entering a value for both the maximum value and the minimum value

10 Complete the Source IP Layer4 Port Range area by either:

- choosing Ignore
- clicking Inspect Source Layer4 Range and entering a value for both the maximum value and the minimum value

11 Enter the name you want to assign to the newly created Layer 2 filter group.

12 Click the arrow on the far left to add the newly created filter into the filter group.

13 Repeat steps 2 to 10 to add additional filters into the filter group.

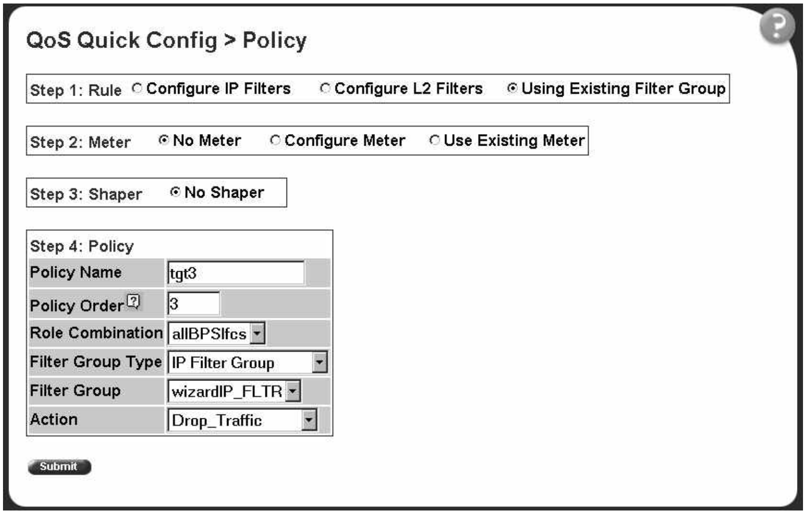
14 Go to“Configuring QoS Quick Config meters” on page 227.

To use an existing filter group:

1 Click Using Existing Filter Group.

A page opens that displays the Using Existing Filter Group option checked (Figure 135).

Figure 135 QoS Quick Config page with existing filter group choice



QoS Quick Config > Policy

Step 1: Rule ○ Configure IP Filters ○ Configure L2 Filters ● Using Existing Filter Group

Step 2: Meter ● No Meter ○ Configure Meter ○ Use Existing Meter

Step 3: Shaper ● No Shaper

Step 4: Policy

Policy Name	tgt3
Policy Order	3
Role Combination	allBPSIfcs
Filter Group Type	IP Filter Group
Filter Group	wizardIP_FLTR
Action	Drop_Traffic

2 Go to “Configuring QoS Quick Config meters” on page 227.

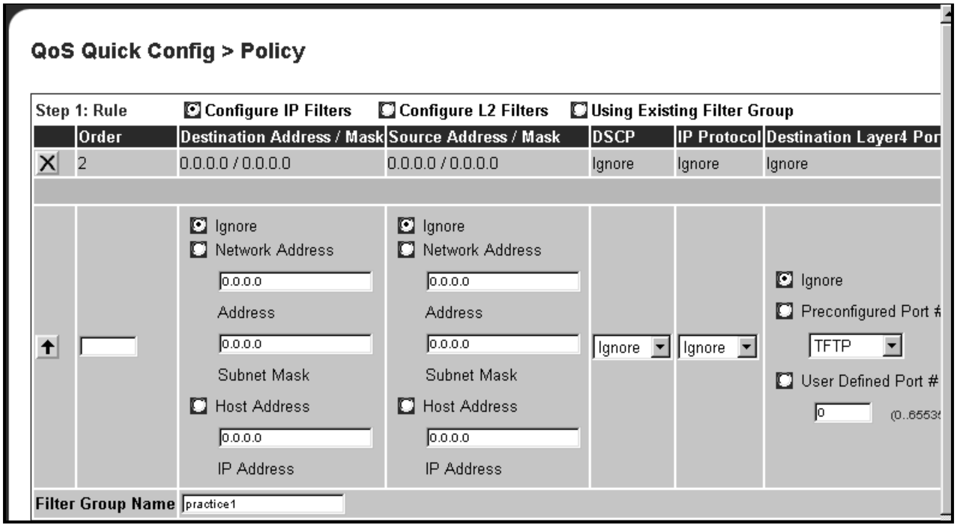
Deleting Qos Quick Config filters from the filter group

The filters of the filter group to be created are displayed in a table at the top of the Step 1: Rule section of the QoS Quick Config Policy page. To delete a filter from the filter group:

1 Click QoS Quick Config > Policy.

The filter group to be configured is displayed in the table at the top of the Step 1: Rule section of the QoS Quick Config Policy page (Figure 136).

Figure 136 QoS Quick Config Policy page with displayed filter group



QoS Quick Config > Policy

Step 1: Rule ● Configure IP Filters ○ Configure L2 Filters ○ Using Existing Filter Group

	Order	Destination Address / Mask	Source Address / Mask	DSCP	IP Protocol	Destination Layer4 Por
☒	2	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Ignore	Ignore	Ignore

Destination Address / Mask: ● Ignore; ○ Network Address: 0.0.0.0 Address, 0.0.0.0 Subnet Mask; ○ Host Address: 0.0.0.0 IP Address

Source Address / Mask: ● Ignore; ○ Network Address: 0.0.0.0 Address, 0.0.0.0 Subnet Mask; ○ Host Address: 0.0.0.0 IP Address

DSCP: Ignore

IP Protocol: Ignore

Destination Layer4 Port: ● Ignore; ○ Preconfigured Port #: TFTP; ○ User Defined Port #: 0 (0..6553

Filter Group Name: practice1

2 To delete the filter from the filter group, click the X icon at the far left of the table.

Configuring QoS Quick Config meters

Using Step 2: Meters, you choose to use nonmetered data for specified flow, to configure a new meter for the flow, or to use an existing meter for the flow.

To choose no metered data for the flow:

1 Click No Meter.

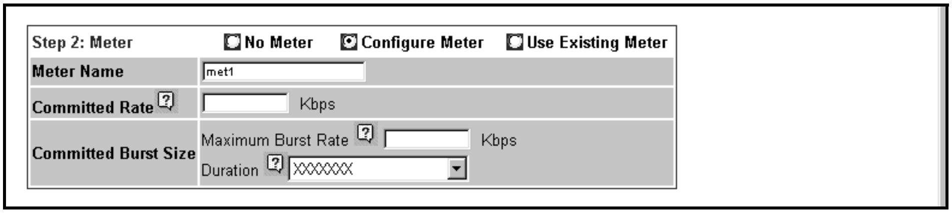
2 Go to "Configuring QoS Quick Config shapers" on page 228.

To create a new meter for the flow:

1 Click Configure Meter.

The system returns a page with the Step 2: Meter area expanded to allow you to configure QoS metering parameters (Figure 137).

Figure 137 QoS Quick Config Policy page with expanded meter area



Step 2: Meter	○ No Meter ● Configure Meter ○ Use Existing Meter
Meter Name	met1
Committed Rate	Kbps
Committed Burst Size	Maximum Burst Rate Kbps Duration XXXXXXX

2 Enter the name you want for the meter in the Meter Name field.

3 In the Committed Rate field, enter the rate you want for your meter.

4 In the Committed Burst Size field:

— Enter the burst you want to allow.

— Choose among the 6 or fewer durations the system calculates for the meter.

5 Go to "Configuring QoS Quick Config shapers" on page 228.

To use an existing meter for the flow:

1 Click Use Existing Meter.

2 Go to "Configuring QoS Quick Config shapers".

Configuring QoS Quick Config shapers

Using Step 3: Shapers, you choose not to shape the data for specified flow, to configure a new shaper for the flow, or to use an existing shaper for the flow, or to reference an aggregate shaping group.

To choose not to shape the data for the flow:

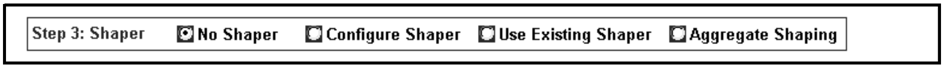
1 Click No Shaper.

2 Go to "Configuring QoS Quick Config policies" on page 230.

To configure a new shaper:

1 Click Configure Shaper, under Step 3: Shaper (Figure 138). The Shaper box opens.

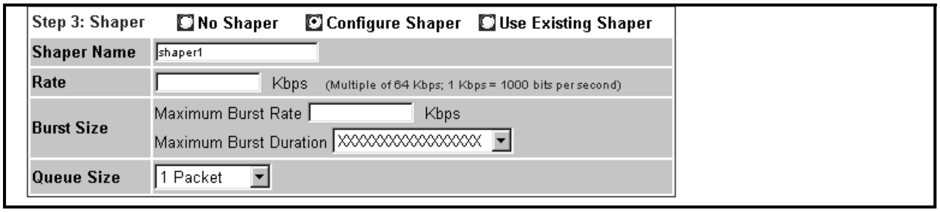
Figure 138 Step 3: Shaper



Step 3: Shaper ● No Shaper ○ Configure Shaper ○ Use Existing Shaper ○ Aggregate Shaping

The Shaper box opens (Figure 139).

Figure 139 Shaper box



Step 3: Shaper ○ No Shaper ● Configure Shaper ○ Use Existing Shaper

Shaper Name	shaper1
Rate	Kbps (Multiple of 64 Kbps; 1 Kbps = 1000 bits per second)
Burst Size	Maximum Burst Rate Kbps Maximum Burst Duration XXXXXXXXXXXXXXXX
Queue Size	1 Packet

2 Enter the name for the shaper you are configuring in the Shaper Name field.

3 In the Rate field, enter the committed rate you want in Kbps.

The system rounds up the shaping rate you enter, including 0, to a multiple of 64 Kbps.

4 Enter the maximum rate in Kbps in the Maximum Burst Rate field.

5 Choose the duration from the drop-down list in the Maximum Burst Duration field.

The system calculates the durations and presents you with 1 to 6 duration choices.

6 Choose the queue size from the drop-down list in the Queue Size field.

The queue size is the amount to traffic that can exceed the maximum burst size and still be queued for transmission. This traffic is delayed for shaping purposes.

7 Go to “Configuring QoS Quick Config policies” on page 230.

To use an existing shaper for the flow:

1 Click Use Existing Shaper, under Step 3: Shaper (Figure 138).

2 Go to "Configuring QoS Quick Config policies".

To use aggregate shaping for the flow:

1 Click Aggregate Shaping, under Step 3: Shaper (Figure 138 on page 229).

2 Go to "Configuring QoS Quick Config policies".

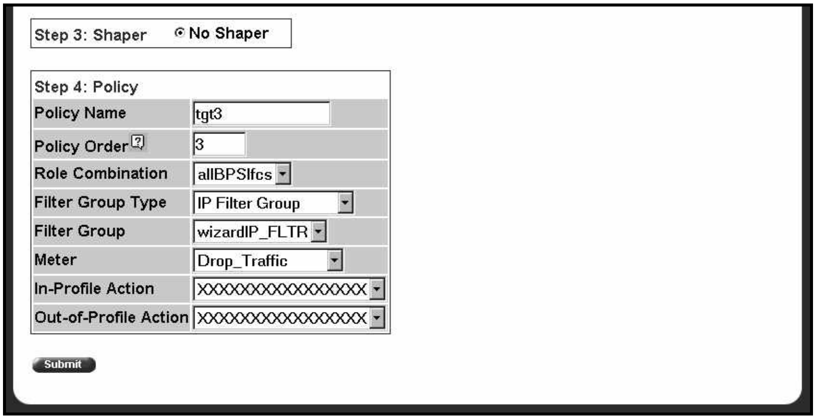
Configuring QoS Quick Config policies

Using the Step 4: Policy area, you apply a policy to the specified flow (Figure 140).

Note: The Step:4 Policy area displays differently, depending on whether you are referencing meters or shapers or both:

- If you are not metering data, only an Action field appears.
- If you are metering data and have already assigned actions to the meter entry, no Action field appears.
- If you are metering data and have not assigned actions to the meter entry, the In-Profile and Out-of-Profile Action fields appear.
- If you are not referencing a shaper or creating a shaper, the Shaper fields do not appear.
- If you are referencing an existing shaper, the Shaper Name field appears.
- If you are referencing aggregate shaping, the Shaping Group field appears.

Figure 140 Policy area of QoS Quick Config Policy page



Step 3: Shaper ● No Shaper

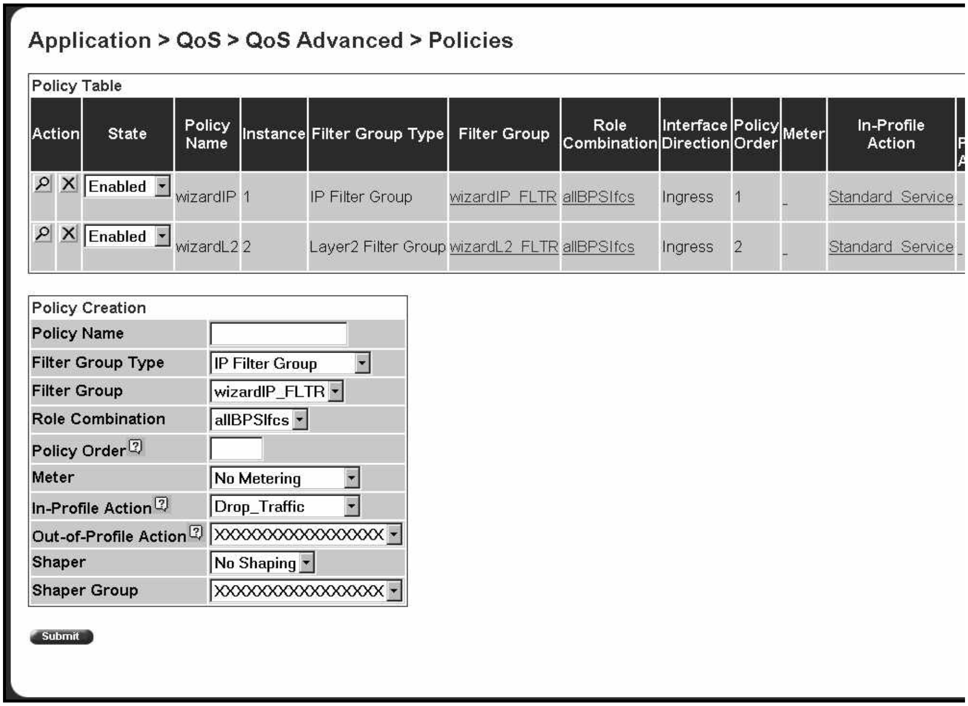
Step 4: Policy

Policy Name	tgt3
Policy Order	3
Role Combination	allBPSIfcs
Filter Group Type	IP Filter Group
Filter Group	wizardIP_FLTR
Meter	Drop_Traffic
In-Profile Action	XXXXXXXXXXXXXXXX
Out-of-Profile Action	XXXXXXXXXXXXXXXX

1. In the Policy Name field, enter a character string to assign a name for the policy you are configuring.
2. In the Policy Order field, enter the value you want for the evaluation order of the policy you are configuring.
3. In the Role Combination field, choose the Role Combination you want.
4. If you are referencing a meter with the policy:
   - Choose the In-Profile Action you want from the drop-down list.
   - Choose the Out-of-Profile Action you want from the drop-down list.
5. If you are referencing a existing shaper with the policy, choose the Shaper Name from the drop-down list.
6. If you are referencing an existing aggregate shaper group with the policy, choose the Shaper Group group from the drop-down list.
7. Click Submit.

The system returns you to the QoS Advanced Policies page, with your newly configured policy displayed in the Policy Table area (Figure 141 and Figure 142).

Figure 141 QoS Advanced Policies page with configured policies (1 of 2)



Application > QoS > QoS Advanced > Policies

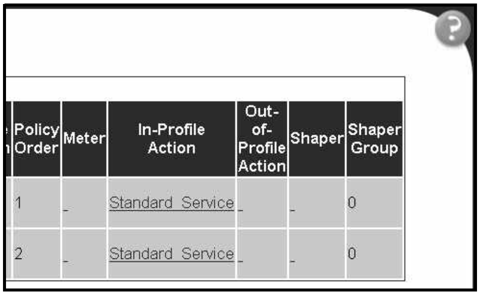
Policy Table

Action	State	Policy Name	Instance	Filter Group Type	Filter Group	Role Combination	Interface Direction	Policy Order	Meter	In-Profile Action
🔍 ✕	Enabled	wizardIP	1	IP Filter Group	wizardIP_FLTR	allBPSIfcs	Ingress	1	_	Standard_Service
🔍 ✕	Enabled	wizardL2	2	Layer2 Filter Group	wizardL2_FLTR	allBPSIfcs	Ingress	2	_	Standard_Service

Policy Creation

Policy Name	
Filter Group Type	IP Filter Group
Filter Group	wizardIP_FLTR
Role Combination	allBPSIfcs
Policy Order	
Meter	No Metering
In-Profile Action	Drop_Traffic
Out-of-Profile Action	XXXXXXXXXXXXXXXXX
Shaper	No Shaping
Shaper Group	XXXXXXXXXXXXXXXXX

Figure 142 QoS Advanced Policies page with configured policies (2 of 2)



Policy Order	Meter	In-Profile Action	Out-of-Profile Action	Shaper	Shaper Group
1	_	Standard_Service	_	_	0
2	_	Standard_Service	_	_	0

Chapter 5
Implementing QoS using QoS Advanced

The QoS application delivers a set of tools that, when optimally configured, combats escalating bandwidth costs and optimizes application performance in your network.

QoS tools allow you to prioritize your critical applications and sensitive traffic. You can tailor appropriate services to support this traffic over the wide area, thus maintaining the necessary performance levels on an end-to-end basis.

You can configure Quality of Service (QoS) features in your network by using the Web-based QoS Wizard, using the QoS Quick Config pages, or using the Advanced QoS configuration pages available in the Web-based management user interface. Refer to "Sample QoS configuration" on page 56 for a sample QoS configuration using the advanced QoS Web pages.

This chapter explains configuring QoS using the Advanced QoS pages. The chapter covers the following topics:

Configuring an interface group

You view existing interface group configurations, or create or modify an interface group if you want ports to assign the same QoS policy to all interfaces in the group.

➡ **Note:** One default role combination covers all ports of the device.

Creating an interface group configuration

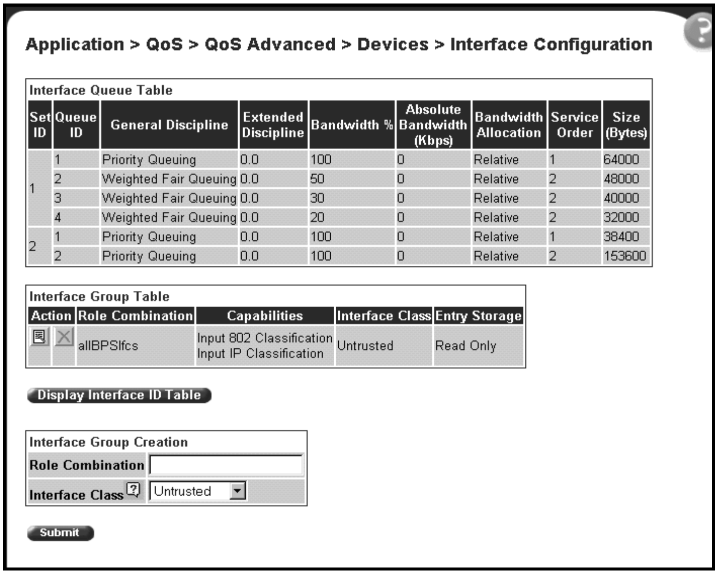
➡ **Note:** For more information on QoS interface groups, or role combinations, refer to Chapter 1, “About QoS,” on page 33.

To create an interface group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Interface Configuration.

The Interface Configuration page opens (Figure 143).

Figure 143 QoS Advanced Interface Configuration page



Application > QoS > QoS Advanced > Devices > Interface Configuration

Interface Queue Table

Set ID	Queue ID	General Discipline	Extended Discipline	Bandwidth %	Absolute Bandwidth (Kbps)	Bandwidth Allocation	Service Order	Size (Bytes)
1	1	Priority Queuing	0.0	100	0	Relative	1	64000
	2	Weighted Fair Queuing	0.0	50	0	Relative	2	48000
	3	Weighted Fair Queuing	0.0	30	0	Relative	2	40000
	4	Weighted Fair Queuing	0.0	20	0	Relative	2	32000
2	1	Priority Queuing	0.0	100	0	Relative	1	38400
	2	Priority Queuing	0.0	100	0	Relative	2	153600

Interface Group Table

Action	Role Combination	Capabilities	Interface Class	Entry Storage
🗎 ☒	allBPSIfcs	Input 802 Classification Input IP Classification	Untrusted	Read Only

Display Interface ID Table

Interface Group Creation

Role Combination	
Interface Class ?	Untrusted ▾

Submit

Table 54 describes the items on the Interface Queue Table section of the QoS Advanced Interface Configuration page.

Table 54 QoS Interface Queue Table section items

Item	Description
Set ID	The number that identifies a specific queue set.
Queue ID	The number that identifies the queue in the given set.
General Discipline	The queueing discipline that is associated with the specified queue. The options are: (1) Other - Use gosIfQueueExtDiscipline, (2) fifo - First In First Out Queuing, (3) pq -Priority Queuing, (4) fg - Fair Queuing, and (5) wfq - Weighted Fair Queuing
Extended Discipline	The queueing discipline that is associated with the specified queue. This attribute provides a means to add additional queueing mechanisms.
Bandwidth	The percentage of available bandwidth consumable to service the queue in one cycle.
Absolute Bandwidth	The absolute bandwidth consumable to service the queue in one cycle.
Bandwidth Allocation	Displays whether absolute or relative bandwidth is specified.

Table 54 QoS Interface Queue Table section items (Continued)

Item	**Description**
Service Order	The order in which a queue is serviced based on the defined discipline.
Size	The maximum size of the queue in bytes.

Table 55 describes the items on the Interface Group Table section of the QoS Advanced Interface Group page.

Table 55 Interface Group Table section items

Item	**Description**
✎	Opens a modification page.
✕	Deletes the row.
Role Combination	The tag used to identify interfaces with the characteristics specified by the attributes of this class instance (string 1..64). These identifiers are used within a number of classes to logically identify a physical set of interfaces to which policy rules and actions are applied.
Capabilities	A list of the interface capabilities used by the PDP or network manager to select which policies and configurations can be pushed to the Policy Enforcement Point (PEP). The options are: (0) Other, (1) InputIpClassification, (2) output Ip Classification, (3) input 802 Classification, (4) output 802 Classification, (5) single Queuing Discipline, and (6) hybrid Queuing Discipline.
Interface Class	The type of traffic received on interfaces associated with the specified role combination. The options are Trusted, Untrusted, and Unrestricted.
Entry Storage	Specifies whether or not the interface group can be deleted.

Note: For more information on QoS interface classes—or trusted, untrusted, and unrestricted ports—refer to Chapter 1, “About QoS,” on page 33.

Table 56 describes the items on the Interface Group Creation section of the QoS Advanced Interface Group page.

Table 56 Interface Group Creation section page items

Item and MIB association	Range	Description
Role Combination (qosInterfaceTypeRoles)	1..64	Type a character string to identify the role combination.
Interface Class (qosInterfaceTypeExtIfClass)	(1) Trusted (2) Untrusted (3) Unrestricted	Choose an interface class: Selecting Trusted requests the incoming DSCP value to not be changed, and instead be used for 802.1p user priority and queue assignment based on values in the DSCP mapping table and DSCP mapping table. Selecting Untrusted forces the incoming DSCP value (and associated mappings) to modify to a standard value by default. Actions associated with untrusted interfaces must re-mark the DSCP. Selecting Unrestricted allows you to configure actions that: • re-mark the DSCP or leave the DSCP as is • re-mark the 802.1p priority value or leave as is

2 In the Interface Group Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new interface group configuration appears in the Interface Group Table (Figure 143 on page 235).

Displaying Interface ID Table

To display the Interface ID Table:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Interface Configuration.

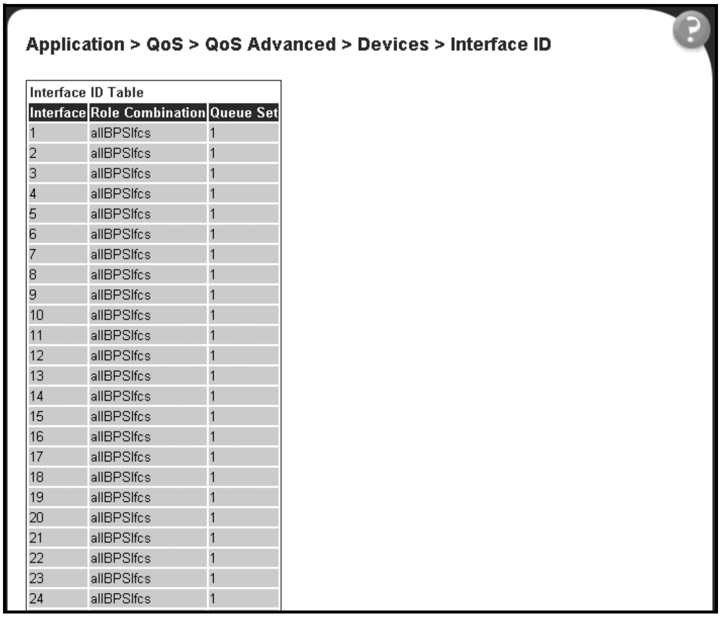
The QoS Advanced Interface Configuration page opens (Figure 143 on page 235).

2 Click Display Interface ID Table.

The Interface ID page opens (Figure 144). 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 all created interface groups, whether created using the Qos Advanced pages, the QoS Wizard, or the QoS Quick config.

Figure 144 Interface ID page



Application > QoS > QoS Advanced > Devices > Interface ID

Interface ID Table

Interface	Role Combination	Queue Set
1	allBPSIfcs	1
2	allBPSIfcs	1
3	allBPSIfcs	1
4	allBPSIfcs	1
5	allBPSIfcs	1
6	allBPSIfcs	1
7	allBPSIfcs	1
8	allBPSIfcs	1
9	allBPSIfcs	1
10	allBPSIfcs	1
11	allBPSIfcs	1
12	allBPSIfcs	1
13	allBPSIfcs	1
14	allBPSIfcs	1
15	allBPSIfcs	1
16	allBPSIfcs	1
17	allBPSIfcs	1
18	allBPSIfcs	1
19	allBPSIfcs	1
20	allBPSIfcs	1
21	allBPSIfcs	1
22	allBPSIfcs	1
23	allBPSIfcs	1
24	allBPSIfcs	1

Table 58 describes the items on the Interface ID page.

Table 57 Interface ID page items

Item	Description
Interface	Displays the unit and port number.
Role Combination	Displays the role combination associated with the interface.
Queue Sets	Displays the queue set associated with this interface.

Adding or removing interface group members

To select or deselect ports as members of an existing interface group:

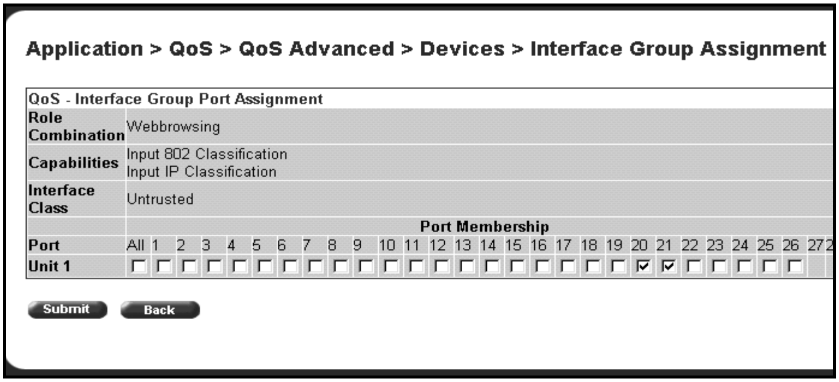
1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Interface Configuration.

The QoS Advanced Interface Configuration page opens (Figure 143 on page 235).

2 In the Interface Group Table section, in the row of your choice, click the Modify icon.

The Interface Group Assignment page opens (Figure 145).

Figure 145 Interface Group Assignment page



Application > QoS > QoS Advanced > Devices > Interface Group Assignment

QoS - Interface Group Port Assignment	
Role Combination	Webbrowsing
Capabilities	Input 802 Classification Input IP Classification
Interface Class	Untrusted

	Port Membership																												
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	2
Unit 1	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	☑	☑	□	□	□	□	□		

Table 58 describes the items on the Interface Group Assignment page.

Table 58 Interface Group Assignment page items

Item	Description
Role Combination	The tag used to identify interfaces with the characteristics specified by the attributes of this class instance (string 1..64). These identifiers are used within a number of classes to logically identify a physical set of interfaces to which policy rules and actions are applied. This is the group of interfaces (interface group) to which policy rules and actions are applied.
Capabilities	A list of the interface capabilities used by the PDP or network manager to select which policies and configurations can be pushed to the Policy Enforcement Point (PEP). The options are: (0) Other, (1) Input Ip Classification, (2) output Ip Classification, (3) input 802 Classification, (4) output 802 Classification, (5) single Queuing Discipline, and (6) hybrid Queuing Discipline
Interface Class	The type of traffic received on interfaces associated with the specified role combination. The options are Trusted, Untrusted, and Unrestricted.
Port Membership	Select the external ports to associate with the interface group, or select ALL to associate all ports on that unit.
Cascade Ports	The cascade (internal) ports to associate with the interface group.

3 In the Port Membership section, click the check boxes of the ports (or ALL to select all ports on the unit) to associate with the interface group.

4 Do one of the following:

- Click Submit.
- Click Back to return to the Interface Configuration page without making changes.

Deleting an interface group configuration

To delete an Interface group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Interface Configuration.

The QoS Advanced Interface Configuration page opens (Figure 143 on page 235).

2 In the Interface Group Table section, in the interface group configuration row of your choice, click the Modify icon.

The Interface Group Assignment page opens (Figure 145 on page 239).

3 In the Port Membership section, click the check boxes to deselect all ports associated with the interface group.

4 Click Submit.

The Interface Configuration page is displayed (Figure 143 on page 235).

5 In the Interface Group Table section, in the configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

6 Do one of the following:

- Click Yes to delete the interface group configuration.
- Click Cancel to return to the Interface Configuration page without making changes.

Configuring 802.1p priority queue assignment

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

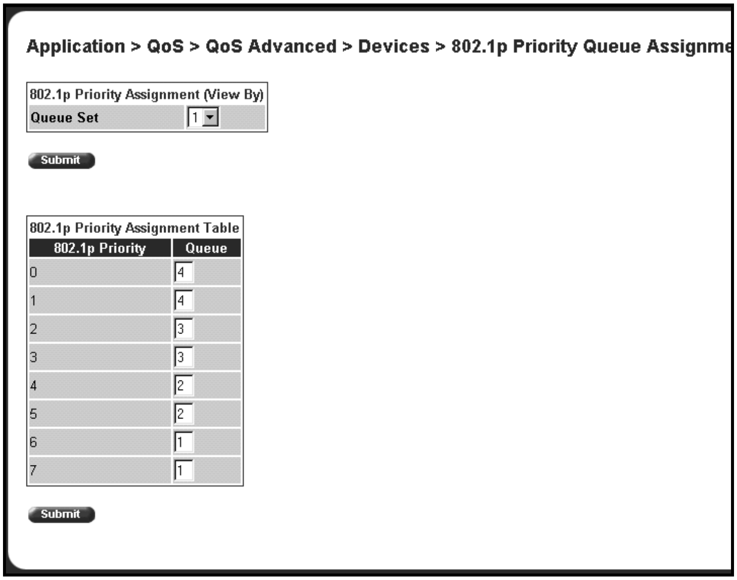
You can assign 802.1p user priority values to a queue for each interface with a specific queue set. This information is used for assigning egress traffic to outbound queues.

To configure 802.1p user priority:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Priority Q Assign.

The 802.1p Priority Queue Assignment page opens (Figure 146).

Figure 146 802.1p Priority Queue Assignment page



Application > QoS > QoS Advanced > Devices > 802.1p Priority Queue Assignme

802.1p Priority Assignment (View By)

Queue Set	1

802.1p Priority Assignment Table

802.1p Priority	Queue
0	4
1	4
2	3
3	3
4	2
5	2
6	1
7	1

Table 59 describes the items on the 802.1p Priority Queue Assignment page.

Table 59 802.1p Priority Assignment Table section page items

Section	Item and MIB association	Description
802.1p Priority Assignment (View By)	Queue Set	Choose the queue set you want to modify.
802.1p Priority Assignment Table	802.1p Priority (ntnQosIfPriAssignmentPri)	The 802.1p user priority mapped to a queue.
	Queue (ntnQosIfPriAssignmentQueuet)	Type a number that signifies the desired queue in the specified queue set with which this priority is associated.

2 In the 802.1p Priority Assignment section, select the queue set to view in the 802.1p Priority Assignment Table.

3 Click Submit.

The table is updated with the queue set you requested.

4 In the 802.1p Priority Assignment Table section, type the information in the text boxes.

5 Click Submit.

Note: Clicking Submit in the 802.1p Priority Assignment Table section results in a system reset.

Configuring 802.1p priority mapping

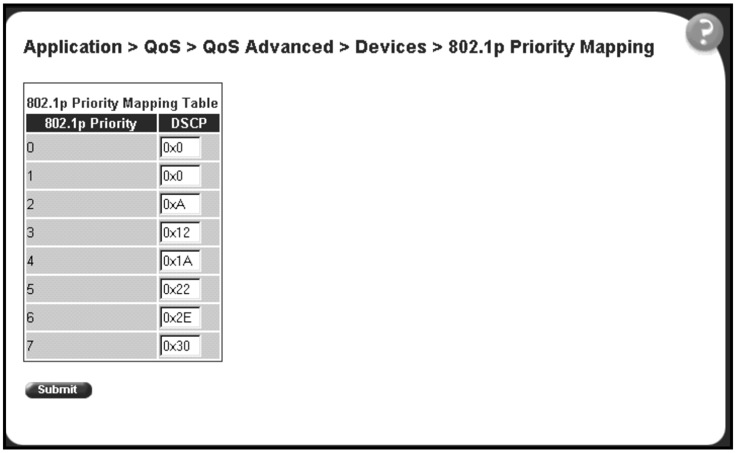
Note: Nortel recommends using the default 802.1p priority to DSCP mappings to ensure end-to-end QoS connectivity.

To configure 802.1p priority to DSCP mapping:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Priority Mapping.

The 802.1p Priority Mapping page opens (Figure 147).

Figure 147 802.1p Priority Mapping page



Application > QoS > QoS Advanced > Devices > 802.1p Priority Mapping

802.1p Priority Mapping Table

802.1p Priority	DSCP
0	0x0
1	0x0
2	0xA
3	0x12
4	0x1A
5	0x22
6	0x2E
7	0x30

Table 60 describes the items on the 802.1p Priority Mapping page.

Table 60 802.1p Priority Mapping page items

Item	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.

2 Type the information in the text boxes.

3 Click Submit.

Creating a DSCP queue assignment

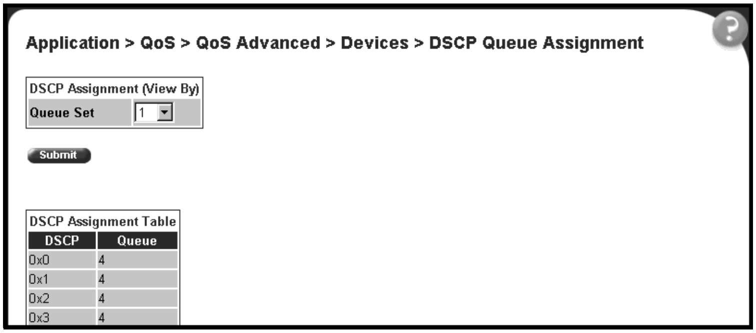
Note: Nortel recommends using the default DSCP to queue set mappings to ensure end-to-end QoS connectivity.

To create a DSCP/queue set association:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > DSCP Q Assignment.

The DSCP Queue Assignment page opens (Figure 148).

Figure 148 DSCP Queue Assignment page



Application > QoS > QoS Advanced > Devices > DSCP Queue Assignment

DSCP Assignment (View By)

Queue Set: 1

DSCP Assignment Table

DSCP	Queue
0x0	4
0x1	4
0x2	4
0x3	4

Table 61 describes the items on the DSCP Queue Assignment page.

Table 61 DSCP Queue Assignment page items

Section	Item	Format
DSCP Assignment (View By)	Queue Set	Choose the queue set to display in the DSCP Assignment Table.
DSCP Assignment Table	DSCP	The DSCP value to map to a queue.
	Queue	The queue set to which the traffic with the given DSCP value is associated.

2 In the DSCP Assignment (View By) section, choose the queue set to display in the DSCP Assignment Table.

The table is updated with information for the selected queue.

3 In the DSCP Assignment Table section, type the information in the text boxes.

4 Click Submit.

Configuring DSCP mapping

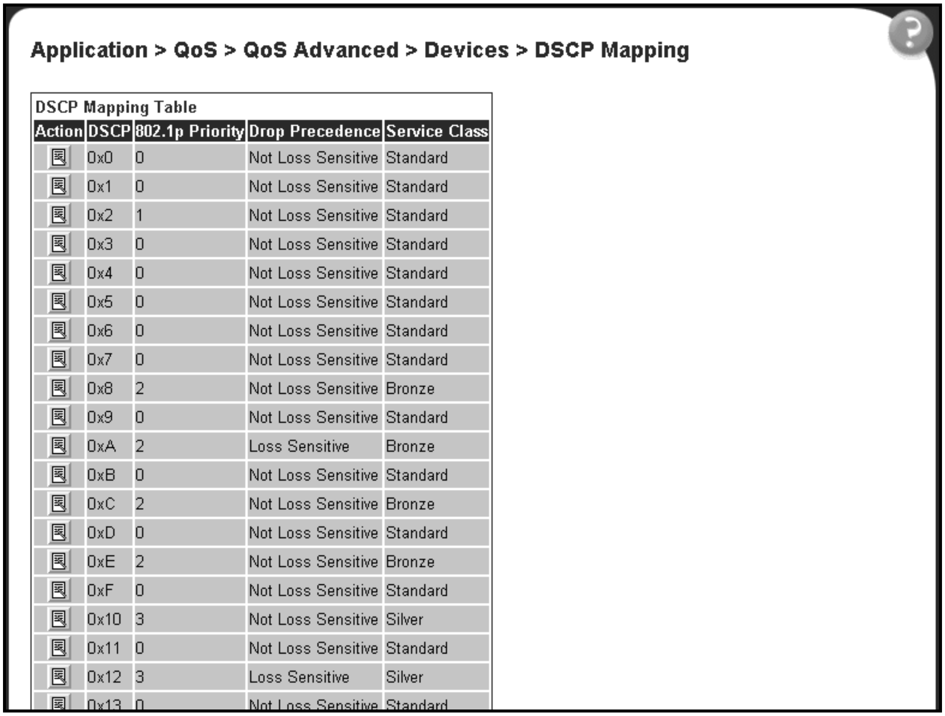
Note: Nortel recommends using the default DSCP mappings to ensure end-to-end QoS connectivity.

To configure DSCP to 802.1p user priority/drop precedence mapping:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > DSCP Mapping.

The DSCP Mapping page opens (Figure 149).

Figure 149 DSCP Mapping Table page



Application > QoS > QoS Advanced > Devices > DSCP Mapping

DSCP Mapping Table

Action	DSCP	802.1p Priority	Drop Precedence	Service Class
▤	0x0	0	Not Loss Sensitive	Standard
▤	0x1	0	Not Loss Sensitive	Standard
▤	0x2	1	Not Loss Sensitive	Standard
▤	0x3	0	Not Loss Sensitive	Standard
▤	0x4	0	Not Loss Sensitive	Standard
▤	0x5	0	Not Loss Sensitive	Standard
▤	0x6	0	Not Loss Sensitive	Standard
▤	0x7	0	Not Loss Sensitive	Standard
▤	0x8	2	Not Loss Sensitive	Bronze
▤	0x9	0	Not Loss Sensitive	Standard
▤	0xA	2	Loss Sensitive	Bronze
▤	0xB	0	Not Loss Sensitive	Standard
▤	0xC	2	Not Loss Sensitive	Bronze
▤	0xD	0	Not Loss Sensitive	Standard
▤	0xE	2	Not Loss Sensitive	Bronze
▤	0xF	0	Not Loss Sensitive	Standard
▤	0x10	3	Not Loss Sensitive	Silver
▤	0x11	0	Not Loss Sensitive	Standard
▤	0x12	3	Loss Sensitive	Silver
▤	0x13	0	Not Loss Sensitive	Standard

Table 62 describes the items on the DSCP Mapping Table page.

Table 62 DSCP Mapping Table page items

Item	Format
▤	Opens a modification page.
DSCP	The attribute used internally to determine the appropriate Layer 2 cost of service (CoS) mappings.
802.1p Priority	The IEEE802 CoS value used when mapping the DSCP value specified by the qos802DscpMappingDscp attribute to an IEEE 802 CoS.

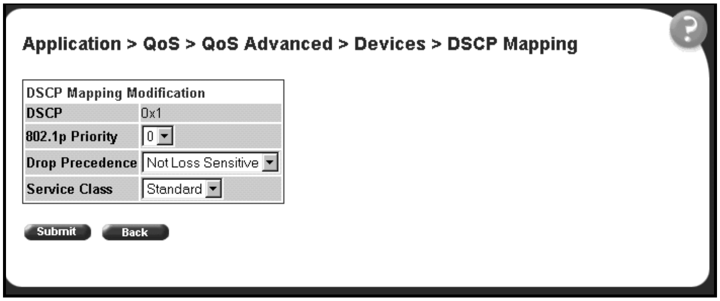
Table 62 DSCP Mapping Table page items (Continued)

Item	Format
Drop Precedence	The drop value precedence used for traffic with the associated 802.1D user priority value with the identified queue. Note: Generally, low packet drop precedence receives preferential treatment.
Service Class	The current service class. The options are: Standard, Bronze, Silver, Gold, Platinum, Premium, and Network. Note: This field corresponds to the adjacent user priority levels.

2 In the row of your choice, click the Modification icon.

The DSCP Mapping Modification page opens (Figure 150).

Figure 150 DSCP Mapping Modification page



Application > QoS > QoS Advanced > Devices > DSCP Mapping

DSCP Mapping Modification	
DSCP	0x1
802.1p Priority	0
Drop Precedence	Not Loss Sensitive
Service Class	Standard

Table 63 describes the items on the DSCP Mapping Modification page.

Table 63 DSCP Mapping Modification page items

Item	Range	Format
DSCP	0..63	Type the attribute to use internally to determine the appropriate Layer 2 cost of service (CoS) mappings.
802.1p Priority	0..7	Choose the IEEE802 CoS value to use when mapping the DSCP value specified by the qos802DscpMappingDscp attribute to an IEEE 802 CoS.

Table 63 DSCP Mapping Modification page items (Continued)

Item	Range	Format
Drop Precedence	Loss Sensitive Not Loss Sensitive	Choose the drop value precedence to use for traffic with the associated 802.1p user priority value with the identified queue. Selecting a Loss Sensitive value specifies a low packet drop precedence; selecting a Not Loss Sensitive value specifies a high packet drop precedence. Note: Generally, low packet drop precedence receives preferential treatment.
Service Class	Standard Bronze Silver Gold Platinum Premium Network	Choose the service class. Note: This field corresponds to the adjacent user priority levels.
	Note: Mappings created on the DSCP mapping modification page are used at egress for marking traffic: Trusted and unrestricted IP traffic—If you select the re-marking action of using the egress map, the mappings determine the 802.1p priority and drop precedence values associated with packets based on the DSCP of the received packet. Untrusted and untresticted traffic—If you select the re-marking action of using default, the mappings determine the 802.1p priority and drop precedence values associated with packets based on the DSCP value you specified in the Update DSCP action field.	

3 Select from a list.

4 Click Submit.

The modified configuration appears in the DSCP Mapping Table (Figure 149 on page 246).

➡ **Note:** For more information on QoS interface classes—or trusted, untrusted, and unrestricted ports—refer to Chapter 1, “About QoS,” on page 33.

IP filter and IP filter group configurations

You can create an IP filter, which enables the switch to classify traffic. In turn, you can create an access control list from a series of defined filters to create an IP filter group. The filter group then determines access to and denial of network services.

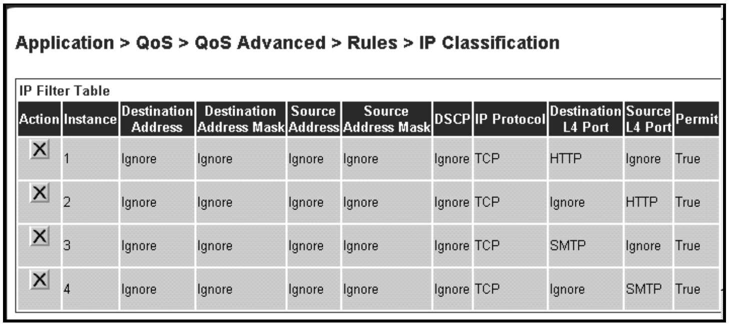
Creating an IP filter configuration

To create an IP filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 151, Figure 152 on page 250 and Figure 153 on page 250).

Figure 151 IP Classification page (1 of 3)

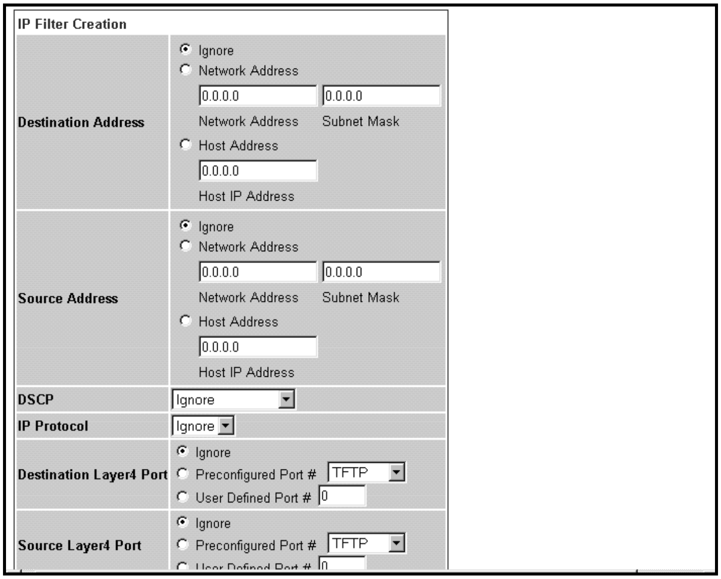


Application > QoS > QoS Advanced > Rules > IP Classification

IP Filter Table

Action	Instance	Destination Address	Destination Address Mask	Source Address	Source Address Mask	DSCP	IP Protocol	Destination L4 Port	Source L4 Port	Permit
☒	1	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	HTTP	Ignore	True
☒	2	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	Ignore	HTTP	True
☒	3	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	SMTP	Ignore	True
☒	4	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	Ignore	SMTP	True

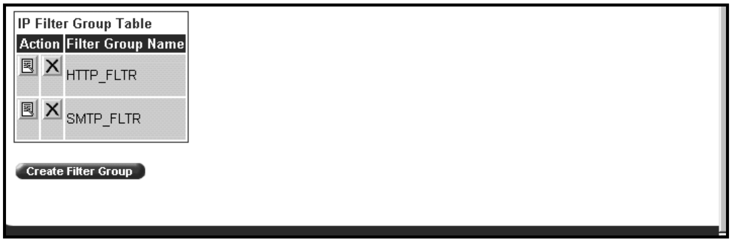
Figure 152 IP Classification page (2 of 3)



IP Filter Creation

Destination Address	● Ignore ○ Network Address 0.0.0.0 0.0.0.0 Network Address Subnet Mask ○ Host Address 0.0.0.0 Host IP Address
Source Address	● Ignore ○ Network Address 0.0.0.0 0.0.0.0 Network Address Subnet Mask ○ Host Address 0.0.0.0 Host IP Address
DSCP	Ignore
IP Protocol	Ignore
Destination Layer4 Port	● Ignore ○ Preconfigured Port # TFTP ○ User Defined Port # 0
Source Layer4 Port	● Ignore ○ Preconfigured Port # TFTP ○ User Defined Port # 0

Figure 153 IP Classification page (3 of 3)



IP Filter Group Table

Action	Filter Group Name
	HTTP_FLTR
	SMTP_FLTR

Note: When you choose the Ignore value, the filter matches all criteria for that parameter.

Table 64 describes the items on the IP Filter Table and IP Filter Creation sections of the IP Classification page.

Table 64 IP Filter Table and Filter Creation sections page items

Section	Item and MIB association	Range	Description
IP Filter Table	Action	☒	Deletes the row. Note: You cannot delete a filter if it is referenced in a filter group.
	Instance		Displays unique identifier.
	Destination Address (qosIpAceDstAddr)	XXX.XXX.XXX.XXX	Displays the IP address to match against the packet destination IP address.
	Destination Address Mask (qosIpAceDstAddrMask)	XXX.XXX.XXX.XXX	Displays the mask for the matching of the destination IP address. A zero bit in the mask means that the corresponding bit in the address always matches. A one (1) bit must be left-justified.
	Source Address (qosIpAceSrcAddr)	XXX.XXX.XXX.XXX	Displays the IP address to match against the packet source IP address.
	Source Address Mask (qosIpAceSrcAddrMask)	XXX.XXX.XXX.XXX	Displays the mask for the matching of the source IP address. One (1) bits must be left-justified.
	DSCP (qosIpAceDscp)	Ignore, Integer (0..63)	Displays the value that the DSCP in the packet must have to match this filter. This displays the DSCP value that this filter attempts to match.
	Protocol (qosIpAceProtocol)	TCP (6) UDP (17) ICMP (1) IGMP (2) RSVP (46) Ignore (0)	Displays the IP protocol to match against the packet IP protocol field.
	Destination L4 Port (qosIpAceDstL4PortMin) (qosIpAceDstL4PortMax)	Integer (0.65535)	Displays the value that the packet Layer 4 destination port number must have to match this filter.
	Source L4 Port (qosIpAceSrcL4PortMin) (qosIpAceSrcL4PortMax)	Integer (0.65535)	Displays the value that the packet Layer 4 source port number must have to match this filter.
	Permit	(1) True (2) False	If the frame matches the filter when this is set to true, the matching process stops.

Table 64 IP Filter Table and Filter Creation sections page items (Continued)

Section	Item and MIB association	Range	Description
IP Filter Creation/ Destination Address	Ignore		Click if you want the filter to ignore the packet destination IP address.
	Network Address	XXX.XXX.XXX.XXX	Click if you want the filter to match the packet destination network address. Enter the IP address to match against the packet destination IP address.
	Subnet Mask)	XXX.XXX.XXX.XXX	Enter the mask for the matching of the destination IP address. A zero bit in the mask means that the corresponding bit in the address always matches. A one (1) bit must be left-justified.
	Host Address)	XXX.XXX.XXX.XXX	Click if you want the filter to match the packet destination host IP address. Enter the IP address to match against the packet destination IP address.
IP Filter Creation/Source Address	Ignore		Click if you want the filter to ignore the packet source IP address.
	Network Address	XXX.XXX.XXX.XXX	Click if you want the filter to match the packet source network address. Enter the IP address to match against the packet source IP address.
	Subnet Mask)	XXX.XXX.XXX.XXX	Enter the mask for the matching of the source IP address. One (1) bits must be left justified.
	Host Address)	XXX.XXX.XXX.XXX	Click if you want the filter to match the packet source host IP address. Enter the IP address to match against the packet source IP address.
IP Filter Creation/DSCP	DSCP (qosIpAceDscp)	Ignore, Integer (0..63)	Choose the value that the DSCP in the packet must have to match this filter.
IP Filter Creation/IP Protocol	Protocol (qosIpAceProtocol)	Ignore (0) TCP (6) UDP (17) ICMP (1) IGMP (2) RSVP (46)	Choose the IP protocol to match against the packet IP protocol field.

Table 64 IP Filter Table and Filter Creation sections page items (Continued)

Section	Item and MIB association	Range	Description
IP Filter Creation/ Destination Layer4 Port	Ignore		Click if you want the filter to ignore the packet Layer 4 destination port.
	Preconfigured Port #	TFTP FTP TELNET SMTP HTTP HTTPS	Choose the value that the packet Layer 4 destination port number must have to match this filter.
	User Defined Port #	Integer	Enter the value that the packet Layer 4 destination port number must have to match this filter.
IP Filter Creation/ Source Layer4 Port	Ignore		Click if you want the filter to ignore the packet Layer 4 source port.
	Preconfigured Port #	TFTP FTP TELNET SMTP HTTP HTTPS	Choose the value that the packet Layer 4 source port number must have to match this filter.
	User Defined Port #	Integer	Enter the value that the packet Layer 4 source port number must have to match this filter.

2 In the IP Filter Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new IP filter configuration appears in the IP Filter Table (Figure 151 on page 249). This table displays all IP filters you created, using QoS wizard, Qos Quick Config, or QoS Advanced pages.

➡ **Note:** An IP filter configuration is not modifiable. The filter must be deleted and then recreated.

Deleting an IP filter configuration

To delete an IP filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 160 on page 272).

2 In the IP Filter Table, in the IP filter configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the IP filter configuration.
- Click Cancel to return to the IP Classification page without making changes.

➡ **Note:** You cannot delete the last filter in a filter group if it is referenced by an installed policy.

Creating an IP filter group configuration

To create an IP filter group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 151 on page 249).

Table 65 describes the items on the IP Filter Group section of the IP Classification page.

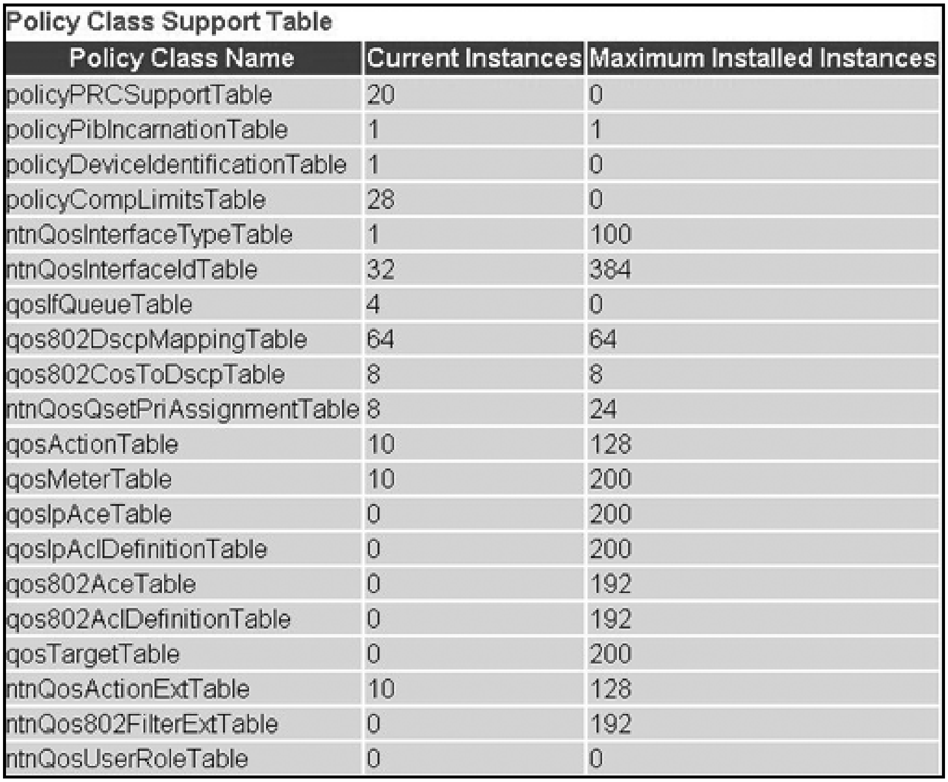
Table 65 IP Filter Group section page items

Item	Description
🗒	Opens a modification page.
☒	Deletes the row.
Filter Group Name	A list of existing filter group configurations.
Create Filter Group	Opens a filter group creation page.

2 Click Create Filter Group.

The IP Classification Group page opens (Figure 154).This table displays all IP filters you created, using QoS wizard, Qos Quick Config, or QoS Advanced pages.

Figure 154 IP Classification Group page



Policy Class Support Table

Policy Class Name	Current Instances	Maximum Installed Instances
policyPRCSupportTable	20	0
policyPibIncarnationTable	1	1
policyDeviceIdentificationTable	1	0
policyCompLimitsTable	28	0
ntnQosInterfaceTypeTable	1	100
ntnQosInterfaceIdTable	32	384
qosIfQueueTable	4	0
qos802DscpMappingTable	64	64
qos802CosToDscpTable	8	8
ntnQosQsetPriAssignmentTable	8	24
qosActionTable	10	128
qosMeterTable	10	200
qosIpAceTable	0	200
qosIpAclDefinitionTable	0	200
qos802AceTable	0	192
qos802AclDefinitionTable	0	192
qosTargetTable	0	200
ntnQosActionExtTable	10	128
ntnQos802FilterExtTable	0	192
ntnQosUserRoleTable	0	0

Table 66 describes the items on the IP Classification Group page.

Table 66 IP Classification Group page items

Item	Range	Description
Filter Group Name	1..16	Enter a character string to create an identity for the filter group configuration.
Group		Select (or deselect) the filter from membership in the filter group.
Order	Integer	Type a number to establish the evaluation order of filters in the group.

Table 66 IP Classification Group page items

Item	Range	Description
Destination Address		The IP address that is matched against the packet destination IP address.
Destination Address Mask		The mask for the matching of the destination IP address. Note: A zero bit in the mask means that the corresponding bit in the address always matches.
Source Address		The IP address that is matched against the packet source IP address.
Source Address Mask		The mask for the matching of the source IP address.
DSCP		The value that the DSCP in the packet must have to match this filter.
Protocol		The IP protocol that is matched against the packet IP protocol field. The options are: Ignore, TCP, UDP, ICMP, IGMP, or RSVP.
Destination L4 Port		The value that the packet Layer 4 destination port number can have to match the filter entry.
Source L4 Port		The value that the packet Layer 4 source port number can have to match the filter entry.
Permit	(1) True (2) False	If the frame matches the filter when this is set to true, the matching process stops.
	Note: To group multiple filters in a single group, assign Filter Index and Filter Order the same filter group name.	

3 Type information in the text boxes, or click the check box.

4 Click Submit.

The new configuration appears in the IP Filter Group Table (Figure 151 on page 249).

Modifying an IP filter group configuration

To modify an IP filter group configuration:

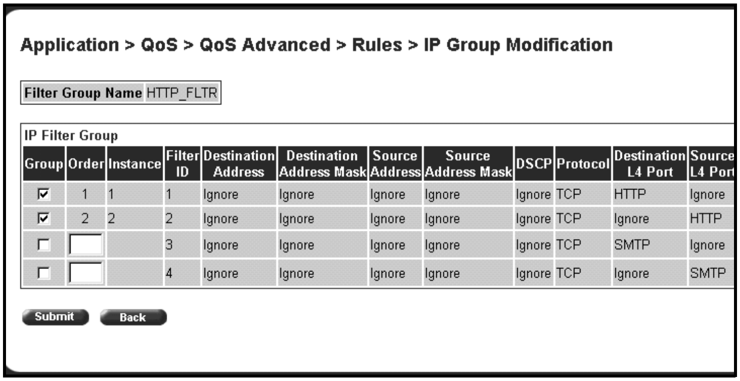
1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 151 on page 249).

2 In the IP Filter Group Table section, in the IP filter group configuration of your choice, click the Modify icon.

The IP Group Modification page opens (Figure 155). This table displays all IP filter you created, using QoS wizard, Qos Quick Config, or QoS Advanced pages.

Figure 155 IP Group Modification page



Application > QoS > QoS Advanced > Rules > IP Group Modification

Filter Group Name HTTP_FLTR

IP Filter Group

Group	Order	Instance	Filter ID	Destination Address	Destination Address Mask	Source Address	Source Address Mask	DSCP	Protocol	Destination L4 Port	Source L4 Port
☑	1	1	1	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	HTTP	Ignore
☑	2	2	2	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	Ignore	HTTP
☐			3	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	SMTP	Ignore
☐			4	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	Ignore	SMTP

Table 67 describes the items on the IP Group Modification page.

Table 67 IP Modification Group page items

Item	Range	Description
Filter Group Name	1..16	Displays the name of the selected the filter group.
Group		Select (or deselect) the filter from membership in the filter group.
Order	Integer	Displays the order for existing groups. Enter the desired order for the entries you are adding to the group.
Instance		Displays unique identifier.
Filter ID		Displays the filter identifier.
Destination Address		The IP address that is matched against the packet destination IP address.
Destination Address Mask		The mask for the matching of the destination IP address. Note: A zero bit in the mask means that the corresponding bit in the address always matches.
Source Address		The IP address that is matched against the packet source IP address.

Table 67 IP Modification Group page items

Item	Range	Description
Source Address Mask		The mask for the matching of the source IP address.
DSCP		The value that the DSCP in the packet must have to match this filter.
Protocol		The IP protocol that is matched against the packet IP protocol field. The options are: Ignore, TCP, UDP, ICMP, IGMP, or RSVP
Destination L4 Port		The value that the packet Layer 4 destination port number can have to match the filter entry.
Source L4 Port		The value that the packet Layer 4 source port number can have to match the filter entry.
Permit	(1) True (2) False	If the frame matches the filter when this is set to true, the matching process stops.
	Note: To group multiple filters in a single group, assign Filter Index and Filter Order the same filter group name.	

3 Select (or deselect) the filter as a member of the Filter Group.

4 Click Submit.

Deleting an IP filter group configuration

To delete an IP filter group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 151 on page 249).

2 In the IP Filter Group Table section, in the IP filter group configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the IP filter group configuration.
- Click Cancel to return to the IP Classification page without making changes.

Note: You cannot delete a filter group that is referenced by a policy. You must first delete the policy.

Layer 2 filter and Layer 2 filter group configurations

You can configure Layer 2 filters by defining IEEE 802-based parameters, and selective Layer 3 and Layer 4 parameters. Layer 2 filter groups are defined by specifying the Layer 2 filter to be included in the given filter group.

Beginning with software version 2.0, you can match up to 32 VLANs in one Layer 2 filter.

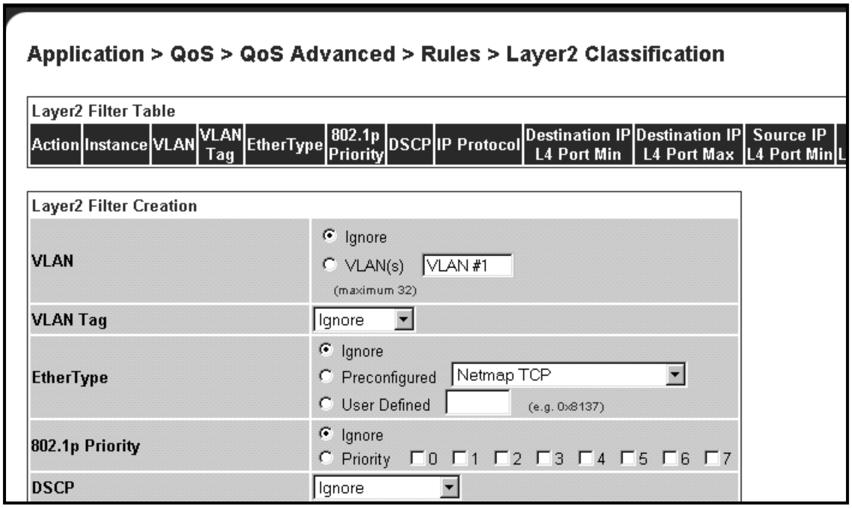
Creating a Layer 2 filter configuration

To create a layer2 filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

2 The Layer 2 Classification page opens (Figure 156).

Figure 156 Layer2 Classification page (1 of 2)



Application > QoS > QoS Advanced > Rules > Layer2 Classification

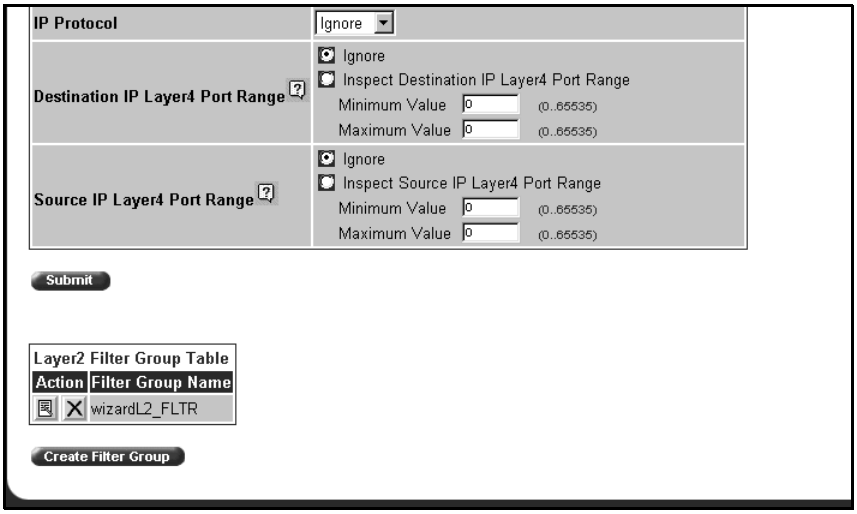
Layer2 Filter Table

Action	Instance	VLAN	VLAN Tag	EtherType	802.1p Priority	DSCP	IP Protocol	Destination IP L4 Port Min	Destination IP L4 Port Max	Source IP L4 Port Min	L

Layer2 Filter Creation

VLAN	● Ignore ○ VLAN(s) VLAN #1 (maximum 32)
VLAN Tag	Ignore ▾
EtherType	● Ignore ○ Preconfigured Netmap TCP ▾ ○ User Defined (e.g. 0x8137)
802.1p Priority	● Ignore ○ Priority □ 0 □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7
DSCP	Ignore ▾

Figure 157 Layer2 Classification page (2 of 2)



IP Protocol	Ignore ▾
Destination IP Layer4 Port Range ?	● Ignore ○ Inspect Destination IP Layer4 Port Range Minimum Value 0 (0..65535) Maximum Value 0 (0..65535)
Source IP Layer4 Port Range ?	● Ignore ○ Inspect Source IP Layer4 Port Range Minimum Value 0 (0..65535) Maximum Value 0 (0..65535)

Layer2 Filter Group Table

Action	Filter Group Name
▤ ☒	wizardL2_FLTR

Table 68 describes the items on the Layer2 Filter Table and Layer2 Filter Creation sections of the Layer2 Classification page.

Table 68 Layer2 Filter Table and Layer2 Filter Creation section items

Section	Item	Range	Description
Layer 2 Filter Table	Action	☒	Deletes the row.
	Instance		Displays unique identifier.
	VLAN	Ignore, 1-32	Click the VLANs you want to reference with this filer, up to 32 VLANs.
	VLAN Tag	(1) Tagged (2) Untagged (3) Ignore	Displays whether or not to check VLAN tagging.
	EtherType	Ignore Netmap TCP Netmap XNS XTP LOOP Vines Vines IP Banyan Vines Echo Vines Banyan Echo ARP RARP IP IPv6 3Com NBP 3Com NBP Ack 3Com NBP ConnReq 3Com NBP ConnRsp 3Com NBP ConnComplt 3Com NBP CloseReq 3Com NBP CloseRsp 3Com NBP Datagram 3Com NBP Broadcast 3Com NBP NBP NameClaim 3Com NBP DelName LAP Atalk ARP Atalk IBM Net Mon IBMRT XNS Compatibility XNS IPX Netware SNMP User Defined	Displays the EtherType to match.

Table 68 Layer2 Filter Table and Layer2 Filter Creation section items (Continued)

Section	Item	Range	Description
	802.1p Priority	Ignore, 0...7.	Displays the 802.1p priority level.
	DSCP	Ignore, Integer (0.63)	Displays the value that the DSCP in the packet must have to match this filter.
	IP Protocol	Ignore TCP UDP ICMP IGMP RSVP	Displays the IP protocol to match against the packet IP protocol field.
	Destination IP L4 Port Min	Ignore, Integer (0.65535)	Displays the least value that the packet Layer 4 destination port number can have to match this filter.
	Destination IP L4 Port Max	Ignore, Integer (0.65535)	Displays the maximum value that the packet Layer 4 destination port number can have to match this filter.
	Source IP L4 Port Min	Ignore, Integer (0.65535)	Displays the least value that the packet Layer 4 source port number can have to match this filter.
	Source IP L4 Port Max	Ignore, Integer (0.65535)	Displays the maximum value that the packet Layer 4 source port number can have to match this filter.
Layer2 Filter Creation	VLAN	Ignore, 1-32	Choose up to 32 VLAN names or ID numbers.
	VLAN Tag	(1) Tagged (2) Untagged (3) Ignore	Choose whether to check VLAN tagging.

Table 68 Layer2 Filter Table and Layer2 Filter Creation section items (Continued)

Section	Item	Range	Description
	EtherType	Ignore Netmap TCP Netmap XNS XTP LOOP Vines Vines IP Banyan Vines Echo Vines Banyon Echo ARP RARP IP IPv6 3Com NBP 3Com NBP Ack 3Com NBP ConnReq 3Com NBP ConnRsp 3Com NBP ConnComplt 3Com NBP CloseReq 3Com NBP CloseRsp 3Com NBP Datagram 3Com NBP Broadcast 3Com NBP NBP NameClaim 3Com NBP DelName LAP Atalk ARP Atalk IBM Net Mon IBMRT XNS Compatibility XNS IPX Netware SNMP User Defined	Choose the EtherType to match. Note: If you choose User Defined, enter the value.
	802.1p Priority	Ignore, 0...7.	Click the 802.1p priority level.
	DSCP	Ignore, Integer (0..63)	Choose the value that the DSCP in the packet must have to match this filter.

Table 68 Layer2 Filter Table and Layer2 Filter Creation section items (Continued)

Section	Item	Range	Description
	IP Protocol	Ignore TCP UDP ICMP IGMP RSVP	Select the IP protocol to match against the packet IP protocol field.
	Destination IP L4 Port Range	Ignore, Min, Max	Choose Ignore or type the minimum value and the maximum value that the packet Layer 4 destination port number can have to match this filter.
	Source IP L4 Port Range	Ignore, Min, Max	Choose Ignore or type the minimum value and the maximum value that the packet Layer 4 source port number can have to match this filter.

3 In the VLAN field, click **VLAN** and choose **VLAN #** 1.

This filter matches packets in VLAN 1.

4 In the VLAN Tag field, choose **Tagge**d.

Only packets that have an IEEE 802.1p tag match this Layer 2 filter.

5 In the EtherType field, click **Ignor**e.

All EtherTypes are ignored.

6 In the 802.1p Priority field, click Priority and 0, 1, 2.

Only packets that have IEEE 802.1p user priority 0, 1, 2 match this filter.

7 In the DSCP field, accept the default Ignore.

Any values that are in the DSCP field are ignored.

8 In the Protocol field, select Ignore.

All IP protocols are matched against the packet IP protocol field.

9 In the Destination IP Layer4 Port Range field, click Ignore.

10 In the Source IP Layer4 Port Range field, click Ignore.

Any values for the packet Layer 4 source port are ignored.

11 Click Submit.

The new Layer 2 filter group configuration appears in the Layer 2 Filter Group Table (Figure 156 on page 261). This table displays all Layer 2 filters you created with QoS Wizard, QoS Quick Config, and QoS Advanced.

The new Layer2 filter configuration appears in the Layer2 Filter Table (Figure 156 on page 261).

Deleting a Layer 2 filter configuration

➡ **Note:** You cannot delete the last filter in a filter group if it is referenced by an installed policy.

To delete a Layer 2 filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

The Layer2 Classification page opens (Figure 2 on page 261). This table displays all Layer 2 filters you created, using QoS wizard, Qos Quick Config, or QoS Advanced pages.

2 In the Layer2 Filter Table, in the Layer 2 filter configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the filter configuration.
- Click Cancel to return to the Layer2 Classification page without making changes.

➡ **Note:** A Layer 2 filter configuration cannot be modified. The configuration must be deleted and then recreated.

Creating a Layer 2 filter group configuration

To create a Layer 2 filter group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

The Layer2 Classification page opens (Figure 2 on page 261). This table displays all Layer 2 filters you created, using QoS wizard, Qos Quick Config, or QoS Advanced pages.

Table 69 describes the items on the Layer2 Filter Group Table section of the Layer2 Classification page.

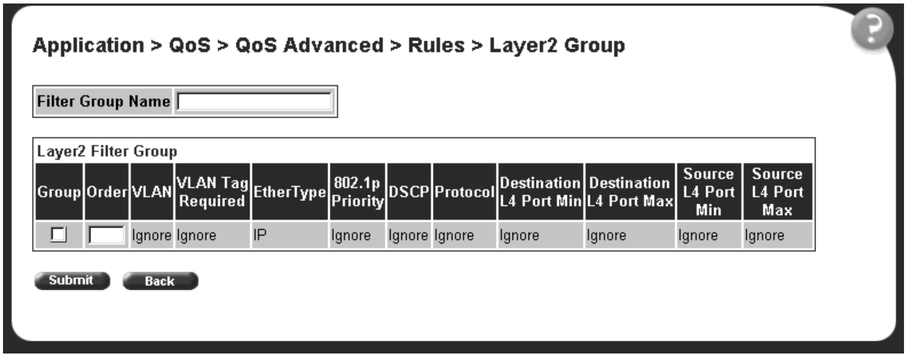
Table 69 IP Filter Group Table section items

Item	Description
📝	Opens a modification page.
☒	Deletes the row.
Filter Group Name	Lists existing filter group configurations.
Create Filter Group	Opens a filter group creation page.

2 Click Create Filter Group.

The Layer2 Group page opens (Figure 158).

Figure 158 Layer2 Group page



Application > QoS > QoS Advanced > Rules > Layer2 Group

Filter Group Name

Layer2 Filter Group

Group	Order	VLAN	VLAN Tag Required	EtherType	802.1p Priority	DSCP	Protocol	Destination L4 Port Min	Destination L4 Port Max	Source L4 Port Min	Source L4 Port Max
□		Ignore	Ignore	IP	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore

Table 70 describes the items on the Layer2 Group page.

Table 70 Layer2 Group page items

Item	Range	Description
Filter Group Name	1..16	Enter a character string to create an identity for the filter group configuration.
Group		Select (or deselect) the filter from membership in the filter group.
Order	Integer	Enter a number to establish the evaluation order of filters in the group.
VLAN		The VLAN IDs specified when the Layer 2 filter was created.
VLAN Tag Required		The VLAN tag requirement option selected when the filter was created.
EtherType		The EtherType selected when the filter was created.
802.1p Priority		The 802.1p priority selected when the filter was created.
DSCP		The value that the DSCP in the packet can have to match this filter.
Protocol		The IP protocol that is matched against the packet IP protocol field. The options are: Ignore, TCP, UDP, ICMP, IGMP, or RSVP.
Destination L4 Port Min		The least value that the packet Layer 4 destination port number can have to match this filter.
Destination L4 Port Max		The maximum value that the packet Layer 4 destination port number can have to match this filter.
Source L4 Port Min		The least value that the packet Layer 4 source port number can have to match this filter.

Table 70 Layer2 Group page items

Item	Range	Description
Source L4 Port Max		The maximum value that the packet Layer 4 source port number can have to match this filter.
	Note: To group multiple filters in a single group, assign Filter Index and Filter Order the same filter group name.	

Modifying a Layer 2 filter group configuration

To modify a Layer 2 filter group configuration:

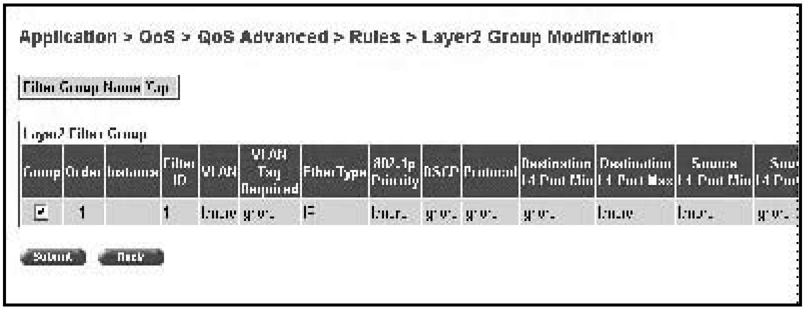
1 From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

The Layer2 Classification page opens (Figure 2 on page 261).

2 In the Layer2 Filter Group Table section, in the Layer 2 filter group configuration of your choice, click the Modify icon.

The Layer2 Group modification page opens (Figure 159). This table displays all Layer 2 Filter Groups you created with QoS Wizard, QoS Quick Config, and QoS Advanced.

Figure 159 Layer2 Group modification page



Application > QoS > QoS Advanced > Rules > Layer2 Group Modification

Filter Group Name [illegible]

Layer2 Filter Group

Group	Order	Instance	Filter ID	VLAN	VLAN Tag Required	Ether Type	802.1p Priority	DSCP	Protocol	Destination L4 Port Min	Destination L4 Port Max	Source L4 Port Min	Sou L4 Por
☑	1		1	Ignore	any	IP	Ignore	any	any	any	Ignore	Ignore	any

Table 71 describes the items on the Layer2 Group modification page.

Table 71 Layer2 Group modification page items

Item	Range	Description
Filter Group Name	1..16	Displays the filter group name.
Group		Select (or deselect) the filter from membership in the filter group.
Order	Integer	Enter a number to establish the evaluation order of filters in the group.
Instance		Displays a unique identifier.
Filter ID		Displays the filter identifier.
VLAN		The VLAN IDs specified when the Layer 2 filter was created.
VLAN Tag Required		The VLAN tag requirement option selected when the filter was created.
EtherType		The EtherType selected when the filter was created.
802.1p Priority		The 802.1p priority selected when the filter was created.
DSCP		The value that the DSCP in the packet can have to match this filter.
Protocol		The IP protocol that is matched against the packet IP protocol field. The options are: Ignore, TCP, UDP, ICMP, IGMP, or RSVP.
Destination L4 Port Min		The least value that the packet Layer 4 destination port number can have to match this filter.
Destination L4 Port Max		The maximum value that the packet Layer 4 destination port number can have to match this filter.
Source L4 Port Min		The least value that the packet Layer 4 source port number can have to match this filter.
Source L4 Port Max		The maximum value that the packet Layer 4 source port number can have to match this filter.

3 Type information in the text boxes, or click the check box.

4 Click Submit.

Deleting a Layer 2 filter group configuration

To delete a Layer 2 filter group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

The Layer2 Classification page opens (Figure 2 on page 261).

2 In the Layer2 Filter Group Table section, in the Layer 2 filter group configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the filter group configuration.
- Click Cancel to return to the Layer2 Classification page without making changes.

➡ **Note:** You cannot delete a filter group that is referenced by a policy. You must first delete the policy.

Configuring QoS actions

When you create a filter action, you specify the actions to be associated with specific IP and IEEE 802 filter groups. An action specifies the type of behavior you want a policy to apply to a flow of packets. When the filters match the incoming packets, the created actions are performed on those packets.

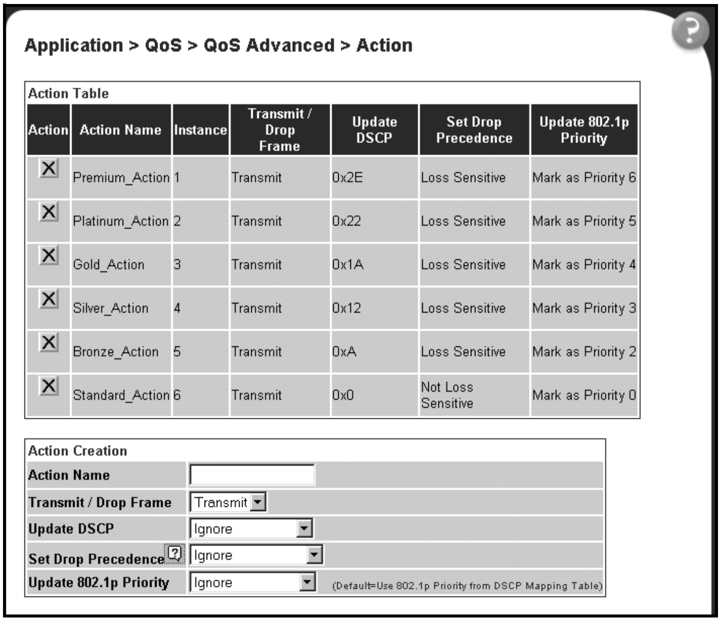
Creating a filter action configuration

To create a filter action configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Actions.

The Action page opens (Figure 160).

Figure 160 Action page



Application > QoS > QoS Advanced > Action

Action Table

Action	Action Name	Instance	Transmit / Drop Frame	Update DSCP	Set Drop Precedence	Update 802.1p Priority
☒	Premium_Action	1	Transmit	0x2E	Loss Sensitive	Mark as Priority 6
☒	Platinum_Action	2	Transmit	0x22	Loss Sensitive	Mark as Priority 5
☒	Gold_Action	3	Transmit	0x1A	Loss Sensitive	Mark as Priority 4
☒	Silver_Action	4	Transmit	0x12	Loss Sensitive	Mark as Priority 3
☒	Bronze_Action	5	Transmit	0xA	Loss Sensitive	Mark as Priority 2
☒	Standard_Action	6	Transmit	0x0	Not Loss Sensitive	Mark as Priority 0

Action Creation

Action Name		
Transmit / Drop Frame	Transmit	
Update DSCP	Ignore	
Set Drop Precedence	Ignore	
Update 802.1p Priority	Ignore	(Default=Use 802.1p Priority from DSCP Mapping Table)

Table 72 describes the items on the Action page.

Table 72 Action page items

Item and MIB association	Range	Description
☒		Deletes the row.
Action Name	1..16	Type a character string to uniquely identify the action configuration.
Instance		Displays the unique identifier.
Transmit/Drop Frame (qosActionDrop)	(1) Transmit (2) Drop	Choose whether the frame being evaluated is dropped or transmitted by this attribute. The default setting is Transmit.

Table 72 Action page items (Continued)

Item and MIB association	Range	Description
Update DSCP (qosActionUpdateDSCP)	Ignore or integer	Type a value. When this field is defined, it causes the value contained in the Differentiated Services (DS) field of an associated IP datagram to be updated with the value of this object. The default setting is Ignore.
Set Drop Precedence (ntnQosActionExtSetDropPrec)	(1) Ignore (2) Loss Sensitive (3) Not loss Sensitive (4) Use Defaults (5) Use Egress Map	Choose a packet drop precedence value. Note: Generally, low packet drop precedence receives preferential treatment. The default setting is Use Defaults.
Update 802.1p Priority (ntnQosActionExtUpdatePri)	(1) Ignore (2) Priority 0 (3) Priority 1 (4) Priority 2 (5) Priority 3 (6) Priority 4 (7) Priority 5 (8) Priority 6 (9) Priority 7 (10) Use Defaults (11) Use Egress Map	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). Note: Use Defaults=Use 802.1p priority from DSCP mapping table. The default setting is Use Defaults.

2 In the Action Creation section, type information in the text boxes, or select from a list

3 Click Submit.

The new filter action configuration appears in the Action Table (Figure 160 on page 272).

Note: Actions are not modifiable. They must be deleted and recreated.

Deleting an action configuration

To delete an action configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Actions.

The Action page opens (Figure 160 on page 272).

2 In the Action Table section, in the filter action configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the filter configuration.
- Click Cancel to return to the Action page without making changes.

➡ **Note:** You cannot delete an action that is referenced by a meter. You must first delete the meter.

Configuring QoS meters

Using the QoS Advanced pages, you can create, view, or delete meters. If you do not want to meter the data in your flow, go to "Configuring QoS shapers" on page 278.

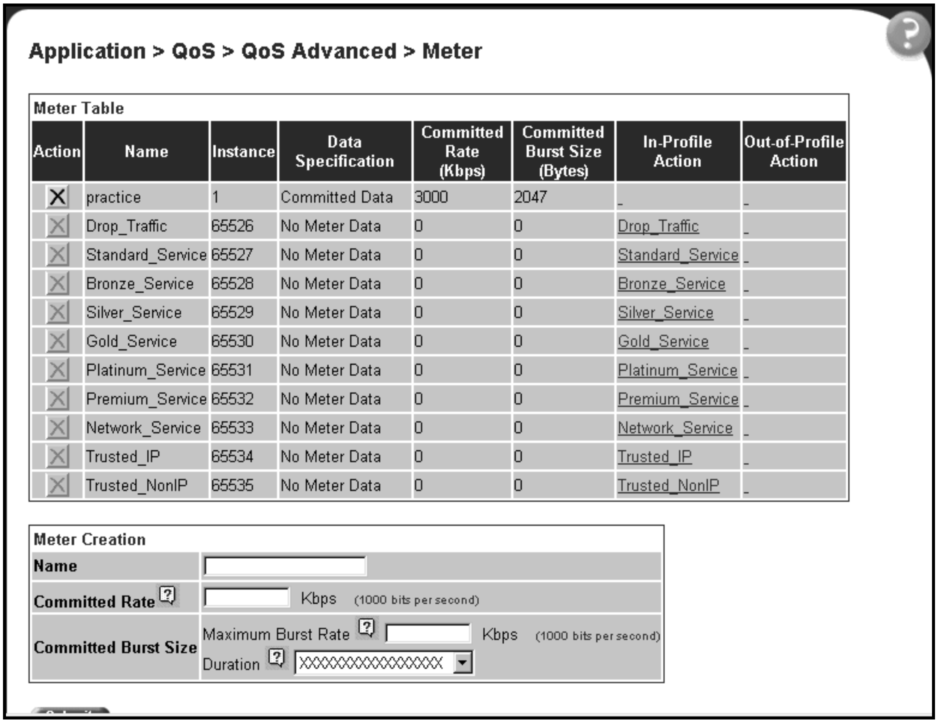
Creating a meter

To create a meter:

1 From the main menu, choose Application > QoS > QoS Advanced > Meters.

The Qos Advanced Meter page opens (Figure 161). This table displays all meters you created with QoS Wizard, QoS Quick Config, and QoS Advanced.

Figure 161 QoS Advanced Meter page



Application > QoS > QoS Advanced > Meter

Meter Table

Action	Name	Instance	Data Specification	Committed Rate (Kbps)	Committed Burst Size (Bytes)	In-Profile Action	Out-of-Profile Action
☒	practice	1	Committed Data	3000	2047	_	_
☒	Drop_Traffic	65526	No Meter Data	0	0	Drop_Traffic	_
☒	Standard_Service	65527	No Meter Data	0	0	Standard_Service	_
☒	Bronze_Service	65528	No Meter Data	0	0	Bronze_Service	_
☒	Silver_Service	65529	No Meter Data	0	0	Silver_Service	_
☒	Gold_Service	65530	No Meter Data	0	0	Gold_Service	_
☒	Platinum_Service	65531	No Meter Data	0	0	Platinum_Service	_
☒	Premium_Service	65532	No Meter Data	0	0	Premium_Service	_
☒	Network_Service	65533	No Meter Data	0	0	Network_Service	_
☒	Trusted_IP	65534	No Meter Data	0	0	Trusted_IP	_
☒	Trusted_NonIP	65535	No Meter Data	0	0	Trusted_NonIP	_

Meter Creation

Name	
Committed Rate	Kbps (1000 bits per second)
Committed Burst Size	Maximum Burst Rate Kbps (1000 bits per second) Duration XXXXXXXXXXXXXXXXX

2 In the Meter Creation area, create the meter.

Table 73 describes the fields in the Meter Creation area, which you use to set new meters.

Table 73 Meter Creation fields

Item	Range	Description
Name	1 to 16 alphanumeric characters with no spaces	Enter the name for the meter you are creating.

Table 73 Meter Creation fields (Continued)

Item	Range	Description
Committed Rate	13 - 1,700,000 Kbps	Enter the Committed Rate in Kbps here.
Committed Burst Size	2,047 to 131,071 bytes Up to 7 durations	Maximum Burst Rate—Enter the Maximum Burst Rate in bytes. Duration—From the drop-down list, choose 1 of up to 7 durations for the period that the Maximum Burst Rate is allowed.

3 Click Submit.

4 If you have not already specified the interface assignments, choose Applications > QoS > QoS Advanced > Devices > Interface Configuration page to connect the desired ports to the desired filters.

The formula for the Committed Burst Size (in bytes) is:

Committed Burst Size = (max-burst-duration * (max-burst-rate - committed rate))/8

Where:

Committed Burst Size is rounded up to one of the following values:

2047, 4095, 8191, 16383, 32767, 65535, 131071

→ **Note:** Meter configurations are not modifiable. They must be deleted and the information re-entered.

Viewing meters

To view a meter:

1 From the main menu, choose Application > QoS > QoS Advanced > Meters.

The QoS Advanced Meters page opens (Figure 161 on page 275).

2 View created meters in the Meter Table. This table displays all the meters you configured, including those with QoS Wizard and QoS Quick Config.

Table 74 describes the fields in the Meter Table area.

Table 74 Meter Table fields

Item	Range	Description
Action	☒	Deletes the meter.
Name		Displays the name of the meter.
Instance		Displays the unique identifier.
Data Specification	(1) No Meter Data (2) Metered Data	Displays whether the meter has metered data or not. (All meters created with software version 2.0 or higher have only metered data.)
Committed Rate	13 - 1,700,000 Kbps	Displays the Committed Rate in kbps.
Committed Burst Size	2,047 to 131,071 bytes	Displays the Committed Burst Size in bytes.
In-Profile Action	Configured, user-defined action	Displays the In-Profile Action for this meter.
Out-Profile Action	Configured, user-defined action	With a meter using metered data, this field displays the action specified for traffic that is out-of-profile. With a meter using no metered data, this field displays N/A. (All meters created with software version 2.0 or higher have only metered data.)

Deleting a meter

To delete a meter:

1 From the main menu, choose Application > QoS > QoS Advanced > Meters.

The Meter page opens (Figure 161 on page 275).

2 In the Meter Table section, click the Delete icon to delete the meter.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the meter configuration.
- Click Cancel to return to the Meter page without making changes.

Note: You cannot delete a meter that is referenced by a policy. You must delete the policy first.

Configuring QoS shapers

Using the QoS Advanced pages, you can create, view, or delete shapers. If you do not want to shape the data in your flow, go to "Configuring QoS policies" on page 281.

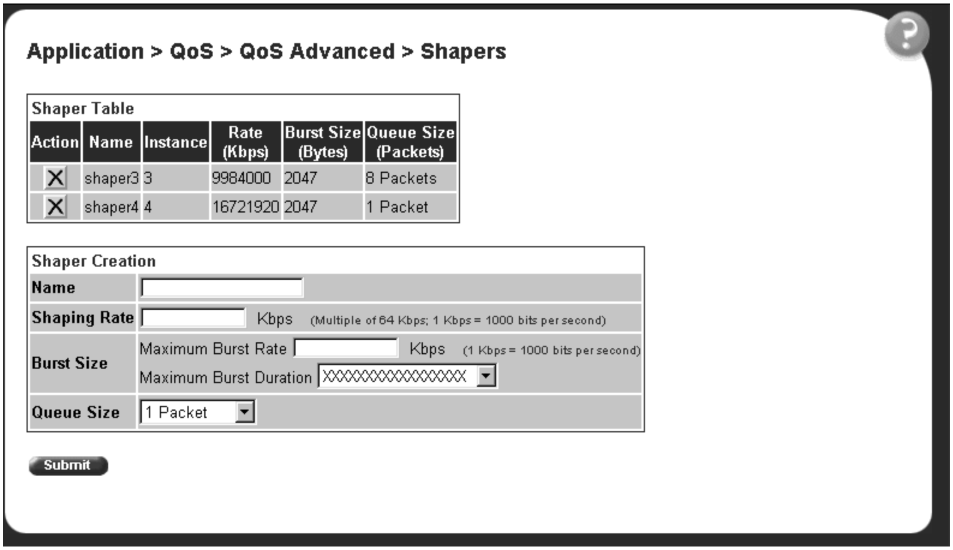
Creating a shaper

To create a shaper:

1 From the main menu, choose Application > QoS > QoS Advanced > Shapers.

The Qos Advanced Shapers page opens (Figure 162). All Shapers, including those created using the QoS Wizard and Qos Quick Config pages, display on this page.

Figure 162 QoS Advanced Shapers page



Application > QoS > QoS Advanced > Shapers

Shaper Table

Action	Name	Instance	Rate (Kbps)	Burst Size (Bytes)	Queue Size (Packets)
☒	shaper3	3	9984000	2047	8 Packets
☒	shaper4	4	16721920	2047	1 Packet

Shaper Creation

Name	
Shaping Rate	Kbps (Multiple of 64 Kbps; 1 Kbps = 1000 bits per second)
Burst Size	Maximum Burst Rate Kbps (1 Kbps = 1000 bits per second) Maximum Burst Duration XXXXXXXXXXXXXXXX ▼
Queue Size	1 Packet ▼

2 In the Shaper Creation area, create the shape.

Table 75 describes the fields in the Shaper Creation area, which you use to set new shapers.

Table 75 Shaper Creation fields

Item	Range	Description
Name	1 to 16 alphanumeric characters with no spaces	Enter the name for the shaper you are creating.
Shaping Rate	1 - 4294967296	Enter the Shaping Rate in Kbps here. This is the maximum rate at which traffic shaped using this shaper is transmitted over a given duration. Note: The system rounds up the shaping rate you enter to a multiple of 64 Kbps.
Burst Size	6 durations	Maximum Burst Rate—Enter the Maximum Burst Rate in Kbps. This determines the maximum traffic burst size that can be transmitted without a shaping delay. Duration—From the drop-down list, choose 1 of the 6 durations for the period that the Maximum Burst Rate is allowed.
Queue Size	1, 2, 4, 8, or 16 packets	Choose the queue depth from the drop-down list. This is the number of packets that can exceed the traffic burst size and still be queued for transmission.

3 Click Submit.

The formula for the Committed Burst Size (in bytes) is:

Committed Burst Size = (max-burst-duration * (max-burst-rate - shape rate))/8

Where:

Committed Burst Size is rounded up to one of the following values:

2047, 4095, 8191, 16383, 32767, 65535

Note: Shaper configurations are not modifiable. They must be deleted and the information re-entered.

Viewing shapers

To view a shaper:

1 From the main menu, choose Application > QoS > QoS Advanced > Shapers.

The QoS Advanced Shapers page opens (Figure 161 on page 275).

2 View created shapers in the Shaper Table. This table displays all the shapers you configured, including those with QoS Wizard and QoS Quick Config.

Table 76 describes the fields in the Shaper Table area.

Table 76 Shaper Table fields

Item	**Range**	**Description**
Action	☒	Deletes the shaper.
Name		Displays the name of the shaper.
Instance		Displays the unique identifier.
Rate	1 - 4294967296	Displays the maximum rate at which traffic shaped using this shaper is transmitted over a given duration. Displays the rate rounded up to multiples of 64 Kbps.
Burst Size		Displays the maximum traffic burst size that can be transmitted without a shaping delay. Calculated internally using the configured Maximum Burst Rate and Maximum Burst Duration.
Queue Size	1, 2, 4, 8, or 16 packets	Displays the number of packets that can exceed the traffic burst size and still be queued for transmission.

Deleting a shaper

To delete a shaper:

1 From the main menu, choose Application > QoS > QoS Advanced > Shapers.

The Qos Advanced Shaper page opens (Figure 162 on page 278).

2 In the Shaper Table section, click the Delete icon to delete the shaper.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the shaper configuration.
- Click Cancel to return to the Shaper page without making changes.

Note: You cannot delete a shaper that is referenced by a policy. You must delete the policy first.

Configuring QoS policies

You can configure QoS policies by creating filters in the hardware that apply a set of packet filtering criteria and actions to individual interfaces.

If you want to meter your data, you must reference both an In-Profile action and an Out-Profile action. The In-Profile action directs the switch how to handle the data flow that is within the meter you set (refer to "Configuring QoS meters" on page 274"), and the Out-Profile directs the switch how to handle all other data.

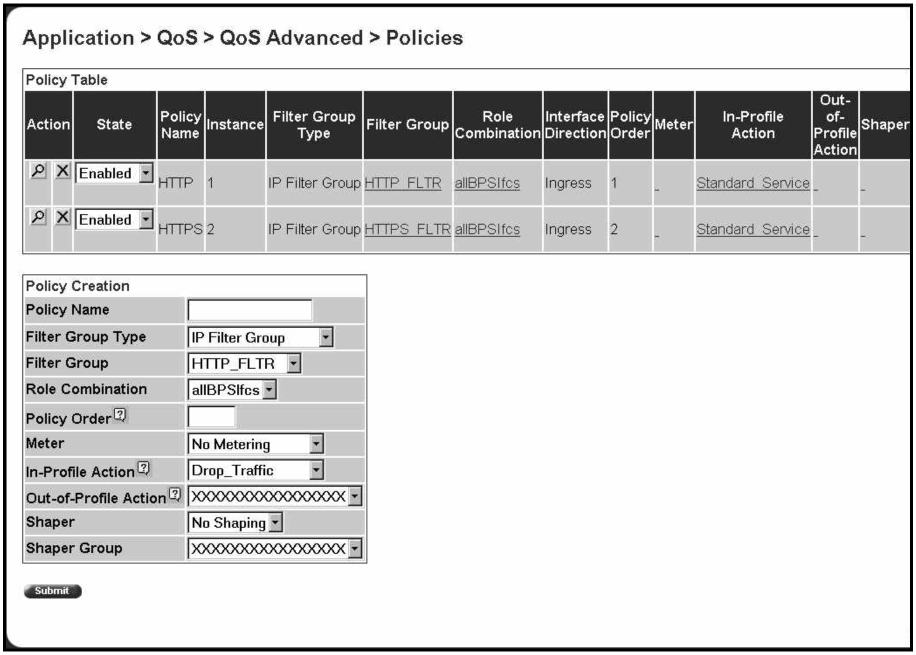
Installing defined filters

To create a hardware policy filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Policies.

The QoS Advanced Policies page opens (Figure 163). This table displays all configured policies, including ones created with QoS Wizard and QoS Quick Config.

Figure 163 QoS Advanced Policies page



Application > QoS > QoS Advanced > Policies

Policy Table

Action	State	Policy Name	Instance	Filter Group Type	Filter Group	Role Combination	Interface Direction	Policy Order	Meter	In-Profile Action	Out-of-Profile Action	Shaper
🔍 X	Enabled	HTTP	1	IP Filter Group	HTTP_FLTR	allBPSIfcs	Ingress	1	_	Standard_Service	_	_
🔍 X	Enabled	HTTPS	2	IP Filter Group	HTTPS_FLTR	allBPSIfcs	Ingress	2	_	Standard_Service	_	_

Policy Creation

Policy Name	
Filter Group Type	IP Filter Group
Filter Group	HTTP_FLTR
Role Combination	allBPSIfcs
Policy Order ?	
Meter	No Metering
In-Profile Action ?	Drop_Traffic
Out-of-Profile Action ?	XXXXXXXXXXXXXXXX
Shaper	No Shaping
Shaper Group	XXXXXXXXXXXXXXXX

Table 77 describes the items on the QoS Advanced Policy page.

Table 77 Policy page items

Section	Item and MIB association	Range	Description
Policy Table	Action	🔍	Opens a view only statistics table. The table displays current filter statistics in bytes and packets.
		☒	Deletes the row.
	State	(1) Enabled (2) Disabled	Enables or disables the policy.
	Policy Name	1..16	A list of the names of existing target configurations.
	Instance		Displays the unique identifier.
	Filter Group Type		The type of filter group that is referenced by this instance of the Target class. The options are: IP Filter Group or Layer2 Filter Group.
	Filter Group		The filter group that is associated with this target.
	Role Combination		The interfaces to which this target specification applies, specified in terms of a role combination tag.
	Interface Direction		The direction of packet flow at the interface to which this target specification applies.
	Policy Order		The number used to determine the order of precedence for this target specification.
	Meter		The meter associated with this entry, if there is one.
	In-Profile Action		Displays the name of the In-Profile action for this policy.
	Out-of-Profile Action		Displays the name of the Out-of-Profile action for this policy. This field applies only to metered data.
	Shaper		Displays the name of the shaper for this policy, if there is one
	Shaper Group	2 - 63	Displays the shaper group ID for this policy.

Table 77 Policy page items

Section	Item and MIB association	Range	Description
Policy Creation	Policy Name	1..64	Type a character string to create a unique name to identify this policy.
	Filter Group Type (qosTargetAclType)	(1) IP Filter Group (2) Layer2 Filter Group	Choose the type of filter group to associate with this policy.
	Filter Group		Choose the filter group to associate with this policy.
	Role Combination (qosTargetInterfaceRoles)		Choose the type of interface to which this policy applies, specified in terms of a role combination.
	Policy Order (qosTargetOrder)	Integer	Enter a number to use as a determinate of the order of precedence for this filter.
	Meter (qosTargetMeter)		Choose the meter associated with this entry.
	In-Profile Action (qosTargetInProfilelAction)		Choose the action you want to take for the data associated with this policy.
	Out-of-Profile Action (qosTargetOutOfProfilelAction)		Choose the action you want to take associated with this policy for metered data that is not within the configured profile.
	Shaper (qosTargetShaping Params)		Choose the shaper, if any, to apply to this policy.
	Shaper Group (qosTargetShapingGroup)	2- 63	Choose the shaper group, if any, to apply to this policy.

2 Complete the fields as described.

3 Click Submit.

Viewing policy statistics

To view statistics for a selected policy configuration:

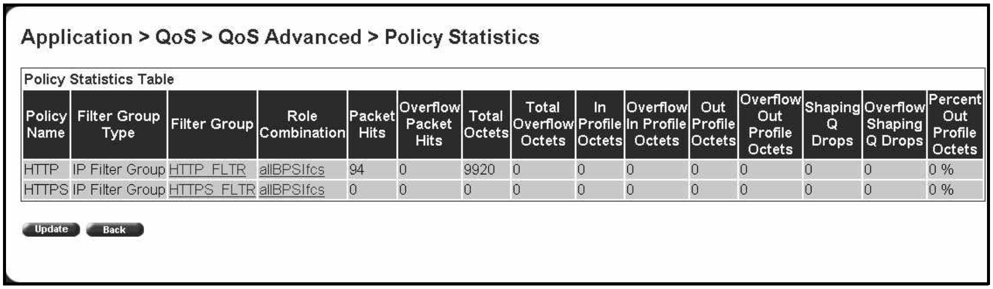
1 From the main menu, choose Application > QoS > QoS Advanced > Policies.

The QoS Advanced Policies page opens (Figure 163 on page 282).

2 In the Policy Table section, in the filter group configuration of your choice, click the View icon.

The Policy Statistics page opens (Figure 164).

Figure 164 Policy Statistics page



Application > QoS > QoS Advanced > Policy Statistics

Policy Statistics Table

Policy Name	Filter Group Type	Filter Group	Role Combination	Packet Hits	Overflow Packet Hits	Total Octets	Total Overflow Octets	In Profile Octets	Overflow In Profile Octets	Out Profile Octets	Overflow Out Profile Octets	Shaping Q Drops	Overflow Shaping Q Drops	Percent Out Profile Octets
HTTP	IP Filter Group	HTTP_FLTR	allBPSIfcs	94	0	9920	0	0	0	0	0	0	0	0 %
HTTPS	IP Filter Group	HTTPS_FLTR	allBPSIfcs	0	0	0	0	0	0	0	0	0	0	0 %

Table 78 describes the items on the Policy Statistics page.

Table 78 Policy Statistics page items

Item and MIB association	Description
Policy Name	The name of the selected policy.
Filter Group Type	The type of group that is referenced by this instance of the filter policy class. The options are: IP Filter Group or Layer2 Filter Group.
Filter Group	The filter group associated with the selected policy.
Role Combination	The interfaces to which this policy applies, specified in terms of a role combination.
Packet Hits (ntnQosTargetStatsPkHits)	The packets selected for additional processing. The action taken is based on a match with specified filter and threshold information.
Overflow Packet Hits (ntnQosTargetStatsOverflowPkHits)	The number of times the associated ntnQosTargetStatsPktHits counter overflowed.
Total Octets (ntnQosTargetStatsTotalOctets)	The total number of octets associated with packet hits for this policy.

Table 78 Policy Statistics page items (Continued)

Item and MIB association	Description
Total Overflow Octets (ntnQosTargetStatsTotalOverflowOctets)	The total number of times the associated ntnQosTargetStatsTotalOctets counter overflowed.
In Profile Octets (ntnQosTargetStatsTotalInProfOctets)	The total number of in-profile octets associated with packet hits for this policy.
Overflow In Profile Octets (ntnQosTargetStatsTotalInProfOverflowOctets)	The number of times the associated ntnQosTargetStatsTotalInProfOctets counter overflowed.
Out Profile Octets (ntnQosTargetStatsTotalOutProfOctets)	The total number of out-of-profile octets associated with packet hits for this policy.
Overflow Out Profile Octets (ntnQosTargetStatsTotalOutProfOverflowOctets)	The number of times the associated ntnQosTargetStatsTotalOutProfOctets counter overflowed.
Shaping Q Drops (ntnQosTargetStatsShapingQDrops)	The total number of octets dropped from the shaping queues for this policy.
Overflow Shaping Q Drops (ntnQosTargetStatsOverflowShapingQDrops)	The number of times the associated ntnQosTargetStatsShapingQDrops counter overflowed.
Percent Out Profile Octets	The percentage of out-of-profile octets associated with packet hits for this policy.

3 To refresh the hardware policy statistics, click Update.

Deleting a policy configuration

To delete a policy configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Policies.

The QoS Advanced Policies page opens (Figure 163 on page 282).

2 In the Policy Table section, in the hardware policy configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the policy configuration.
- Click Cancel to return to the Policy page without making changes.

Configuring QoS Policy Agent (QPA) characteristics

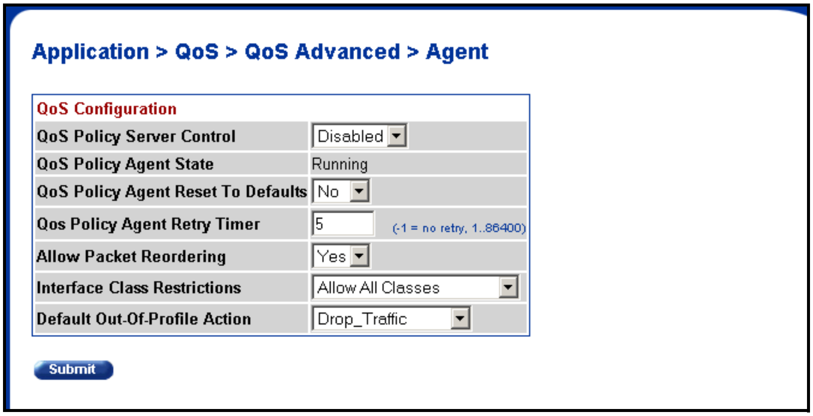
You can configure QPA operational parameters.

To open the Agent page:

1 From the main menu, choose Application > QoS > QoS Advanced > Agent.

The Agent page opens (Figure 165 and Figure 166).

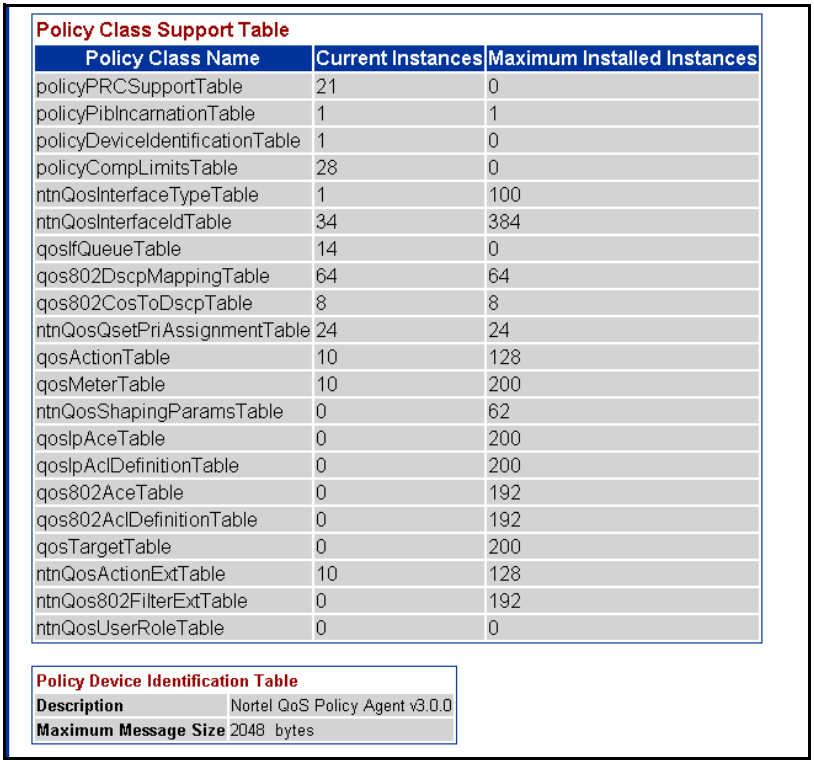
Figure 165 Agent page (1 of 2)



Application > QoS > QoS Advanced > Agent

QoS Configuration	
QoS Policy Server Control	Disabled
QoS Policy Agent State	Running
QoS Policy Agent Reset To Defaults	No
Qos Policy Agent Retry Timer	5 (-1 = no retry, 1..86400)
Allow Packet Reordering	Yes
Interface Class Restrictions	Allow All Classes
Default Out-Of-Profile Action	Drop_Traffic

Figure 166 Agent page (2 of 2)



Policy Class Support Table

Policy Class Name	Current Instances	Maximum Installed Instances
policyPRCSupportTable	21	0
policyPibIncarnationTable	1	1
policyDeviceIdentificationTable	1	0
policyCompLimitsTable	28	0
ntnQosInterfaceTypeTable	1	100
ntnQosInterfaceIdTable	34	384
qosIfQueueTable	14	0
qos802DscpMappingTable	64	64
qos802CosToDscpTable	8	8
ntnQosQsetPriAssignmentTable	24	24
qosActionTable	10	128
qosMeterTable	10	200
ntnQosShapingParamsTable	0	62
qosIpAceTable	0	200
qosIpAclDefinitionTable	0	200
qos802AceTable	0	192
qos802AclDefinitionTable	0	192
qosTargetTable	0	200
ntnQosActionExtTable	10	128
ntnQos802FilterExtTable	0	192
ntnQosUserRoleTable	0	0

Policy Device Identification Table	
Description	Nortel QoS Policy Agent v3.0.0
Maximum Message Size	2048 bytes

Table 79 describes the items on the Agent page.

Table 79 Agent page items

Section	Item and MIB association	Range	Description
QoS Configuration	QoS Policy Server Control	Enabled Disabled	Choose to enable or disable the QoS Policy server control. Note: Choosing to enable COPS disables local policy control.
	QoS Policy Agent State (ntnQosConfigQpaState)	Running Initialized Disabled	The current status of the policy agent.
	QoS Policy Agent Reset to Defaults (ntnQosConfigQpaState)	(1) Yes (2) No	Choose whether to reset the policy agent to the default settings.
	QoS Policy Agent Retry Timer (ntnQosConfigQpaRetryTimer)	-1 = no retry, 1..86400	Type the time, in seconds, between the receipt of a connection termination/ rejection indication and the start of a new connection request. Note: A value of -1 indicates that a connection retry should not be attempted after a failed attempt.
	Allow Packet Reordering (ntnQosConfigAllowPacket Reordering)	(1) Yes (2) No	Support for certain PHBs requires that packets within a flow not be reordered when transmitted. Choose: • Yes—Allows full flexibility of assigning packet to egress queue. • No—Agent verifies that in-profile and out-of-profile actions associated with the flow do not cause packets from same flow to be assigned to different egress queues.

Table 79 Agent page items (Continued)

Section	Item and MIB association	Range	Description
	Interface Class Restrictions (ntnQosConfigIfcClassRestrictions)	Allow All Classes Trusted and Unrestricted Unrestricted Only	Specify which interface class types can be defined by the user. Default filters are installed to support the different interface classes. Limiting the classes that can be used reduces, or eliminates entirely, the default filter resources that must be consumed, making these resources available for administrator use. Note: Modifications to this attribute do not take effect until the system is initialized.
Policy Class Support Table	Policy Class Names		The name of the policy.
	Current Instances		The current class entries.
	Maximum Installed Instances		The maximum number of allowed class entries.
Policy Device Identification Table	Description		The system description.
	Maximum Message Size		The maximum target message size supported by the device.

2 In the QoS Configuration section, type information in the text boxes, or select from a list.

3 Click Submit.

Chapter 6 Implementing Common Open Policy Services using Web-based management

Enabling COPS in your networks allows the policy server to:

- Gather all relevant information.
- Make a decision based on your (as network administrator) set policies and network resources,
- Communicate that decision in the form of proper service to the appropriate group or client (bandwidth, ACLs, QoS).

A solid COPS strategy is closely tied to Internet Protocol (IP) address management and network management.

This chapter discusses the COPS options available to you in the Web-based management interface.

The COPS options are:

- Viewing COPS statistics and capabilities (page 292)
- Creating COPS client configurations (page 297)

Viewing COPS statistics and capabilities

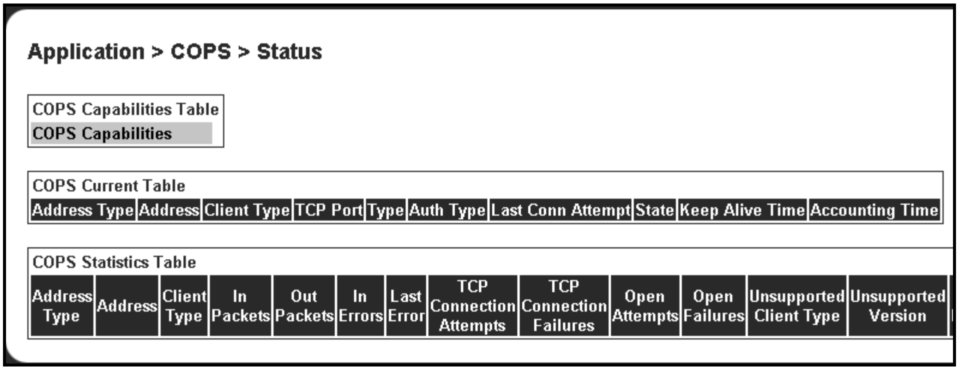
You can view a list of the capabilities of the COPS client to connect to a COPS server and view a table displaying the current status of all COPS server connections.

To view COPS capabilities and statistics:

1 From the main menu, choose Application > COPS > Status.

The Status page opens (Figure 167).

Figure 167 Status page



Application > COPS > Status

COPS Capabilities Table

COPS Capabilities

COPS Current Table

Address Type	Address	Client Type	TCP Port	Type	Auth Type	Last Conn Attempt	State	Keep Alive Time	Accounting Time

COPS Statistics Table

Address Type	Address	Client Type	In Packets	Out Packets	In Errors	Last Error	TCP Connection Attempts	TCP Connection Failures	Open Attempts	Open Failures	Unsupported Client Type	Unsupported Version

Table 80 describes the items on the Status page.

Table 80 Status page items

Section	Item	Descriptions
COPS Capabilities Table	COPS Capabilities	A list of COPS protocols supported by the Ethernet Switch 470-48T 10/100/1000 Switch. The current supported version is COPSv1 protocol.

Table 80 Status page items (Continued)

Section	**Item**	**Descriptions**
COPS Current Table	Address Type	The type of address in copsClientServerAddress.
	Address	The IPv4 address of a COPS server.
	Client Type	The protocol client type for this entry. Note: Multiple client types can be served by a single COPS server. Note: The value 0 (zero) indicates that this entry contains information about the underlying connection.
	TCP Port	The TCP port number on the COPS server to which the client is connected.
	Type	The indicator of the source of the COPS server information. Note: COPS servers can be configured by network management into copsClientServerConfigTable and appear in this entry with type copsServerStatic(1). Alternatively, the type, or entry, can be a notification from another COPS server by way of the COPS PDP-Redirect mechanism and appear as copsServerRedirect(2).
	Authorization Type	The indicator of the current security mode in use between the client and the COPS server.
	Last Conn Attempt	The timestamp of the last time the client attempted to connect to this COPS server.
	State	The operational state of the connection and COPS protocol with respect to this COPS server.
	Keep Alive Time	The value of the Keepalive timeout, in centiseconds, currently in use by the client, as specified by the COPS server in the Client-Accept operation. Note: A value of 0 (zero) indicates no keepalive activity is expected.
	Accounting Time	The value of the COPS protocol Accounting timeout, in centiseconds, currently in use by the client, as specified by the COPS server in the Client-Accept operation. Note: A value of 0 (zero) indicates that the client should not send any unsolicited accounting reports.

Table 80 Status page items (Continued)

Section	**Item**	**Descriptions**
COPS Statistics Table	Address Type	The type of address in copsClientServerAddress.
	Address	The IPv4 address of a COPS server.
	Client Type	The protocol client type for this entry. Note: Multiple client types can be served by a single COPS server. Note: The value 0 (zero) indicates that this entry contains information about the underlying connection.
	In Packets	The total number of COPS packets that the client has received from this COPS server marked for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
	Out Packets	The total number of COPS packets that the client has sent to this COPS server marked for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
	In Errors	The total number of COPS packets that the client has received from this COPS server marked for the selected client type that contained errors in syntax. Note: This is a cumulative value and *is not* zeroed on new connections.
	Last Error	The code contained in the last COPS protocol Error Object received by the client from this COPS server marked for the selected client type. Note: This value *is not* zeroed on COPS Client-Open operations.
	TCP Connection Attempts	The number of times that the COPS client attempted to open a TCP connection to the COPS server. Note: This value is valid only for client type 0. Note: This is a cumulative value and *is not* zeroed on new connections.
	TCP Connection Failures	The number of times that the COPS client failed to open a TCP connection to the COPS server. Note: This value is valid only for client type 0. Note: This is a cumulative value and *is not* zeroed on new connections.

Table 80 Status page items (Continued)

Section	Item	Descriptions
COPS Statistics Table, cont.	Open Attempts	The number of times that the COPS client attempted to perform a COPS Client-Open to a COPS server for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
	Open Failures	The number of times that the COPS client failed to perform a COPS Client-Open to a COPS server for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
	Unsupported Client Type	The total number of COPS packets that this client has received from COPS servers that referred to client types that are unsupported by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Unsupported Version	The total number of COPS packets that this client has received from COPS servers marked for the selected client type that had a COPS protocol version number that is unsupported by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Length Mismatch	The total number of COPS packets that the client received from COPS servers marked for the selected client type that had a COPS protocol message length that did not match the actual received packet. Note: This is a cumulative value and *is not* zeroed on new connections.
	Unknown Opcode	The total number of COPS packets that the client received from COPS servers marked for the selected client type having a COPS protocol Op Code not recognized by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Unknown Cnum	The total number of COPS packets that the client received from COPS servers marked for the selected client type containing a COPS protocol object C-Num not recognized by the client. Note: This is a cumulative value and *is not* zeroed on new connections.

Table 80 Status page items (Continued)

Section	**Item**	**Descriptions**
COPS Statistics Table, cont.	Bad Ctype	The total number of COPS packets that the client received from COPS servers marked for the selected client type containing a COPS protocol object C-Type not defined for the C-Nums known by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Bad Sends	The total number of COPS packets that the client attempted to send to COPS servers marked for the selected client type that resulted in a transmit error. Note: This is a cumulative value and *is not* zeroed on new connections.
	Wrong Objects	The total number of COPS packets that the client received from COPS servers marked for the selected client type not containing a permitted set of COPS protocol objects. Note: This is a cumulative value and *is not* zeroed on new connections.
	Wrong OpCode	The total number of COPS packets that the client received from COPS servers marked for the selected client type having a COPS protocol Op Code that should not have been sent to a COPS client, for example, Open-Requests. Note: This is a cumulative value and *is not* zeroed on new connections.
	Timedout Clients	The total number of times that the client has been shut down for the selected client type by COPS servers that detected a COPS protocolKeepalive timeout. Note: This is a cumulative value and *is not* zeroed on new connections.
	Auth Failures	The total number of times that the client received a COPS packet marked for the selected client type that could not be authenticated using the authentication mechanism used by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Auth Missing	The total number of times that the client received a COPS packet marked for this client type not containing authentication information.

Creating a COPS configuration

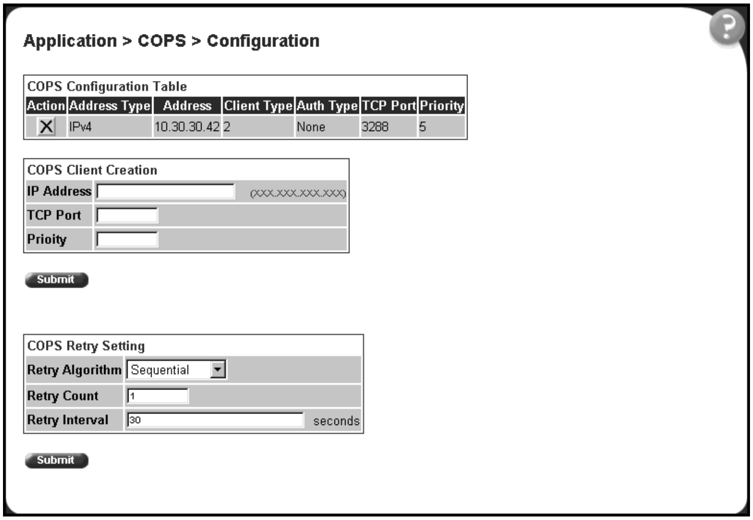
You can select the COPS server(s) to use to obtain policy information by creating COPS configurations.

To create a COPS configuration:

1 From the main menu, choose Application > COPS > Configuration.

The Configuration page opens (Figure 168).

Figure 168 Configuration page



Application > COPS > Configuration

COPS Configuration Table

Action	Address Type	Address	Client Type	Auth Type	TCP Port	Priority
☒	IPv4	10.30.30.42	2	None	3288	5

COPS Client Creation

IP Address		(XXX.XXX.XXX.XXX)
TCP Port		
Prioity		

Submit

COPS Retry Setting

Retry Algorithm	Sequential	
Retry Count	1	
Retry Interval	30	seconds

Submit

Table 81 describes the items on the COPS Configuration Table section of the Configuration page.

Table 81 COPS Configuration Table section items

Section	Item	Range	Description
COPS Configuration Table	☒		Deletes the row.
	Address Type		The type of address in copsClientServerConfigAddress.
	Address		The IPv4 address of the COPS server.

Table 81 COPS Configuration Table section items (Continued)

Section	Item	Range	Description
	Client Type		The COPS protocol client type this COPS server is capable of serving. Note: A single COPS server can serve multiple client types.
COPS Configuration Table, cont.	Auth Type		The authentication mechanism for this COPS client to request when negotiating security at the start of a connection to a COPS server.
	TCP Port		The TCP port number on the COPS server.
	Priority		The level of priority assigned to the client. Note: When a COPS client attempts to contact COPS servers for the appropriate client type, it contacts higher numbers (priority) first. The order used for server entries with the same priority is undefined. COPS servers notified to the client using the COPS protocol PDP-Redirect mechanism are always processed with higher priority than any entries in this table.
COPS Client Creation	IP Address	XXX.XXX.XXX.XXX	The IP address of the COPS client.
	TCP Port	Integer	Type the TCP port number on the COPS server.
	Priority		Type a number that represents the level of priority. Note: When a COPS client attempts to contact COPS servers for the appropriate client type, it contacts higher numbers (priority) first. The order used for server entries with the same priority is undefined. COPS servers notified to the client using the COPS protocol PDP-Redirect mechanism are always processed with higher priority than any entries in this table.
COPS Retry Setting	Retry Algorithm	(1) Sequential (2) Round Robin	Choose the type of algorithm to use.
	Retry Count	Integer	Type the number of retry attempts.
	Retry Interval	Integer	Type, in seconds, the retry interval.

2 Type information in the text boxes, or select from a list.

3 Click Submit.

Note: COPS configurations are not modifiable. They must be deleted and the information recreated.

Deleting a COPS client configuration

To delete a COPS client configuration:

1. From the main menu, choose Application > COPS > Configuration.

   The Configuration page opens (Figure 168 on page 297).

2. In the COPS Configuration Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:

   - Click Yes to delete the configuration.
   - Click Cancel to return to the Configuration page without making changes.

Index