Part No. 316433-C Rev 00
May 2004

4655 Great America Parkway
Santa Clara, CA 95054

Configuring QoS and IP Filtering

Passport 8000 Series Software Release 3.7

NORTEL NETWORKS™

Copyright © 2003 Nortel Networks

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

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

Trademarks

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.

The asterisk after a name denotes a trademarked item.

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).

Nortel Networks Inc. software license agreement

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

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

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

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

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER’S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The 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-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

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

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

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

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

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

Contents

Figures

Tables

Preface

This guide provides instructions for using the Command Line Interface (CLI) and the Device Manager graphical user interface (GUI) to perform QoS and IP filtering operations on Passport 8000 switches.

For details about how to perform various QoS and IP filtering tasks, with step-by-step procedures using the CLI commands, see Chapter 2, “Configuration examples,” on page 49.

For more information about using Passport 8000 Series switches, refer to the Related Publications section of the release notes that accompany this release.

Before you begin

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

- Basic knowledge of networks, Ethernet bridging, and IP routing
- Familiarity with networking concepts and terminology
- Basic knowledge of network topologies
- Experience with windowing systems or graphical user interfaces (GUIs)

Text conventions

This guide uses the following 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 `ping <ip_address>`, you enter `ping 192.32.10.12`
`bold Courier text`	Indicates command names and options and text that you need to enter. Example: Use the **`dinfo`** command. Example: Enter **`show ip`** {**`alerts`**|**`routes`**}.
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 `show ip {alerts|routes}`, you must enter either `show ip alerts` or `show ip routes`, but not both.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is `show ip interfaces [-alerts]`, you can enter either `show ip interfaces` or `show ip interfaces -alerts`.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is `ethernet/2/1 [<parameter> <value>]...`, you enter `ethernet/2/1` and as many parameter-value pairs as needed.

italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is `show at <valid_route>`, `valid_route` is one variable and you substitute one value for it.
`plain Courier text`	Indicates command syntax and system output, for example, prompts and system messages. Example: `Set Trap Monitor Filters`
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP command on the Protocols menu.
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 `show ip {alerts|routes}`, you enter either `show ip alerts` or `show ip routes`, but not both.

Hard-copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. 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 Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

How to get help

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

If you purchased a Nortel Networks service program, contact Nortel Networks Technical Support. To obtain contact information online, go to the www.nortelnetworks.com/cgi-bin/comments/comments.cgi URL, then click on Technical Support.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, you can call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel Networks 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 the http://www.nortelnetworks.com/help/contact/erc/index.html URL.

Chapter 1
QoS and IP filtering concepts

This chapter describes a range of features on the Passport 8000 Series Switch that allows you to allocate network resources to mission-critical applications at the expense of applications that are less sensitive to such factors as time delays or network congestion. You can configure your network to prioritize specific types of traffic, ensuring that they receive the appropriate Quality of Service (QoS) level.

Traffic prioritization features on the Passport 8000 switch allow you to manage bandwidth allocation for traffic flows on the LAN. These traffic flows are switched in the Passport 8000 switch at the layer 2 level.

Traffic flows on the WAN are routed by the Passport 8000 switch at the layer 3 level through a differentiated services (DiffServ) network architecture.

Traffic filtering is a mechanism that helps you to manage traffic by defining filtering conditions and associating these conditions with specific actions. Within a DiffServ network, IP filtering allows you to assign QoS levels that can be based on a range of filtering conditions.

Note: See Chapter 2, “Configuration examples,” on page 49, for configuration examples, including commands, for most of the concepts described in this chapter.

This chapter includes the following topics:

Quality of Service

By assigning QoS levels to traffic flows on your LAN and WAN, you can ensure that network resources are allocated where they are needed most. To be effective, you must configure QoS functionality from end-to-end of the network: across different devices, such as routers, switches, and servers; across platforms and media; and across link layers, such as Ethernet, ATM, and frame relay.

In the case of WANs, purchasing additional bandwidth to meet increasing demand for network connectivity enables you to offer guaranteed levels of service for specific types of traffic flows. This approach to bandwidth provisioning can be expensive and may be less efficient in resource utilization than delivering bandwidth on demand. If you configure a DiffServ network architecture you can allocate bandwidth to specified services as required, but this bandwidth will be reallocated to lower classes of service when available.

The Passport 8000 switch supports QoS functionality at layer 2 and layer 3 levels, managing switched and routed traffic flows. The Passport 8000 switch can also assign layer 2 or layer 3 QoS and priority levels to applications based on TCP or UDP ports used by this application.

QoS and LAN traffic

The Passport 8000 switch provides hardware-based QoS functionality by classifying packets at switching speeds based on information stored in the Ethernet packet header. This functionality ensures that latency-sensitive traffic flows, such are real-time video and audio, can be prioritized within a LAN.

You can assign QoS levels for non-IP traffic based on any of the following parameters:

- Membership of a VLAN that is associated with a specific QoS level
- MAC address
- ingress port

When you create a VLAN you can assign a QoS level for traffic on that VLAN. The IEEE 802.1p portion of the Ethernet packet header stores the relevant QoS classification information. In cases where different QoS levels are assigned by a combination of parameters, the highest QoS level is honored.

On Passport 8000 switches, layer 2 QoS functionality operates in association with a DiffServ network, which delivers layer 3 QoS functionality for IP traffic. IEEE 802.1p bits in the Ethernet packet header are substituted with DiffServ codepoints as they leave the LAN and enter the WAN.

DiffServ network

QoS functionality for IP traffic is implemented on the Passport 8000 switch through a DiffServ network architecture. A DiffServ network allows for either end-to-end or intra-domain QoS functionality by implementing complex classification and mapping functions at the network boundary or access points. Within a DiffServ domain, packet behavior is regulated by this classification and mapping.

Table 1 defines common DiffServ terms and concepts.

Table 1 DiffServ terms and concepts

Term	Definition
DS boundary or access point	The edge of a DS domain where classifiers and traffic conditioners are likely to be deployed is the DS boundary.
DS field	The DiffServ (DS) field is what was formerly called the IPv4 Type of Service (TOS) octet or the IPv6 Traffic Class octet. The first six bits of the DS field are called the DiffServ codepoint (DSCP) and the value of the DSCP determines the PHB.
Microflow	Microflow is a single instance of an application-to-application flow of packets, which is identified by source address, destination address, protocol ID, and source port.
Marking	Marking is the process of setting the DSCP in a packet based on defined rules.
PHB	Per-hop-behavior (PHB) is the forwarding treatment applied by a DiffServ node to a packet in a DiffServ network.
Policing	Policing ensures that a traffic stream performs in accordance with the domain's service provisioning policy or Service Level Agreement (SLA).

Table 1 DiffServ terms and concepts

Term	Definition
Re-marking	Re-marking is changing the DSCP of a packet, usually performed in accordance with an SLA.
SLA	A Service Level Agreement (SLA) is a service contract that specifies the forwarding service traffic should receive.
Traffic profile	Traffic profile represents the temporal properties of a traffic stream such as rate.

This section includes the following topics:

Packet classification and marking

Traffic is classified as it enters the DiffServ network and is assigned appropriate PHB based on that classification. To differentiate between classes of service, the DiffServ (DS) field in the IP packet header, as defined in RFC 2474 and RFC 2475, is marked. The DS field in the IP header is an octet, and the first 6 bits, called the DS codepoint (DSCP), are used in the DiffServ architecture. The DSCP is marked to define the forwarding treatment given to the packet at each network hop. This marking (or classification) occurs at the edge of the DiffServ domain and is based on the policy or filter associated with the particular microflow or aggregate flow.

You can configure the mapping of DSCPs to forwarding behaviors and the DSCP may 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.

Per-hop behavior

When traffic enters the DiffServ network, 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 these packets traverse the DiffServ network, the video stream is forwarded before any other packets.

Two standard PHBs are defined in RFC 2597 and RFC 2598: the Assured Forwarding PHB group and the Expedited Forwarding PHB group.

Assured Forwarding PHB group

RFC 2597 describes the Assured Forwarding PHB group, which further divides delivery of IP packets into four independent classes. The Assured Forwarding PHB group offers different levels of forwarding resources in each DiffServ node. Within each Assured Forwarding PHB group, IP packets are marked with one of three possible drop precedence values. In case of network congestion, the drop precedence of a packet determines its relative importance with the Assured Forwarding group.

Expedited Forwarding PHB group

RFC 2598 describes the Expedited Forwarding PHB group as the “Premium” service, the best service your network can offer. Expedited Forwarding PHB is defined as a forwarding treatment for a DiffServ microflow when the rate of its transmission ensures that it is the highest priority and experiences no packet loss for in-profile traffic.

Policing

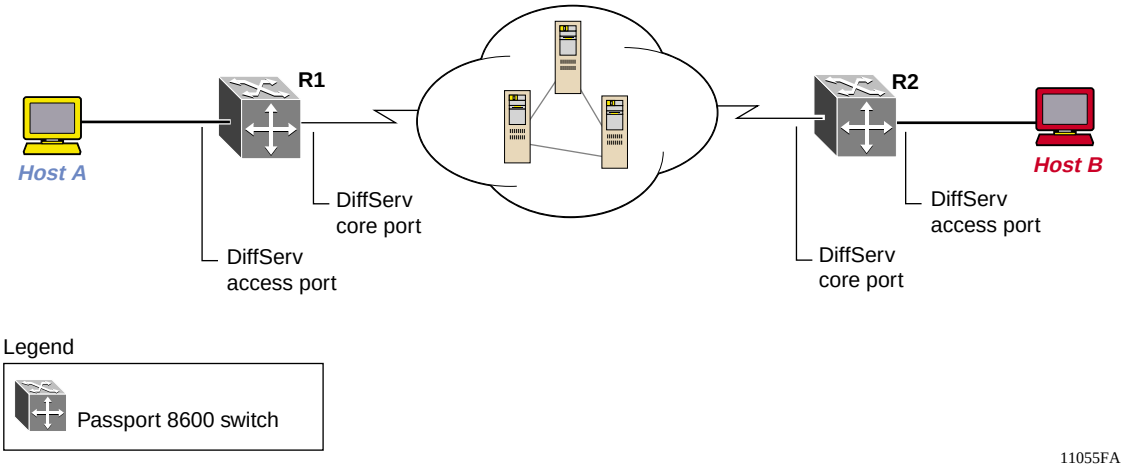
As the traffic moves within the DiffServ network, policing ensures that traffic marked by the different DSCPs is treated according to that marking. Policing ensures that the traffic flow conforms to a Service Level Agreement (SLA) to provide certain levels of service in terms of bandwidth for different types of network traffic.

How the Passport 8000 Series Switch implements DiffServ

The Passport 8000 Series Switch implements a DiffServ architecture as defined in RFC 2474 and RFC 2475. The DSCP and the IEEE 802.1p marking found in VLANs are both used to mark the packet to its appropriate PHB and QoS level, providing layer 2 and layer 3 QoS functionality.

Figure 1 illustrates a model of a DiffServ network. You can configure DiffServ access ports and DiffServ core ports in the Device Manager software, on a port-by-port basis.

Figure 1 DiffServ network model



The following sections describe how to implement a DiffServ network on an Passport 8000 switch:

- "DiffServ access port," next
- "DiffServ core port" on page 31
- "Classification and policing" on page 33
- "Priority queuing and servicing" on page 35

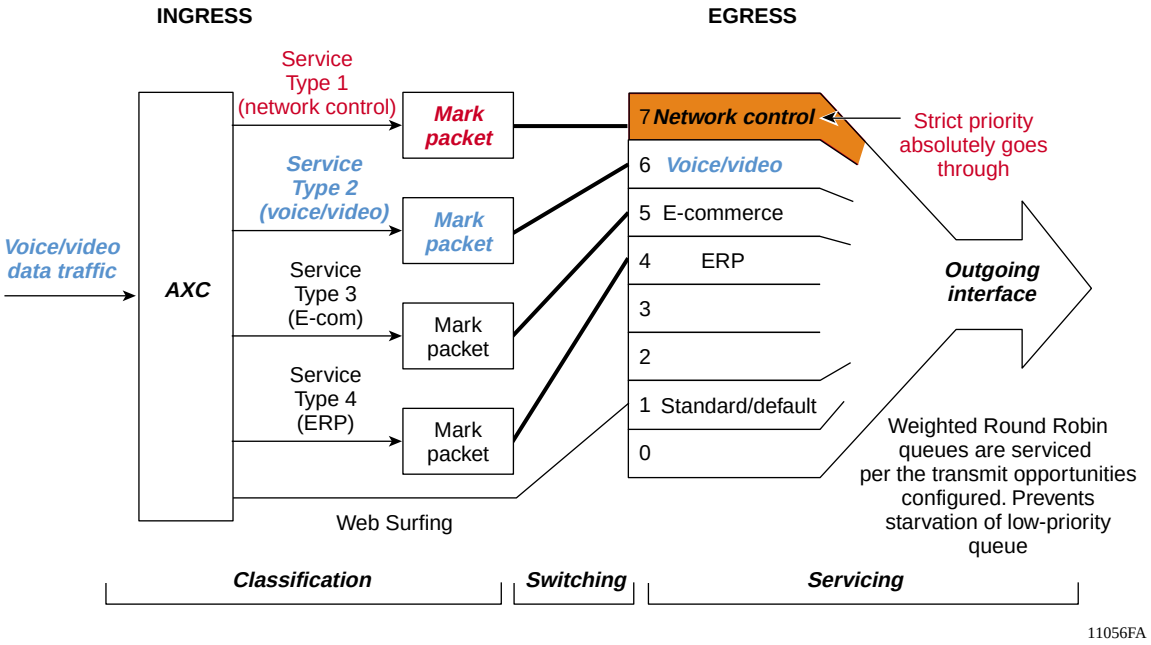
DiffServ access port

The DiffServ access port, shown in Figure 2 at the edge of a DS network, classifies traffic by marking it with the appropriate DSCP.

The classified traffic is assigned to an internal QoS level based on the filters and traffic policies you enable.

Traffic filters allow you to set criteria for identifying a microflow or an aggregate flow by matching on multiple fields in the IP packet.

Figure 2 DiffServ access port



Tagged traffic

In IP traffic that is tagged, the packet's QoS level is derived from the packet's IEEE 802.1p bits or its DSCP, depending on whether the traffic is bridged or routed. In bridged IP packets, the switch examines the IEEE 802.1p bits as the packets enter the DiffServ access port and bases the QoS level on the ingress Tag-to-QoS mapping (Table 2).

Table 2 Ingress DSCP and IEEE 802.1p to QoS level mapping

DSCP[1]	IEEE 802.1p	QoS level	Traffic service class
CS7 (111000), CS6 (110000)	7	7	Network
EF (101110), CS5 (101000)	7	6	Premium
AF41 (100010), AF42 (100100), AF43 (100110), CS4 (100000)	6	5	Platinum
AF31 (011010), AF32 (011100), AF33 (011110), CS3 (011000)	5	4	Gold
AF21 (010010), AF22 (010100), AF23 (010110), CS2 (010000)	4	3	Silver
AF11 (001010), AF12 (001100), AF13 (001110), CS1 (001000)	3	2	Bronze
DE (000000) and all undefined codepoints	0	1	Standard
User-defined codepoints	2	0	Standby

1 The DSCP is represented in both the PHB group (AF = Assured Forwarding; EF = Expedited Forwarding; CS = Class Selector; DE = Default or Best Effort) format and the PHB's equivalent in binary format.

As the tagged, bridged packet leaves the DS network via an access port, the switch re-marks the packet's IEEE 802.1p bits and DSCP based on whether the packet is part of a port-based VLAN or a policy-based VLAN and if global filters are enabled.

Re-marking occurs as follows:

- A bridged, tagged packet's IEEE 802.1p bits will be re-marked by the global filter only if the IEEE 802.1p value in the filter is higher than the value already marked on the packet.

- If a global filter is present and set to modify DSCP, the bridged, tagged packet's DSCP will be re-marked according to the filter.
- When no global filter is present, packets that are part of port-based VLAN are re-marked with a DSCP according to the egress mapping based on the port QoS level.
- When no global filter is present, the packets that are part of the policy-based VLAN are re-marked with a DSCP according to the egress mapping based on the VLAN QoS level.

In tagged, routed IP packets entering the access port, the switch sets the DSCP to the default (000000 binary) unless the traffic filters set for that port indicate otherwise. Based on the new DSCP marking, the packets are then given the appropriate PHB and assigned a QoS level based on the ingress DSCP-to-QoS mapping (Table 2 on page 28). When a tagged IP packet leaves the DS network, the switch sets the IEEE 802.1p bits based on the egress mapping table (Table 3), unless traffic filters indicate otherwise.

Table 3 Egress QoS level to DSCP and IEEE 802.1p mapping

DSCP[1]	IEEE 802.1p	QoS level	Traffic service class
EF (101110)	7	7	Network
EF (101110)	7	6	Premium
AF41 (100010)	6	5	Platinum
AF31 (011010)	5	4	Gold
AF21 (010010)	4	3	Silver
AF11 (001010)	3	2	Bronze
DE (000000)	0	1	Standard
DE (000000)	2	0	Standby

1 The DSCP is represented in both the PHB group (AF = Assured Forwarding; EF = Expedited Forwarding; DE = Default or Best Effort) format and the PHB's equivalent in binary format.

Untagged traffic

All bridged, untagged IP traffic ingressing a DS access port is assigned a QoS level based on the QoS setting at the port, the VLAN or MAC address level, or the DSCP-to-QoS mapping.

When the packet enters a DS access port, the assigned QoS level is one of the QoS levels you assigned at the MAC address level, Port level or VLAN level. If the untagged packet used a port-based/policy based VLAN, then the QoS level assigned is the greater of the QoS levels found at:

- the MAC address level
- the port level
- the VLAN level

If global filters are used, the QoS level is determined differently. A global filter re-marks the packet's DSCP according to that filter, and the QoS level is then determined by the highest QoS levels, derived from the:

- DSCP-to-QoS mapping—port or MAC level if the packet is using a port-based VLAN.
- DSCP-to-QoS mapping—VLAN or MAC level if the packet is using a policy-based VLAN.

As the packet leaves the DS network via an access port, the switch re-marks the packet's DSCP based on the egress QoS-to-DSCP mapping (Table 3 on page 29).

The DSCP of routed, untagged IP traffic is reset to the default DSCP (000000 binary) unless a traffic filter indicates otherwise.

The switch can use an IP filter to re-mark the DSCP of untagged IP traffic entering the DS access port. When a routed, untagged packet leaves the DS network, its DSCP remains unchanged.

Table 4 summarizes the actions the DiffServ access port takes to identify a QoS level for the IP traffic.

Table 4 Access port actions

Type of traffic	Ingress	Egress
Tagged and bridged	Use Tag-to-QoS mapping to map the IEEE 802.1p bits to a QoS level, if no global filter is present. With global filter, re-mark IEEE 802.1p bits with filter value only if the filter value is higher. Preserve DSCP.	Use the QoS-to-Tag mapping to reset the IEEE 802.1p bits based on the QoS level. Use the QoS-to-DSCP mapping to set the DSCP, if no filter is present. Otherwise, re-mark DSCP to filter DSCP.
Tagged and routed	Reset DSCP to zero, and use traffic filters to set the new DSCP. Use the DSCP-to-QoS mapping to map the new DSCP to a QoS level. Ignore IEEE 802.1p bits.	Use the QoS-to-Tag mapping to reset the IEEE 802.1p bits based on the QoS level.
Untagged and bridged	If a global filter is used, set the new DSCP according to that filter. Assign QoS level based on highest QoS level in either the DSCP mapping or port, VLAN, or MAC address.	Use the QoS-to-DSCP mapping to reset the DSCP.
Untagged and routed	Reset DSCP to zero, and use traffic filters to set the new DSCP. Use the DSCP-to-QoS mapping to map the new DSCP to a QoS level.	No action is performed.

DiffServ core port

The DiffServ core port does not change packet classification or marking done in the DiffServ access port. The core port preserves the DSCP or IEEE 802.1p bit marking of all incoming packets and uses these markings to assign the packet to an internal queue.

Tagged traffic

For all IP tagged traffic, the switch examines the DSCP of the packets and places the packets in the appropriate queue based on the ingress DSCP-to-QoS mapping table (Table 2 on page 28). All DSCP and IEEE 802.1p bit markings are preserved.

Untagged traffic

For untagged IP traffic, the switch examines the DSCP of the packets and places the packets in the appropriate queue based on the ingress DS-to-QoS mapping table (Table 2 on page 28).

Table 5 summarizes the actions the DiffServ core port takes to assign a QoS level for the IP traffic.

Table 5 Core port actions

Type of traffic	Ingress	Egress
Tagged and bridged	Place the packet in the QoS queue based on the DSCP-to-QoS mapping. Ignore the IEEE 802.1p bits.	No action is performed.
Tagged and routed	Place the packet in the QoS queue based on the DSCP-to-QoS mapping. Ignore the IEEE 802.1p bits.	Use the QoS-to-Tag mapping to reset the IEEE 802.1p bits based on the QoS level.
Untagged and bridged	Place the packet in the QoS queue based on the DSCP-to-QoS mapping.	No action is performed.
Untagged and routed	Place the packet in the QoS queue based on the DSCP-to-QoS mapping.	No action is performed.

Classification and policing

Policing is performed according to the traffic filter profile assigned to the traffic flow. This policing is required to ensure that traffic flows conform to criteria assigned by network managers. For example, you may choose to limit the traffic rate from one department to give mission-critical traffic unlimited access to the network.

Traffic profiles contain the parameters necessary to police traffic flows. They contain the following information:

- Profile ID
- Average rate (see the "Rate metering" section that follows)
- In-profile DSCP marking
- Out-of-profile behavior
  - Mark (change the DSCP value)
  - Discard

Note: A maximum of 64 profiles per system is supported, and each port can support up to 64 policing profiles attached to it.

Packets exceeding the average rate can be marked Out-of-Profile and either discarded or re-marked with a new DSCP.

Rate metering

In the Passport 8000 switch, QoS rate metering is accomplished in increments of 64 bytes every 2.5 milliseconds. Table 6, Table 7, and Table 8 list the throughput in megabits per second (Mb/s) for various traffic flows using different rate-limiting values, using source and destination filters.

All traffic loads are at 100% of interface speed, using fixed-sized packets of the size indicated (in bytes). The Target Average Rate for each interface type is shown, in increments of 10% of total interface speed.

Table 6 lists the values for 10 Mb/s Ethernet.

Table 6 10 Mb/s Ethernet line rate metering

Packet size in bytes	10%[1]	20%	30%	40%	50%	60%	70%	80%	90%	100%
64	1.03[2]	2.05	3.08	4.10	5.12	6.15	7.17	7.62	7.62	7.62
128	1.23	2.05	3.28	4.10	5.33	6.15	7.38	8.20	8.65	8.65
256	1.64	2.46	3.28	4.10	5.74	6.56	7.38	8.19	9.28	9.28
512	1.64	3.28	3.28	4.92	6.56	6.56	8.20	8.20	9.62	9.62
1024	3.28	3.28	3.28	6.56	6.56	6.56	9.81	9.81	9.81	9.81
1518	4.86	4.86	4.86	4.86	9.72	9.72	9.72	9.72	9.72	9.87

1 target average percentage of line rate

2 rate in megabits per second

Table 7 lists the values for 100 Mb/s Ethernet.

Table 7 100 Mb/s Ethernet line rate metering

Packet size in bytes	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
64	10.25	20.49	30.74	40.99	51.23	61.15	71.72	76.19	76.19	76.19
128	10.25	20.49	30.74	40.99	51.24	61.48	71.72	81.97	86.49	86.49
256	10.66	20.47	31.11	40.93	51.58	61.40	72.04	81.97	92.62	92.75
512	11.48	21.32	31.15	40.99	52.46	62.29	72.13	81.97	93.44	96.24
1024	13.12	22.96	32.80	42.63	52.46	62.30	72.13	81.97	95.08	98.08
1518	14.58	24.31	34.02	43.75	53.47	68.05	77.77	87.49	97.20	98.70

Table 8 lists the values for Gigabit Ethernet.

Table 8 Gigabit Ethernet line rate metering

Packet size in bytes	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
64	102.50	205.00	307.47	409.93	446.61	446.61	446.61	446.61	446.61	446.61
64[1]	102.29	204.78	307.25	409.75	512.20	614.65	650.94	650.94	650.94	650.94
128	102.50	204.93	307.43	409.95	512.38	614.80	717.24	819.67	922.11	927.54
256	102.49	204.96	307.43	409.95	512.38	614.80	717.24	819.67	922.11	927.54
512	103.32	204.99	308.30	409.86	513.13	614.79	718.07	819.68	922.93	962.41
1024	104.92	206.57	308.23	409.96	514.85	616.45	718.07	819.68	924.57	980.84
1518	106.93	213.89	320.90	422.93	529.87	636.78	743.68	845.72	952.62	986.99

1 Results listed in this row were obtained using a global filter instead of a source filter and illustrate the source filter lookup rate limit of the hardware. These results are for comparison only

When assigning QoS levels note the following considerations that may impact on bandwidth availability:

- The switch forwards the entire packet, even if it receives only part of a packet.
- The Ethernet overhead—interpacket gap (IPG) and the preamble—must be subtracted from the overall rate. For example, in Table 6, at 100% of the offered rate, the output for a 10 Mb/s line should be 10 Mb/s; but because of the overhead imposed by IPG and the preamble in Ethernet, the rate is 7.62 Mb/s.

Priority queuing and servicing

The Passport 8000 switch supports eight output queues per port into which the packet can be placed. Each of the eight queues is mapped to one of the eight QoS levels, and queues are serviced using guaranteed Weighted Round Robin.

Table 9 lists the eight traffic service classes corresponding to the QoS levels. The priority is assigned from the highest (7) to the lowest (0). For example, traffic assigned to QoS level 5 is a higher priority than traffic in QoS level 4.

Note: The Network class is not configurable and is reserved for network node initiated traffic.

The premium class is assigned a DSCP for Expedited Forwarding PHB because this class is provided for traffic with stringent requirements such as voice and video traffic that must go through without delay. The platinum, gold, silver, and bronze classes comprise the four groups within the Assured Forwarding PHB.

In the Passport 8000 switch, the default queue for all traffic is QoS level 1 or the standard traffic service class.

Table 9 Traffic service classes mapping to QoS levels

Traffic Service Class	QoS level	PHB	Packet transmit opportunity	Percentage weight
Network	7		2	6%
Premium	6	Expedited Forwarding	32	100%
Platinum	5	Assured Forwarding	10	31%
Gold	4	Assured Forwarding	8	25%
Silver	3	Assured Forwarding	6	18%
Bronze	2	Assured Forwarding	4	12%
Standard	1	Default	2	6%
User-defined	0		0	0%

After the packets are placed in the queues, the queues are serviced according to the guaranteed Weighted Round Robin (WRR) mechanism. This mechanism ensures strict priority for the queue assigned to the Premium class, and the other queues are serviced according to WRR. The WRR mechanism uses the queue's packet transmit opportunity to determine which queue is serviced first.

When the packet transmit opportunity allocated to a particular time slot arrives and the level contains data, it is serviced. If two queues contain data and their time slots arrive simultaneously, the queue with the higher priority is serviced first. See Table 9 for the relationship between the QoS level, packet transmit opportunity, and percentage weight. For each port, every queue level, except for the network class, can be configured to own any, all, or none of the packet transmit opportunities.

The switch uses the percentage weight to configure the packet transmit opportunity for each queue.

IP filtering

You can use IP filtering to manage traffic and, in some cases, to provide security. Each filter set defines the conditions that must match for inclusion in the filter set and also the actions that should be performed when a match is made.

Filtering actions include

- forward
- forward to next hop
- drop
- prioritize
- mirror
- stop-on-match

IP filters apply to all IP packets to be forwarded through the switch on specified ingress ports. The filters are applied to the switch ingress ports with a default action to forward or drop. All packets not matching any filter are forwarded or dropped, depending on the port's default action. You can apply two types of filters: traffic filters or global filters.

Traffic filtering can be applied to the following parameters:

- source IP address
- destination IP address
- DiffServ field

- ICMP request
- IP fragment

Filters are applied to ports using filter sets, and actions are assigned when applying a filter set to a port. The actions of individual filters can overwrite the default actions of the port.

This section includes the following topics:

Enabling ARP traffic

The Passport 8000 switch accepts and processes Spanning Tree BPDUs and Topology Discovery Protocol (TDP) packets on *port-based* VLANs with the default port action set to DROP. To permit ARP traffic, you must use the command line interface to do the following:

- Configure a user-defined protocol-based VLAN for ARP EtherType (byprotocol usrDefined 0x0806)
- Set the ports with a default port action of DROP

You then need to add these ports to the VLAN as static members. Finally, set the port Default VLAN ID to the correct port-based VLAN where the ARPs will be processed.

Note: It is not necessary for you to make any configuration changes for the BPDU and TDP packets.

The ARP configuration sequence is demonstrated in the example that follows:

1. To create a user-defined protocol-based VLAN with ethertype 0x0806 (specific to the ARP protocol), enter:

   ```
   vlan 4000 create byprotocol 1 usrDefined 2054 name 'ARP'
   ```

2. To remove all ports from this user-defined protocol-based VLAN, type:

   ```
   vlan 4000 ports remove 1/1-1/48,4/1-4/8 member portmember
   ```

3. To add all the ports with the default port action set to DROP for this protocol-based VLAN, enter:

   ```
   vlan 4000 ports add 1/26,1/32 member portmember
   vlan 4000 ports add 1/26,1/32 member static
   ```

Only one user-defined protocol-based VLAN for ARP is allowed per STG. If the ports with the default port action set to DROP are in different STGs, you need to create additional user-defined protocol-based VLANs.

Note: This procedure is effective ONLY with port based VLANs.

Filter characteristics

Filters on Passport 8000 switches have the following characteristics and requirements:

- Up to 3071 filter IDs can be defined among all ports or on a single port, including source/destination and global filters.
- Up to 200 filter sets can be defined for source/destination filters, while up to 100 filter sets can be defined for global filters.
- A collection of source/destination filters is defined in a set, and the set is applied to a port or group of ports. Multiple sets can be assigned to any given port.
- A collection of global filters is defined in a global set (not exceeding eight per set), and the set is applied to a port or group of ports. Multiple sets may be applied to a given port or set of ports, but the maximum number of global filters that can be enabled on a given port set is eight.

Filter counters are maintained for all active filters. Each time an active filter is encounters a packet, the filter counter is incremented by one. These counters are maintained chassis-wide and may be viewed or reset administratively at any time.

Note: In order to check and optimize your configuration, it is recommended that you first consult with the Passport 8000 switch product management team regarding filtering requirements.

Source and destination filters

Source and destination filters (traffic filters) instruct a router interface to selectively handle specified IP traffic. You determine which packets receive special handling based on information in the packet headers. Using traffic filters, you can reduce network congestion and control access to network resources by blocking, forwarding, or prioritizing specified traffic on an interface. You can apply multiple traffic filters to a single interface.

Source filters must specify a source IP address and mask, and they may optionally specify a destination IP address and mask. Destination filters must specify a destination IP address and mask, and they may optionally specify a source IP address and mask. You can configure source filters with 0.0.0.0/0.0.0.0 as the source address however, the filter will be connected to all forwarding records. You can configure destination filters with 0.0.0.0/0.0.0.0 as the destination address.

A source or destination filter can cause the following actions to be applied to a packet that matches the filter record:

- Forward the packet when the filter is applied with a forward action
- Drop the packet when the filter is applied with a drop action
- Mirror the packet to the defined mirror port
- Forward it to the next hop
- Modify the DS codepoint (only on DiffServ access ports)
- Modify IEEE 802.1p
- Policing

Configuring source or destination filters for nonlocal routes will cause corresponding routing entries to be created and updated, as needed, in the routing table, thus maintaining the effectiveness of these filters.

Global filters

Global filters can specify a source IP address and mask, a destination IP address and mask, both of these, or neither of these. Global filters have the following characteristics:

- No minimum or maximum mask length exists.
- Up to eight global filters can be applied on any given set of RaptARU ports. A set includes eight 10/100 Mb/s ports or one gigabit port, each of which can accommodate eight global filters.
- A global filter can cause the same actions described above for source/ destination filters.

Filter configuration

Matching criteria for filters in the Passport 8000 switch can be any of the following:

- Destination address or address range
- Source address or address range
- Exact IP protocol match (TCP, UDP, or ICMP)
- TCP or UDP port numbers
- TCP connections established from within the network only or bidirectional establishment allowed
- ICMP request
- DS field
- IP frame fragment

Configurable actions are:

- Drop
- Forward
- Forward to next hop
- Mirror
- Police
- TCP connect (prevents incoming TCP sessions)

- Stop on match
- Modify the DS field
- Modify the IEEE 802.1p bit

Actions

Each filter has an associated *action mode* that determines whether packets matching this filter are forwarded (routed) through the switch.

Each filtered port on the Passport 8000 switch has a default action of *forward* or *drop* associated with it. When the filter's action mode matches the port's default action, the port's default action is used.

When the port default action is drop, packets are forwarded only if a matching filter's action mode is "forward." If a single match occurs with an action mode of forward, it does not matter how many matching filters are found with an action mode of drop; the frame is forwarded. For example, if a packet matches multiple filters, and any of the filter action modes are set to forward, the packet is forwarded.

When the port mode is set to forward, packets are dropped only if a matching filter's action mode is "drop" (if a single match occurs with a drop action, it does not matter how many matching filters have forwarding actions; the packet is dropped). For example, if a packet matches multiple filters, and any of the filter action modes are set to drop, the packet is dropped.

The final decision is a logical OR between the result of the Global, Destination and Source filters:

- When the port's default action is drop, if a single match occurs with an action of forward, the frame is forwarded.
- When the port's default action is forward, if a single match occurs with an action of drop, the frame is dropped.

Table 10 indicates the forward/drop behavior of a port if filter matches are found for a packet.

Table 10 Port actions for filters

Port mode	Filter mode	Packet action
Forward	Default	Forward all packets that match the filter
Drop	Default	Drop all packets
Forward	Forward	Forward all packets that match the filter
Drop	Forward	Drop all packets except those that match the filter
Forward	Drop	Drop all packets that match the filter
Drop	Drop	Drop all packets

IP telephony and multimedia default filters

The speed and performance quality of LAN solutions has previously been limited to single-purpose IP data networks. Delay- and packet-loss-sensitive applications such as telephony and video services transported over IP networks, require network planners to focus on traffic prioritization strategies as a priority.

QoS in IP-based networks is essential because the connectionless nature of IP. A simple IP network provides a best-effort service that can make no guarantees about when, or how much, data it can deliver. To enable IP technology to offer a transparent service when compared to more traditional leased-line services or virtual circuit services such as Frame Relay and ATM, requires a QoS strategy that provide predictable service in an increasingly IP-based world, especially during periods of congestion.

It is these periods of congestion that are the target of QoS's traffic prioritization mechanisms. There are a number of key parameters that define QoS in a network, including (Table 11.)

Table 11 QoS network parameters

Parameter	Description
Latency (propagation delay)	The time between transmission and receipt of the message
Jitter	The variance of delay when packets do not arrive at the destination address in consecutive order or on a timely basis and the signal varies from its original reference timing. This distortion is particularly damaging to multimedia traffic. For example, the playback of audio or video data may have a jittery or shaky quality.
Bandwidth	The amount of data that can be delivered per second, usually expressed in kilobits per second (Kbps) or megabits per second (Mbps).
Packet loss	A percentage of packets that could be dropped over a specified interval. Packet loss must be kept at a minimum to deliver effective IP telephony and IP video services. With IP Telephony, the selection of a CODEC compression algorithm is important with respect to packet loss. For example, G.729 is more susceptible to the service impairment with packet loss than the G.711 algorithm.
Availability	High availability is fundamental to delivering effective QoS. IP networks must be engineered to be telephony-grade IP networks to make delay-sensitive or jitter-sensitive applications successful over IP.

This section includes the following topics:

- "QoS implementation," next
- "IP telephony traffic" on page 45
- "Signaling and media traffic parameters" on page 47

QoS implementation

The 8600 switch provides a hardware-based QoS platform through hardware packet classification. Packet classification is based on examining the various QoS fields within the Ethernet packet, primarily the DSCP and the 802.1p fields. Unlike legacy routers that require CPU processing cycles for packet classification, which has a negative impact on router performance speed, the hardware-based QoS performs packet classification in hardware at switching speeds.

IP telephony traffic

IP telephony traffic must be treated to ensure the quality of the communication. IP filters identify the IP telephony traffic and either preserve or modify the DSCP to provide appropriate QoS. IP telephony devices and multimedia applications typically use a signaling protocol data stream and voice data stream. Each of these has to be identified and prioritized with better QoS to effectively improve communication quality and experience. The default IP telephony filters easily configure this prioritization, not only for IP telephony but also for some video conference applications and streaming multimedia applications.

Note: In the remainder of this document, *IP telephony* refers to both IP telephony and multimedia applications.

The IP telephony filter feature relieves you of having to know all the configuration details of every filter type used with each type of IP telephony device. You are presented with a list of supported IP telephony devices and the types of signaling protocols supported by that particular device.

When you set the IP Telephony and multimedia filters, information representing these filters is propagated from the IP routing > Filter dialog box to the following tabs:

Note: When using the JDM for configuration, the status of Diffserv on a port is modified automatically when you assign or remove an IP telephony media filter. However, when using the CLI, the status of DiffServ on a port is not automatically enabled when you apply an IP telephony media filter to the port.

- Filter
- Control
- DiffServs
- Source/Destination Sets

Most of the options are set to defaults. If you need to configure any options that might affect the identification of the telephony traffic, then you must tune the 8600 IP telephony filters accordingly. Any improper configuration could impact the network. This impact can range from adverse affects to network stability and quality to giving unpredictable and undesired treatment to some flows. In addition, some flows can be affected by these filters if the definition is not correct.

You can use IP telephony filters on the following platforms:

- None (default)
- CSE 1000
- CSE 2000
- CSE 3000
- BCM
- MERIDIAN LINE CARD
- MERIDIAN TRUNK CARD
- MSL100IP
- VCON
- Minerva
- Custom (user-defined)

Note: Flows can be affected by these filters that are incorrectly defined.

For each of these platforms, there are the following preconfigured devices

- None (default)
- I2002
- I2004
- I2050
- Terminal Proxy Server (TPS)

- Voice Gateway
- Custom (user-defined)

Signaling and media traffic parameters

Table 12 provides UDP/TCP port parameters.

Table 12 UDP/TCP port parameters for signaling and media traffic

Platform Devices			Streams			
Port	**Platform**	**Device**	**Proto**	**Port-range**	**Option**	**Type**
01	CSE1000		udp	5000-5000	src	signal
02	BCM		udp	5000-5000	src	signal
				51000-52000	src-dst	media
03	BCM		udp	7000-7000	dst	signal
04	BCM	VoiceGateway	udp	28000-28255	src-dst	media
			tcp	1720-1720	dst	signal
			tcp	1719-1719	src-dst	signal
05	MeridianTrunk	VoiceGateway	tcp	1720-1720	dst	signal
			udp	1719-1719	src-dst	signal
			udp	1720-1720	src-dst	signal
			udp	2300-2363	src-dst	media
06	CSE2000[1]	I2004	udp	5000-5000	src	signal
			udp	6000-6011	src-dst	media
07	CSE2000	TPS	udp	5000-5000	dst	signal
			udp	6066-6066	src-dst	signal
08	CSE2000	VoiceGateway	udp	5000-5000	src-dst	signal
			tcp	1718-1720	src-dst	signal
			udp	2326-2445	src-dst	media
09	VCon	Custom	udp	5004-6004	src-dst	media
			udp	36100-36100	src-dst	media
			udp	36101-36101	src-dst	media
10	Minerva	Custom	udp	2001-2001	src-dst	media

1 CSE2000 and MSL100IP are same. CSE3000 is not supported (project is changed to CSEMX).

Chapter 2
Configuration examples

This chapter provides important information about traffic filtering, as implemented by the Passport 8600 switch. Also included in this chapter are examples of common QoS and IP filtering configuration tasks, including the CLI commands you use to create the example configuration.

Note: For a complete description of CLI commands you can use to configure specific QoS tasks, including those shown in this chapter, see the appropriate CLI chapter in this guide (refer to "Contents," on page 5).

This chapter includes the following topics:

Configuring filters on the Passport 8600 switch

You can use IP filtering to manage traffic and to provide security. Each filter set defines the conditions that must match for inclusion in the filter set and also defines the actions that be performed when a match is made.

This section includes the following topics:

Supported filter types

The Passport 8600 switch supports two different kinds of filters:

Global filters

Global filters can specify a source IP address and mask, a destination IP address and mask, both source and destination IP address and mask, or none.

You can configure a global filter for routed traffic if the filter is only used for non-DiffServ operations, such as "filter on protocol type." For IP bridged traffic only, any of the following DiffServ operations are functional:

• Modify DS byte

• Modify P-bits

Note: The above functions are not supported for IP routed traffic.

Global filters are fully operational for bridged traffic providing the bridged traffic is IP traffic.

The following applies to global filters:

- No minimum or maximum mask length exists.
- Up to eight global filters can be applied on any given set of Address Resolution Unit (ARU) ports.

  A set includes eight 10/100 ports (8648TXE, 8624FXE) or one Gigabit port (8608SXE, 8608GBE).
- Global filters must only be used for bridged IP traffic
- Global filters can not be used for matches that are based on the DSCP field.

Source/destination filters

Source filters must specify a source IP address and a mask, and they may optionally specify a destination IP address and mask.

Destination filters must specify a destination IP address and mask, and they may optionally specify a source IP address and mask.

Filtering criteria

You can define various filtering criteria when creating a filter for the Passport 8600 switch. This section describes the criteria that you should consider when creating the filter and includes the following topics:

- "Modification criteria," next
- "Action criteria" on page 52
- "Matching criteria" on page 53

Modification criteria

You can configure filters to modify the following fields:

- 802.1p (VLAN priority)
- DSCP (IP priority)

Refer to “Global filters” on page 50, for any limitations.

Action criteria

Filtering actions include:

- Drop
- Forward
- Forward to next hop
- Mirror — copies the traffic to another port
- Police — enforces a Service Level Agreement, at ingress
- TCP connect — allows incoming TCP sessions even though the filter action on this port is DROP.
- Stop-on-match — stops the filtering process if the condition matches
- Modify the DS field — changes the QoS of the traffic (remarking) at the layer 3 (IP), using the DiffServ field.
- Modify the IEEE 802.1p bit — changes the QoS of the traffic (remarking) at the layer 2 (Ethernet).

IP filters apply to all routed IP packets that are forwarded by the switch on specified ingress ports.

The final filtering decision is a logical OR between the result of the Global, Destination and Source filters:

- When the port’s default action is drop, if a single match occurs with an action of forward, the frame is forwarded.
- When the port’s default action is forward, if a single match occurs with an action of drop, the frame is dropped.

Table 13 defines packet actions for all occurrences of port and filter modes.

Table 13 Port modes and filter actions

Port mode	Filter mode	Packet action
Forward	Default	Forward all packets that match the filter
Drop	Default	Drop all packets
Forward	Forward	Forward all packets that match the filter

Table 13 Port modes and filter actions

Port mode	Filter mode	Packet action
Drop	Forward	Drop all packets except that match the filter
Forward	Drop	Drop all packets that match the filter
Drop	Drop	Drop all packets

Matching criteria

Filtering can be applied to the following matching criteria:

- Destination address or address range
- Source address or address range
- Exact IP protocol match (TCP, UDP or ICMP)
- TCP or UDP port numbers
- TCP connections established from within the network only or bidirectional establishment allowed
- IP frame fragment
- DiffServ field (only for source/destination filters)
- ICMP request

Filters are applied to a port using filter sets, and actions are assigned when applying a filter set to a port. The actions of individual filters can overwrite the default actions of the port.

Configuring filters

This section describes how to configure filters on the Passport 8600 switch and includes the following topics:

- "Filtering tasks," next
- "Global filter commands" on page 55
- "Source and destination filter commands" on page 57

Filtering tasks

Three tasks are required when you create filters on the Passport 8600 switch:

1. Create the filter template, and define the following:
   - **a** The type of filter — global or source/destination.
   - **b** The criteria used to match the traffic.
   - **c** The action performed if the traffic matches the condition.
2. Define a filter set:

   The filter list is always defined after you define the template. A list comprising a template and filter type is called a *set*. Two types of sets can be defined: global sets (including global filters) and source/destination sets (including source/destination filters). A template (filter) can be added to several sets.

3. Apply a filter set to a port (or ports):

   You can apply a single filter set to multiple ports; you do not have to recreate the same set.

   To apply a set, you must specify that the filtering action will be applied on a port (you cannot to assign a filter to a VLAN or to multiple ports in one action). After you specify the filtering action, you can assign one or multiple sets to that port.

Note: For bridged traffic with IP flows, only Global filters can be used. Source/destination filters are not supported for bridged traffic, and can only be used for routed IP traffic.

Note: To create a filter template with a match on a DSCP value, you must either use a Source or a Destination filter. You cannot use a Global template to match on a DSCP value. However, you can still modify either an 802.1p or a DSCP value with either a Global filter or a Source/ Destination Filter.

Global filter commands

For global filters, assign the *fid* (*fid* = filter id) field a value in the range 1 and 100.

The source IP address and the destination IP address are optional and are dependent on the filter type that is applied. If no source IP address or destination IP address is specified, the filter is applied to all traffic going through this port.

After you define the filter parameters, you can define the filter's action. The filter's *action* specifies whether incoming traffic is dropped or forwarded.

You can define three filter actions:

- forward
- drop
- default.

Creating a global filter:

To create a global filter, complete the following steps:

1 Create a global traffic filter and then specify the filtering action:

a Create a global traffic filter:

The following command creates a global traffic filter, which has a gsetid value in the range 1 and 3071. The src-ip and dst-ip addresses are optional.

```
Passport-8610:5# config ip traffic-filter create
global src-ip <value> dst-ip <value> id <fid>
```

b Specify the filter action:

The following command specifies which action, match, or modification to apply (see "Configuring filters on the Passport 8600 switch" on page 50).

```
Passport-8610:5# config ip traffic-filter filter <fid>
[<action>, <match>, or <modify>]
```

2 Configure the filter set:

a Create a global filter set:

The following command creates a global filter set with a global list id in the range 1 and 100. **Note:** You can assign a name to a list, but when you apply the list to a port you must use the global set id.

```
Passport-8610:5# config ip traffic-filter global-set
<gsetid> create name "<global filter name>"
```

b Add the traffic filter to the filter set:

The following command adds the filters created in Step 1 to the global filter set.

```
Passport-8610:5# config ip traffic-filter global-set <
gsetid> add-filter <fid>
```

3 Apply Filter Set and Enable DiffServ on a port basis:

The following steps show how to enable DiffServ access, as opposed to DiffServ core, to the access port(s) where you want to apply the newly created Global filter set. To do this, you first enable DiffServ at a physical port level, then you add the Global Filter Set (that you previously created in set 2) to these ports.

a Enable DiffServ access ports:

The following commands enable DiffServ access on the desired port(s) assuming the port type is Ethernet.

```
Passport-8610:5# config ethernet <slot/port>
enable-diffserv true
Passport-8610:5# config ethernet <slot/port>
access-diffserv true
```

b Add the global set to the physical port:

The following commands add the global set to the physical port level.

```
Passport-8610:5# config ethernet <slot/port> ip
traffic-filter create
Passport-8610:5# config ethernet <slot/port> ip
traffic-filter add set <gsetid>
```

c Enable the traffic filter:

The following commands enable the traffic filter and set the default action to forward.

```
Passport-8610:5# config ethernet <slot/port> ip
traffic-filter default-action [<forward>,<drop>,
<none>]
Passport-8610:5# config ethernet <slot/port> ip
traffic-filter enable
```

Source and destination filter commands

This section describes the commands you can use to create source/destination filters. For source/destination filters, assign the *fid* (*fid* = filter id) field a value in the range 1 and 4096.

Creating a source/destination filter:

To create a source/destination filter, complete the following steps:

1 Create a source traffic filter and then specify the filtering action:

a Create a source traffic filter:

The following command creates a source traffic filter, which has an id value in the range 1 and 3071.

```
Passport-8610:5# config ip traffic-filter create
source src-ip <value> dst-ip <value> id <fid>
```

b Create a destination traffic filter:

The following command creates a destination traffic filter, which has an id value in the range 1 and 3071.

```
Passport-8610:5# config ip traffic-filter create
destination src-ip <value> dst-ip <value> id <fid>
```

c Specify the filter action:

The following command specifies which action, match, or modification to apply (see "Configuring filters on the Passport 8600 switch" on page 50).

```
Passport-8610:5# config ip traffic-filter filter <fid>
[<action>, <match>, or <modify>]
```

2 Configure the filter set:

a Create a global filter set:

The following command creates a filter set where the list id has an id value in the range 300 and 1000. **Note:** You can assign a name to a list, but when you apply the list to a port you must use the filter set list id.

```
Passport-8610:5# config ip traffic-filter set <listid>
create name "<src/dst filter name>"
```

b Add the traffic filter to the filter set:

The following command adds the traffic filters created in Step 1 to the filter set.

```
Passport-8610:5# config ip traffic-filter set
<listid> add-filter <fid>
```

3 Apply Filter Set and Enable DiffServ on a Port basis:

The following steps show how to enable DiffServ access, as opposed to DiffServ core, to the access port(s) where you want to apply the newly created source/destination filter set. To do this, you first enable DiffServ at a physical port level, then you add the source/destination filter set (that you previously created in set 2) to these ports.

a Enable DiffServ access ports:

The following command enables DiffServ access on the desired port(s) assuming the port type is Ethernet.

```
Passport-8610:5# config ethernet <slot/port>
enable-diffserv true
Passport-8610:5# config ethernet <slot/port>
access-diffserv true
```

b Add the global set to the physical port:

The following commands add the source or destination filter set from Step 2, to the physical port level.

```
Passport-8610:5# config ethernet <slot/port> ip
traffic-filter create
Passport-8610:5# config ethernet <slot/port> ip
traffic-filter add set <listid>
```

c Enable the traffic filter:

The following commands enable the traffic filter and sets the default action to forward.

```
Passport-8610:5# config ethernet <slot/port> ip
traffic-filter default-action [<forward>,<drop>,
<none>]
Passport-8610:5# config ethernet <slot/port> ip
traffic-filter enable
```

Policing traffic

Policing is the process of assigning a traffic rate to a micro-flow or aggregate flow as it traverses the DiffServ network. The micro-flow or aggregate flow is evaluated against defined traffic profiles. When a traffic profile is in effect, it checks each packet for the average rate.

If the rate is within the value defined in the profile (that is, the packet is "in profile"), the packets are marked with the in-profile DSCP. If the rate exceeds the defined value, the packets are either marked with the out-of-profile DSCP or they are discarded, based on the action defined in the traffic profile.

The average rate policed on the Passport 8600 switch is in 1-megabit increments with 1 Mb/s as the minimum value. The Passport 8600 switch uses a token bucket scheme where the bucket is 2.5ms wide (400 buckets per second). When you set a rate limit, you determine how many bits the bucket can hold. If the ingress traffic is within the set rate limits, then the entire frame is accepted.

The traffic profile commands are as follows:

1. Create a traffic profile:

   The following command creates a traffic profile, which has an id value in the range 1 and 64.

   ```
   Passport-8610:5# config ip traffic-filter create
   traffic-profile <pid>
   ```

2. Add a profile name:

   The following command adds a name to the newly created traffic profile.

   ```
   Passport-8610:5# config ip traffic-filter
   traffic-profile <pid> name "<profile name>"
   ```

3. Enable or disable traffic discarding:

   The following command enables or disables discarding of traffic, if out of profile.

   ```
   Passport-8610:5# config ip traffic-filter traffic-profile
   <pid> discard-out-profile enable/disable
   ```

4. Configure DSCP for all in-profile traffic:

   The following command configures the DSCP value for all in-profile traffic.

   ```
   Passport-8610:5# config ip traffic-filter traffic-profile
   <pid> in-dscp <value>
   ```

5. Configure DSCP for all out-of-profile traffic:

   The following command configures the DSCP value for all out-of-profile traffic if enabled.

   ```
   Passport-8610:5# config ip traffic-filter traffic-profile
   <pid> out-dscp <value>
   ```

6. Enable DSCP translation:

   The following command configures the DSCP value for all out-of-profile traffic if enabled.

   ```
   Passport-8610:5# config ip traffic-filter traffic-profile
   <pid> translate-dscp enable
   ```

7 Configure the in-profile average rate:

The following command configures the in-profile average rate, where the value is an integer value in the range 1 and 65535. To calculate the average rate that you want to use, divide the average rate (in Mb/s) by 204800.

For example, if you want the average rate to be 10 Mb/s, then the value you enter is 49 (10 Mb/s, divided by 204800 = 49).

```
Passport-8610:5# config ip traffic-filter traffic-profile
1 average-rate <value>
```

8 Enable the traffic profile:

The following command enables the traffic profile.

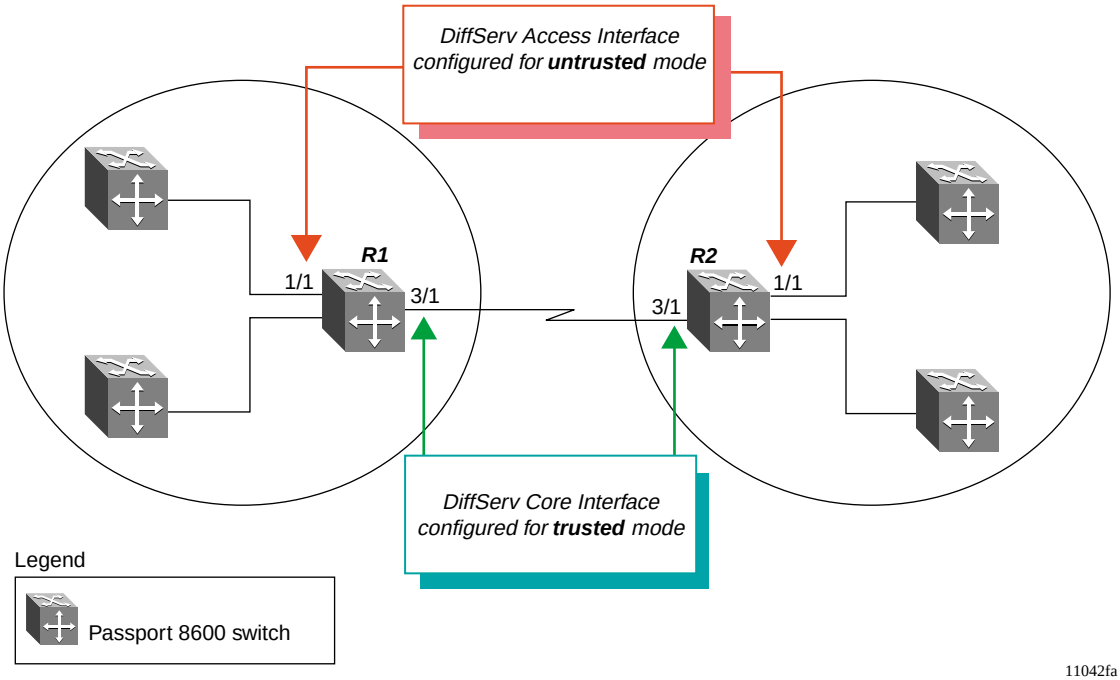
```
Passport-8610:5# config ip traffic-filter traffic-profile
<pid> enable true
```

Configuration example — DiffServ trusted or untrusted interfaces

You can configure the Passport 8600 switch, on a per port basis, as a DiffServ-enabled core port (*trusted interface*) or access port (*untrusted interface*). If you configure the Passport 8600 switch as a DiffServ core port, the switch does not remark the 802.1p or DiffServ Code Point marking, and the DSCP value is preserved. If the ingress and egress ports are tagged, the 802.1p bits are preserved. If the egress port only is tagged, 802.1p bits are defined according to internal QoS.

In the configuration example shown in Figure 3, the interface between Passport 8600 switches R1 and R2 is configured for DiffServ Core (*trusted mode*). The access ports for both switches are set for DiffServ Access (*untrusted mode*).

Figure 3 Classification by trusted interface



The following section provides a step-by-step procedure that shows how to configure R1, for the example configuration shown in Figure 3. The configuration steps for R2 are the same as for R1, and are not shown in this procedure.

Configuring R1

1 Enable DiffServ support for ports 1/1 and 3/1 on R1:

The following command enables DiffServ support for ports 1/1 and 3/1. You can also specify a range of ports by using a dash between the port range (for example, 1/1-1/5).

```
Passport-8610:5# config ethernet 1/1,3/1 enable-diffserv
true
```

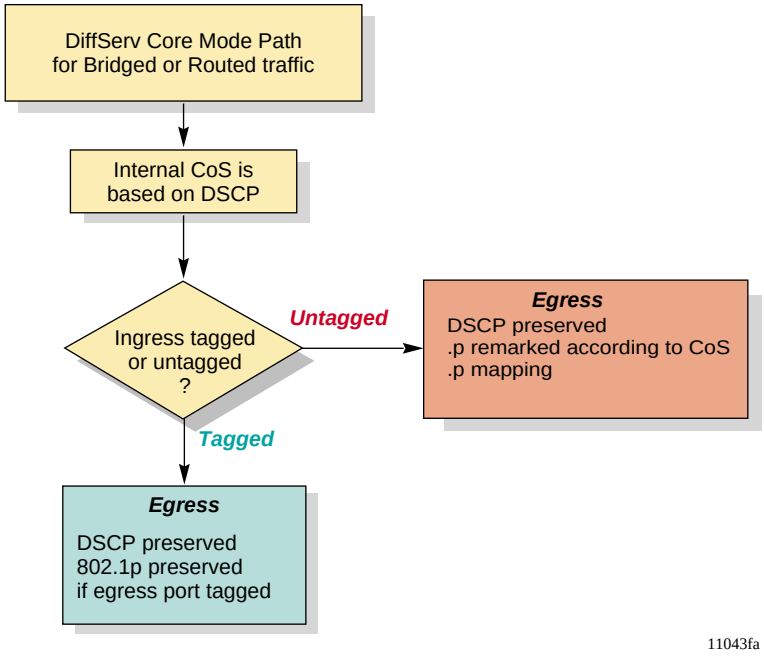
2 Enable DiffServ access support on a port:

Enables DiffServ access support on a port. For a DiffServ Core port, set the value to *false*.

```
Passport-8610:5# config ethernet 1/1 access-diffserv
true
```

Figure 4 shows a flowchart that describes default actions when the port is configured as a DiffServ Core Port.

Figure 4 DiffServ default action flowchart



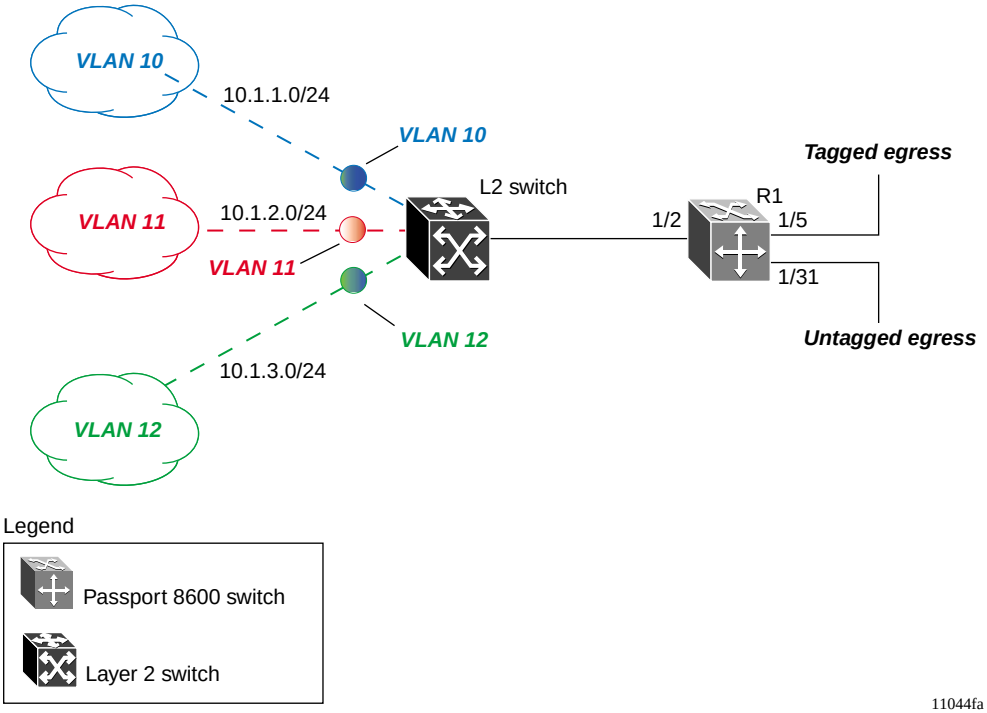
Configuration example — Classifying per-port traffic for port-based VLANs

The configuration example shown in Figure 5 shows how to configure Passport 8600 switch R1 to accomplish the following tasks:

R1 tasks:

- For a source IP address of 10.1.1.1, set DSCP = CS7 (111000).
- For all Hypertext Transfer Protocol (HTTP) flows (TCP port = 80), set DSCP = AF31 (011010).
- For all other traffic, set DSCP = AF11 (001010).
- Configure ingress port 1/2 for DiffServ Access (*untrusted mode*).
- Configure egress ports 1/5 and 1/31 for DiffServ Core (*trusted mode*).

Figure 5 Classifying per-port traffic



Expected Results on R1:

1. Regardless of ingress VLAN on port 1/2, R1 will remark the DiffServ DSCP in the following order:
   a. CS7 for traffic from host 10.1.1.1
   b. AF31 for traffic from any flow with TCP port number 80
   c. AF 11 for other flows
2. On tagged egress port 1/5, R1 will mark both the 802.1p and DSCP values.
3. On untagged egress port 1/31, R1 will mark the DSCP.

Configuration commands:

The following section provides a step-by-step procedure that shows how to configure R1 for the example configuration shown in Figure 5 on page 64.

Configure filter templates on R1

The following steps configure three filter templates for R1.

1. Configure the first filter template:
   a. Create a global filter with ID = 1.

      The following command creates a global filter with ID = 1. If the destination address is not specified, it automatically becomes 0.0.0.0/0.0.0.0.

      ```
      Passport-8610:5# config ip traffic-filter create
      global src-ip 10.1.1.1/32 id 1
      ```

   b. Set the DSCP value.

      The following commands set the DSCP value to 101110 and enable statistics upon receiving a src-ip address of 10.1.1.1/32. Note that when you set the DSCP value to 101110 (EF class-of-service), R1 automatically sets the 802.1p value to 6, for traffic service class of Premium. For tagged egress ports, R1 marks both the 802.1p and the DSCP values.

      ```
      Passport-8610:5# config ip traffic-filter filter 1
      action mode forward
      ```

```
Passport-8610:5# config ip traffic-filter filter 1
action statistic enable
Passport-8610:5# config ip traffic-filter filter 1
modify dscp 101110
Passport-8610:5# config ip traffic-filter filter 1
modify dscp-enable enable
Passport-8610:5# config ip traffic-filter filter 1
name "fil_1"
```

2 Configure the second filter template:

a Create a global filter with ID = 2.

The following command creates a global filter with ID = 2.

```
Passport-8610:5# config ip traffic-filter create
global id 2
```

b Set the DSCP value.

The following commands set the DSCP value to 011010 and enable statistics upon receiving traffic with TCP port = 80. Note that when you set the DSCP value to 011010 (AF31 class-of-service), R1 *automatically* sets the 802.1p value to 4 for traffic service class of Gold. For tagged egress ports, R1 marks both the 802.1p and the DSCP values.

```
Passport-8610:5# config ip traffic-filter filter 2
action mode forward
Passport-8610:5# config ip traffic-filter filter 2
action statistic enable
Passport-8610:5# config ip traffic-filter filter 2
match dst-port 80 dst-option equal
Passport-8610:5# config ip traffic-filter filter 2
match protocol tcp
Passport-8610:5# config ip traffic-filter filter 2
modify dscp 011010
Passport-8610:5# config ip traffic-filter filter 2
modify dscp-enable enable
Passport-8610:5# config ip traffic-filter filter 2
name "fil_2"
```

3 Configure the third filter template:

a Create a global filter with ID = 3.

The following command creates a global filter with ID = 3.

```
Passport-8610:5# config ip traffic-filter create
global id 3
```

b Set the DSCP value.

The following commands set the DSCP value to 001010 and enable statistics upon receiving any traffic outside of global filters 1 and 2. Note that when you set the DSCP value to 001010 (AF11 class-of-service), R1 *automatically* sets the 802.1p value to 2 for traffic service class of Bronze. For tagged egress ports, R1 marks both the 802.1p and the DSCP values.

```
Passport-8610:5# config ip traffic-filter filter 3
action mode forward
Passport-8610:5# config ip traffic-filter filter 3
action statistic enable
Passport-8610:5# config ip traffic-filter filter 3
modify dscp 001010
Passport-8610:5# config ip traffic-filter filter 3
modify dscp-enable enable
Passport-8610:5# config ip traffic-filter filter 3
name "fil_3"
```

Create the global filter list on R1

The following steps configure the global filter list for R1.

1 Create a global set with ID = 1:

The following commands create a global set with ID = 1.

```
Passport-8610:5# config ip traffic-filter global-set 1
create name "gset_1"
```

2 Add the three previously created filters to the global set 1:

The following commands add the previously created filters to the global set with ID = 1.

```
Passport-8610:5# config ip traffic-filter global-set 1
add-filter 1
Passport-8610:5# config ip traffic-filter global-set 1
add-filter 2
Passport-8610:5# config ip traffic-filter global-set 1
add-filter 3
```

Enable DiffServ access to ingress ports:

The following steps enable DiffServ access on the R1 ingress ports.

1 Enable DiffServ access on port 1/2:

The following commands enable DiffServ access on Ethernet port 1/2 and add the global filter set created previously.

```
Passport-8610:5# config ethernet 1/2 enable-diffserv
true
Passport-8610:5# config ethernet 1/2 access-diffserv
true
Passport-8610:5# config ethernet 1/2 ip traffic-filter
create
Passport-8610:5# config ethernet 1/2 ip traffic-filter
add set 1
Passport-8610:5# config ethernet 1/2 ip traffic-filter
default-action forward
Passport-8610:5# config ethernet 1/2 ip traffic-filter
enable
```

2 Enable DiffServ core on ports 1/5 and 1/31:

The following commands enable DiffServ core on ports 1/5 and 1/31.

```
Passport-8610:5# config ethernet 1/5 enable-diffserv
true
Passport-8610:5# config ethernet 1/31 enable-diffserv
true
```

Showing traffic filter statistics:

Because the previous commands included enabling of statistics for each traffic filter, you can use the following show command to display statistics:

```
Passport-8610:5# show ip traffic-filter stats
```

Figure 6 shows sample output for the `show ip traffic-filter stats` command.

Figure 6 show ip traffic-filter stats

```
Passport-8610:5# show ip traffic-filter stats

================================================================================
                          Ip Traffic-filter Stats
================================================================================
                                                      TRAFFIC PROFILE
  FILTER ID     FILTER-PKTS      FILTER-OCTETS      DISCARD PKTS
--------------------------------------------------------------------------------
  2             22839306         1644430032         0
  3             27224892         1960192224         0
  1             18727778         1348400016         0
```

Configuration example — Classifying and policing traffic

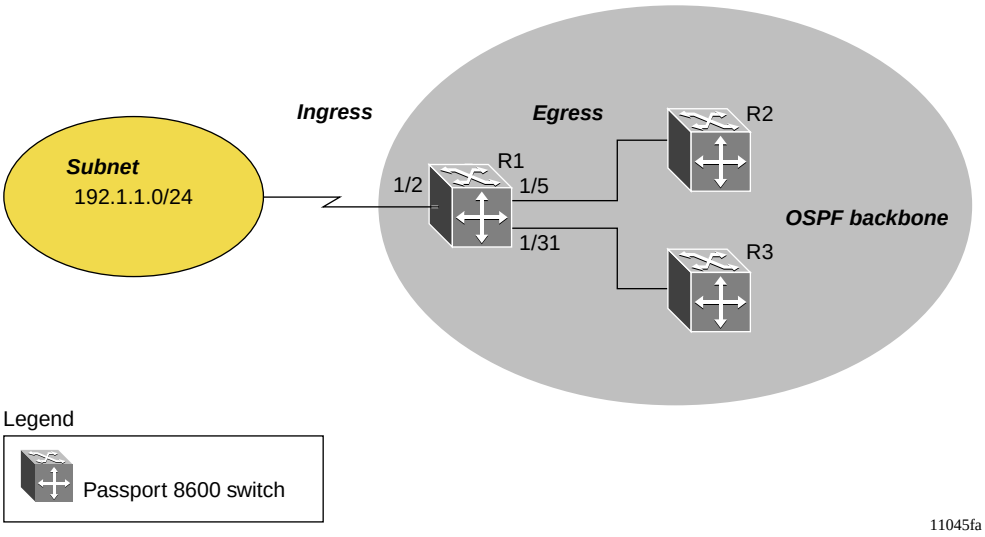
The configuration example shown in Figure 7 shows how to configure Passport 8600 switch R1 to accomplish the following tasks:

R1 tasks:

For IP source subnet 192.1.1.0/24:

- Police all traffic with TCP port number from 19 to 80 at 10 Mb/s in profile with a Gold Traffic Service Class — DSCP AF31 (011010).
- Police all other traffic at 1 Mb/s with a Bronze Traffic Service Class — DSCP value AF11 (001010). Discard all traffic that exceeds an average 1 Mb/s rate.

Figure 7 Classifying and policing traffic example



The following section provides a step-by-step procedure that shows how to configure R1 for the example configuration shown in Figure 7.

Configure traffic profiles on R1

The following steps configure two traffic profiles for R1.

1 Configure the first traffic profile:

a Create traffic profile 1:

The following command creates a traffic profile with ID = 1.

```
Passport-8610:5# config ip traffic-filter create
traffic-profile 1
```

b Set the in-profile DSCP value for AF31:

The following commands create traffic profile 1 and set the in-profile DSCP for AF31. The average rate is configured for 5 Mb/s (25 x 204800 = approximately 5 Mb/s).

```
Passport-8610:5# config ip traffic-filter
traffic-profile 1 name "Profile 1"
Passport-8610:5# config ip traffic-filter
traffic-profile 1 translate-dscp enable
Passport-8610:5# config ip traffic-filter
traffic-profile 1 in-dscp 011010
Passport-8610:5# config ip traffic-filter
traffic-profile 1 average-rate 24
Passport-8610:5# config ip traffic-filter
traffic-profile 1 discard-out-profile enable
Passport-8610:5# config ip traffic-filter
traffic-profile 1 enable true
```

2 Configure the second traffic profile:

a Create traffic profile 2:

The following command creates a traffic profile with ID = 2.

```
Passport-8610:5# config ip traffic-filter create
traffic-profile 2
```

b Set the in-profile DSCP value for AF11:

The following commands create traffic profile 2 and set the in-profile DSCP for AF11. The average rate is configured for 1Mb/s (5 x 204800 = approximately. 1 Mb/s).

```
Passport-8610:5# config ip traffic-filter
traffic-profile 2 name "Profile 2"
Passport-8610:5# config ip traffic-filter
traffic-profile 2 translate-dscp enable
Passport-8610:5# config ip traffic-filter
traffic-profile 2 in-dscp 001010
Passport-8610:5# config ip traffic-filter
traffic-profile 2 average-rate 5
Passport-8610:5# config ip traffic-filter
traffic-profile 2 discard-out-profile enable
Passport-8610:5# config ip traffic-filter
traffic-profile 2 enable true
```

Configure filter templates on R1

The following steps configure three filter templates for R1.

1 Configure the first filter template:

a Create a source filter with ID = 1.

The following command creates a source filter with ID = 1.

```
Passport-8610:5# config ip traffic-filter create
source src-ip 192.1.1.0/255.255.255.0 dst-ip 0.0.0.0/
0.0.0.0 id 1
```

b Setup the source filter.

The following commands set the source filter to look for TCP port < 19 and apply the Traffic Policy “traffic-profile 2” configured previously.

```
Passport-8610:5# config ip traffic-filter filter 1
action mode forward
Passport-8610:5# config ip traffic-filter filter 1
action statistic enable
Passport-8610:5# config ip traffic-filter filter 1
action traffic-profile 2
```

```
Passport-8610:5# config ip traffic-filter filter 1
match dst-port 19 dst-option less
Passport-8610:5# config ip traffic-filter filter 1
match protocol tcp
Passport-8610:5# config ip traffic-filter filter 1
name "fil_1"
```

2 Configure the second filter template:

a Create a source filter with ID = 2.

The following command creates a source filter with ID = 2.

```
Passport-8610:5# config ip traffic-filter create
source src-ip 192.1.1.0/255.255.255.0 dst-ip 0.0.0.0/
0.0.0.0 id 2
```

b Set up the source filter.

The following commands set the source filter to look for TCP port < 81 and apply the police rate (5 Mb/s) configured previously.

```
Passport-8610:5# config ip traffic-filter filter 2
action mode forward
Passport-8610:5# config ip traffic-filter filter 2
action statistic enable
Passport-8610:5# config ip traffic-filter filter 2
action traffic-profile 1
Passport-8610:5# config ip traffic-filter filter 2
match dst-port 81 dst-option less
Passport-8610:5# config ip traffic-filter filter 2
match protocol tcp
Passport-8610:5# config ip traffic-filter filter 2
name "fil_2"
```

3 Configure the third filter template:

a Create a source filter with ID = 3.

The following command creates a source filter with ID = 3.

```
Passport-8610:5# config ip traffic-filter create
source src-ip 192.1.1.0/255.255.255.0 dst-ip 0.0.0.0/
0.0.0.0 id 3
```

b Setup the source filter.

The following commands set the source filter to apply the police rate (1 Mb/s) by using the traffic policy configured previously.

```
Passport-8610:5# config ip traffic-filter filter 3
action mode forward
Passport-8610:5# config ip traffic-filter filter 3
action statistic enable
Passport-8610:5# config ip traffic-filter filter 3
action traffic-profile 2
Passport-8610:5# config ip traffic-filter filter 3
name "fil_3"
```

Create the source filter list on R1

The following steps configure the source filter list for R1.

1 Create a source set with ID = 300:

The following commands create a source set with ID = 300.

```
Passport-8610:5# config ip traffic-filter set 300 create
name "Fil_set_1"
```

2 Add the three previously created filters to the source set 300:

The following commands add the previously created filters to the source set with ID = 300.

```
Passport-8610:5# config ip traffic-filter set 300
add-filter 1
Passport-8610:5# config ip traffic-filter set 300
add-filter 2
Passport-8610:5# config ip traffic-filter set 300
add-filter 3
```

Enable DiffServ access to ingress ports:

The following step enables DiffServ access on the R1 ingress port 1/2.

➡ Enable DiffServ access on ingress port 1/2:

The following commands enable DiffServ access on Ethernet port 1/2 and add the source filter set created previously.

```
Passport-8610:5# config ethernet 1/2 enable-diffserv
true
Passport-8610:5# config ethernet 1/2 access-diffserv
true
Passport-8610:5# config ethernet 1/2 ip traffic-filter
create
Passport-8610:5# config ethernet 1/2 ip traffic-filter
add set 300
Passport-8610:5# config ethernet 1/2 ip traffic-filter
default-action forward
Passport-8610:5# config ethernet 1/2 ip traffic-filter
enable
```

Configuration example — Marking and dropping traffic, based on port-range

The configuration example shown in Figure 8, shows how to configure Passport 8600 switch R1 to accomplish the following tasks:

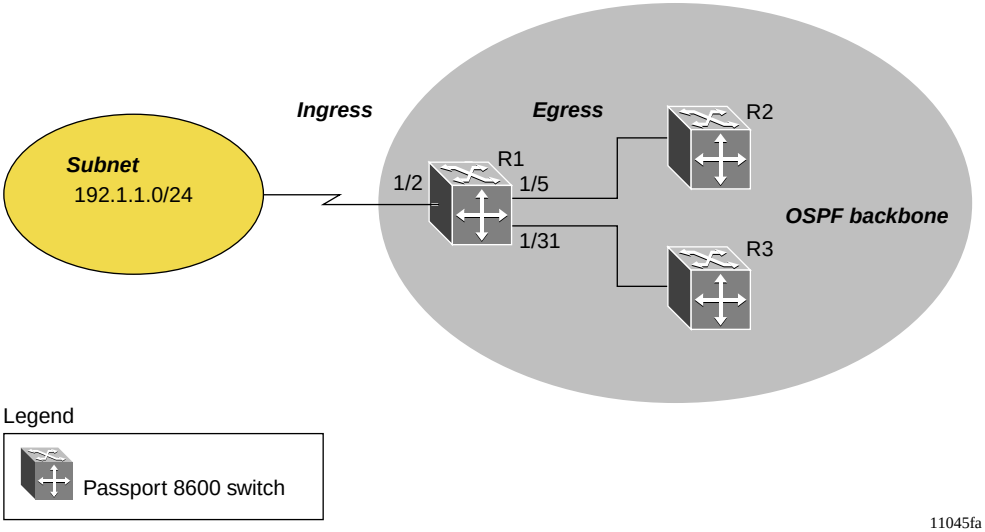
R1 tasks:

For this example, R1 is configured to:

- Filter on a range of TCP port numbers.

  For this example, the objective is to drop all packets for TCP ports in the range 20 and 30, and for TCP ports in the range 80 and 120.
- Mark all TCP traffic in-profile (10 Mb/s or less) with Gold Traffic Service Class — DSCP AF31 (011010), and out-of-profile with Bronze Traffic Service Class — DSCP value of AF11 (001010).
- Discard all other traffic.

Figure 8 Marking and dropping port-range traffic example



The following section provides a step-by-step procedure that shows how to configure R1 for the example configuration shown in Figure 8.

Configure traffic profiles on R1

The following steps configure two traffic profiles for R1.

1 Configure the traffic profile:

a Create traffic profile 1:

The following command creates a traffic profile with ID = 1.

```
Passport-8610:5# config ip traffic-filter create
traffic-profile 1
```

b Set the in-profile DSCP value for AF31:

The following commands create traffic profile 1 and set the in-profile DSCP for AF31 and out-of-profile to AF11. The average in-profile rate is configured for 10 Mb/s (49 x 204800 = approximately 10 Mb/s). Notice that discard-out-profile is not enabled because the objective is to only re-mark the traffic when the average rate is exceeded.

```
Passport-8610:5# config ip traffic-filter
traffic-profile 1 name "profile_1"
Passport-8610:5# config ip traffic-filter
traffic-profile 1 translate-dscp enable
Passport-8610:5# config ip traffic-filter
traffic-profile 1 in-dscp 011010
Passport-8610:5# config ip traffic-filter
traffic-profile 1 out-dscp 001010
Passport-8610:5# config ip traffic-filter
traffic-profile 1 average-rate 49
Passport-8610:5# config ip traffic-filter
traffic-profile 1 enable true
```

Configure filter templates on R1

The following steps configure six filter templates for R1.

1 Configure the first filter template:

a Create a source filter with ID = 1.

The following command creates a source filter with ID = 1.

```
Passport-8610:5# config ip traffic-filter create
source src-ip 0.0.0.0/0.0.0.0 dst-ip 0.0.0.0/
0.0.0.0 id 1
```

b Setup the source filter.

The following commands set the source filter to look for TCP port > 120, set the default action to forward, and apply the Traffic Policy "traffic-profile 1" configured previously.

```
Passport-8610:5# config ip traffic-filter filter 1
action mode forward
Passport-8610:5# config ip traffic-filter filter 1
action statistic enable
Passport-8610:5# config ip traffic-filter filter 1
action traffic-profile 1
Passport-8610:5# config ip traffic-filter filter 1
match src-port 120 src-option greater
Passport-8610:5# config ip traffic-filter filter 1
match protocol tcp
Passport-8610:5# config ip traffic-filter filter 1
name "src_1"
```

2 Configure the second filter template:

a Create a source filter with ID = 2.

The following command creates a source filter with ID = 2.

```
Passport-8610:5# config ip traffic-filter create
source src-ip 0.0.0.0/0.0.0.0 dst-ip 0.0.0.0/
0.0.0.0 id 2
```

b Setup the source filter.

The following commands set the source filter to look for TCP port > 80 and set the default action to drop.

```
Passport-8610:5# config ip traffic-filter filter 2
action mode drop
Passport-8610:5# config ip traffic-filter filter 2
action statistic enable
Passport-8610:5# config ip traffic-filter filter 2
match src-port 80 src-option greater
Passport-8610:5# config ip traffic-filter filter 2
match protocol tcp
Passport-8610:5# config ip traffic-filter filter 2
name "src_2"
```

3 Configure the third filter template:

a Create a source filter with ID = 3.

The following command creates a source filter with ID = 3.

```
Passport-8610:5# config ip traffic-filter create
source src-ip 0.0.0.0/0.0.0.0 dst-ip 0.0.0.0/
0.0.0.0 id 3
```

b Setup the source filter.

The following commands set the source filter to look for TCP port > 30, set the default action to forward, and apply the traffic profile configured previously.

```
Passport-8610:5# config ip traffic-filter filter 3
action mode forward
Passport-8610:5# config ip traffic-filter filter 3
action statistic enable
Passport-8610:5# config ip traffic-filter
filter 1 action traffic-profile 1
Passport-8610:5# config ip traffic-filter filter 3
match src-port 30 src-option greater
Passport-8610:5# config ip traffic-filter filter 3
match protocol tcp
Passport-8610:5# config ip traffic-filter filter 3
name "src_3"
```

4 Configure the fourth filter template:

a Create a source filter with ID = 4.

The following command creates a source filter with ID = 4.

```
Passport-8610:5# config ip traffic-filter create
source src-ip 0.0.0.0/0.0.0.0 dst-ip 0.0.0.0/
0.0.0.0 id 4
```

b Setup the source filter.

The following commands set the source filter to look for TCP port > 20, and set the default action to drop.

```
Passport-8610:5# config ip traffic-filter filter 4
action mode drop
Passport-8610:5# config ip traffic-filter filter 4
action statistic enable
Passport-8610:5# config ip traffic-filter filter 4
match src-port 20 src-option greater
Passport-8610:5# config ip traffic-filter filter 4
match protocol tcp
Passport-8610:5# config ip traffic-filter filter 4
name "src_4"
```

5 Configure the fifth filter template:

a Create a source filter with ID = 5.

The following command creates a source filter with ID = 5.

```
Passport-8610:5# config ip traffic-filter create
source src-ip 0.0.0.0/0.0.0.0 dst-ip 0.0.0.0/
0.0.0.0 id 5
```

b Setup the source filter.

The following commands set the source filter to look for TCP port > 0, set the default action to forward, and apply the traffic profile “profile_1” created previously.

```
Passport-8610:5# config ip traffic-filter filter 5
action mode forward
Passport-8610:5# config ip traffic-filter filter 5
action statistic enable
```

```
Passport-8610:5# config ip traffic-filter filter 5
action traffic-profile 1
Passport-8610:5# config ip traffic-filter filter 5
match src-port 0 src-option greater
Passport-8610:5# config ip traffic-filter filter 5
match protocol tcp
Passport-8610:5# config ip traffic-filter filter 5
name "src_5"
```

6 Configure the sixth filter template:

a Create a source filter with ID = 6.

The following command creates a source filter with ID = 6.

```
Passport-8610:5# config ip traffic-filter create
source src-ip 0.0.0.0/0.0.0.0 dst-ip 0.0.0.0/
0.0.0.0 id 6
```

b Setup the source filter.

The following commands set the source filter to drop all traffic.

```
Passport-8610:5# config ip traffic-filter filter 6
action mode drop
Passport-8610:5# config ip traffic-filter filter 6
action statistic enable
Passport-8610:5# config ip traffic-filter filter 6
name "src_6"
```

Create the source filter list on R1

The following steps configure the source filter list for R1.

1 Create a source set with ID = 300:

The following commands create a source set with ID = 300.

```
Passport-8610:5# config ip traffic-filter set 300 create
name "src_group1"
```

2 Add the six previously created filters to the source set 300:

The following commands add the six previously created filters to the source filter set with ID = 300.

```
Passport-8610:5# config ip traffic-filter set 300
add-filter 1
Passport-8610:5# config ip traffic-filter set 300
add-filter 2
Passport-8610:5# config ip traffic-filter set 300
add-filter 3
Passport-8610:5# config ip traffic-filter set 300
add-filter 4
Passport-8610:5# config ip traffic-filter set 300
add-filter 5
Passport-8610:5# config ip traffic-filter set 300
add-filter 6
```

Enable DiffServ access to ingress ports:

The following step enables DiffServ access on the R1 ingress port 1/2.

➡ Enable DiffServ access on ingress port 1/2:

The following commands enable DiffServ access on Ethernet port 1/2 and add the source filter set created previously.

```
Passport-8610:5# config ethernet 1/2 enable-diffserv
true
Passport-8610:5# config ethernet 1/2 access-diffserv
true
Passport-8610:5# config ethernet 1/2 ip traffic-filter
create
Passport-8610:5# config ethernet 1/2 ip traffic-filter
add set 300
Passport-8610:5# config ethernet 1/2 ip traffic-filter
default-action forward
Passport-8610:5# config ethernet 1/2 ip traffic-filter
enable
```

Configuration example — Forward-to-next-hop filtering

The configuration example shown in Figure 9 shows how to configure Passport 8600 switch R1 to accomplish the following tasks:

R1 tasks:

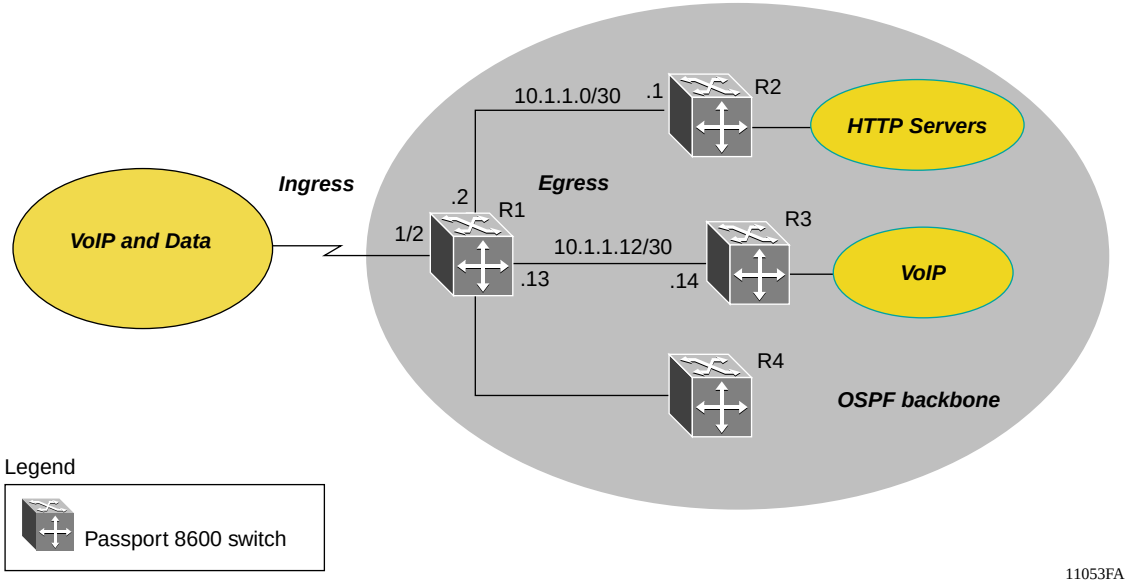
For this example, R1 is configured to:

- Forward all HTTP traffic directly to the WEB servers, using a forward-to-next hop of 10.1.1.1.

  Mark all HTTP traffic (TCP port = 80) with Bronze Traffic Service Class — DSCP value of AF11 (001010)
- Forward all VoIP traffic directly to the VoIP servers using a forward-to-next hop of 10.1.1.14.

  Mark all VoIP traffic (UDP port 2300-2363) with Premium Traffic Service Class — DSCP value of EF (101110)
- Mark all other traffic as Best Effort - DSCP DE (000000)

Figure 9 Forward-to-next hop filtering example



The following section provides a step-by-step procedure that shows how to configure R1 for the example configuration shown in Figure 9 on page 83.

Configure filter templates on R1

The following steps configure four filter templates for R1.

1 Configure the first filter template:

a Create a destination filter with ID = 1.

The following command creates a destination filter with ID = 1.

```
Passport-8610:5# config ip traffic-filter create
destination dst-ip 0.0.0.0/0.0.0.0 src-ip
0.0.0.0/0.0.0.0 id 1
```

b Setup the source filter.

The following commands set the source filter to look for TCP port = 80, set the default action to forward-to-next-hop 10.1.1.1, and set the DSCP value to AF11

```
      Passport-8610:5# config ip traffic-filter filter 1
action mode forward-to-next-hop
      Passport-8610:5# config ip traffic-filter filter 1
action statistic enable
      Passport-8610:5# config ip traffic-filter filter 1
action next-hop-forward ip-address 10.1.1.1
      Passport-8610:5# config ip traffic-filter filter 1
action next-hop-forward next-hop-unreachable-drop enable
      Passport-8610:5# config ip traffic-filter filter 1
match dst-port 80 dst-option equal
      Passport-8610:5# config ip traffic-filter filter 1
match protocol tcp
      Passport-8610:5# config ip traffic-filter filter 1
modify dscp 001010
      Passport-8610:5# config ip traffic-filter filter 1
modify dscp-enable enable
      Passport-8610:5# config ip traffic-filter filter 1
name "dst_1"
```

2 Configure the second filter template:

a Create a destination filter with ID = 2.

The following command creates a destination filter with ID = 2.

```
Passport-8610:5# config ip traffic-filter create
destination dst-ip 0.0.0.0/0.0.0.0 src-ip
0.0.0.0/0.0.0.0 id 2
```

b Setup the source filter.

The following commands set the source filter to look for UDP port < 2300, and set the DSCP value to DE.

```
Passport-8610:5# config ip traffic-filter filter 2
action mode forward
Passport-8610:5# config ip traffic-filter filter 2
action statistic enable
Passport-8610:5# config ip traffic-filter filter 2
match dst-port 2300 dst-option less
Passport-8610:5# config ip traffic-filter filter 2
match protocol udp
Passport-8610:5# config ip traffic-filter filter 2
modify dscp-enable enable
Passport-8610:5# config ip traffic-filter filter 2
name "dst_2"
```

3 Configure the third filter template:

a Create a destination filter with ID = 3.

The following command creates a destination filter with ID = 3.

```
Passport-8610:5# config ip traffic-filter create
destination dst-ip 0.0.0.0/0.0.0.0 src-ip
0.0.0.0/0.0.0.0 id 3
```

b Setup the source filter.

The following commands set up the source filter to look for UDP port < 2364, set the default action to forward-to-next-hop 10.1.1.13, and set the DSCP value to EF.

```
Passport-8610:5# config ip traffic-filter filter 3
action mode forward-to-next-hop
```

```
Passport-8610:5# config ip traffic-filter filter 3
action statistic enable
Passport-8610:5# config ip traffic-filter filter 3
action next-hop-forward ip-address 10.1.1.14
Passport-8610:5# config ip traffic-filter filter 3
match dst-port 2364 dst-option less
Passport-8610:5# config ip traffic-filter filter 3
match protocol udp
Passport-8610:5# config ip traffic-filter filter 3
modify dscp 101110
Passport-8610:5# config ip traffic-filter filter 3
modify dscp-enable enable
Passport-8610:5# config ip traffic-filter filter 3
name "dst_3"
```

4 Configure the fourth filter template:

a Create a destination filter with ID = 4.

The following command creates a destination filter with ID = 4.

```
Passport-8610:5# config ip traffic-filter create
destination dst-ip 0.0.0.0/0.0.0.0 src-ip
0.0.0.0/0.0.0.0 id 4
```

b Setup the source filter.

The following commands set the DSCP value to DE for all other traffic.

```
Passport-8610:5# config ip traffic-filter filter 4
action mode forward
Passport-8610:5# config ip traffic-filter filter 4
action statistic enable
Passport-8610:5# config ip traffic-filter filter 4
modify dscp-enable enable
Passport-8610:5# config ip traffic-filter filter 4
name "dst_4"
```

Create the destination filter list on R1

The following steps configure the destination filter list for R1.

1 Create a destination set with ID = 300:

The following command creates a destination set with ID = 300.

```
Passport-8610:5# config ip traffic-filter set 300 create
name "dst_set_1"
```

2 Add the four previously created filters to the source set 300:

The following commands add the four previously created filters to the source filter set with ID = 300.

```
Passport-8610:5# config ip traffic-filter set 300
add-filter 1
Passport-8610:5# config ip traffic-filter set 300
add-filter 2
Passport-8610:5# config ip traffic-filter set 300
add-filter 3
Passport-8610:5# config ip traffic-filter set 300
add-filter 4
```

Enable DiffServ access to ingress ports:

The following step enables DiffServ access on the R1 ingress port 1/2.

➡ Enable DiffServ access on ingress port 1/2:

The following commands enable DiffServ access on Ethernet port 1/2 and add the source filter set created previously.

```
Passport-8610:5# config ethernet 1/2 enable-diffserv
true
Passport-8610:5# config ethernet 1/2 access-diffserv
true
Passport-8610:5# config ethernet 1/2 ip traffic-filter
create
Passport-8610:5# config ethernet 1/2 ip traffic-filter
add set 300
Passport-8610:5# config ethernet 1/2 ip traffic-filter
default-action forward
Passport-8610:5# config ethernet 1/2 ip traffic-filter
enable
```

Chapter 3
Configuring QoS using Device Manager

This chapter describes Passport 8000 Series switch features you can use to allocate network resources to mission-critical applications in place of applications that are less sensitive to such factors as time delays or network congestion. You can configure your network to prioritize specific types of traffic, ensuring that they receive the appropriate Quality of Service (QoS) level.

On the Passport 8600 Switch traffic flows on the WAN are routed at the layer 3 level through a differentiated services (DiffServ) network architecture. Traffic filtering is a mechanism that helps you to manage traffic by defining filtering conditions and associating these conditions with specific actions.

IP filtering allows you to assign QoS levels, within a DiffServ network that are based on a range of filtering conditions.

Within the DiffServ network, the marked packets are placed in a queue according to their marking. For example, if a video stream is marked to receive the highest priority, it is placed in a high-priority queue. As those packets traverse the DiffServ network, the video stream is forwarded before any other packets.

Note: The Passport 8000 switch is shipped with QoS parameters already set to default values that will operate successfully in your network. You need only enable DiffServ access ports and core ports.

By assigning QoS levels to traffic flows on your LAN and WAN, you can ensure that network resources are allocated where they are needed most. To be effective, you must configure QoS functionality from end-to-end of the network: across different devices, such as routers, switches, and servers; across platforms and media; and across link layers, such as Ethernet, ATM, and frame relay.

This chapter describes how to use Device Manager to configure and manage the QoS feature on Passport 8000 switches.

- For conceptual information about QoS, see Chapter 1, “QoS and IP filtering concepts,” on page 21.
- For configuration examples, including the required CLI commands, see Chapter 2, “Configuration examples,” on page 49.

This chapter includes the following topics:

Enabling DiffServ

The Passport 8000 switch is designed to perform DiffServ functions properly as soon as you identify and enable DiffServ and identify the DiffServ access ports and core ports. All the mapping tables are set up with default values that ensure communication between the DiffServ domain and the rest of your network.

Unless you plan to modify filters, traffic profiles, or mapping tables, to implement QoS on an Passport 8000 switch, you need only enable the DiffServ command and select the DiffServ ports and their type, either access ports or core ports.

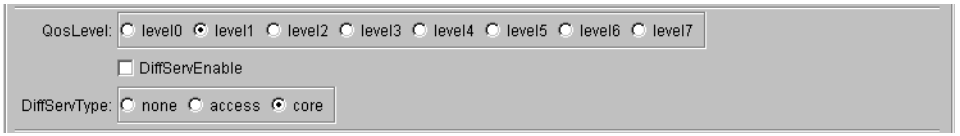
On a Passport 8000 switch, using a global filter to apply a QoS rate-limiting profile to a DiffServ access port results in a nondeterministic effective rate for that flow. For DiffServ access ports, use a source/destination filter to impose a specific rate limit for a flow ingressing those ports.

To enable DiffServ:

1. On the device view, select a port.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed. Figure 10 displays the QoS section of the Interface tab.

Figure 10 QoS section of the Interface tab



3. In the QoS section of the Interface, enable DiffServ by setting DiffServEnable to true (Figure 10).
4. Specify the port type by setting DiffServType to access or core.

Overview of QOS service classes and administrative weights

The Passport 8600 Switch supports eight output queues per port into which the packet can be placed. Each of the eight queues is mapped to one of the eight QoS levels, and queues are serviced using guaranteed Weighted Round Robin.

Administrative weights are assigned to each queue as a percentage of the total number of possible packet transmit opportunities. For example, an administrative weight of 100 indicates that this queue has 32 packet transmit opportunities. An administrative weight of 50 indicates that this queue has 50% of the possible 32 packet transmit opportunities, or 16.

Table 14 lists the eight traffic service classes corresponding to the QoS levels and their configurable administrative weight. The priority is assigned from the highest (7) to the lowest (0). For example, traffic assigned to QoS level 5 is a higher priority than traffic in QoS level 4. For an in-depth discussion on queue service and administrative weights, see *Networking Concepts for the Passport 8000 Series Switch*.

Table 14 Qos traffic service classes

Traffic service class	QoS level	PHB (best service offered)	Packet transmit opportunity (administrative weight)	Percentage weight
Network	7	Not configurable; reserved for network node initiated traffic	2	6%
Premium	6	Expedite forwarding	32	100%
Platinum	5	Assured forwarding	10	31%
Gold	4	Assured forwarding	8	25%
Silver	3	Assured forwarding	6	18%
Bronze	2	Assured forwarding	4	12%
Standard	1	Default	2	6%
User-defined	0		0	0%

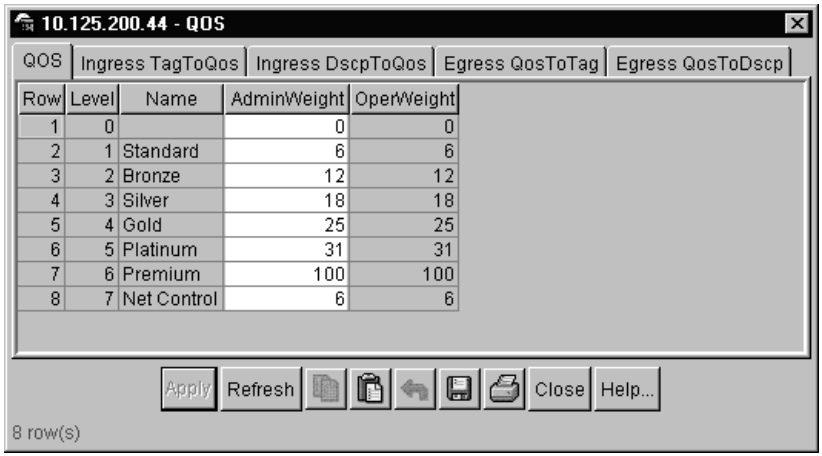
Editing a service class' administrative weight

To edit a service class' administrative weight:

1 From the Device Manager menu bar, choose QOS > QOS.

The QOS dialog box opens with the QOS tab displayed (Figure 11).

Figure 11 QOS dialog box—QOS tab



2 In the row of the service class to be edited, double click in the AdminWeight field and enter the new administrative weight.

3 Click Apply.

Table 15 describes the QOS tab fields.

Table 15 QOS tab fields

Field	Description
Row	Represents eight egress QoS levels.
Level	QoS level (0 to 7) associated with the traffic service class.
Name	Specifies the priority handling for traffic in this queue. Names are Network, Premium, Platinum, Gold, Silver, Bronze, and Standard.
AdminWeight	Administrative transmit opportunity, expressed as a percentage of the total number of packet transmit opportunities (32).
OperWeight	Operational transmit opportunity, expressed as a percentage of the total number of packet transmit opportunities (32).

Viewing and configuring ingress mapping tables

The Passport 8000 switch can specify certain quality of service treatment for ingress packets. The Passport 8000 switch provides tables for ingress packets that map the DSCP or the IEEE 802.1p bits to QoS levels, depending on if the IP traffic is bridged or routed and tagged or untagged.

Table 16 Default QoS parameters

Passport 8600		**DiffServ Code Point Allocation**				
802.1p	**Qos Level**	**IP Service Class**	**Traffic Class**			
			Dec	Hex	PHB	DSCP
	7	Critical	56	0x38	CS7	111 000’
	7	Network	48	0x30	CS6	110 000’
7	6	Premium	46	0x2E	EF	101 110’
			40	0x28	CS5	101 000’
6	5	Platinum	34	0x22	AF41	100 010’
			36	0x24	AF42	100 100’
			38	0x26	AF43	100 110’
			32	0x20	CS4	100 000’
5	4	Gold	26	0x1A	AF31	011 010’
			28	0x1C	AF32	011 100’
			30	0x1E	AF33	011 110’
			24	0x18	CS3	011 000’
4	3	Silver	18	0x12	AF21	010 010’
			20	0x14	AF22	010 100’
			22	0x16	AF23	010 110’
			16	0x10	CS2	010 000’
3	2	Bronze	10	0xA	AF11	001 010’
			12	0xC	AF12	001 100’

			14	0xE	AF13	001 110’
			8	0x8	CS1	001 000’
2, 1	0	Standard	0	0	CS0(DE)	000 000’
0 (Default)	1	Custom				

This section includes the following topics:

Viewing and configuring IEEE 802.1p bits and QoS levels

You can view and configure the mapping between the IEEE 802.1p bits and QoS levels. For bridged, tagged traffic, the switch determines the QoS level based on the IEEE 802.1p bits and the mapping of those bits to QoS levels via the Ingress TagToQos mapping table.

Note: Nortel Networks recommends not changing the default values. If you change the values, make sure that the values are consistent on all other Passport 8000 switches and other devices in your network. Inconsistent mapping of table values can result in unpredictable service levels.

To view and configure IEE 802.1p bit and QoS level mapping:

1. From the Device Manager menu bar, choose QOS > QOS.

   The QOS dialog box opens with the QOS tab displayed (Figure 11).

2. Click the Ingress TagToQos tab.

   The Ingress TagToQos tab opens (Figure 12).

Figure 12 QOS dialog box—Ingress TagToQos tab

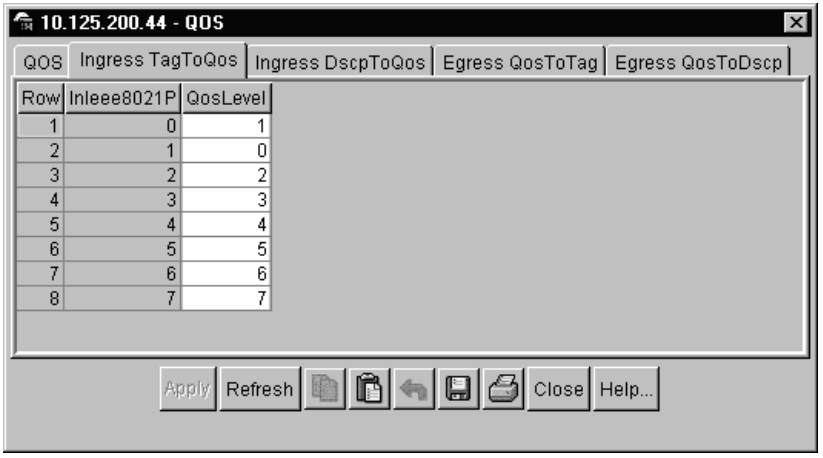


Table 17 describes the Ingress TagToQos tab fields.

Table 17 Ingress TagToQos tab fields

Field	Description
Row	Represents eight egress QoS levels.
InIeee8021P	Value of the IEEE802.1 p bit of the incoming packet.
QosLevel	Equivalent QoS egress (0 to 7).

Viewing and configuring DSCP and QoS level mapping

You can view and configure the mapping between the DSCP and QoS levels. For all routed IP packets, the port maps the DSCP to the QoS level according to the Ingress DscpToQos table. Note that changes to the mapping table do not take effect until you reboot the switch.

Note: Nortel Networks recommends not changing the default values. If you change the values, make sure that the values are consistent on all other Passport 8000 switches and other devices in your network. Inconsistent mapping of table values can result in unpredictable service levels.

To view and configure DSCP and QoS level ingress table mapping:

1 From the Device Manager menu bar, choose QOS > QOS.

The QOS dialog box opens with the QOS tab displayed (Figure 11).

2 Click the Ingress DSCPToQos tab.

The Ingress DSCPToQos tab opens (Figure 13).

Figure 13 QOS dialog box—Ingress DscpToQos tab

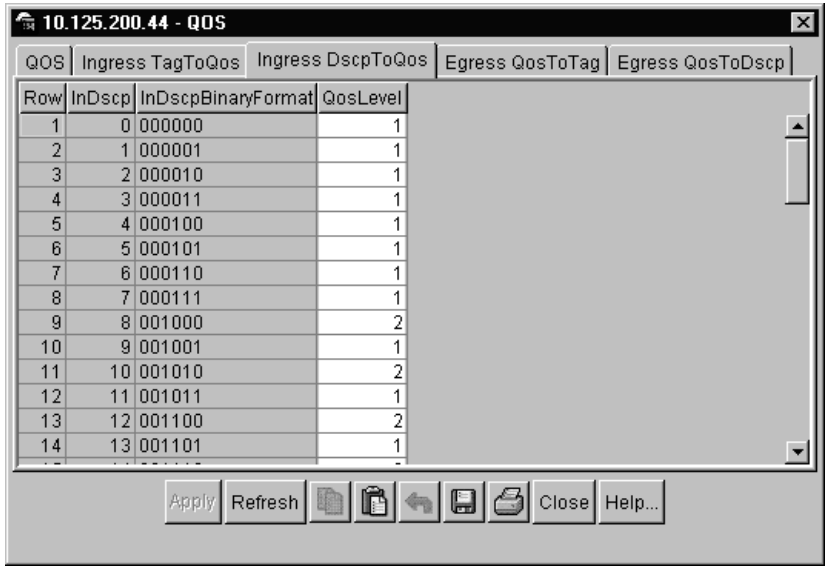


Table 18 describes the Ingress DscpToQos tab fields.

Table 18 Ingress DscpToQos tab fields

Field	Description
Row	This is used to uniquely identify a row in the table.
InDscp	Value of the DiffServ Code Point (in decimal format) in the IP header of the incoming packet.
InDscpBinaryFormat	Value of the DiffServ Code Point in binary format in the IP header of the incoming packet.
QosLevel	Equivalent Quality of Service level.

Viewing and configuring egress mapping tables

At the egress node, packets are examined to determine if their IEEE 802.1p bits or DSCP will be re-marked before leaving the DiffServ network. Upon examination, if the packet is egressing as a tagged packet, the IEEE 802.1p tag is set based on the QoS level-to-IEEE 802.1p bit mapping. In routed packets, the DSCP remains unchanged; in bridged packets, however, the DSCP is reset based on the QoS level.

This section includes the following topics:

Viewing and configuring QoS level and IEEE 802.1p bit mapping

You can view and configure the mapping between the QoS levels and the IEEE 802.1p bits. If the packets egress tagged, then the appropriate IEEE 802.1p bits are set according to the Egress QosToTag tab.

Note: Nortel Networks recommends not changing the default values. If you change the values, make sure that the values are consistent on all other Passport 8000 switches and other devices in your network. Inconsistent mapping of table values can result in unpredictable service levels.

To view and configure QoS level and IEEE 802.1p bit mapping:

1. From the Device Manager menu bar, choose QOS > QOS.

   The QOS dialog box opens with the QOS tab displayed (Figure 11).

2. Click the Egress QosToTag tab.

   The Egress QosToTab opens (Figure 14).

Figure 14 QOS dialog box—Egress QosToTag tab

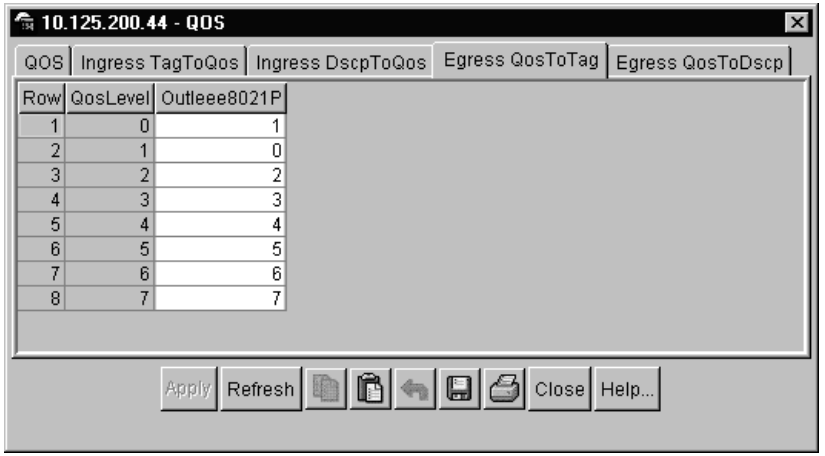


Table 19 describes the Egress QosToTag tab fields.

Table 19 Egress QosToTag tab fields

Field	Description
Row	This is used to uniquely identify a row in the table.
QosLevel	QoS level of the outgoing packet.
Outleee8021P	Equivalent value of the IEEE 802.1p bit.

Viewing and configuring QoS level and DSCP mapping

You can view and configure the mapping between the QoS levels and the DSCP. When no traffic filter is used, the DSCP of bridged IP traffic is reset according to the QoS level as the traffic egresses. Changes to the mapping table do not take effect until you reboot the switch.

Note: Nortel Networks recommends not changing the default values. If you change the values, make sure that the values are consistent on all other Passport 8000 switches and other devices in your network. Inconsistent mapping of table values can result in unpredictable service levels.

To view and configure QoS level and DSCP mapping:

1 From the Device Manager menu bar, choose QOS > QOS.

The QOS dialog box opens with the QOS tab displayed (Figure 11).

2 Click the Egress QosToDscp tab.

The Egress QosToDscp tab opens (Figure 15).

Figure 15 QOS dialog box—Egress QosToDscp tab

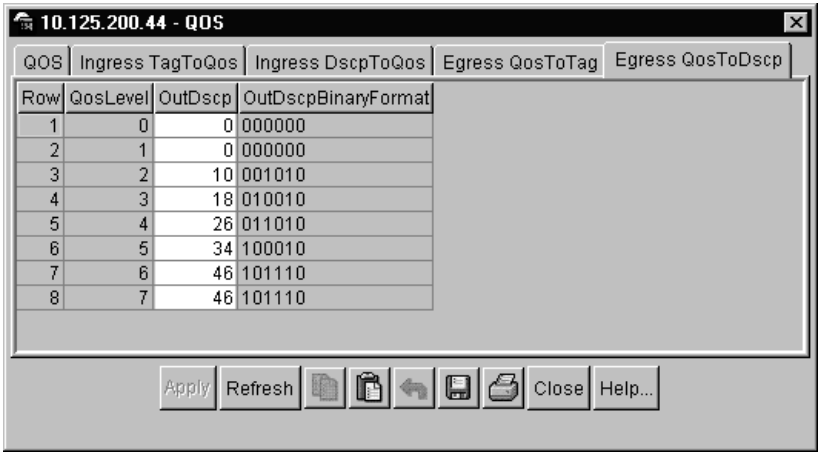


Table 20 describes the Egress QosToDscp tab fields.

Table 20 Egress QosToDscp tab fields

Field	Description
Row	This is used to uniquely identify a row in the table.
QosLevel	QoS level of the outgoing packet.
OutDscp	Equivalent value of the DiffServ codepoint (in decimal format).
OutDscpBinaryFormat	Equivalent value of DiffServ codepoint in binary format.

Assigning QoS levels to non-IP traffic

The Passport 8000 switch allows you to assign QoS levels to non-IP traffic.

This section includes the following topics:

Note: In cases where the VLAN, port, MAC address, and DiffServ access port have all set a QoS level, the highest level is honored.

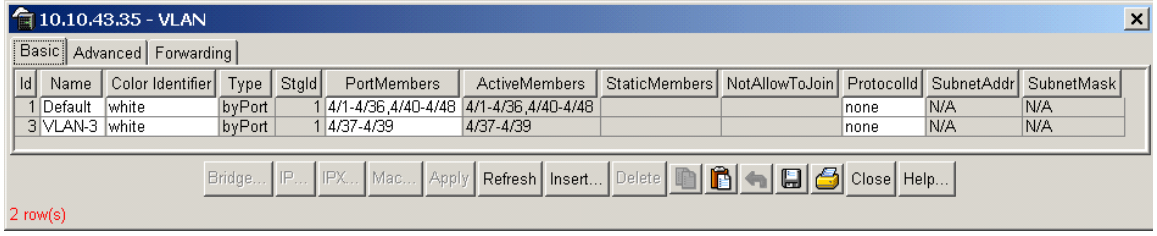
Managing QoS levels by VLAN membership

To view or assign QoS levels for VLANs:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens with the Basic tab displayed (Figure 16).

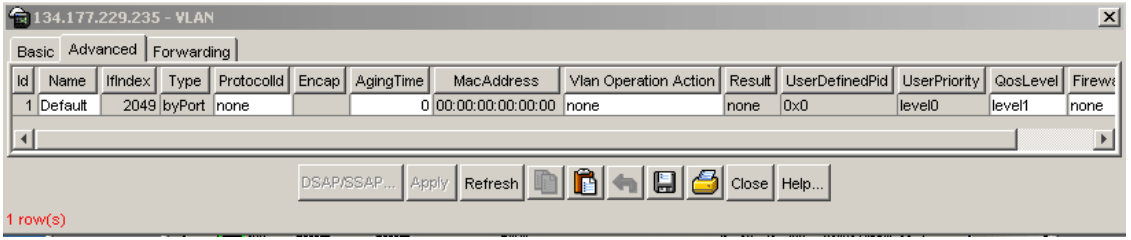
Figure 16 VLAN dialog box—Basic tab



2 In the VLAN dialog box—Basic tab, click the Advanced tab.

The VLAN dialog box—Advanced tab opens (Figure 17).

Figure 17 VLAN dialog box—Advanced tab



3 To change the assigned QoS level for all traffic from a specified VLAN, double click in the QoSLevel field, and select a new level from the list.

Table 21 describes the VLAN dialog box—Advanced tab fields.

Table 21 Advanced tab fields

Field	Description
Id	A value that uniquely identifies the Virtual LAN associated with this entry.
Name	An administratively assigned name for this VLAN.
IfIndex	The logical ifIndex assigned to this VLAN; select a value from 2049 to 4095.
Type	Type of VLAN: • byPort • byIpSubnet • byProtocolId (8600 modules and 8100 modules) • bySrcMac (8600 modules only) • bySvlan (8600 modules only) • byIds

Table 21 Advanced tab fields (continued)

Field	Description
ProtocolId	The protocol identifier for protocol-based VLANs. This value is taken from the Assigned Numbers RFC. • ip (IP version 4) • ipx802dot3 (Novell IPX on Ethernet 802.3 frames) • ipx802dot2 (Novell IPX on IEEE 802.2 frames) • ipxSnap (Novell IPX on Ethernet SNAP frames) • ipxEthernet2 (Novell IPX on Ethernet Type 2 frames) • appleTalk (AppleTalk on Ethernet Type 2 and Ethernet SNAP frames) • decLat (DEC LAT protocol) • decOther (Other DEC protocols) • sna802dot2 (IBM SNA on IEEE 802.2 frames) • snaEthernet2 (IBM SNA on Ethernet Type 2 frames) • netBIOS (NetBIOS protocol) • xns (Xerox XNS) • vines (Banyan VINES) • ipv6 (IP version 6) • usrDefined (user-defined protocol) • RARP (Reverse Address Resolution protocol) • PPPoE (Point-to-point protocol over Ethernet) **Note**: if the VLAN type is port-based, *None* is displayed in the Basic tab ProtocolId field.
Encap	The encapsulation method. Values are: • Ethernet II • SNAP • LLC • RAW
AgingTime	The timeout period (in seconds) for aging out dynamic member ports of policy-based VLANs.
MacAddress	MAC address assigned to the virtual router interface of this VLAN. This field is meaningful only if rcVlanRoutingEnable is equal to true(1).
Vlan Operation Action	VLAN-related actions.
Result	Result from the last VLAN action.
UserDefinedPid	When rcVlanProtocolId is set to usrDefined(15) in a protocol-based VLAN, this field represents the 16-bit user defined protocol identifier.
UserPriority	Priority level.

Table 21 Advanced tab fields (continued)

Field	Description
QosLevel	The assigned QoS level for all traffic from a VLAN.
FirewallVlanType	The Firewall VLAN type used for this VLAN. Values are • None • NAAP • Enforceable • Peering

Viewing and assigning QoS levels by port

To view or assign QoS levels by port:

From the Device Manager menu bar, choose Edit > Port.

The Port dialog box opens with the Interface tab displayed. Figure 18 illustrates the QoS area of the Interface tab.

Figure 18 QoS area of Interface tab

The QosLevel field shows the QoS level assigned to the specified port.

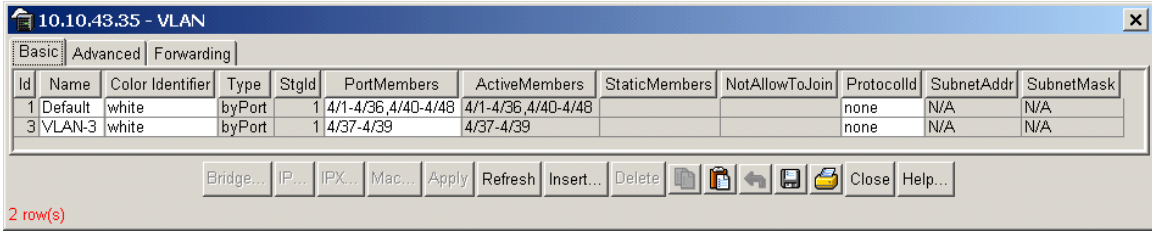
Viewing and assigning QoS levels by MAC address

To view or assign QoS levels by MAC address:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens with the Basic tab displayed (Figure 19).

Figure 19 VLAN dialog box—Basic tab



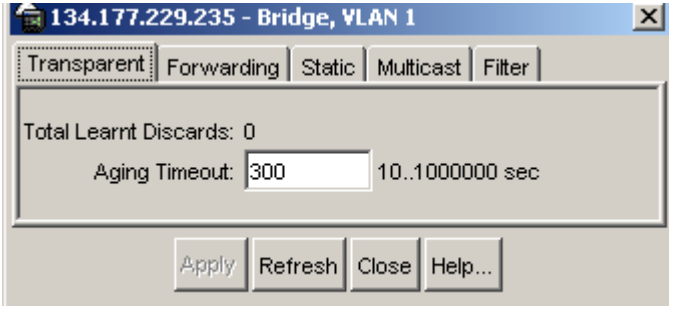
2 In the VLAN dialog box—Basic tab, select a VLAN.

The Bridge button is highlighted.

3 Click Bridge.

The Bridge, VLAN dialog box opens with the Transparent tab displayed (Figure 20).

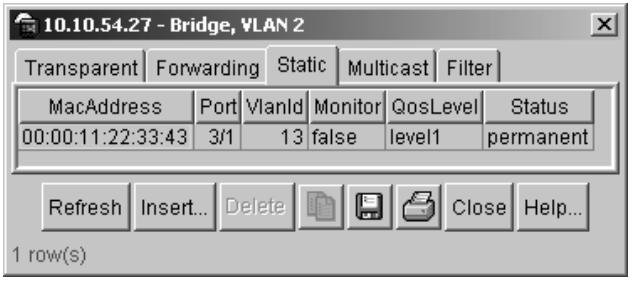
Figure 20 Bridge, VLAN dialog box—Transparent tab



4 Select the Static tab.

The Bridge, VLAN dialog box—Static tab opens (Figure 21).

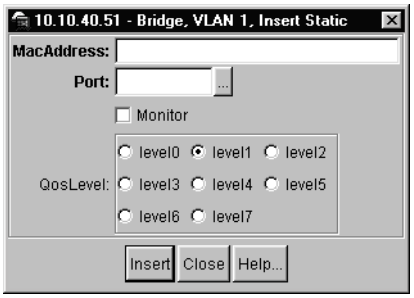
Figure 21 Bridge, VLAN dialog box—Static tab



5 In the Bridge, VLAN dialog box—Static tab, click Insert.

The Bridge, VLAN, Insert Static dialog box opens (Figure 22).

Figure 22 Bridge, VLAN Insert Static dialog box



6 In the MacAddress text box, type a MAC address.

7 In the Port text box, click the ellipsis button and select the port(s).

8 In the QosLevel area, select the QoS level.

9 Click Insert.

Creating and managing a traffic profile

Policing is the process of assigning a traffic rate to a microflow or aggregate flow as it traverses the DiffServ network. The microflow or aggregate flow is evaluated against defined traffic profiles. When a traffic profile is in effect, it checks each packet for the average rate. If the rate is within the value defined in the profile (that is, the packet is “in profile”), the packets are marked with the in-profile DSCP. If the rate exceeds the defined value, the packets either are marked with the out-of-profile DSCP or are discarded, based on the action defined in the traffic profile. The following section describe how to configure a traffic profile.

This section includes the following topics:

- “Creating a traffic profile,” next
- “Editing a traffic profile” on page 108

Creating a traffic profile

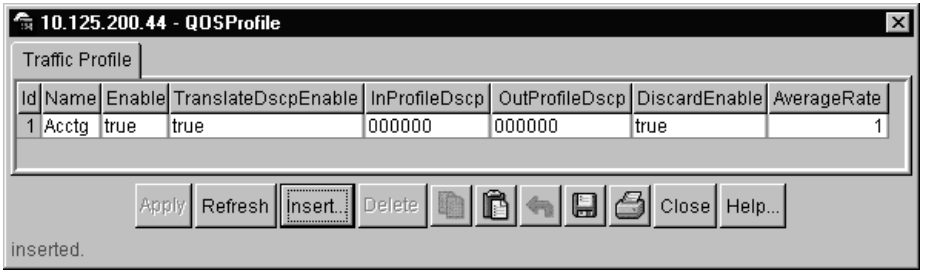
A traffic profile specifies the handling properties of a traffic flow selected by a classifier. It provides rules for determining whether a particular packet is in profile or out of profile; this determination results in the policing of IP packets within a traffic flow.

To create a traffic profile:

1 From the Device Manager menu bar, choose QOS > Profile.

The QOSProfile dialog box opens (Figure 23).

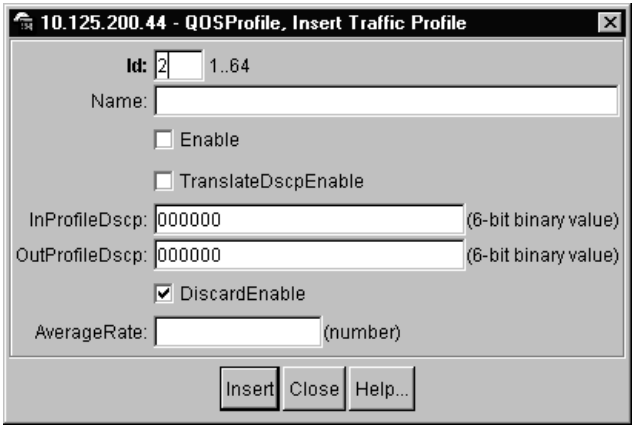
Figure 23 QOSProfile dialog box



2 Click Insert.

The QOSProfile, Insert dialog box opens (Figure 24).

Figure 24 QOSProfile, Insert dialog box



3 Type information in the appropriate fields.

4 Click Insert.

Table 22 describes the fields in the QOSProfile, Insert dialog box.

Table 22 QOSProfile, Insert dialog box fields

Field	Description
Id	Profile ID.
Name	Profile name.
Enable	Enables (true) or disables (false) the profile.
TranslateDscpEnable	Specifies whether translation of the DSCP should be performed. If true is selected, packets that fall within the traffic profile are re-marked with the InProfileDscp value. Packets that fall outside the traffic profile are re-marked with the OutProfileDscp value. If false is selected, no translation is performed.
InProfileDscp	Specifies the DSCP value for “good” packets. A value of zero (000000) means leave the DSCP field unchanged.
OutProfileDscp	Specifies the DSCP value for “violation” packets. A value of zero (000000) means leave the DSCP unchanged.
DiscardEnable	Specifies whether or not packets that fall outside the traffic profile should be discarded.
AverageRate	Average rate is accomplished in increments of 64 bytes every 2.5 milliseconds.

Editing a traffic profile

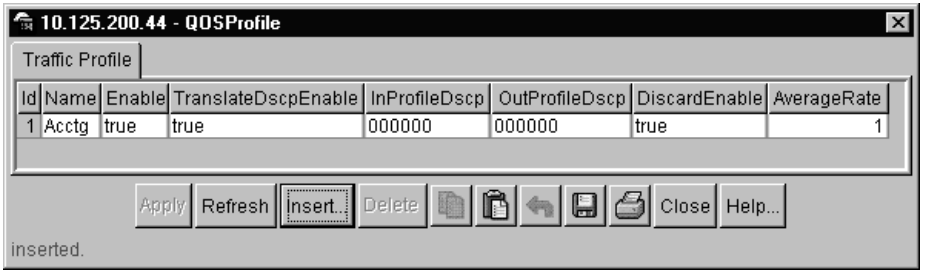
A traffic profile specifies the handling properties of a traffic flow selected by a classifier. It provides rules for determining whether a particular packet is in profile or out of profile; this determination results in the policing of IP packets within a traffic flow.

To edit a traffic profile:

1 From the Device Manager menu bar, choose QOS > Profile.

The QOSProfile dialog box opens with the Traffic Profile tab displayed (Figure 25).

Figure 25 Traffic Profile tab—QOSProfile dialog box



2 To change the name of a traffic profile, double click in the name field and enter a new name.

3 To enable or disable a traffic profile feature, double click in the desired field and select enable (true) or disable (false) from the list, as shown in Figure 26.

Figure 26 Editing a traffic profile

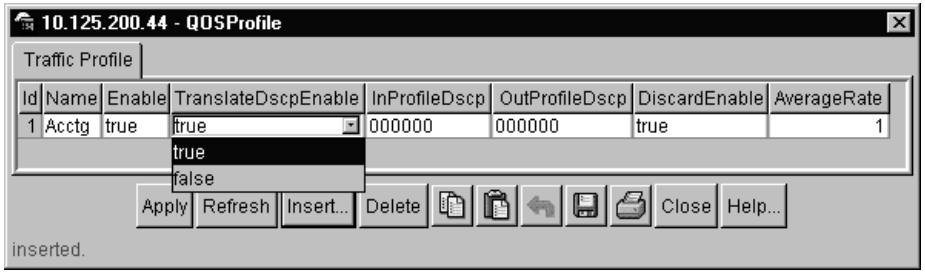


Table 23 describes the Traffic Profile tab fields.

Table 23 Traffic Profile tab fields

Field	Description
Id	Profile ID.
Name	Profile name.
Enable	Enables (true) or disables (false) the profile.
TranslateDscpEnable	Specifies whether translation of the DSCP should be performed. If true is selected, packets that fall within the traffic profile are re-marked with the InProfileDscp value. Packets that fall outside the traffic profile are re-marked with the OutProfileDscp value. If false is selected, no translation is performed.

Table 23 Traffic Profile tab fields (continued)

Field	Description
InProfileDscp	Specifies the DSCP value for “good” packets. A value of zero (000000) means leave the DSCP field unchanged.
OutProfileDscp	Specifies the DSCP value for “violation” packets. A value of zero (000000) means leave the DSCP unchanged.
DiscardEnable	Specifies whether or not packets that fall outside the traffic profile should be discarded.
AverageRate	Average rate is accomplished in increments of 64 bytes every 2.5 milliseconds.

Chapter 4
Configuring QoS using the CLI

This chapter describes CLI commands that are used to configure IP QoS and the IP forwarding database in your Passport 8000 Series Switch.

- For conceptual information about QoS, see Chapter 1, “QoS and IP filtering concepts,” on page 21.
- For configuration examples, including the required CLI commands, see Chapter 2, “Configuration examples,” on page 49.

This chapter includes the following topics:

Roadmap of IP commands

The following roadmap lists some of the IP commands and their parameters. Use this list as a quick reference or click on any command or parameter entry for more information.

Command	Parameter
config ethernet <ports> enable-diffserv true	
config ethernet <ports> access-diffserv true	
config ethernet <ports> access-diffserv false	
config qos egressmap <level>	info
	1p <level> <ieee1p>
	ds <level> <dscp>
config qos ingressmap <level>	info
	1p <ieee1p> <level>
	ds <dscp> <level>
show qos queue <level>	

IP QoS commands

The IP QoS commands allow you to enable the Quality of Service (QoS) features on the switch. Refer to Chapter 1, "QoS and IP filtering concepts," on page 21 for general information about Quality of Service features.

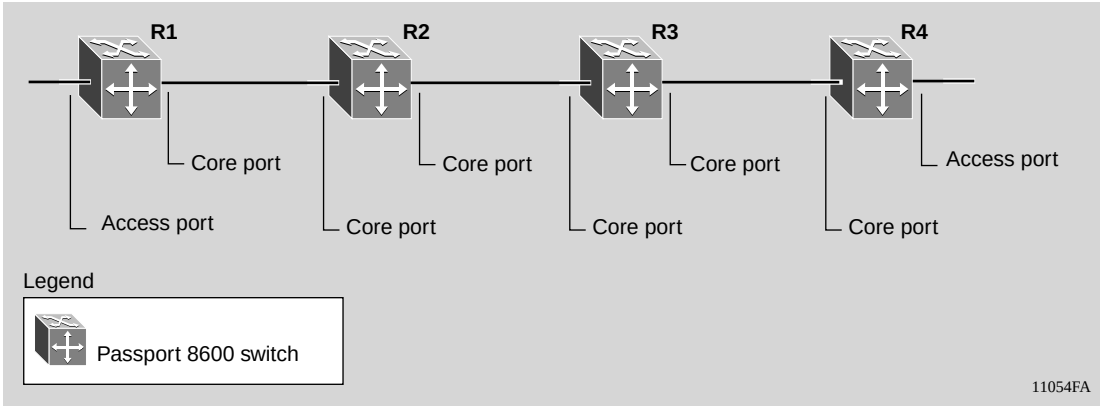
This chapter includes the following topics:

Configuring DiffServ ports

On a Passport 8000 switch, using a global filter to apply a QoS rate-limiting profile to a DiffServ access port results in a nondeterministic effective rate for that flow. To impose a specific rate limit for traffic flow ingressing those ports, use a source/destination filter for the DiffServ access ports.

To enable end-to-end QoS for IP traffic, you must identify which ports will serve as the DiffServ access ports (*untrusted* ports) and which ports will serve as DiffServ core port (*trusted* ports) and set them accordingly (Figure 27).

Figure 27 Access and core ports



Enabling Diffserv on a port

To enable DiffServ on a port, use the following command:

```
config ethernet <ports> enable-diffserv true
```

When you first enable DiffServ on a port, the port type is set to "core," by default, which means the Type of Service (TOS)[1] bits are trusted.

Changing the default core port to an access port

To change the default core port to an access port, use the following command:

```
config ethernet <ports> access-diffserv true
```

Note that Access ports are untrusted ports.

Changing an access port to a core port

You can change an untrusted access port to a (trusted) core port using the following command:

```
config ethernet <ports> access-diffserv false
```

Viewing traffic classification and policing variables

Your Passport 8000 Series switch contains the QoS mapping needed to enable a DiffServ domain. You can view the default QoS configurations, including the following:

- The egress and ingress mapping tables for the DiffServ codepoints (DSCP) and the eight QoS levels
- The traffic classification and policing variables

[1] IP allows a Type of Service implementation, providing traffic prioritization and Quality of Service (QOS) attributes.

To view the traffic classification and policing variables, use the following commands:

```
show qos queue
config ip traffic-filter traffic-profile <pid> info
config qos ingressmap info
config qos egressmap info
```

To view the DiffServ settings for non-IP traffic, use the following commands to display the QoS setting for VLANs, ports, and MAC addresses, respectively:

```
config vlan <vid> info
config ethernet <ports> info
show vlan info fdb-entry <vid>
```

Caution: Nortel Networks recommends not changing the default values. If you change the values, make sure that the values are consistent on all other Passport 8000 Series switches and other devices in your network. Inconsistent mapping of values can result in unpredictable service levels.

Configuring the QoS egress map table

To configure IEEE 802.1p levels and DSCP bytes to QoS level maps, use the following command:

`config qos egressmap <level>`

This command includes the following options:

`config qos egressmap <level>` followed by:	
`info`	Displays which DSCP and IEEE 802.1p levels are mapped to QoS levels for egress traffic (Figure 28).
`1p <level> <ieee1p>`	Maps the QoS level to IEEE 1p priority bits. Changes to this mapping table will not take effect until you save and reboot the switch. • *`level`* is the QoS level {0..7}. • *`ieee1p`* is the IEEE 802.1p bits {0..7}.
`ds <level> <dscp>`	Maps the QoS level to the DSCP. Changes to this mapping table will not take effect until you save and reboot the switch. • *`level`* is the QoS level {0..7}. • *`dscp`* is a 6-bit binary number.

Figure 28 on page 117 shows sample output for this command.

Figure 28 config qos egressmap info command output

```
Passport-8610# config qos egressmap info
               1p
                    level : 0
                   ieee1p : 1
               1p
                    level : 1
                   ieee1p : 0
               1p
                    level : 2
                   ieee1p : 2
               1p
                    level : 3
                   ieee1p : 3
               1p
                    level : 4
                   ieee1p : 4
               1p
                    level : 5
                   ieee1p : 5
               1p
                    level : 6
                   ieee1p : 6
               1p
                    level : 7
                   ieee1p : 7
               ds
                    level : 0
                     DSCP : 0
                DSCP-bin : 000000
               ds
                    level : 1
                     DSCP : 0
                DSCP-bin : 000000
               ds
```

Configuring the QoS ingress map table

To configure the IEEE 802.1p levels and DSCP bytes to QoS level maps and to change those settings, if necessary

`config qos ingressmap <level>`

This command includes the following options:

`config qos ingressmap <level>` followed by:	
`info`	Displays which DSCP and IEEE 802.1p levels are mapped to QoS levels for egress traffic (Figure 29).
`1p <ieee1p> <level>`	Maps the QoS level to IEEE 1p priority bits. Changes to this mapping table will not take effect until you save and reboot the switch. • *<ieee1p>* is the IEEE 802.1p bits {0..7}. • *<level>* is the QoS level {0..7}.
`ds <dscp> <level>`	Maps the QoS level to the DSCP. Changes to this mapping table will not take effect until you save and reboot the switch. • *<dscp>* is a 6-bit binary number. • *<level>* is the QoS level {0..7}.

Figure 29 shows an example of the output for this command.

Figure 29 config qos ingressmap info command output

```
Passport-8610# config qos ingressmap info

                  1p
                      ieee1p : 0
                       level : 1
                  1p
                      ieee1p : 1
                       level : 0
                  1p
                      ieee1p : 2
                       level : 2
                  1p
                      ieee1p : 3
                       level : 3
                  1p
                      ieee1p : 4
                       level : 4
                  1p
                      ieee1p : 5
                       level : 5
                  1p
                      ieee1p : 6
                       level : 6
                  1p
                      ieee1p : 7
                       level : 7
                  ds
                        DSCP : 0
                    DSCP-bin : 000000
                       level : 1
                  ds
                        DSCP : 1
                    DSCP-bin : 000001
                       level : 1
```

Showing QoS queue information

To show the DiffServ queue settings for the eight queues on the switch, use the following command:

```
show qos queue <level>
```

The queues are serviced using guaranteed Weighted Round Robin mechanism. QoS level 7 is reserved for network control traffic, and you cannot change the settings for that queue. Refer to Chapter 1, “QoS and IP filtering concepts,” on page 21 for more information about these queues.

Figure 30 shows sample output for this command.

Figure 30 show qos queue 3 command output

```
Passport-8610# show qos queue 3

================================================================================
                                Qos Queue Table
================================================================================
       SERVICE          ADMIN     OPER
LEVEL  CLASS            WEIGHT    WEIGHT
--------------------------------------------------------------------------------

3      Silver           18        18
```

Chapter 5
Configuring IP filters using Device Manager

IP filters are used to manage traffic and, in some cases, to provide security. Each filter set includes match conditions (a list of filter records defining the match criteria) and actions (forward, drop, prioritize, mirror, modify DS field, modify IEEE 802.1p priority, or prevent incoming TCP connections) to be performed when a match condition is satisfied.

However certain configurations that require a large number of IP filters are known to block the processing of LED information. Therefore, the CPU Utilization LED display may not be updated when the CPU is at 100% utilization.

This chapter describes how to use Device Manager to configure IP filters that are supported on a Passport 8000 Series Switch.

- For conceptual information about QoS, see Chapter 1, “QoS and IP filtering concepts,” on page 21.
- For configuration examples, including the required CLI commands, see Chapter 2, “Configuration examples,” on page 49.

This chapter includes the following topics:

Filter characteristics

IP filters apply to all routed IP packets to be forwarded through a switch on specified ingress ports. The filters are applied to the switch ingress ports with a default action to forward or drop. All packets not matching any filter are forwarded or dropped, depending on the port's default action.

This section includes the following topics:

Note: Filters are applied to a port using filter sets, and actions are assigned when applying a filter set to a port. The actions of individual filters can override the default actions of the port.

Filters on an [Product Family] have the following characteristics and requirements:

- Global filter set lists must have an ID of 1 through 100 (100 total).
- Source and destination filter set lists must have an ID of 300 to 1000 (700 total).

Note: You can have only a combined total of 128 global filter sets and source/destination filter sets.

- Source, destination, and global filter names do not have to be unique.
- A set of source/destination filters is defined in a list, and the list is applied to a port or set of ports. Multiple lists can be assigned to any given port.
- A set of global filters is defined in a list (not exceeding eight per list), and the list is applied to a port or set of ports. Multiple lists may be applied to a given port or set of ports, but the maximum number of global filters that can be enabled on a given port set is eight.

Global filters

Global filters may specify a source IP address and mask, a destination IP address and mask, both of these, or neither of these. Global filters have the following characteristics:

- No minimum or maximum mask length exists.
- Only one unique global filter of each source/address pair can be defined.
- Up to eight global filters can be applied to a port or set of ports on an [Product Family].
- A global filter can cause the same actions as described above for source/destination filters.

Note: Global filters for IP routed traffic can only be applied to non-DiffServ enabled ports.

Traffic filters (source and destination)

Source filters must specify a source IP address and mask, and they may optionally specify a destination IP address and mask. Destination filters must specify a destination IP address and mask, and they may optionally specify a source IP address and mask. You can configure source filters with 0.0.0.0/0.0.0.0 as the source address however, this filter will be connected to all forwarding records. You can configure destination filters with 0.0.0.0/0.0.0.0 as the destination address.

- Forward the packet when the filter is applied with a forward action.
- Drop the packet when the filter is applied with a drop action.
- Mirror the packet to the defined mirror port.
- Match the DS field.
- Modify the DS codepoint (only on DiffServ access ports).
- Modify IEEE 802.1p.

Action modes

Each brouter port on an [Product Family] has a default action mode of forward associated with it. A packet that matches any filter with the action mode of drop will be dropped. A packet that matches one filter having the action mode of forward will be forwarded if and only if it does not also match a filter with the drop action mode. If a packet matches multiple filters, if any one of them is drop, the packet will be dropped.

Table 24 indicates the forward/drop behavior of a port if filter matches are found for a packet.

Table 24 Port actions for filters

Port mode	Filter mode	Packet action
Forward	Default	Forward all packets that match the filter.
Drop	Default	Drop all packets.
Forward	Forward	Forward all packets that match the filter.
Drop	Forward	Drop all packets except those that match the filter.
Forward	Drop	Drop all packets that match the filter.
Drop	Drop	Drop all packets.

Managing filters

You can edit and create filter and DiffServ information from the Filters tab. The following sections describe tasks involved in managing filters:

- "Inserting a filter," next
- "Graphing a filter" on page 136
- "Editing a filter" on page 137

Inserting a filter

On an Passport 8000 Series Switch chassis, you can create global, destination, and source filters.

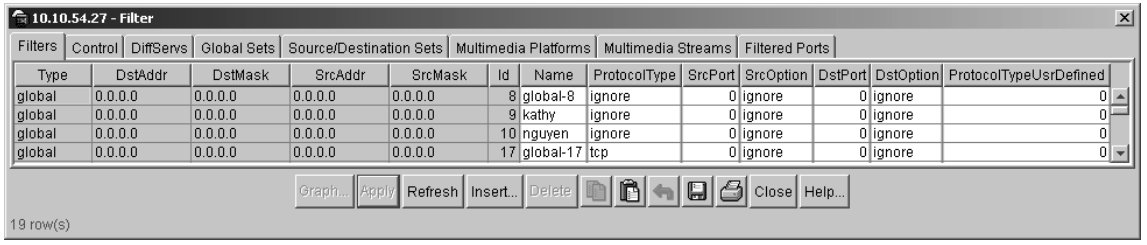
Inserting a global filter

To insert a global filter:

1. From the Device Manager menu bar, choose IP Routing > Filter.

   The Filter dialog box opens with the Filters tab displayed (Figure 31).

Figure 31 Filter dialog box—Filters tab



2. Click Insert.

   The Filter, Insert Filters dialog box opens (Figure 32).

   You can use this dialog box to select the criteria for global filters and DiffServ filters. The DiffServ filter fields are described in Table 28 on page 140.

   The values displayed in Figure 32 are the default values, and the only criteria that is automatically enabled on a filter is StopOnMatch.

3. In the Type field, select Global.
4. In the DstAddr field, type the destination IP address (optional).
5. In the DstMask field, type the destination subnet mask (optional).
6. In the SrcAddr field, type the source IP address (optional).
7. In the SrcMask field, type the subnet mask (optional).
8. Type the name of the filter (optional).
9. Set the ProtocolType: ignore (none), icmp, tcp, or udp (optional).

10 Type the source port, and select the source option (equal, not equal, greater, less, or ignore).

This step is applicable only if a TCP or UDP protocol was selected.

11 Type the destination port, and select the destination option (equal, not equal, greater, less, or ignore).

This step is applicable only if a TCP or UDP protocol was selected.

12 Set the following parameters (optional):

— Mirror

— TcpConnect

13 In the Mode field, select the mode (useDefaultAction, forward, drop, or forwardToNextHop).

14 In the Set StopOnMatch option box, click to enable or disable.

15 In the MatchIcmpRequest option box, click to enable if you want matching on ICMP request packets performed.

16 In the MatchIpFragment option box, click to enable if you want matching on fragmented IP packets performed.

17 In the EnableStatistic option box, click to enable if you want statistics for this filter.

18 Select the DiffServModifyIeee8021PEnable option box if you want to modify the IEEE 802.1p field.

Note: When you enable a traffic filter to modify either the DSCP or the IEEE 802.1p bits, the traffic filter also modifies the other value based on the corresponding value in the QoS ingress tables.

19 If you do not want to use the IEEE 802.1p value automatically assigned based on the QoS Table, you can enter the modify value of the IEEE 802.1p field.

20 In the DiffServModifyDscpEnable option box, click to enable if you want to modify the DiffServ codepoint field.

21 In the DiffServModifyDscp field, you can type the value of the DiffServ codepoint if you do not want to use the DSCP value automatically assigned based on the QoS Table.

22 Specify the DiffServTrafficProfileId of the traffic profile, if any, to be associated with this filter.

23 Click Insert.

The new filter is displayed in the Filters tab (see Figure 31 on page 125). If you changed the DiffServ filter fields, that information is displayed in the DiffServ tab (see Figure 38 on page 140).

Figure 32 Filter, Insert Filters dialog box—global type selected

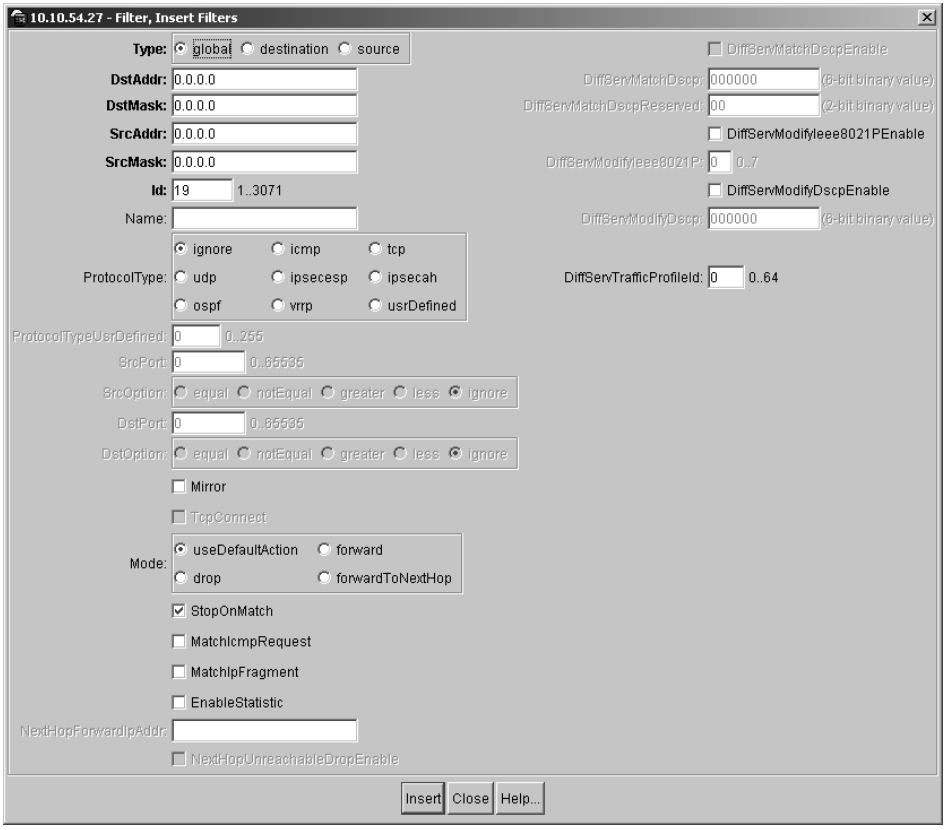


Table 25 describes the Filter, Insert Filters dialog box fields.

Table 25 Filter, Insert Filters dialog box fields

Field	Description
Type	Source filter, destination filter, global filter.
DstAddr	Destination IP address.
DstMask	Destination subnet mask.
SrcAddr	Source IP address.
SrcMask	Source subnet mask.
Id	The filter ID (1 to 4096).
Name	The IP filter name.
ProtocolType	The IP protocol type (icmp, tcp, udp).
ProtocolTypeUsrDefined	When the ProtocolType is set to 256 in an IP Filter, this field represents the 8-bit user defined protocol identifier. The default is 0.
SrcPort (tcp/udp only)	The TCP/UDP source port number.
SrcOption (tcp/udp only)	The TCP/UDP source port option (ignore, equal, less, greater, or not equal).
DstPort (tcp/udp only)	The TCP/UDP destination port number.
DstOption (tcp/udp only)	The TCP/UDP destination port option (ignore, equal, less, greater, or not equal).
Mirror	Set to enable to mirror the packet to the defined mirror port.
TcpConnect (tcp only)	Set to enable to allow only TCP connections established from within the network or disable to allow bidirectional establishment.
Mode	This field can be set to useDefaultAction, forward, dropforwardToNextHop.
StopOnMatch	Sets the filter to stop on match, the default setting.
MatchIcmpRequest	Set MatchIcmpRequest to enable if matching on ICMP request packets should be performed.
MatchIpFragment	Set MatchIpFragment to enable if matching on fragmented IP packets should be performed.
EnableStatistic	Set EnableStatistic to enable if you want statistics for this filter.
NextHopForwardIpAddr (destination/source filter only)	Set NextHopForwardIpAddr to apply filter to the next hop.

Table 25 Filter, Insert Filters dialog box fields (continued)

Field	Description
NextHopUnreachableDropEnable (destination/source filter only)	Set NextHopUnreachableDropEnable to enable if you want drop action.
DiffServMatchDscpEnable (destination/source filter only)	Set to enable to allow a match on the DS field (8 bits), which is composed of the 6-bit DS codepoint (DSCP) and the 2-bit reserved fields.
DiffServMatchDscp	This field is used to specify the match value for the DSCP. The user must enter a 6-bit binary value, and, by default, the value is 000000. If the DSCP in the incoming packet matches this value, then this filter is applied to the packet.
DiffServMatchDscpReserved	This field is reserved for future use. The default is a 2-bit binary value of 00 and should not be changed.
DiffServModifyIeee8021PEnable	Set to enable to allow the IEEE 802.1p field to be modified on packets ingressing DiffServ access ports only. By default, the IEEE 802.1p field is set to zero.
DiffServModifyIeee8021P	If you do not want the IEEE 802.1p field set to zero, use this field to specify the value of the IEEE 802.1p field. You first must enter a value, set the ModifyIeee8021PEnable field to false, and then set it to true.
DiffServModifyDscpEnable	Set to enable to allow the DSCP (6 bits) to be modified on packets ingressing DiffServ access ports only. By default, the DS codepoint is set to 000000.
DiffServModifyDscp	If you do not want the DSCP set to zero, use this field to specify the value of the DSCP. You first must enter a 6-bit value, set the ModifyDscpEnable field to false, and then set it to true.
DiffServTrafficProfileId	This field is used to specify which traffic profile should be applied to packets matching this filter. A zero value means do not apply any traffic profile.

Inserting a destination filter

To insert a destination filter:

1 From the Device Manager menu bar, choose IP Routing > Filter.

The Filter dialog box opens with the Filters tab displayed (Figure 31 on page 125).

2 From the Filters tab, click Insert.

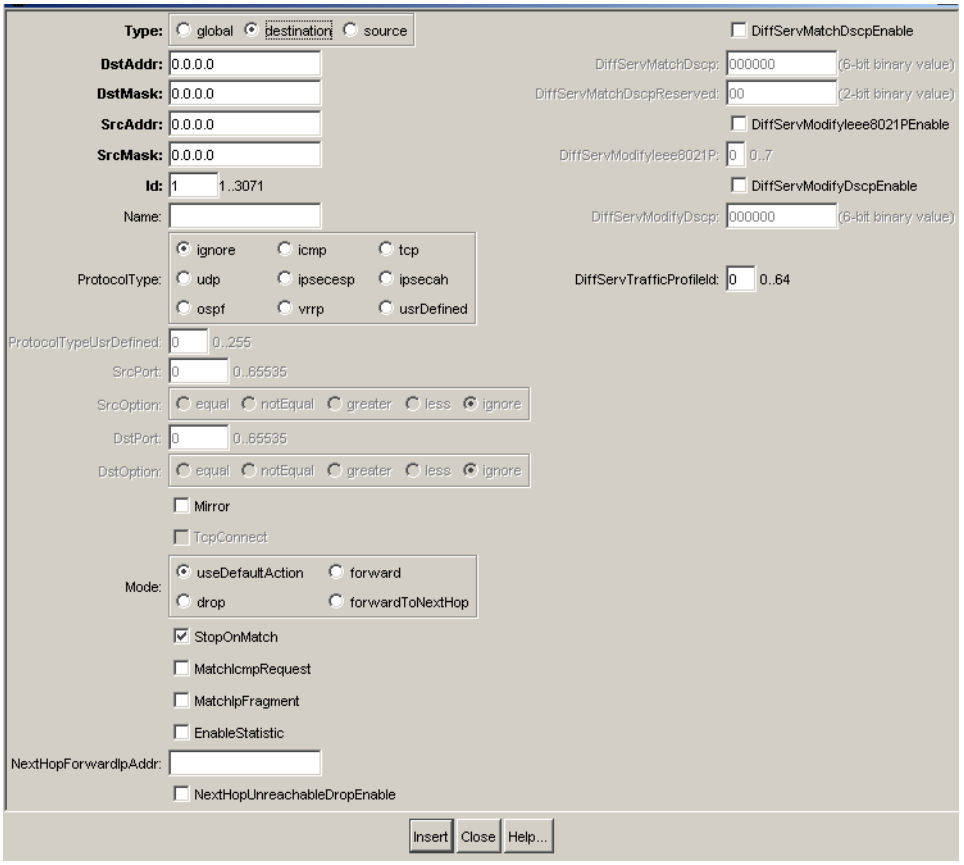
The Filter, Insert Filters dialog box opens (Figure 33).

Table 25 on page 128 describes the Filter, Insert Filters dialog box fields.

3 In the Type field, select destination.

The Insert Filters dialog box with destination selected for type is shown in (Figure 33).

Figure 33 Filter, Insert Filters dialog box—destination type selected



4 For destination filters, type the destination IP address and subnet mask.

5 In the DstAddr field, type the destination IP address.

6 In the DstMask field, type the destination subnet mask.

7 In the SrcAddr field, type the source IP address (optional).

8 In the SrcMask field, type the subnet mask (optional).

9 Type the name of the filter (optional).

10 Set the ProtocolType: ignore (none), icmp, tcp, or udp (optional).

11 Set the ProtocolTypeUsrDefined.

12 Type the source port and select the source option (equal, not equal, greater, less, or ignore).

This step is applicable only if a TCP or UDP protocol was selected.

13 Type the destination port and select the destination option (equal, not equal, greater, less, or ignore).

This step is applicable only if a TCP or UDP protocol was selected.

14 Set the following parameters (optional):

— Mirror

— TcpConnect

15 In the Mode field, select the mode (useDefaultAction, forward, drop, or forwardToNextHop).

16 In the Set StopOnMatch option box, click to enable or disable.

17 In the MatchIcmpRequest option box, click to enable if you want matching on ICMP request packets performed.

18 In the MatchIpFragment option box, click to enable if you want matching on fragmented IP packets performed.

19 In the EnableStatistic option box, click to enable if you want statistics for this filter.

20 In the NextHopForwardIpAddr field, type the IP address of the forwarding hop.

21 In the NextHopUnreachableDropEnable option box, click to enable or disable.

22 Select the DiffServMatchDscpEnable option box, if you want to modify the DiffServMatchDscp field.

23 Enter the DiffServMatchDscp value (in binary format) to match the DiffServ codepoint field.

24 Leave the DiffServMatchDscpReserved field at its default of 00.

Note: When you enable a traffic filter to modify either the DSCP or the IEEE 802.1p bits, the traffic filter also modifies the other value based on the corresponding value in the QoS ingress tables.

25 In the DiffServModifyIeee8021PEnable option box, click to enable if you want to modify the IEEE 802.1p field.

26 If you do not want to use the IEEE 802.1p value automatically assigned based on the QoS Table, you can enter the modify value of the IEEE 802.1p field.

Note: When you enable a traffic filter to modify either the DSCP or the IEEE 802.1p bits, the traffic filter also modifies the other value based on the corresponding value in the QoS ingress tables.

27 In the DiffServModifyDscpEnable option box, click to enable if you want to modify the DiffServ codepoint field.

28 In the DiffServModifyDscp field, you can type the value of the DiffServ codepoint if you do not want to use the DSCP value automatically assigned based on the QoS Table.

29 Specify the DiffServTrafficProfileId of the traffic profile, if any, to be associated with this filter.

30 Click Insert.

The new filter is displayed in the Filters tab (see Figure 31 on page 125). If you changed the DiffServ filter fields, that information is displayed in the Filters DiffServ dialog box (see Figure 38 on page 140).

Inserting a source filter

To insert a source filter:

1 From the Device Manager menu bar, choose IP Routing > Filter.

The Filter dialog box opens with the Filters tab displayed (see Figure 31 on page 125).

2 Click Insert.

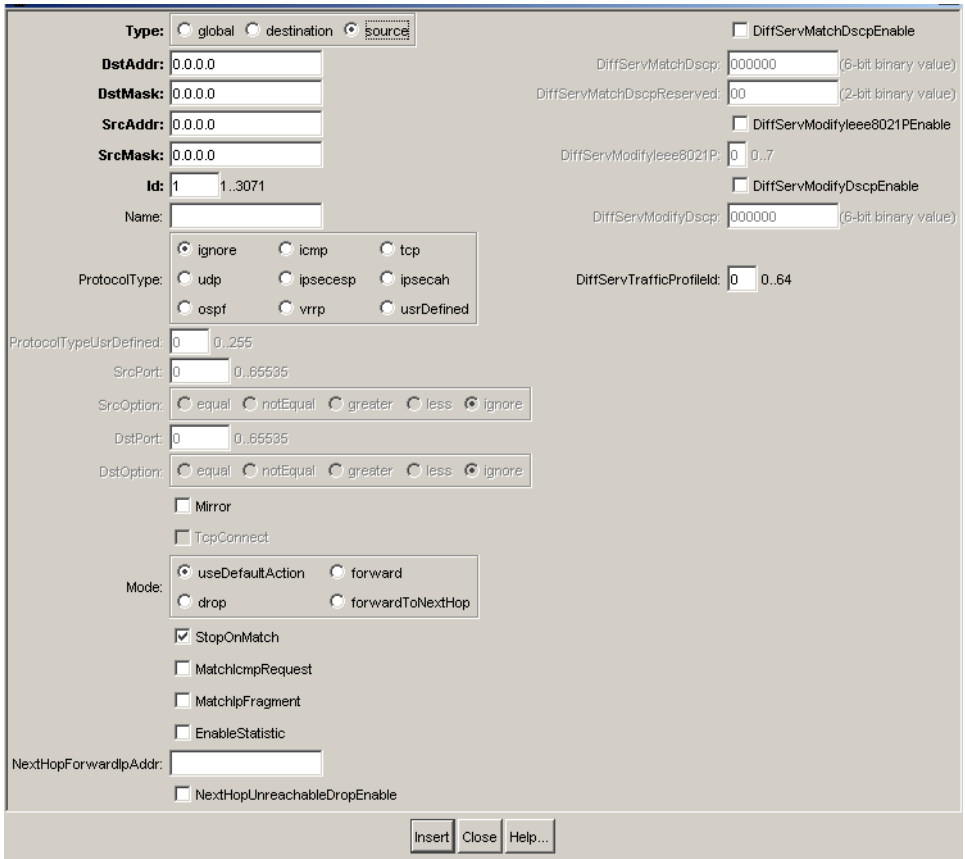
The Filters, Insert Filters dialog box opens (see Figure 32 on page 127).

Table 25 on page 128 describes the Filter, Insert Filters dialog box fields.

3 In the Type field, select Source.

The Filters, Insert Filters dialog box with Source selected for type is shown in Figure 34.

Figure 34 Filter, Insert Filters dialog box—source type selected



4 In the DstAddr field, type the destination IP address (optional)

5 In the DstMask field, type the destination subnet mask (optional).

6 In the SrcAddr field, type the source IP address.

7 In the SrcMask field, type the subnet mask.

8 Type the name of the filter (optional).

9. Set the ProtocolType: ignore (none), icmp, tcp, or udp (optional).
10. Set the ProtocolTypeUsrDefined.
11. Type the source port, and select the source option (equal, not equal, greater, less, or ignore).

    This step is applicable only if a TCP or UDP protocol was selected.
12. Type the destination port, and select the destination option (equal, not equal, greater, less, or ignore).

    This step is applicable only if a TCP or UDP protocol was selected.
13. Set the following parameters (optional):
    - Mirror
    - TcpConnect
14. Set the Mode (use default, forward, or drop).
15. In the StopOnMatch option box, click to enable or disable.
16. In the MatchIcmpRequest option box, click to enable if you want matching on ICMP request packets performed.
17. In the MatchIpFragment option box, click to enable if you want matching on fragmented IP packets performed.
18. In the EnableStatistic option box, click to enable if you want statistics for this filter.
19. In the NextHopForwardIpAddr field, type the IP address of the forwarding hop.
20. In the NextHopUnreachableDropEnable option box, click to enable or disable.
21. Select the DiffServMatchDscpEnable option box if you want to modify the DiffServMatchDscp field.
22. Enter the DiffServMatchDscp value (in binary format) to match the DiffServ codepoint field.
23. Leave the DiffServMatchDscpReserved field at its default of 00.

Note: When you enable a traffic filter to modify either the DSCP or the IEEE 802.1p bits, the traffic filter also modifies the other value based on the corresponding value in the QoS ingress tables.

24 In the DiffServModifyIeee8021PEnable option box, click to enable if you want to modify the IEEE 802.1p field.

25 If you do not want to use the IEEE 802.1p value automatically assigned based on the QoS Table, you can enter the modify value of the IEEE 802.1p field.

Note: When you enable a traffic filter to modify either the DSCP or the IEEE 802.1p bits, the traffic filter also modifies the other value based on the corresponding value in the QoS ingress tables.

26 In the DiffServModifyDscpEnable option box, click to enable if you want to modify the DiffServ codepoint field.

27 In the DiffServModifyDscp field, you can type the value of the DiffServ codepoint if you do not want to use the DSCP value automatically assigned based on the QoS Table.

28 Specify the DiffServTrafficProfileId of the traffic profile, if any, to be associated with this filter.

29 Click Insert.

The new filter is displayed in the Filters tab (see Figure 31 on page 125). If you changed the DiffServ filter fields, that information is displayed in the Filters DiffServ dialog box (see Figure 38 on page 140).

Graphing a filter

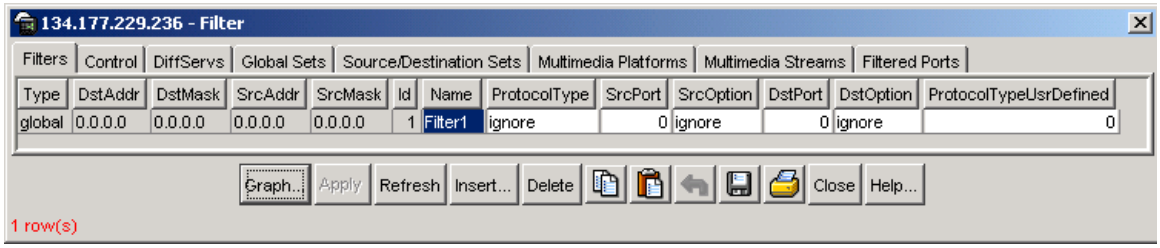
Use the Filter tab to graph filter statistics.

To graph filter statistics:

1. From the Device Manager menu bar, choose IP Routing > Filter.

   The Filter dialog box opens with the Filters tab displayed (Figure 35).

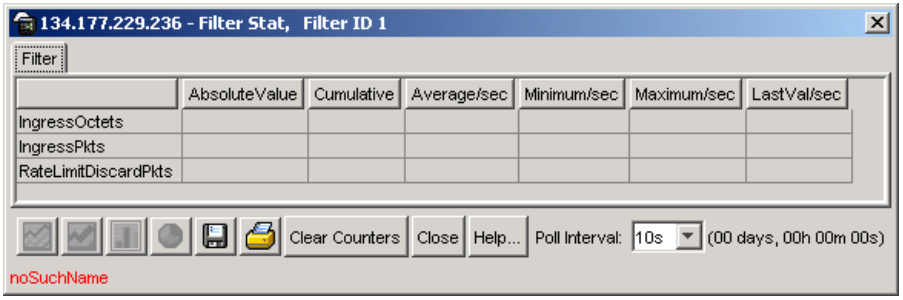
Figure 35 Filters tab—Filter selected



2. Click the name of the filter to graph.
3. Click Graph.

   The FilterStat dialog box opens with the Filter tab displayed (Figure 36).

Figure 36 FilterStat dialog box— Filter tab



4. Select the statistic(s) you want to graph.
5. In the Poll Interval box, select the polling interval.
6. Click the Graph button (bar, pie, chart, line).

Table 26 Filter tab fields

Field	Description
IngressOctets	The total number of igress octets received for this filter.
IngressPkts	The total number of ingress packets received for this filter
RateLimitDiscardPkts	The total number of rate limit discard packets for this filter.

Editing a filter

To edit basic filter information:

1. From the Device Manager menu bar, choose IP Routing > Filter.

   The Filter dialog box opens with the Filters tab displayed (see Figure 31 on page 125). Packets matching a filter match criteria follow the filter action specified in the filter. The options set for DiffServ can be seen in the DiffServ tab (see Figure 38 on page 140), not the Filters tab.

   Table 25 on page 128 describes the Filters tab fields.

2. Click any of the fields with white backgrounds. You will have the option either to select a new value from the pop-up menu or to enter a new value.
3. Click Apply.
4. Click Refresh.
5. After you finish editing the filter, you must reapply the ports associated with that filter.

Controlling filters

After you insert a filter, you can view and manage filter information in the Control tab.

To control filter information:

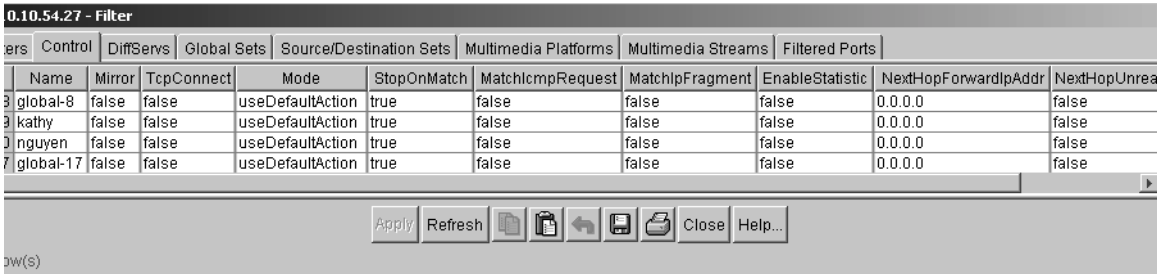
1. From the Device Manager menu bar, choose IP Routing > Filter.

The Filter dialog box opens with the Filters tab displayed (see Figure 31 on page 125).

2 Click the Control tab.

The Control tab opens (Figure 37).

Figure 37 Filter dialog box—Control tab



3 Click Refresh.

4 Select the parameter(s) that you want to modify for each filter.

5 Click Apply.

Table 27 describes the Control tab fields.

Table 27 Control tab fields

Field	Description
Id	A unique identifier for the filter.
Name	The IP filter name.
Mirror	Set to enable to mirror the packet to the defined mirror port.
TcpConnect	Set to true to allow only TCP connections established from within the network or disable to allow bidirectional establishment.
Mode	This field can be set to: • UseDefaultAction • Forward • Drop • ForwardToNextHop
StopOnMatch	Sets to true to stop on match, the default setting.

Table 27 Control tab fields (continued)

Field	Description
MatchIcmpRequest	Set MatchIcmpRequest to true if matching on ICMP request packets should be performed.
MatchIpFragment	Set MatchIpFragment to true if matching on fragmented IP packets should be performed.
EnableStatistic	Set EnableStatistic to true if you want statistics for this filter.
NextHopForwardIpAddr	Set NextHopForwardIpAddr to apply filter to the next hop.
NextHopUnreachableDropEnable	Set NextHopUnreachableDropEnable to enable if you want drop action.

6 Click any of the fields with white backgrounds. You will have the option either to select a new value from the pop-up menu or to enter a new value.

If you change a value in the ModifyDscp or the ModifyIeee8021P field, you must set the ModifyDscpEnable or ModifyIeee8021PEnable field to disable. Click the Apply and the Refresh buttons, set that field to enable, and then click the Apply and the Refresh buttons again.

7 Click Apply.

8 Click Refresh.

9 After you finish editing the filter, you must reapply the ports associated with that filter.

Editing Diffserv information

To edit DiffServ information:

1 From the Device Manager menu bar, choose IP Routing > Filter.

The Filter dialog box opens with the Filters tab displayed (see Figure 31 on page 125).

2 Click the DiffServs tab.

The DiffServs tab opens (Figure 38). Packets matching a filter criteria follow the filter action specified in the filter.

Note: When you enable a traffic filter to modify either the DSCP or the IEEE 802.1p bits, the traffic filter also modifies the other value based on the corresponding value in the QoS ingress tables.

Figure 38 Filter dialog box—Diffservs tab

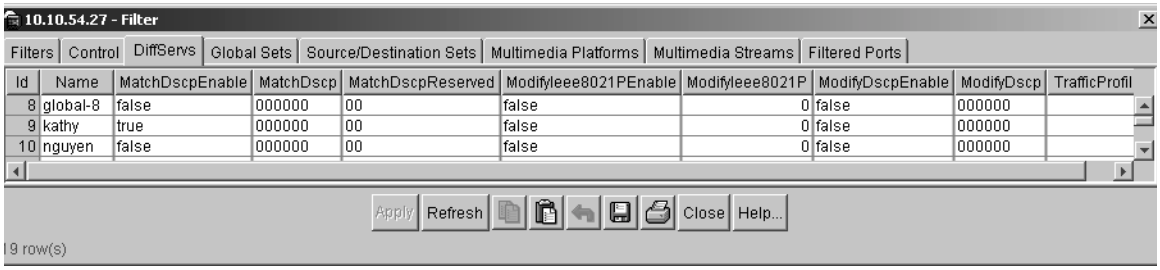


Table 28 describes the DiffServs tab fields.

Table 28 DiffServs tab fields

Field	Description
Id	This field is the filter's unique identifier (id). This field is automatically generated by the system when a filter is created.
Name	The IP filter name.
MatchDscpEnable	Set to enable to allow a match on the DS field (8 bits), which is composed of the 6-bit DS codepoint (DSCP) and the 2-bit reserved fields.
MatchDscp	This field is used to specify the match value for the DSCP. The user must enter a 6-bit binary value, and, by default, the value is 000000. If the DSCP in the incoming packet matches this value, then this filter is applied to the packet.
MatchDscpReserved	This field is reserved for future use. The default is a 2-bit binary value of 00 and should not be changed.
ModifyIeee8021PEnable	Set to enable to allow the IEEE 802.1p field to be modified on packets ingressing DiffServ access ports only. By default, the IEEE 802.1p field is set to zero.

Table 28 DiffServs tab fields (continued)

Field	Description
ModifyIeee8021P	If you do not want the IEEE 802.1p field set to zero, use this field to specify the value of the IEEE 802.1p field. You first must enter a value, set the ModifyIeee8021PEnable field to disable, and then set it to enable.
ModifyDscpEnable	Set to enable to allow the DSCP (6 bits) to be modified on packets ingressing DiffServ access ports only. By default, the DS codepoint is set to 000000.
ModifyDscp	If you do not want the DSCP set to zero, use this field to specify the value of the DSCP. You first must enter a 6-bit value, set the ModifyDscpEnable field to disable, and then set it to enable.
TrafficProfileId	This field is used to specify which traffic profile should be applied to packets matching this filter. A zero value means do not apply any traffic profile.

3 Click any of the fields with white backgrounds. You will have the option either to select a new value from the pop-up menu or to enter a new value.

If you change a value in the ModifyDscp or the ModifyIeee8021P field, you must set the ModifyDscpEnable or ModifyIeee8021PEnable field to disable. Click the Apply and the Refresh buttons, set that field to enable, and then click the Apply and the Refresh buttons again.

4 Click Apply.

5 Click Refresh.

6 After you finish editing the filter, you must reapply the ports associated with that filter.

Building global filter sets

To build a list of global filter sets:

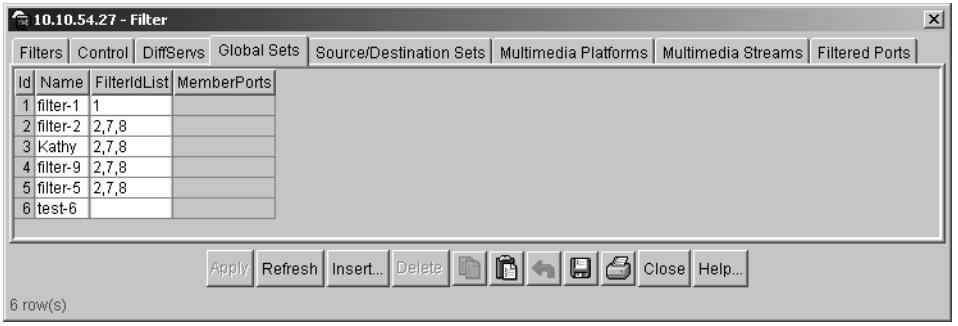
1 From the Device Manager menu bar, choose IP Routing > Filter.

The Filter dialog box opens with the Filters tab displayed (see Figure 31 on page 125).

2 Click the Global Sets tab.

The Global Sets tab opens (Figure 39).

Figure 39 Filter dialog box—Global Sets tab

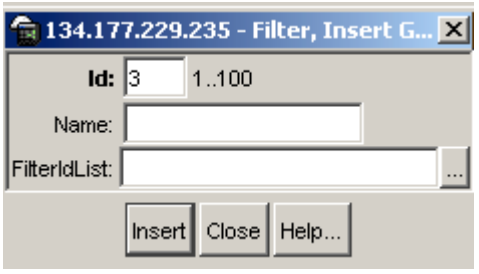


3 Click Refresh.

4 Click Insert.

The Filter, Insert Global Sets dialog box opens (Figure 40).

Figure 40 Filter, Insert Global Sets dialog box



5 Type the filter name and select filter ids.

6 Click Insert.

Table 29 describes the fields in the Global Sets tab.

Table 29 Global Sets tab fields

Field	Field
Id	An unique value to identify a particular global filter list.
Name	The name that is given to the filter list.
FilterIdList	This is used to indicate the number of filters that are associated with this filter list.
MemberPorts	The names of the ports the filter is used on.

Building source and destination filter sets

To build source or destination filter sets:

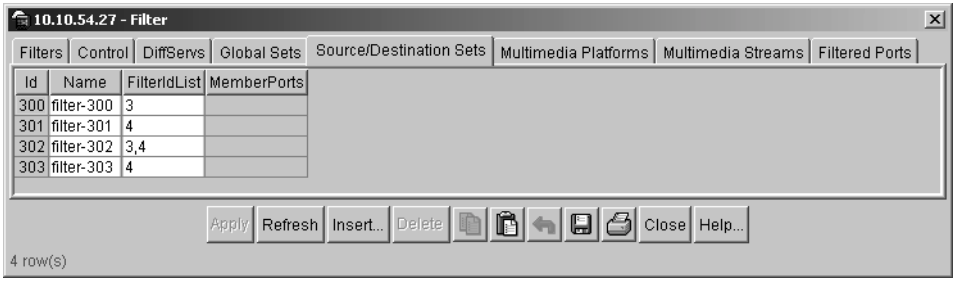
1. From the Device Manager menu bar, choose IP Routing > Filter.

   The Filter dialog box opens with the Filters tab displayed (see Figure 31 on page 125).

2. Click the Source/Destination Sets tab.

   The Source/Destination Sets tab opens (Figure 41).

Figure 41 Filter dialog box—Source/Destination Sets tab

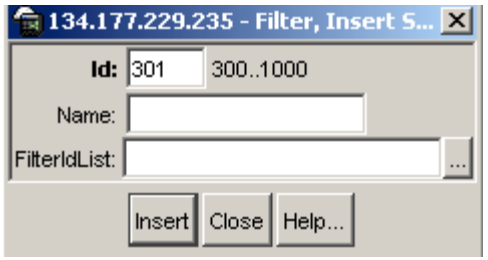


3. Click Refresh.

4. Click Insert.

   The Filter, Insert Source/Destination Sets dialog box opens (Figure 42). You can use this dialog box to build a list of source and destination filters.

Figure 42 Filter, Insert Source/Destination Sets dialog box



5 Type the filter ID and name, and select the filter ID in the FilterIdList.

Editing filtered ports

To edit filtered ports:

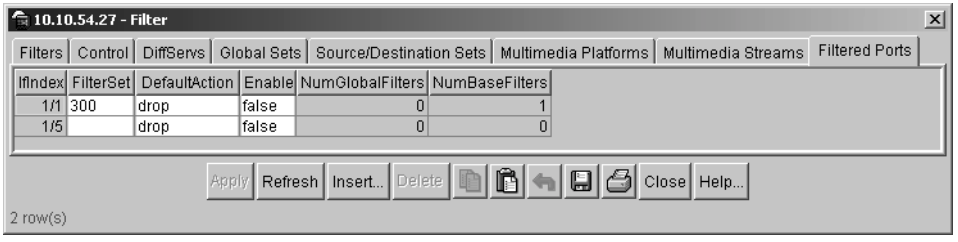
1 From the Device Manager menu bar, choose IP Routing > Filter.

The Filter dialog box opens with the Filters tab displayed (see Figure 31 on page 125).

2 Click the Filtered Ports tab.

The Filtered Ports tab opens (Figure 43).

Figure 43 Filter dialog box—Filtered Ports tab

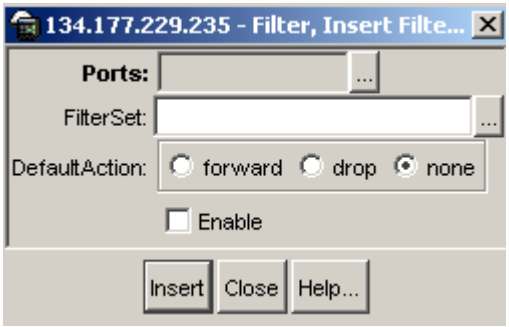


3 Click Refresh.

4 Click Insert.

The Filter, Insert Filtered Ports dialog box opens (Figure 44).

Figure 44 Filter, Insert Filtered Ports dialog box



5 In the Ports field, click the ellipsis button to the right of the Ports field and select ports.

6 Click on the ellipsis button next to the FilterSet field and select a filter set.

7 In the DefaultAction option box, select the action mode to forward, drop, or none.

8 Click Insert.

Table 30 describes the fields in the Filtered Ports tab.

Table 30 Filtered Ports tab fields

Field	Field
IfIndex	The port associated with the filter.
Ports	The port(s) to which the filter sets need to be applied. **Note:** You must select physical ports, not logical ports like MLT.
FilterSet	The selection of filter lists, both global and nonglobal.
DefaultAction	This action will be forward, drop, or none.
Enable	To make the filters active. **Note:** Whenever you change a filter parameter, you must first disable the filter on its filter ports and then enable the filter again to reapply the changed filter to the ports.
NumGlobalFilters	The number of global filters applied to this port.
NumBaseFilters	The number of base source/destination filters applied to this port.

Configuring IP telephony and multimedia platform filters

To configure IP telephony multimedia platform filters:

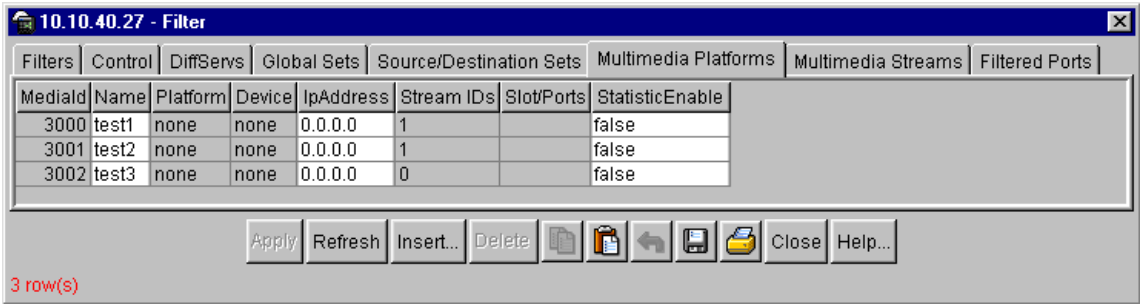
1. From the Device Manager menu bar, choose IP routing > Filter

   The Filter dialog box opens with the Filters tab displayed (see Figure 31 on page 125).

2. Click the Multimedia Platforms tab.

   The Multimedia Platforms tab is displayed (Figure 45).

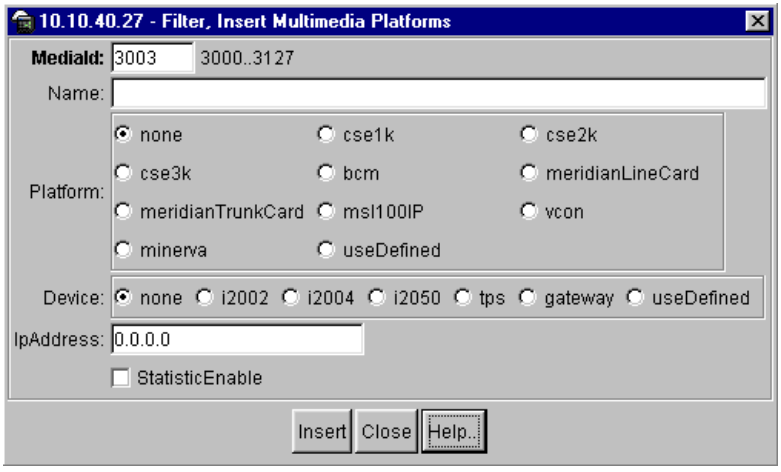
Figure 45 Filter dialog box—Multimedia Platforms tab



3. Click Insert.

   The Filter, Insert Multimedia Platforms dialog box opens (Figure 46).

Figure 46 Filter, Insert Multimedia Platforms dialog box



4 Specify optional name.

5 Select device.

6 Select platform.

7 Specify optional gateway-IP address.

8 Click optional statistics enable

9 Click Insert

Table 31 describes the fields in the Multimedia Platforms tab.

Table 31 Insert Multimedia Platform fields

Field	Description
MediaId	The number assigned to the filter set. The range is from 3000 to 3127.
Name	Specifies a name for the multimedia platform.
Platform	Specifies the type of multimedia platform used.
Device	Specifies the type of multimedia device used.
IP Address	IP address of the interface you are specifying.
StatisticEnable	Enables or disables the display of statistics on the filter.

Configuring IP telephony and multimedia streams

To configure IP telephony and multimedia streams:

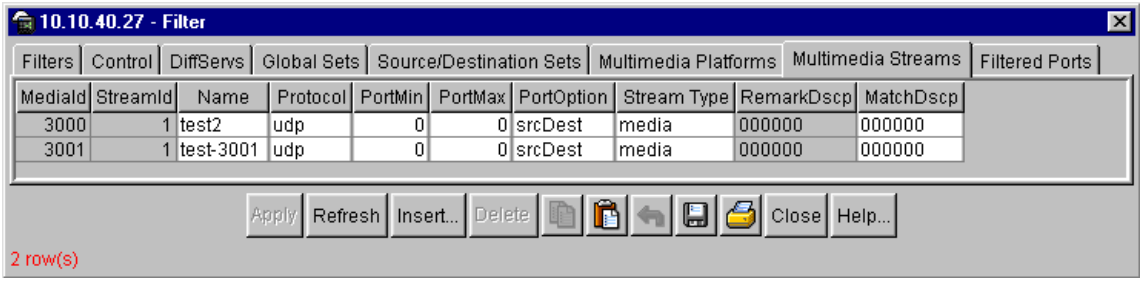
1 From the Device Manager menu bar, choose IP routing > Filter

The Filter dialog box opens with the Filters tab displayed (see Figure 31 on page 125).

2 Click the Multimedia Streams tab.

The Multimedia Streams tab displays (Figure 47).

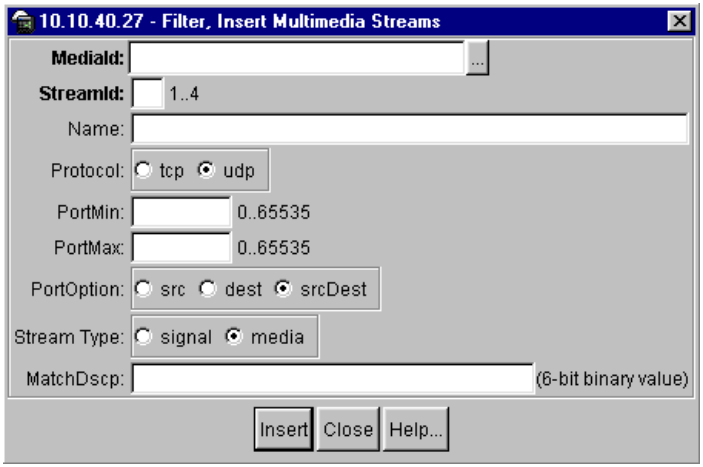
Figure 47 Filter dialog box—Multimedia Streams tab



3 Click Insert.

The Filter, Insert Multimedia Streams dialog box opens (Figure 48).

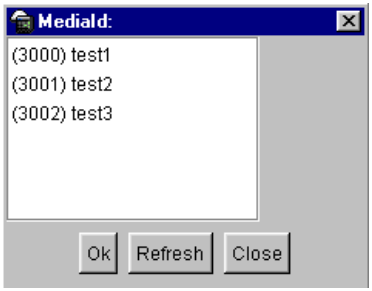
Figure 48 Filter, Insert Multimedia Streams dialog box



4 Click the ellipsis button to the right of the MediaId field.

The MediaId list box opens (Figure 49).

Figure 49 MediaId list box



5 Select a MediaId from the list box.

6 Click OK.

7 In the Filter, Insert Multimedia Stream dialog box, specify Stream Id

8 Specify optional name

9 Select optional Protocol.

10 Specify optional PortMin.

11 Specify optional PortMax.

12 Select PortOption.

13 Select Type.

14 Specify MatchDSCP.

Table 32 describes the Filter, Insert Multimedia Streams dialog box fields.

Table 32 Filter, Insert Multimedia Streams dialog box fields

Field	Description
MediaId	Displays the Media Id in Media ID Table. (Missing the pop up screen when selecting the Media Id see attachment).
StreamID	Displays the Port range Id.
Name	Enter the stream name.
Protocol	Select either TCP or UDP protocol.
Port Min	TCP/UDP source or destination port to filter on.
Port Max	TCP/UDP source or destination port to filter on.

Table 32 Filter, Insert Multimedia Streams dialog box fields (continued)

Field	Description
PortOption	Select source port or destination port or both.
Stream Type	Type of stream to filter on. Signal or media.
MatchDscp	Used to specify what the value of the DSCP should be modified to if this stream is identified. The modification is applied at the egress point. The DSCP represents the high-order 6 bits of the TOS byte.

Configuring IP telephony and multimedia filter lists on a port

Note: When you create filters for a particular IP telephony device, they are exclusive for the device.

To configure an IP telephony filter with defaults:

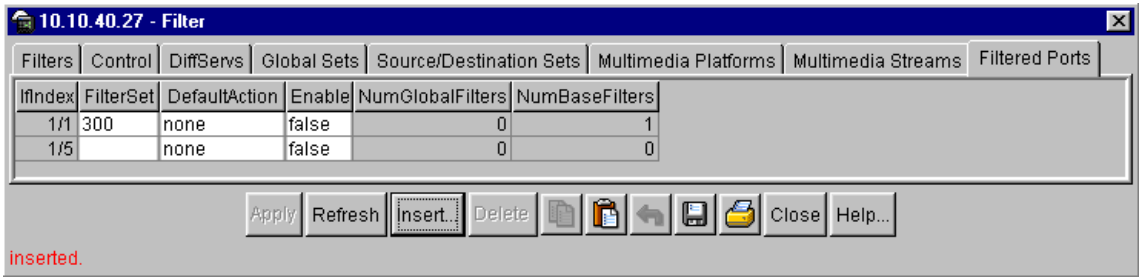
1. From the Device Manager menu bar, choose IP routing > Filter.

   The Filter dialog box opens with the Filters tab displayed (see Figure 31 on page 125).

2. Click the Filtered Ports tab.

   The Filtered Ports tab opens (Figure 50).

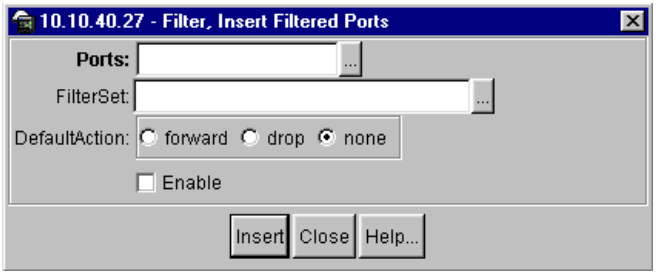
Figure 50 Filter dialog box—Filtered Ports tab



3. Click Insert.

   The Filter, Insert Filtered Ports dialog box opens (Figure 51).

Figure 51 Filter, Insert Filtered Ports dialog box



4 Click the Port list box selection button.

The IpFilterPortIfIndex dialog box opens (Figure 52).

Figure 52 FilterPortIfIndex dialog box

5 Select a port.

6 Click OK.

7 Click on the ellipsis button to the right of the FilterSet field.

8 Select a filter set.

9 Click OK.

10 Select forward.

11 Check Enable.

12 Click Insert.

The filtered port is enabled and appears in the Filter dialog box.

Table 33 describes the Filter, Insert Filtered Ports dialog box fields

Table 33 Filter, Insert Filtered Ports fields

Field	Description
Ports	Specifies the slot/port numbers of the filtered port.
Filterset	Identifies the filter set to be enabled.
Enable	Enables and disables the filter. The default is disabled.
Default Action	Defines the default action. Options are forward, drop, and none.

Enabling and Disabling an IP telephony and multimedia filter on a port

To enable an IP telephony and multimedia filter on a port:

1. From the Device Manager menu bar, choose IP routing > Filter.

   The Filter dialog box opens with the Filters tab displayed (see Figure 31 on page 125).

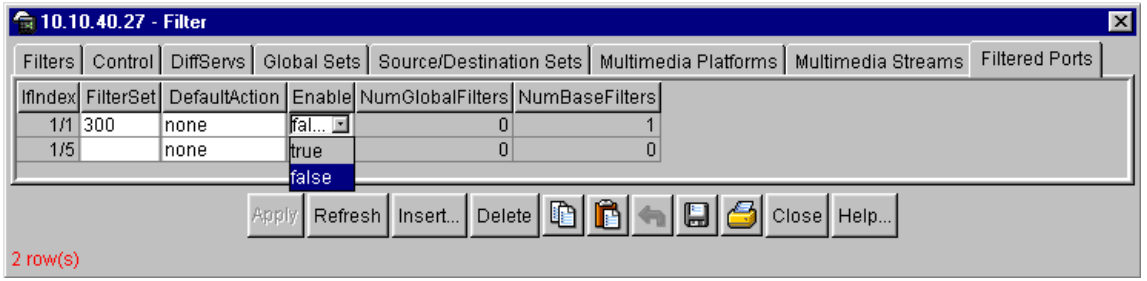
2. Click the Filtered Ports tab.

   The Filtered Ports tab opens (Figure 53).

3. Double click on the Enable column of the filter you want to enable.

   A list box opens (Figure 53).

Figure 53 Filter dialog box—Filtered Ports tab.



4. Select true or false.

5 Click Apply.

Deleting an IP telephony and multimedia filter list from a port

To delete an IP telephony filter:

1 From the Device Manager menu bar, choose IP routing > Filter.

The Filter dialog box opens with the Filters tab displayed (see Figure 31 on page 125).

2 Click the Filtered Ports tab.

The Filtered Ports tab opens (Figure 53).

3 Select the row with slot/port number of the filter you want to delete.

4 Click Delete.

The port is removed from the list of filtered ports.

Chapter 6
Configuring IP filters using the CLI

This chapter describes CLI commands that are used to configure IP traffic filters on the Passport 8000 Series Switch.

Certain configurations that require a large number of IP filters are known to block the processing of LED information. Therefore, the CPU Utilization LED display may not be updated when the CPU is at 100% utilization.

- For conceptual information about QoS, see Chapter 1, “QoS and IP filtering concepts,” on page 21.
- For configuration examples, including the required CLI commands, see Chapter 2, “Configuration examples,” on page 49.

This chapter includes the following topics:

Roadmap of IP commands

The following roadmap lists some of the IP commands and their parameters. Use this list as a quick reference or click on any command or parameter entry for more information.

Command	Parameter
config ip traffic-filter	info
	clear-stats [<fid>]
config ip traffic-filter create	info
	destination dst-ip <value> [src-ip <value>] [id <value>]
	global [src-ip <value>] [dst-ip <value>] [id <value>]
	source src-ip <value> [dst-ip <value>] [id <value>]
	traffic-profile <pid>
config ip traffic-filter filter <fid>	info
	delete
	name <name>
config ip traffic-filter filter <fid> action	info
	mirror <enable|disable>
	mode <default|forward |drop|forward-to-next-hop>
	next-hop-forward ip-address <ipaddr>
	next-hop-forward info
	next-hop-forward next-hop-unreachable-drop <enable|disable>

Command	Parameter
	statistic <enable|disable>
	stop-on-match <true|false>
	tcp-connect <enable|disable>
config ip traffic-filter filter <fid> action next-hop-forward	info
	ip-address <ipaddr>
	next-hop-unreachable-drop <enable | disable>
config ip traffic-filter filter <fid> match	info
	ds-field <6-bit dscp> <2-bit reserved>
	ds-field-enable <enable|disable>
	dst-port <port> [dst-option <value>]
	icmp-request <true | false>
	ip-fragment <true | false>
	protocol <protocoltype> [<pid>]
	src-port <port> [src-option <value>]
config ip traffic-filter media <mediaId>	info
	create
	delete
	gateway-ip
	name
	statistic
	stream

Command	Parameter
config ip traffic-filter media <mediaId> streams <streamId>	info
	create
	delete
	gateway-ip
	match-dscp
	name
	port-option
	ports min
	protocol
config ip traffic-filter filter <fid> modify	info
	dscp <6-bit dscp>
	dscp-enable <enable|disable>
	ieee8021p <integer>
	ieee8021p-enable <enable|disable>
config ip traffic-filter global-set <gsetid>	info
	add-filter <fid>
	create [name <value>]
	delete
	remove-filter <fid>
config ip traffic-filter set <setid>	info
	add-filter <fid>
	create [name <value>]

Command	Parameter
	delete
	remove-filter <fid>
config ip traffic-filter traffic-profile <pid>	info
	average-rate <int>
	delete
	discard-out-profile <enable|disable>
	enable <true|false>
	in-dscp <value>
	name <name>
	out-dscp <value>
	translate-dscp <enable | disable>
config ethernet <ports> ip traffic-filter	info
	add set <value>
	create
	delete
	disable
	enable
	remove set <value>
config ethernet <ports> ip traffic-filter default-action	info
	forward
	drop
	none
config ethernet <ports> multimedia	info

Command	Parameter
	disable
	enable
	select <select>
show ip traffic-filter active	
show ip traffic-filter destination [<fid>]	
show ip traffic-filter disabled [<ports>]	
show ip traffic-filter enabled [<ports>]	
show ip traffic-filter global [<fid>]	
show ip traffic-filter interface <ports>	
show ip traffic-filter media	
show ip traffic-filter source [<fid>]	
show ip traffic-filter stream	
show ip traffic-filter stats [<fid>]	
show ip traffic-filter info global-set [<id>]	
show ip traffic-filter info set [<id>]	
show ip traffic-filter traffic-profile info [<id>]	

Configuring IP traffic filter commands

The IP filters on your Passport 8000 Series switch allow you to manage traffic and, in some cases, to provide security. Each filter set includes match conditions and actions to be performed when a match condition is satisfied.

Packet filters apply to all routed packets to be forwarded through the switch on specified ingress ports. The filter sets are applied to the port, and a default action (forward or drop) is set for the port. All packets that do not match any filter take the default action; packets that match any single filter with the opposite action will take that action.

For more information about filtering, refer to Chapter 1, "QoS and IP filtering concepts," on page 21.

This section includes the following topics:

Clearing traffic filter statistics

The **`config ip traffic-filter`** command includes the following options:

`config ip traffic-filter` followed by:	
`info`	Displays which IP traffic filters are set for the `clear-stats` command.
`clear-stats [<fid>]`	Clears filter statistics for the specified filter ID. • *<fid >* is the traffic filter ID range of 1 to 4000.

Creating traffic filters

The **`config ip traffic-filter create`** command allows you to configure source, destination, and global traffic filters for the interface.

The command includes the following options:

`config ip traffic-filter create` followed by:	
`info`	Displays the destination, source, and global filters that have been created (Figure 54).
`destination dst-ip <value> [src-ip <value>] [id <value>]`	Creates a destination filter: • `dst-ip <value>` is the destination IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}. • `src-ip <value>` is the source IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}. • `id <value>` is the traffic filter ID {1..4096}.
`global [src-ip <value>] [dst-ip <value>] [id <value>]`	Creates a global filter: • `src-ip <value>` is the source IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x |default}. • `dst-ip <value>` is the destination IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}. • `id <value>` is the traffic filter ID {1..4096}.
`source src-ip <value> [dst-ip <value>] [id <value>]`	Creates a source filter: • `src-ip <value>` is the source IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}. • `dst-ip <value>` is the destination IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}. • `id <value>` is the traffic filter ID {1..4096}.
`traffic-profile <pid>`	Specifies a traffic profile to use with this traffic filter. • `<pid>` is the profile number {1..64}.

Figure 54 shows sample output for the **`config ip traffic-filter create`** command.

Figure 54 config ip traffic-filter create info command output

```
Passport-8610/config/ip/traffic-filter# create info

Sub-Context: create filter global-set set traffic-profile
Current Context:

                      global : (id 2)
                               src-ip - 0.0.0.0/0.0.0.0
                               dst-ip - 0.0.0.0/0.0.0.0
                      source : not created
                 destination : (id 1)
                               src-ip - 1.2.4.0/255.255.255.0
                               dst-ip - 1.2.3.0/255.255.255.0
              traffic-profile : (id 1)
```

Creating destination traffic filters

The **`config ip traffic-filter create destination dst-ip <value>`** command allows you to configure destination traffic filters for the interface.

The command includes the following options:

`config ip traffic-filter create` followed by:	
`destination dst-ip <value>` `[src-ip <value>]` `[id <value>]`	Creates a destination filter: • `dst-ip <value>` is the destination IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}. • `src-ip <value>` is the source IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}. • `id <value>` is the traffic filter ID {1..4096}.

Figure 55 shows sample configuration output for the **`config ip traffic-filter create destination dst-ip and config ip traffic-filter create source src-ip`** command. The example also shows use of the **`info`** command to display information about the filter.

Creating source traffic-filters

The **`config ip traffic-filter create source src-ip <value>`** command allows you to configure source traffic filters for the interface.

The command includes the following options:

`config ip traffic-filter create` followed by:	
`source src-ip <value> [dst-ip <value>] [id <value>]`	Creates a source filter: • `src-ip <value>` is the source IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}. • `dst-ip <value>` is the destination IP/mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}. • `id <value>` is the traffic filter ID {1..4096}.

Figure 55 shows sample configuration output for the **`config ip traffic-filter create destination dst-ip and config ip traffic-filter create source src-ip`** command. The example also shows use of the **`info`** command to display information about the filter.

Figure 55 config ip traffic-filter create configuration output

```
Passport-8603:3/config/ip/traffic-filter/create# destination
dst-ip 0.0.0.0/0
Destination filter 1 is created.
Passport-8603:3/config/ip/traffic-filter/create# source src-ip
0.0.0.0/0
Source filter 2 is created.
Passport-8603:3/config/ip/traffic-filter/create# info
             Sub-Context:
             Current Context:
             global : not created
             source : (id 2)
             src-ip - 0.0.0.0/0.0.0.0
             dst-ip - 0.0.0.0/0.0.0.0
             destination : (id 1)
             src-ip - 0.0.0.0/0.0.0.0
             dst-ip - 0.0.0.0/0.0.0.0
             traffic-profile : not created
Passport-8603:3/config/ip/traffic-filter# set 300
Passport-8603:3/config/ip/traffic-filter/set/300# create
Passport-8603:3/config/ip/traffic-filter/set/300# add-filter 1
Passport-8603:3/config/ip/traffic-filter/set/300# add-filter 2
Passport-8603:3/config/ip/traffic-filter/set/300# info
             Sub-Context:
             Current Context:
             create :
             name -
             delete : N/A
             add-filter : 1 2
             remove-filter : N/A
Passport-8603:3# config ethernet 2/1
Passport-8603:3/config/ethernet/2/1# ip traffic-filter
Passport-8603:3/config/ethernet/2/1/ip/traffic-filter#
Passport-8603:3/config/ethernet/2/1/ip/traffic-filter# create
Passport-8603:3/config/ethernet/2/1/ip/traffic-filter# add set
300
```

Configuring a specific traffic filter

The **`config ip traffic-filter filter <fid>`** command allows you to set up traffic filters where `<fid>` is the traffic filter ID (1 to 4000).

The command includes the following options:

`config ip traffic-filter filter <fid>` followed by:	
`info`	Displays the settings for the specified filter.
`delete`	Deletes the specified traffic filter.
`name <name>`	Names the filter. • `name <name>` is the IP filter name {string}.

Configuring traffic-filter action parameters

The **`config ip traffic-filter filter <fid> action`** command is used to set action parameters for IP filters by enabling or disabling the filters where `<fid>` is the traffic filter ID (1 to 4000).

The command includes the following options:

`config ip traffic-filter filter <fid> action` followed by:	
`info`	Displays configure actions for the filter (Figure 56).
`mirror <enable|disable>`	Enables or disables the traffic filter mirror option.
`mode <default|forward|drop|forward-to-next-hop>`	Sets the action to occur when a filter is applied. • `default` is the default action. • `forward` forwards the packet. • `drop` drops the packet. • `forward-to-next-hop` forwards the packet to the next-hop router.

config ip traffic-filter filter <*fid*> action followed by:	
`next-hop-forward ip-address <ipaddr>`	Specifies the IP address of the next-hop router to be used by the **`mode forward-to-next-hop`** option. If the next-hop router is unreachable (no ARP resolution is possible), packets that match the filter are forwarded normally unless the **`next-hop-unreachable-drop`** option is enabled (see below).
`next-hop-forward info`	Displays information about the next-hop-forward filter settings.
`next-hop-forward next-hop-unreachable-drop <enable|disable>`	When enabled, specifies that if the next-hop address is unreachable, the packet is dropped.
`statistic <enable|disable>`	Enables or disables the option to collect statistics on the traffic filter. The default setting is disable. If disabled, the **`show ip traffic-filter stats`** command will display zeros for this filter.
`stop-on-match <true|false>`	Stops further filtering if the current filter is applied.
`tcp-connect <enable|disable>`	Enables or disables the traffic filter TCP-connect option, which allows only TCP connections established from within the network (enabled) or allows bidirectional establishment (disabled). The default is disabled.

Figure 56 shows sample output for the **`config ip traffic-filter filter action info`** command output.

Figure 56 config ip traffic-filter filter action info command output

```
Passport-8610/config/ip/traffic-filter# filter 2 action info

Sub-Context: create filter global-set set traffic-profile
Current Context:

                       mode : useDefaultAction
                     mirror : false
                 statistics : disable
              stop-on-match : false
                tcp-connect : false
            traffic-profile : 0
```

Configuring the traffic filter next hop IP address

The **`config ip traffic-filter filter <fid> action next-hop-forward`** command allows you to specify the IP address of the next-hop router to be used by the **`mode forward-to-next-hop`** option. If the next-hop router is unreachable (no ARP resolution is possible), packets that match the filter are forwarded normally unless the **`next-hop-unreachable-drop`** option is enabled (see below).

The **`config ip traffic-filter filter <fid> action next-hop-forward`** command includes the following options:

`config ip traffic-filter filter <fid> action next-hop-forward` followed by:	
`info`	Displays information about the next-hop-forward filter settings.
`ip-address <ipaddr>`	Specifies the IP address of the next-hop router. • `<ipaddr>` is an IP address in dotted-decimal notation.
`next-hop-unreachable-drop <enable | disable>`	When enabled, specifies that if the next-hop address is unreachable, the packet is dropped.

Configuring traffic filter match settings

The **`config ip traffic-filter filter <fid> match`** command allows you to create matching criteria for filters. The commands require a <*fid*> that is the traffic filter ID (1 to 4000).

The command includes the following options:

`config ip traffic-filter filter <fid> match` followed by:	
`info`	Displays the matching settings for the filter (Figure 57).
`ds-field <6-bit dscp> <2-bit reserved>`	Sets the DS field to a specific number. This field is used to specify the match value for the DS field. The user must enter an 8-bit value, which is composed of the 6-bit DSCP and the 2-bit DSCP reserved fields. If the DS field in the incoming packet matches this value, then this filter will be applied to the packet. • *`6-bit dscp`* is a binary number. • *`2-bit reserved`* is a binary number.
`ds-field-enable <enable|disable>`	Enables or disables the traffic filter to match on the DS field set for the traffic filter.
`dst-port <port> [dst-option <value>]`	Sets the TCP/UDP destination port and destination option. • *`port`* is the TCP/UDP destination port to filter on (0 to 65535). • `dst-option <value>` is the TCP/UDP destination port option. {ignore|equal|less|greater|notequal}.
`icmp-request <true | false>`	Enables or disables the traffic filter to match ICMP requests.
`ip-fragment <true | false>`	Enables or disables the traffic filter to allow IP fragments to be filtered.

config ip traffic-filter filter <*fid*> match followed by:	
protocol <*protocoltype*> [<*pid*>]	Sets the protocol type for the filter. • *protocoltype* is {ignore |I CMP | TCP | UDP | vrrp | ospf | ipsec_esp | ipsec_ah | usrDefined}. • <*pid*> is the pid number in decimal {0..255} format that you assign.
src-port <*port*> [src-option <*value*>]	Sets the TCP/UDP source port and source option. • *port* is the TCP/UDP source port to filter on (0 to 65535). • src-option <*value*> is the option {ignore|equal|less|greater|notequal}.

Figure 57 shows sample output for the **config ip traffic-filter filter match info** command.

Figure 57 config ip traffic-filter filter match info command output

```
Passport-8610:6/config/ip/traffic-filter/filter/1/match# info

Sub-Context:
Current Context:

                    ds-field : 001000
           ds-field-reserved : 11
             ds-field-enable : disable
                icmp-request : false
                 ip-fragment : false
                    src-port : 0
                  src-option : ignore
                    dst-port : 0
                  dst-option : ignore
                    protocol : ignore
```

Configuring traffic filters for DiffServ access ports

The **`config ip traffic-filter filter <fid> modify`** command allows you to modify traffic entering DiffServ access ports that meets the traffic filter. The command requires a traffic filter ID <*fid* > between 1 and 4000.

The command includes the following options:

`config ip traffic-filter filter <fid> modify` followed by:	
`info`	Displays the modify settings for the filter (Figure 58).
`dscp <6-bit dscp>`	If you want the DS codepoint (DSCP) modified to another value instead of zero, use this command to specify the value for the DSCP. After entering the binary number, you first must disable and then enable the traffic filter to ensure that it takes effect. • *`6-bit dscp`* is a binary number.
`dscp-enable <enable|disable>`	Enables or disables the traffic filter to modify the DSCP to zero on packets ingressing a DiffServ access port only.
`ieee8021p <integer>`	If you want IEEE 802.1p bits modified to another value instead of zero, use this field to specify the value for the IEEE 802.1p bits. After entering the number, you first must disable and then enable the traffic filter to ensure that it takes effect. • *`integer`* is a number between 0 and 7.
`ieee8021p-enable <enable|disable>`	Enables or disables the traffic filter to modify the IEEE 802.1p bits to zero on packets ingressing a DiffServ access port only.

Note: When you enable a traffic filter to modify either the DSCP or IEEE 802.1p bits, the traffic filter will also modify the other value based on a corresponding value in the QoS ingress tables.

Figure 58 shows sample output for the **config ip traffic-filter filter modify info** command.

Figure 58 config ip traffic-filter filter modify info command output

```
Passport-8610# config ip traffic-filter filter 3 modify# info

Sub-Context:
Current Context:

                    ds-field : 0.0.0.0
              ds-field-enable : disable
                     eee8021p : 0
              eee8021p-enable : disable
```

Configuring global traffic filter settings

The **config ip traffic-filter global-set** command allow you to set a global filter and specify a global set ID <*gsetid*> between 1 and 100.

The command includes the following options:

config ip traffic-filter global-set <*gsetid*> followed by:	
info	Displays the global set characteristics (Figure 59).
add-filter <*fid*>	Adds a global filter to a global set. • <*fid*> is the traffic filter ID range of 1 to 4000.
create [name <*value*>]	Creates a global set. • name <*value*> sets a name to the filter.
delete	Deletes a global set.
remove-filter <*fid*>	Removes a global filter from a global set. • <*fid*> is the traffic filter ID range of 1 to 4000.

Figure 59 shows sample output for the **`config ip traffic-filter global-set info`** command.

Figure 59 config ip traffic-filter global-set info command output

```
Passport-8610/config/ip/traffic-filter# global-set 1 info

Sub-Context: create filter global-set set traffic-profile
Current Context:

                      create :
                                   name -
                      delete : N/A
                  add-filter : 2
               remove-filter : N/A
```

Configuring traffic filter media

To enable IP traffic filter media on the 8000 Series switch, use the following command:

`config ip traffic-filter media <mediaId>`

Note: The range on the media ID number is 3000 to 3127.

The **`config ip traffic-filter media <mediaId>`** command includes the following options:

`config ip traffic-filter media <mediaId>` followed by:	
`info`	Displays information about the traffic filter media (Figure 60).
`create`	Creates IP traffic filter media for a platform or a device. • *`[<platform <value>]`* • *`[device <value>]`*
`delete`	Deletes IP traffic-filter media.
`gateway-ip`	Specifies the IP address of the gateway. • *`<ipaddr>`*
`create`	Creates a multimedia filter.
`delete`	Deletes a multimedia filter.
`gateway-ip`	Specifies gateway IP address.
`name`	Specifies the name of the selected media device.
`statistic`	Enables or disables the display of statistics on the filter.
`stream`	Configures a multimedia filter stream.

Figure 60 shows sample output for the **config ip traffic-filter media info** command. This configuration example uses the above commands to enable IP traffic filter media, assign a filter name, and display information about the traffic filter media.

Figure 60 config ip traffic-filter media command output

```
8610:5# config ip traffic-filter media 3127 create

8610:5/config ip/traffic-filter/media/3127# gateway-ip
67.140.94.222

8610:5/config ip/traffic-filter/media/3127# config ip
traffic-filter media 3127 info
create: platform 0 device 0
gateway IP : 67.140.94.222
name : 3127-none:none
statistics : disable
```

Configuring a traffic filter media stream

To enable IP traffic filter media streams on the 8000 Series switch, use the following command:

config ip traffic-filter media<mediaId> streams <streamId>

This command includes the following options:

config ip traffic-filter media <mediaId> streams <streamId> followed by:	
info	Displays information about the traffic filter media. (Figure 61).
create	Creates a stream for the traffic filter media.
delete	Deletes a stream from the traffic filter media.
gateway-ip	Specifies the IP address of the gateway.
match-dscp	Specifies a 6-bit binary value for the stream. • *<6-bit dscpVal>*

config ip traffic-filter media <mediaId> streams <streamId> followed by:	
`name`	Specifies a name for the stream.
`port-option`	Specifies a port option, either src, dest, or srcDest. • *<src|dst src|dst>*
`ports min`	Specifies the minimum port number. • *<value [max <value>]*
`protocol`	Specifies either a TCP or UDP protocol. • *<udp | tcp>*

Figure 61 shows sample output for the **config ip traffic-filter media stream <*streamId*> info** command. This configuration example uses the above commands to enable IP traffic filter media streams, assign a filter name, and display information about the traffic filter media.

Figure 61 config ip traffic-filter media stream <streamId> command output

```
8610:5# config ip traffic-filter media 3000
8610:5/config/ip/traffic-filter/media/3000# stream 4
8610:5/config/ip/traffic-filter/media/3000/stream/4#
```

Figure 62 shows sample output of filter definitions for some supported media types.

Figure 62 Filter definitions for supported media types sample output

```
CSE1000, I2004
config ip traffic-filter media 3000 create platform 1 device 2
config ip traffic-filter media 3000 stream 1 create
config ip traffic-filter media 3000 stream 1 port-option src
config ip traffic-filter media 3000 stream 1 ports min 5000 max
5000
config ip traffic-filter media 3000 stream 1 stream-type signal

BCM, I2004
config ip traffic-filter media 3001 create platform 4 device 2
config ip traffic-filter media 3001 stream 1 create
config ip traffic-filter media 3001 stream 1 port-option src
config ip traffic-filter media 3001 stream 1 ports min 5000 max
5000
config ip traffic-filter media 3001 stream 1 stream-type signal
config ip traffic-filter media 3001 stream 2 create
config ip traffic-filter media 3001 stream 2 ports min 51000 max
52000
BCM, TPS
config ip traffic-filter media 3002 create platform 4 device 4
config ip traffic-filter media 3002 stream 1 create
config ip traffic-filter media 3002 stream 1 port-option dst
config ip traffic-filter media 3002 stream 1 ports min 7000 max
7000
config ip traffic-filter media 3002 stream 1 stream-type signal

BCM, Voice Gateway
config ip traffic-filter media 3003 create platform 4 device 5
config ip traffic-filter media 3003 stream 1 create
config ip traffic-filter media 3003 stream 1 ports min 28000 max
28255
config ip traffic-filter media 3003 stream 2 create
config ip traffic-filter media 3003 stream 2 port-option dst
config ip traffic-filter media 3003 stream 2 ports min 1720 max
1720
config ip traffic-filter media 3003 stream 2 protocol tcp
config ip traffic-filter media 3003 stream 2 stream-type signal
config ip traffic-filter media 3003 stream 3 create
config ip traffic-filter media 3003 stream 3 ports min 1719 max
1719
```

Configuring a traffic filter source/destination set

The **`config ip traffic-filter set`** command allows you to configure the source/destination set where *`setid`* is the set ID (300 to 1000). Only source/destination filters can be added to this set. You cannot add a global filter to it.

The command includes the following options:

`config ip traffic-filter set <setid>` followed by:	
`info`	Displays the filter set characteristics (Figure 63).
`add-filter <fid>`	Adds a filter to a filter set. • *`fid`* is the traffic filter ID range of 1 to 4000.
`create [name <value>]`	Creates a filter set. • `name <value>` is the set name {string}.
`delete`	Deletes a filter set.
`remove-filter <fid>`	Removes a filter from a filter set. • *`fid`* is the traffic filter ID range of 1 to 4000.

Figure 63 shows sample output for the **`config ip traffic-filter set info`** command output.

Figure 63 config ip traffic-filter set info command output

```
Passport-8610/config/ip/traffic-filter# set 301 info

Sub-Context: create filter global-set set traffic-profile
Current Context:

                     create :
                                 name -
                     delete : N/A
                 add-filter :
              remove-filter : N/A
```

Configuring traffic filter rate-limiting profiles

The **`config ip traffic-filter traffic-profile <pid>`** command allows you to set rate limiting profiles to police traffic streams. This command uses a Profile ID <*pid*> between 1 and 64.

The command includes the following options:

`config ip traffic-filter traffic-profile <pid>` followed by:	
`info`	Displays the traffic profile settings (Figure 64).
`average-rate <int>`	Sets the traffic profile's average rate. See "Implementing rate limiting in the Passport 8000 switch" on page 180" for more information. • *int* is the rate {0..65535}, which is expressed in 64-byte segments of data allowed in a 2.5 millisecond timeslot.
`delete`	Deletes the traffic profile.
`discard-out-profile <enable|disable>`	Enables or disables the ability to discard the traffic that violates the traffic profile's average rate.
`enable <true|false>`	Enables or disables the traffic profile.
`in-dscp <value>`	Marks traffic that conforms to the average rate in the traffic profile. • *value* is the DSCP expressed as a 6-bit binary number.
`name <name>`	Names the traffic profile. • *name* is a string of 0 to 32 characters.
`out-dscp <value>`	Marks traffic that falls outside the traffic profile's average rate. • *value* is the DSCP expressed as a 6-bit binary number.
`translate-dscp <enable | disable>`	Enables or disables remarking of traffic as either `in-dscp` or `out-dscp`. This command must be enabled for any traffic to be marked.

Implementing rate limiting in the Passport 8000 switch

The Passport 8000 switch performs QoS rate metering every 2.5 milliseconds, in increments of 64 bytes. Table 34, Table 35, and Table 36 present the measured line rates, in multiples of 64, for the three Ethernet speeds tested, with the expected results. The rates were obtained using a source/destination filter. Refer to Chapter 1, "QoS and IP filtering concepts," on page 21 for more information about rate metering.

The three tables illustrate the effective throughput in megabits per second (Mb/s) for various traffic flows using different rate limiting values. All traffic loads are at 100% of interface speed, using fixed-sized packets of the size indicated (in bytes). Using these tables, you can determine the appropriate average rate value for the metering rate that you desire.

The Target Average Rate for each interface type is shown, in increments of 10% of total interface speed, to help you determine the appropriate average-rate value to use for that interface. The actual throughput rate typically differs slightly from the target rate as illustrated. For example, to configure a traffic profile with an average rate limit of 50% of a 100 Mb/s interface (or 50 Mb/s), enter 250 in the `average-rate` field in the CLI. Traffic is then limited to between 51.23 Mb/s and 53.47 Mb/s, depending on the size of the packets.

Table 34 10 Mb/s Ethernet line rate metering

average-rate <int>										
	5	**10**	**15**	**20**	**25**	**30**	**35**	**40**	**45**	**50**
Packet size in (bytes)	**10%***	**20%**	**30%**	**40%**	**50%**	**60%**	**70%**	**80%**	**90%**	**100%**
64	1.03†	2.05	3.08	4.10	5.12	6.15	7.17	7.62	7.62	7.62
128	1.23	2.05	3.28	4.10	5.33	6.15	7.38	8.20	8.65	8.65
256	1.64	2.46	3.28	4.10	5.74	6.56	7.38	8.19	9.28	9.28
512	1.64	3.28	3.28	4.92	6.56	6.56	8.20	8.20	9.62	9.62
1024	3.28	3.28	3.28	6.56	6.56	6.56	9.81	9.81	9.81	9.81
1518	4.86	4.86	4.86	4.86	9.72	9.72	9.72	9.72	9.72	9.87

* target average percentage of line rate

† rate in megabits per second

Table 35 100 Mb/s Ethernet line rate metering

average-rate <int>										
	50	**100**	**150**	**200**	**250**	**300**	**350**	**400**	**450**	**500**
Packet size in (bytes)	**10%**	**20%**	**30%**	**40%**	**50%**	**60%**	**70%**	**80%**	**90%**	**100%**
64	10.25	20.49	30.74	40.99	51.23	61.15	71.72	76.19	76.19	76.19
128	10.25	20.49	30.74	40.99	51.24	61.48	71.72	81.97	86.49	86.49
256	10.66	20.47	31.11	40.93	51.58	61.40	72.04	81.97	92.62	92.75
512	11.48	21.32	31.15	40.99	52.46	62.29	72.13	81.97	93.44	96.24
1024	13.12	22.96	32.80	42.63	52.46	62.30	72.13	81.97	95.08	98.08
1518	14.58	24.31	34.02	43.75	53.47	68.05	77.77	87.49	97.20	98.70

Table 36 Gigabit Ethernet line rate metering

average-rate <int>										
	500	**1000**	**1500**	**2000**	**2500**	**3000**	**3500**	**4000**	**4500**	**5000**
Packet size in (bytes)	**10%**	**20%**	**30%**	**40%**	**50%**	**60%**	**70%**	**80%**	**90%**	**100%**
64	102.50	205.00	307.47	409.93	446.61	446.61	446.61	446.61	446.61	446.61
128	102.50	204.93	307.43	409.95	512.38	614.80	717.24	819.67	922.11	927.54
256	102.49	204.96	307.43	409.95	512.38	614.80	717.24	819.67	922.11	927.54
512	103.32	204.99	308.30	409.86	513.13	614.79	718.07	819.68	922.93	962.41
1024	104.92	206.57	308.23	409.96	514.85	616.45	718.07	819.68	924.57	980.84
1518	106.93	213.89	320.90	422.93	529.87	636.78	743.68	845.72	952.62	986.99

Figure 64 shows sample output for the **`config ip traffic-filter traffic-profile info`** command.

Figure 64 config ip traffic-filter traffic-profile info command output

```
Passport-8610:5# config ip traffic-filter traffic-profile 1 info

Sub-Context: clear config dump monitor show test trace
Current Context:

                        name : test
                      enable : true
             translate-dscp : disable
                    in-dscp : 000000
                   out-dscp : 000000
        discard-out-profile : enable
               average-rate : 0
```

Configuring Ethernet IP traffic filter commands

This section describes Ethernet IP traffic filter commands, and includes the following topics:

Configuring traffic filters on a port

The **`config ethernet <ports> ip traffic-filter`** command allows you to set filters at the port level to manage traffic. Each filter set includes match conditions and actions to be performed when a match condition is satisfied. This command includes *<ports>* as the port list {slot/port[-slot/port][,...]}.

`config ethernet <ports> ip traffic-filter` followed by:	
`info`	Displays the traffic filters applied to the port.
`add set <value>`	Adds a set filter to a port. • *<value>* is the global or source/destination filter set ID (1 to 1000).
`create`	Creates a traffic filtering entity on a port.
`delete`	Removes filtering from a port.
`disable`	Disables filtering on a port. **Note:** Whenever you change a filter parameter, you must first disable the filter on its filter ports and then enable the filter again to reapply the changed filter to the ports.
`enable`	Enables filtering on a port. **Note:** Whenever you change a filter parameter, you must first disable the filter on its filter ports and then enable the filter again to reapply the changed filter to the ports.
`remove set <value>`	Removes a filter set from a port. • *<value>* is the filter set ID (1 to 1000).

For more detailed information about the specific forward/drop behavior of a port, refer to Chapter 1, “QoS and IP filtering concepts,” on page 21.

Configuring forward/drop action on a port traffic filter

The **`config ethernet <ports> ip traffic-filter default-action`** command allows you to set the port filter default action to forward and drop. It also displays port default action configuration.

The command includes the following options:

`config ethernet <ports> ip traffic-filter default-action` followed by:	
`info`	Displays the port default action configuration.
`forward`	Sets the port filter default action to forward.
`drop`	Sets the port filter default action to drop.
`none`	Does not apply any policy to filtered ports.

Configuring multimedia on a port traffic filter

To assign an ethernet slot/port for a multimedia filter on the 8000 Series switch, use the following command:

The **`config ethernet <ports> multimedia`** command includes the following options:

`config ethernet <ports> multimedia` followed by:	
`info`	Displays information on the multimedia ethernet ports (Figure 65).
`disable`	Disables a multimedia ethernet port.
`enable`	Enables a multimedia ethernet port.
`select <select>`	Selects a multimedia ethernet port.

Figure 65 shows sample output for the **`config ethernet <ports> multimedia`** command.

Figure 65 config ethernet <ports> multimedia command output

```
8610:5# config eth 2/1 multimedia
8610:5#
```

Showing ip traffic filter commands

The section describes show ip traffic filter commands, and includes the following topics:

Showing the active traffic filters

To display the list of active filters, use the following command:

```
show ip traffic-filter active
```

Showing traffic filter source and destination(s)

To display the source and destination(s) for the active destination traffic filter(s), use the following command:

```
show ip traffic-filter destination [<fid>]
```

If you enter a filter ID *<fid>*, the switch displays data for the specific filter; otherwise, all filters are shown.

Figure 66 shows sample output for the **show ip traffic-filter destination** command for one filter ID.

Figure 66 show ip traffic-filter destination command output

```
Passport-8610# show ip traffic-filter destination

================================================================================
                 Ip Traffic-filter Destination Filters
================================================================================

ID  NAME            TYPE            SRC_OPTION DST_OPTION PROTOCOL   MIRROR
1                   destination     ignore     ignore     ignore     false

DST_ADDR        DST_MASK        DSTPT SRC_ADDR        SRC_MASK        SRCPT
    0.0.0.0         0.0.0.0         0     0.0.0.0         0.0.0.0         0

    TCPCONNECT      MODE            STOP_ON_MATCH
    false           useDefaultAction true

    DS_MT_DS_FIELD  DS_MT_DS_RSVED  DS_MD_8021P     DS_MD_DSCP
    000000          00:disable      0:enable        100011:enable

    DS_PRO_ID       M_ICMP_REQ      M_IP_FRAG       STATISTICS
    0               false           false           disable
```

Showing disabled traffic filters

To display information about the disabled filters on the switch, use the following command:

`show ip traffic-filter disabled [<ports>]`

If port numbers are entered, information is displayed only for those ports.

Figure 67 shows sample output for the **`show ip traffic-filter disabled`** command for all ports.

Figure 67 show ip traffic-filter disabled command output

```
Passport-8606:6# show ip traffic-filter disable

================================================================================
                                      Ip Traffic-filter Disable List
================================================================================

port 1/1 :
         Access List : Id 300 : Base

ID  NAME           TYPE           SRC_OPTION DST_OPTION PROTOCOL        MIRROR
3   src-3          source          ignore     ignore     ignore          false

    DST_ADDR       DST_MASK        DSTPT SRC_ADDR       SRC_MASK        SRCPT
    0.0.0.0        0.0.0.0          0     201.0.0.0       255.255.255.0   0

    TCPCONNECT     MODE                  STOP_ON_MATCH
    false          useDefaultAction      true

    DS_MT_DS_FIELD DS_MT_DS_RSVED DS_MD_8021P     DS_MD_DSCP
    000000         00:disable     0:disable       000000:disable

    DS_PRO_ID      M_ICMP_REQ     M_IP_FRAG       STATISTICS
    0              false          false           disable


    N_H_FORWARD_IP N_H_UNREACHABLEDROPE
```

Showing enabled traffic filters

To display information about the enabled filters on the switch or on a specified port, use the following command:

```
show ip traffic-filter enabled [<ports>]
```

Figure 68 shows sample output for the **show ip traffic-filter enabled** command for all ports.

Figure 68 show ip traffic-filter enabled command output

```
Passport-8606:6# show ip traffic-filter enabled

================================================================================
                                      Ip Traffic-filter Disable List
================================================================================

port 1/11 :
         Access List : Id 300 : Base

ID  NAME           TYPE           SRC_OPTION DST_OPTION PROTOCOL        MIRROR
3   src-3          source          ignore     ignore     ignore          false

    DST_ADDR       DST_MASK       DSTPT SRC_ADDR       SRC_MASK        SRCPT
    0.0.0.0        0.0.0.0         0     201.0.0.0       255.255.255.0   0

    TCPCONNECT     MODE                  STOP_ON_MATCH
    false          useDefaultAction      true

    DS_MT_DS_FIELD DS_MT_DS_RSVED DS_MD_8021P     DS_MD_DSCP
    000000         00:disable     0:disable       000000:disable

    DS_PRO_ID      M_ICMP_REQ     M_IP_FRAG       STATISTICS
    0              false          false           disable


    N_H_FORWARD_IP N_H_UNREACHABLEDROPE
```

Showing global traffic filters

To display global filters for the switch or for the specified filter IDs, use the following command:

```
show ip traffic-filter global [<fid>]
```

Figure 69 shows sample output for the **`show ip traffic-filter global`** command.

Figure 69 show ip traffic-filter global command output

```
Passport-8606:6# show ip traffic-filter global

================================================================================
                                    Ip Traffic-filter Global Filters
================================================================================

ID  NAME            TYPE            SRC_OPTION DST_OPTION PROTOCOL        MIRROR
8   global-8        global           ignore     ignore     ignore          false

    DST_ADDR        DST_MASK        DSTPT SRC_ADDR        SRC_MASK        SRCPT
    0.0.0.0          0.0.0.0         0     0.0.0.0          0.0.0.0         0

    TCPCONNECT      MODE                  STOP_ON_MATCH
    false           useDefaultAction      true

    DS_MT_DS_FIELD  DS_MT_DS_RSVED  DS_MD_8021P     DS_MD_DSCP
    000000          00:disable      0:disable       000000:disable

    DS_PRO_ID       M_ICMP_REQ      M_IP_FRAG       STATISTICS
    0               false           false           disable

    N_H_FORWARD_IP  N_H_UNREACHABLEDROPE
    0.0.0.0         false
```

Showing traffic filter interface information

To display information about the traffic filter interface for the switch or for specified ports, use the following command:

```
show ip traffic-filter interface <ports>
```

Figure 70 shows sample output for the **show ip traffic-filter interface** command for port 9/2.

Figure 70 show ip traffic-filter interface command output

```
Passport-8606# show ip traffic-filter interface 9/2

============================================================
             Ip Traffic-filter Interface
============================================================

                       IfIndex : 577
                 FilterListSize : 1
                     FilterList : 301
                         Enable : false
                  DefaultAction : none
```

Showing traffic filter media information

To display the media platforms and devices by filter ID, use the following command:

```
show ip traffic-filter media
```

Figure 71 shows sample output for the **show ip traffic-filter media** command for one filter ID.

Figure 71 show ip traffic-filter media command output

```
Passport-8606:6# show ip traffic-filter media

================================================================================
                                      Multimedia Platforms & Devices
================================================================================
  Id                                Name Platform Device      Gateway-IP  Stat
--------------------------------------------------------------------------------
3000                                  m1    CSE1K   none         0.0.0.0   dis

         Num. of entries  : 1

         MLcard : MeridianLineCard
         MTcard : MeridianTrunkCard
         VG     : Voice Gateway
         ena    : Enable      dis  : Disable
```

Showing active source traffic filter information

To display information about the active source traffic filter, use the following command:

`show ip traffic-filter source [<fid>]`

Figure 72 shows sample output for the **`show ip traffic-filter source`** command for one filter ID.

Figure 72 show ip traffic-filter source command output

```
Passport-8606:6# show ip traffic-filter source

================================================================================
                                    Ip Traffic-filter Source Filters
================================================================================

ID  NAME            TYPE            SRC_OPTION DST_OPTION PROTOCOL        MIRROR
3   src-3           source           ignore     ignore     ignore          false

    DST_ADDR        DST_MASK        DSTPT SRC_ADDR        SRC_MASK        SRCPT
    0.0.0.0         0.0.0.0          0     201.0.0.0       255.255.255.0   0

    TCPCONNECT      MODE                  STOP_ON_MATCH
    false           useDefaultAction      true

    DS_MT_DS_FIELD  DS_MT_DS_RSVED  DS_MD_8021P     DS_MD_DSCP
    000000          00:disable      0:disable       000000:disable

    DS_PRO_ID       M_ICMP_REQ      M_IP_FRAG       STATISTICS
    0               false           false           disable

    N_H_FORWARD_IP  N_H_UNREACHABLEDROPE
    0.0.0.0         false
```

Showing traffic filter streams

To display the media platforms and devices by filter ID, use the following command:

```
show ip traffic-filter stream
```

Figure 73 shows sample output for the **`show ip traffic-filter stream`** command.

Figure 73 show ip traffic-filter stream command output

```
8610:5/show/ip/traffic-filter# stream

            ========================================================
            ====================

            Multimedia Streams

            ========================================================
            ====================

MId    SId Name            Proto  Port-range    Option    Type   MaDSCP
ReDSCP
-----------------------------------------------------------------
3000   1   CSE1000Stream    tcp    80 - 81       src-dst   media  000000
101110
```

Showing traffic filter statistics

To display the filter ID and counter information for all filters or the specified filter ID that have statistics gathering enabled, use the following command:

`show ip traffic-filter stats [<fid>]`

Figure 74 shows sample output for the **`show ip traffic-filter stats`** command.

Figure 74 show ip traffic-filter stats command output

```
8610:5/show/ip/traffic-filter# stats

            ========================================================
            ====================

                  Ip Traffic-filter Stats

            ========================================================
            ====================
```

Showing ip traffic-filter info commands

The section describes show ip traffic-filter info commands, and includes the following topics:

Showing traffic filter global-set information

To display information about the specified global filter list or all global filter lists configured on the switch, use the following command:

```
show ip traffic-filter info global-set [<id>]
```

Figure 75 shows sample output for the **`Show ip traffic-filter info global-set`** command.

Figure 75 show ip traffic-filter info global-set command output

```
Passport-8606# show ip traffic-filter info global-set 1

================================================================================
                        Ip Traffic-filter Global List
================================================================================

ID    NAME                 LIST_SIZE  FILTER_ID_LIST
--------------------------------------------------------------------------------
1                          1          2
```

Showing traffic filter set information

To display information for the specified source/destination filter list or all source/destination filter lists, use the following command:

```
show ip traffic-filter info set [<id>]
```

Figure 76 shows sample output for the **show ip traffic-filter info set** command.

Figure 76 show ip traffic-filter info set command output

```
Passport-8606# show ip traffic-filter info set

================================================================================
                        Ip Traffic-filter Base List
================================================================================

ID    NAME                  LIST_SIZE  FILTER_ID_LIST
--------------------------------------------------------------------------------
301                         0
```

Showing traffic filter traffic-profile information

To display the traffic profile settings, use the following command:

`show ip traffic-filter traffic-profile info [<id>]`

Figure 77 shows sample output for the **show ip traffic-filter traffic-profile info** command.

Figure 77 show ip traffic-filter traffic-profile command output

```
Passport-8610:5/show/ip/traffic-filter/traffic-profile# info

================================================================================
                        Ip Traffic-filter Profile
================================================================================

ID  NAME       ENABLE     TRANS_DSFIELD   IN_DSFIELD      OUT_DSFIELD
1              true       enable          11111111 11111111

    DISCARD_OUT_PROFILE   AVERAGE_RATE
    enable                0
```

Index

E

F

G

I

L

M

N

O

P

Q

R

S

T

U

V