Nortel Ethernet Routing Switch 8600

Configuration — QoS and IP Filtering for Classic Modules

Release: 5.0
Document Revision: 01.04

www.nortel.com

NN46205-508 316433-F Rev 04

Nortel Ethernet Routing Switch 8600
Release: 5.0
Publication: NN46205-508
Document release date: 21 April 2009

Printed in Canada, India, and the United States of America
LEGAL NOTICE

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

ATTENTION

For information about the safety precautions, read "Safety messages" in this guide.

For information about the software license, read "Software license" in this guide.

Contents

New in this release

The following sections detail what’s new in *Nortel Ethernet Routing Switch 8600 Configuration — QoS and IP Filtering for Classic Modules* (NN46205-508) for Release 5.0:

- “Features” (page 5)
- “Other changes” (page 5)

Features

See the following section for information about feature changes:

Nortel Command Line Interface

The Nortel Ethernet Routing Switch 8600 Release 5.0 uses the Nortel command line interface (NNCLI). See *Ethernet Routing Switch 8600 User Interface Fundamentals* (NN46205-308) and the NNCLI chapters in this document.

Other changes

For information about changes that are not feature-related, see the following sections:

Document changes

This document is modified to meet Nortel Customer Documentation Standards. For more information about these standards, see *Ethernet Routing Switch 8600 Documentation Roadmap* (NN46205-103) .

Configuration examples

Configuration examples are moved to the*Filters and QoS Technical Configuration Guide*. You can find this Technical Configuration Guide at www.nortel.com/documentation. Choose Routers & Routing Switches, and then Ethernet Routing Switch 8600. The following examples are moved:

- IP filter on the Ethernet Routing Switch 8600
- DiffServ trusted or untrusted interfaces
- Classifying port traffic for port-based VLAN

- Classifying and policing traffic
- Marking and dropping traffic based on port-range
- Forward-to-next-hop filtering

QoS Configuration using the CLI

QoS Configuration using the CLI information is added. See “Configuring Layer 3 trusted/untrusted ports” (page 69).

Statistics

Statistics information is moved to *Nortel Ethernet Routing Switch 8600 Performance Management* (NN46205-704) .

Source and Destination filters

This document is up-issued to include the addition of an attention in the section *Source and Destination filters* to reflect that Source Destination IP Filters will not work for Multicast Traffic, only Global Filters can be used to filter.

Safety messages

This section describes the different precautionary notices used in this document. This section also contains precautionary notices that you must read for safe operation of the Nortel Ethernet Routing Switch 8600.

Notices

Notice paragraphs alert you about issues that require your attention. The following sections describe the types of notices.

Attention notice

ATTENTION
An attention notice provides important information regarding the installation and operation of Nortel products.

Caution ESD notice

CAUTION
ESD
ESD notices provide information about how to avoid discharge of static electricity and subsequent damage to Nortel products.

CAUTION
ESD (décharge électrostatique)
La mention ESD fournit des informations sur les moyens de prévenir une décharge électrostatique et d’éviter d’endommager les produits Nortel.

CAUTION
ACHTUNG ESD
ESD-Hinweise bieten Information dazu, wie man die Entladung von statischer Elektrizität und Folgeschäden an Nortel-Produkten verhindert.

CAUTION
PRECAUCIÓN ESD (Descarga electrostática)
El aviso de ESD brinda información acerca de cómo evitar una descarga de electricidad estática y el daño posterior a los productos Nortel.

CAUTION
CUIDADO ESD
Os avisos do ESD oferecem informações sobre como evitar descarga de eletricidade estática e os conseqüentes danos aos produtos da Nortel.

CAUTION
ATTENZIONE ESD
Le indicazioni ESD forniscono informazioni per evitare scariche di elettricità statica e i danni correlati per i prodotti Nortel.

Caution notice

CAUTION
Caution notices provide information about how to avoid possible service disruption or damage to Nortel products.

CAUTION
ATTENTION
La mention Attention fournit des informations sur les moyens de prévenir une perturbation possible du service et d’éviter d’endommager les produits Nortel.

CAUTION
ACHTUNG
Achtungshinweise bieten Informationen dazu, wie man mögliche Dienstunterbrechungen oder Schäden an Nortel-Produkten verhindert.

CAUTION
PRECAUCIÓN
Los avisos de Precaución brindan información acerca de cómo evitar posibles interrupciones del servicio o el daño a los productos Nortel.

CAUTION
CUIDADO
Os avisos de cuidado oferecem informações sobre como evitar possíveis interrupções do serviço ou danos aos produtos da Nortel.

CAUTION

ATTENZIONE

Le indicazioni di attenzione forniscono informazioni per evitare possibili interruzioni del servizio o danni ai prodotti Nortel.

Software license

This section contains the Nortel Networks software license.

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

1. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer

software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

2. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.
3. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer’s use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.
4. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.
5. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.
6. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Introduction

This guide provides instructions for using the command line interface (CLI), the Nortel command line interface (NNCLI), and Device Manager to configure Quality of Service (QoS) and filtering operations functions on the Ethernet Routing Switch 8600 Classic modules. For instructions about configuring QoS and filtering for R and RS modules, see *Ethernet Routing Switch 8600 Configuration – QoS and IP Filtering for R and RS Modules* (NN46205-507) .

Navigation

QoS fundamentals

Use the information in this section to help you understand Quality of Service (QoS).

This section describes a range of features that you can use with the Ethernet Routing Switch 8600 to allocate network resources to critical applications. You can configure your network to prioritize specific types of traffic to ensure traffic receives the appropriate QoS level. Allocate priority to protocol and application data depending on required parameters, for example, minimum data rate or minimum time delay.

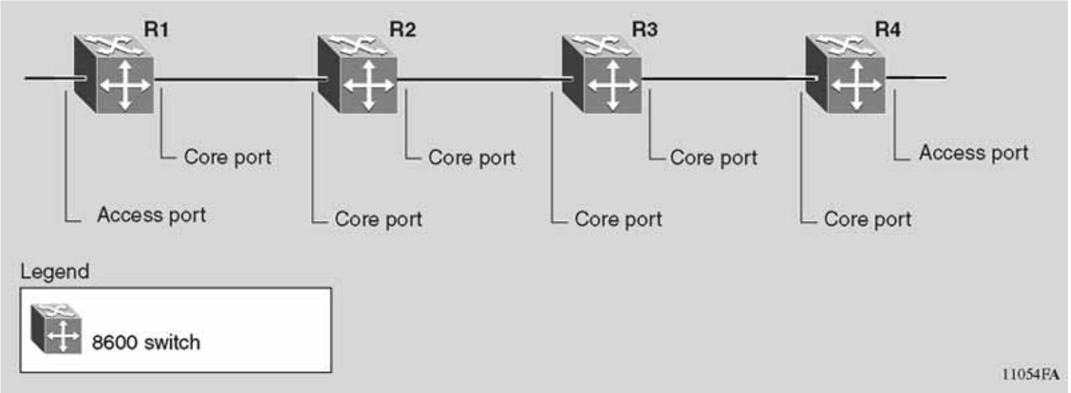
For information about how to use the command line interface (CLI), the Nortel Command Line Interface (NNCLI), and Device Manager, see *Ethernet Routing Switch 8600 Fundamentals — User Interfaces* (NN46205-308) .

Navigation

Introduction to QoS

Quality of Service (QoS) can be defined as the extent to which a service delivery meets user expectations. In a QoS-aware network, a user can expect the network to meet certain performance expectations. These performance expectations are specified in terms of service availability, packet loss, packet delay, and packet delay variation.

Figure 1
Access and core port



By assigning QoS levels to traffic flows on your Local Area Network (LAN), 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 in the network: across different devices, such as routers, switches, and end stations; across platforms and media; and across link layers, such as Ethernet.

The Ethernet Routing Switch 8600 supports QoS classification for both L2 (802.1p bits) and L3 (Differentiated Services Code Point bits) parameters. The Ethernet Routing Switch 8600 provides QoS functionality that can differ for both Layer 2 (bridged) and Layer 3 (routed) traffic flows. The Ethernet Routing Switch 8600 can also assign QoS levels based on multiple criteria including (but not limited to) Transport Control Protocol (TCP) or User Datagram Protocol (UDP) ports used by an application.

To effectively use QoS functions in your network, you must

- Identify traffic sources and types.
- Determine the required QoS parameters based on the traffic to be carried.
- Perform traffic management (QoS) operations based on the required parameters.

QoS functionality for IP traffic is implemented on the Ethernet Routing Switch 8600 through a Differentiated Services (DiffServ) network architecture.

QoS for R and Classic modules

Release 5.0 contains three QoS implementations:

- The pre-4.0 implementation that involves E and M modules (Classic modules).
- Beginning with Release 4.0, an implementation that uses specific R module features and includes support for the 8630GBR, 8648GTR, 8683XLR, and 8683XZR modules.
- Beginning with Release 5.0, an implementation for RS modules that performs all features of R modules, and offers advanced policing capabilities.

R mode is not required for many of the advanced QoS features of the R module implementation. However, you must enable R mode to enable Feedback Output Queueing. For more information, see *Ethernet Routing Switch 8600 Configuration — QoS and IP Filtering for R and RS Modules* (NN46205-507) .

The following table shows the differences in the level of support for the Classic and Advanced QoS implementations.

In this table, E denotes enabled, D denotes disabled, and N/A denotes not applicable. CLAS denotes Classic and ADV denotes advanced. 32K, 128K, and 256K denote the number of records in kilobytes supported for each mode.

Table 1
Features supported for each operation mode for Classic and R series modules

Chassis config	**Mode**	**Module type**			**Features supported on respective modules**			
		R	**M**	**E**	**QoS**	**Filters**	**Policing**	**Shaping**
Same- module chassis	Default (32K)	—	—	E	CLAS	CLAS	CLAS	N/A
	M (128K)	—	E	—	CLAS	CLAS	CLAS	N/A
	R (256K)	E	—	—	ADV	ADV	ADV	ADV
Mixed- module chassis	Default (32K)	E	E	E	CLAS (ADV on R module); no FOQ	CLAS (ADV on R module)	CLAS (ADV on R module)	ADV on R module
	M (128K)	E	E	D	CLAS (ADV on R module); no FOQ	CLAS (ADV on R module)	CLAS (ADV on R module)	ADV on R module
	R (256K)	E	D	D	ADV; FOQ	ADV	ADV	ADV

A same-module configuration means the chassis contains:

- all R modules with the 8692 SF/CPU (switch fabric/CPU module)
- all Classic (E and M) modules with 8692 SF/CPU, or 8690 or 8691 SF/CPU

A mixed-module configuration means the chassis contains Classic modules and R modules with the 8692 SF/CPU.

In a mixed-module chassis configuration that operates in either Default or M mode, the following features are available only on R modules:

- advanced QoS with bandwidth reservation capabilities
- two-rate three-color-marker ingress policing
- egress shaping: port or queue-based
- advanced ingress and egress Access Control Lists (ACL)
- Split Multilink Trunking (SMLT) and InterSwitch Trunking (IST) on 10 Gbit/s ports

An all-R module chassis configuration that operates in R mode includes all the features previously listed and provides:

- Feedback Output Queueing (FOQ)
- high scaling; for more information, see the latest Ethernet Routing Switch 8600 Release Notes

If R mode is enabled, E, and M modules are disabled. If M mode is enabled and one or more modules installed in the chassis is an E module, the E modules are disabled. This action protects the system forwarding database from inconsistencies.

You can configure up to 128 MultiLink Trunking (MLT) groups, and up to 8 Equal Cost Multi-Path (ECMP) routing paths. These features, like FOQ, are available only when the chassis contains only R modules, and R mode is enabled.

Enhanced Operational Mode increases virtual local area network (VLAN) MLT scalability. Use Enhanced Operational Mode to provide up to 1980 MLT VLANs. For more information about Enhanced Operational Mode, VLANs, and VLAN scalability, see *Ethernet Routing Switch 8600 Configuration — VLANs and Spanning Tree* (NN46205-517) .

R series modules support both ingress and egress filtering through the use of ACLs. Classic filters can only filter at ingress.

QoS and filters

The Ethernet Routing Switch 8600 has many functions you can use to provide appropriate QoS levels to traffic on a per-customer basis. These include egress-queue-set-based shapers, port-based shapers, DiffServ access or core port settings, policy-based policers, and port-based policers. The Ethernet Routing Switch 8600 also provides Classic (E and M modules) and Advanced (for R series modules—ACL-based) filters. You do not have to use filters to provide QoS; however, filters aid in prioritizing customer traffic. Filters also provide protection by blocking unwanted traffic.

Policers are applied at ingress; Classic or ACL-based filters are applied next; and shapers are applied at egress.

DiffServ networks

DiffServ divides traffic into different classes (behavior aggregates) to give each class differentiated treatment.

A DiffServ network allows either end-to-end or intradomain QoS functionality by implementing classification and mapping functions at the network boundary or access points. Within a core) network, DiffServ regulates packet behavior by this classification and mapping.

DiffServ, as defined by RFC 2475, provides QoS for aggregate traffic flows [as opposed to individual traffic flows, which use an Integrated Services architecture (IntServ—RFC 1633)]. DiffServ provides QoS by using traffic management and conditioning functions (packet classification, marking, policing, and shaping) on network edge devices, and by using Per-Hop Behaviors (PHB), which includes queueing and dropping traffic, on network core devices. The Ethernet Routing Switch can perform all of these QoS functions. The order of DiffServ operations for a packet is:

- packet classification— IEEE 802.1p, EXP-bit, and DSCP markings are used to classify (map) the packet to its appropriate PHB and QoS level,
- policing—packets are rate-limited and colored; excessive traffic can be dropped or re-marked,
- re-marking—packets can be re-marked according to QoS actions configured into the switch (internal QoS mappings),
- shaping—packets are delayed and transmitted to produce an even and predictable flow rate. The Ethernet Routing Switch 8600 provides both queue-based and port-based shaping. Egress queue shaping provides shaping for each queue; port-based shaping shapes all outgoing traffic to a specific rate.

Although filters are not required for QoS operation, you can use filters to provide traffic management actions. Ingress filters are applied after policing and egress filters are applied before shaping.

Packet classification, marking, and mapping

Traffic classification includes functions that examine a packet to determine further actions according to defined rules. Classification involves identifying flows so that the router can modify the packet contents or PHB, apply conditioning treatments to the packet, and determine how to forward the packet to the egress interface. Packet classification depends on the service type of the packet and the point in the traffic management process where the classification occurs.

Traffic is classified as it enters the DiffServ network, and is assigned appropriate PHB based on the classification. To differentiate between classes of service, the DiffServ (DS) parameter in the IP packet header, as defined in RFC 2474 and RFC 2475, is marked. The DSCP is marked to define the forwarding treatment of 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 DSCP-to-forwarding behaviors and DSCP re-markings. Re-marking the DSCP allows the treatment of packets to be reset based on new network specifications or desired levels of service.

Layer 3 marking involves the DSCP parameter. Layer 2 (Ethernet) marking involves the 802.1p-bit parameter.

For Layer 2 packets, priority bits (or 802.1p bits) define the traffic priority of the Ethernet packet. You can configure an Ethernet interface to map DSCP to 802.1p bits on egress traffic and to map 802.1p bits to DSCP on ingress traffic. Ethernet VLAN QoS requirements are met through 802.1p bit mapping, which is needed to assess the 802.1p bit and to derive an appropriate DSCP.

Within the network, a packet PHB associated with the DSCP determines how a device forwards the packet to the next hop—if at all. Consequently, nodes can allocate buffer and bandwidth resources to each competing traffic stream. The initial setting of the DSCP is based on network policies that are based on the type of service required. The objective of DSCP-to-NNSC mapping is to translate the QoS characteristics defined by the packet DSCP marker to a Nortel Networks Service Class (NNSC). The DSCP-to-NNSC mapping occurs at ingress. For each received packet, the mapping function assigns an NNSC.

The Ethernet Routing Switch maintains six mapping tables. These tables translate the ingress 802.1p-bit, EXP-bit, or DSCP markings to an internal QoS level, and then re-translate the internal QoS level to an egress DSCP, EXP-bit, or 802.1p-bit markings, as follows:

- Ingress 802.1p-bit to QoS level
- Ingress DSCP to QoS level
- Ingress MultiProtocol Label Switching (MPLS) EXP-bit to QoS level
- QoS level to egress 802.1p-bit
- QoS level to egress DSCP
- QoS level to egress MPLS EXP-bit

PHB

When traffic enters the DiffServ network, packets are placed in a queue according to their marking, which determines the PHB of the packets. For example, if a video stream is marked to receive the highest priority, it is placed in a high-priority queue. As these packets traverse the DiffServ network, the video stream is forwarded before other packets.

Two standard PHBs are defined in RFC 2597 and RFC 2598: the Assured Forwarding PHB group and the Expedited Forwarding PHB group. The Ethernet Routing Switch 8600 also uses the DF and CS groups. DF represents the default PHB on the system and CS represents Class Selector. Class Selector is provided in a DiffServ network for backward compatibility with IP precedence.

IP precedence is used to classify packets in a nonDiffServ network. Although the DSCP uses the first six bits of the TOS field, IP precedence uses the first three. Using IP precedence provides eight possible precedence values (CS0 to CS7) and is appropriate for simple QoS solutions. When additional customization is required, configure a custom DSCP mapping for a DiffServ network.

Assured Forwarding PHB group

RFC 2597 describes the Assured Forwarding PHB group, which 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 the case of network congestion, the drop precedence of a packet determines its relative importance within the Assured Forwarding PHB group.

Expedited Forwarding PHB group

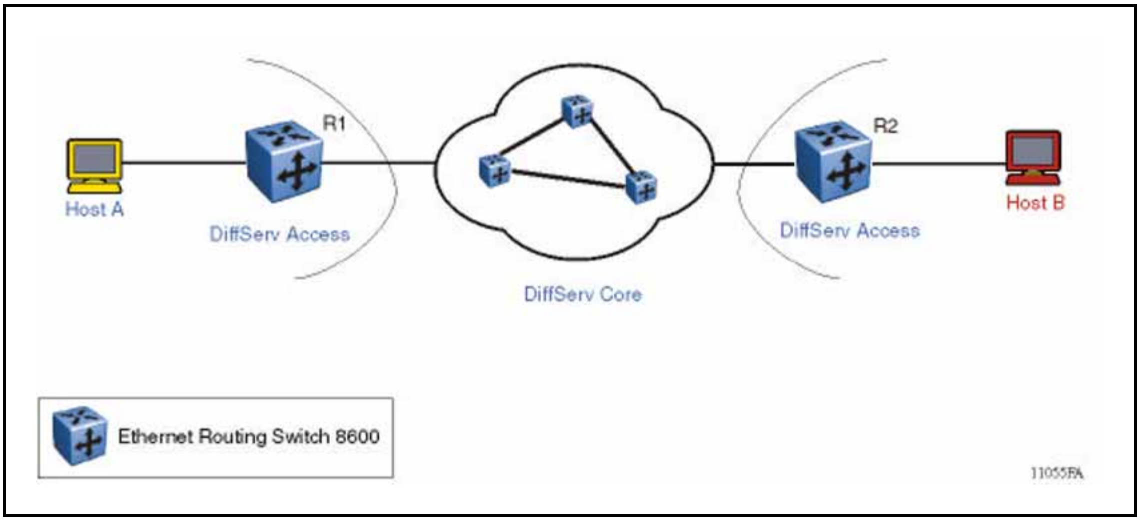
RFC 2598 describes the Expedited Forwarding PHB group as the Premium service: the best service the network can offer. Expedited Forwarding PHB is defined as a forwarding treatment for a DiffServ microflow when the rate of its transmission ensures that it is the highest priority and it experiences no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

DiffServ and the Ethernet Routing Switch 8600

The Ethernet Routing Switch 8600 implements a DiffServ architecture as defined in RFC 2474 and RFC 2475. The IEEE 802.1p and the DSCP markings found in virtual local area networks (VLAN) are used to classify the packet to its appropriate PHB and QoS level, providing Layer 2 and Layer 3 QoS functionality, respectively

The following figure illustrates DiffServ network operations. Ethernet Routing Switch 8600s are shown on the network edge, where they perform classification, marking, policing, and shaping functions. Ethernet Routing Switch 8600s are used in the network core. They do not need to perform classification, marking, policing, or shaping; they need only perform the actions defined by the PHB of the packet. To determine whether a port acts as an edge (access) or a core device, configure each port as access or core. The default is core.

Figure 2
DiffServ network core and edge devices



When a port is configured as a core port, packet markings are trusted. When a port is configured as an access port, packet markings are not trusted.

DiffServ access port (untrusted)

A DiffServ access port, shown in Figure 2 "DiffServ network core and edge devices" (page 24), is used at the edge of a DS network. The access port classifies traffic by re-marking the L3 DSCP parameter to zero (it does not trust the traffic markings) or by ignoring the 802.1p bits within a Dot1Q-tagged packet. Dot1Q headers are stripped at ingress, and are added back at egress only when the egress port is configured as a tagged or trunk port.

DiffServ core port (trusted)

A DiffServ core port does not change packet classification or markings; the port trusts the incoming traffic markings. A core port preserves the DSCP marking of all incoming packets, and uses these markings to assign the packet to an internal QoS level. For tagged packets, the port honors the 802.1p bits within a Dot1Q header, and uses these bits to classify ingress traffic.

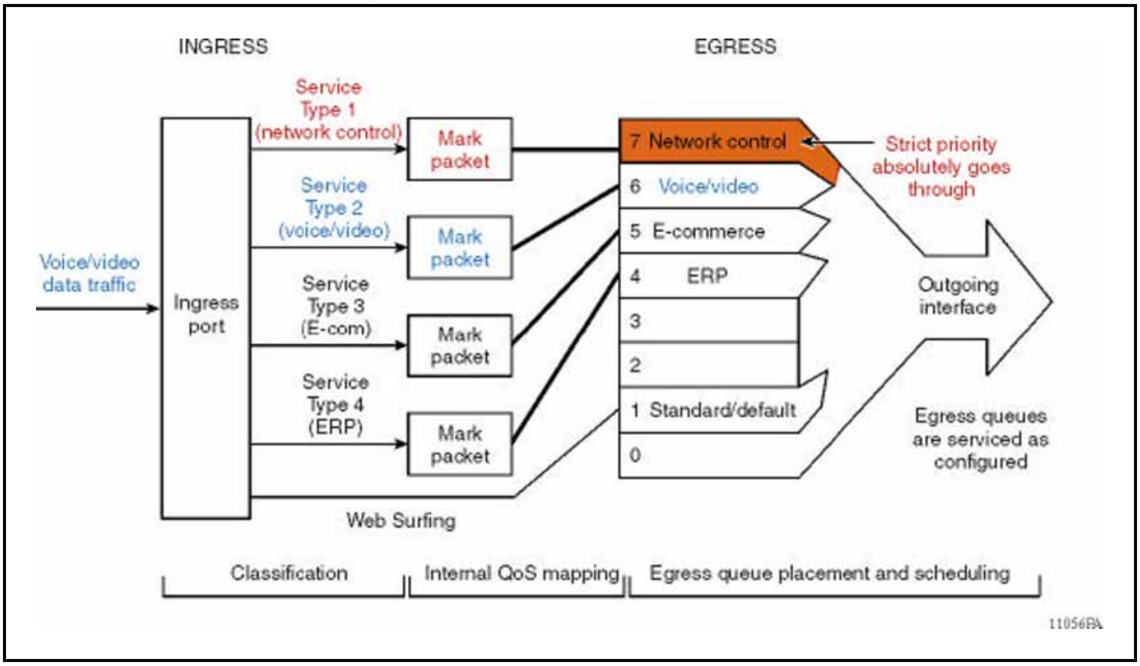
QoS operations for IPv4 and IPv6 are the same. All IP traffic can be associated with MAC, port, and VLAN QoS levels, rather than with 802.1p bits or the DSCP parameter.

QoS implementation

The following figure shows how the Ethernet Routing Switch 8600 provides QoS functionality. The order of operations is:

- ingress classification of the packet
- mapping of ingress classification to an internal QoS value
- placement of the packet into an egress queue based on the internal QoS to egress queue mapping
- egress servicing of the packet by a scheduler

Figure 3
Overview of Ethernet Routing Switch 8600 QoS operations



Ingress QoS configuration parameters determine traffic classification. Classification creates a mapping to an internal QoS level (0 to 7) that maps to an egress queue. The egress queue mapping determines the output packet DSCP, EXP-bit, or 802.1p markings. Whether a packet is part of a Layer 2 (bridged) or a Layer 3 (routed) traffic flow can affect QoS operations.

At ingress, you can modify traffic classification with filters (Access Control Lists—ACL); however, QoS deployment does not require the use of traffic filters. You can use traffic filters to configure criteria to identify a microflow or an aggregate flow. The filters can match multiple parameters in the IP packet, and can assign actions that match the criteria you specify. Filters override the standard ingress QoS or DiffServ operations.

Implement a DiffServ network on the Ethernet Routing Switch 8600 by configuring a port as trusted or untrusted.

DiffServ and nonIP traffic

DiffServ applies only to IP packets. NonIP traffic is mapped to a MAC, port, or VLAN QoS level. For R series module ports, traffic is first mapped to the MAC QoS level. With no MAC QoS level setting or match, the Ethernet Routing Switch 8600 chooses between port and VLAN QoS levels by selecting the highest QoS level setting. Normal egress QoS operation then occurs, although egress mapping tables associated with DSCP are not applicable—DSCP is an IP-only parameter.

DiffServ configuration parameters

You can use a number of parameters to configure DiffServ and QoS. All packets receive QoS operation handling. The following sections describe these parameters; in these sections, Device Manager terms are used.

- "DiffServ—true or false" (page 27)
- "Layer3Trust—core or access" (page 27)
- "Port-based QoS level" (page 27)
- "VLAN-based QoS level" (page 28)

DiffServ—true or false

You can configure the DiffServ parameter to true or false; false is the default. This parameter works in conjunction with the Layer3Trust parameter. The DiffServ parameter is a global parameter that affects QoS L3 DSCP operations.

If the DiffServ parameter is false (DiffServ disabled), the L3 DSCP parameter is not used for classification or modified. When set to true, it activates the Layer3Trust parameter.

Layer3Trust—core or access

You can configure the Layer3Trust parameter to core or access; core is the default. Core configures the port to a trusted state and access configures the port to an untrusted state.

If DiffServ is false, Layer3Trust has no effect; there is no modification of the DSCP or TOS bits. If DiffServ is true, the core and access settings take affect as described in "DiffServ access port (untrusted)" (page 25) and "DiffServ core port (trusted)" (page 25).

Port-based QoS level

Use the port-based QoS level to set the default QoS level for a port. You can configure the QoS level from zero to six (level seven is reserved for internal switch use— network control traffic). The default value is one.

For VoIP traffic, Nortel recommends that you use QoS level six.

Ingress and egress mapping tables affect QoS operations. There can be instances where Layer 2 (bridged) traffic flows obtain different QoS treatment than Layer 3 (routed) traffic flows. These instances are independent of L2 (802.1p) and L3 (DSCP) parameter settings.

VLAN-based QoS level

Use the VLAN-based QoS level to set a default QoS level for a VLAN. You can configure a QoS level from zero to six (level seven is reserved for internal switch use— network control traffic). The default value is one.

Use VLAN-based QoS levels to customize VLANs for traffic applications. For example, add a Voice VLAN to an Edge switch to carry VoIP traffic. Then you can apply a QoS level to the Voice VLAN to ensure proper handling of time-sensitive VoIP traffic without using filters. For VoIP traffic, Nortel recommends that you use QoS level six.

Queueing

Queuing is a congestion-avoidance function that prioritizes packet delivery. Queuing ensures discriminate packet discard during network congestion, and can delay a packet in memory until it is scheduled for transmission.

You can use queuing to manage congestion. Queueing determines the order in which packets are sent out of an interface based on priorities assigned to those packets. Congestion management involves the creation of queues, assignment of packets to the queues based on the classification of the packet, and scheduling of the packets in a queue for transmission.

When no congestion exists (periods of low traffic volume), packets are sent out of the interface when they arrive. During periods of transmission congestion at the outgoing interface, packets arrive faster than the interface can send them. If you use congestion management features, packets that accumulate at an interface are queued until the interface can send them. The packets are scheduled for transmission according to their assigned priority and the queuing mechanism configured for the interface. The Ethernet Routing Switch 8600 scheduler determines the order of packet transmission by controlling how queues are serviced with respect to each other.

Queues are used to aggregate packets in some administratively significant manner.

For more information about queueing, see *Ethernet Routing Switch 8600 Configuration — QoS and IP Filtering for R and RS Modules* (NN46205-507) .

The following sections describe the default egress queue sets (NNSC templates).

Critical/Network NNSC

The switch uses the Critical/Network NNSC for traffic within a single administrative network domain. If such traffic does not get through, the network cannot function. Examples of such types of traffic are heartbeats between core network switches or routers. The Spanning Tree Bridge Protocol Data Units (BPDU) also use the Critical NNSC to enter and exit the Ethernet Routing Switch 8600. NNSCs also include network control traffic packets for OSPF, BGP, STP, and other protocols.

Premium NNSC

The switch uses the Premium NNSC for IP telephony services, and provides the low latency and low jitter required to support such services. IP telephony services include Voice over IP (VoIP), voice signaling, Fax over IP (FoIP), and voice-band data services over IP (for example, analog modem). The switch can also use the Premium NNSC for Circuit Emulation Services over IP (CESoIP).

Metal NNSCs

The Platinum, Gold, Silver, and Bronze NNSCs are collectively referred to as the metal classes. The metal NNSCs provide a minimum bandwidth guarantee and are used for variable bit rate or bursty types of traffic. Applications that use the metal NNSCs support mechanisms that dynamically adjust their transmit rate and burst size based on congestion (packet loss) detected in the network.

Platinum NNSC

The switch uses the Platinum NNSC for applications that require low latency, for example, real-time services such as video conferencing and interactive gaming. Platinum NNSC traffic provides the low latency required for interhuman (interactive) communications. The Platinum NNSC provides a minimum bandwidth assurance for AF41 (Assured Forwarding 41) and CS4 (Class Selector 4)-marked flows. When the network is congested, DiffServ nodes use drop precedence to control variable bit rates that exceed the minimum assured bandwidth.

Gold NNSC

The switch uses the Gold NNSC for applications that require near-real-time service and are not as delay-sensitive as applications that use the Platinum service. Such applications include streaming audio and video, video on demand, and surveillance video.

The Gold NNSC assumes that traffic is buffered at the source and destination and, therefore, the traffic is less sensitive to delay and jitter. By default, the Gold NNSC provides a minimum bandwidth assurance for AF31, AF32, AF33 and CS3-marked flows. When the network is congested, DiffServ nodes use drop precedence to control variable bit rates and burst sizes that exceed the minimum assured bandwidth.

Silver NNSC

The switch uses the Silver NNSC for responsive (typically client- and server-based) applications. Such applications include Systems Network Architecture (SNA) terminals (for example, a PC or Automatic Teller Machine) to mainframe (host) transactions that use Data Link Switching (SNA over IP), Telnet sessions, Web-based ordering and credit card processing, financial wire transfers, and Enterprise Resource Planning applications.

Silver NNSC applications require a fast response and have asymmetrical bandwidth needs. The client sends a short message to the server and the server responds with a much larger data flow back to the client. For example, when a user clicks a hyperlink (that sends a few dozen bytes) on a Web page, a new Web page is loaded (that downloads kilobytes of data). The Silver NNSC provides a minimum bandwidth assurance for AF21 and CS2-marked flows.

The Silver NNSC favors short-lived, low-bandwidth TCP-based flows. During network congestion, DiffServ nodes use drop precedence to control variable bit rates and burst sizes that exceed the minimum assured bandwidth.

Bronze NNSC

The switch uses the Bronze NNSC for longer-lived TCP-based flows, such as file transfers, e-mail, or noncritical Operation, Administration, and Maintenance (OAM) traffic. The Bronze NNSC provides a minimum bandwidth assurance for AF11 and CS1-marked flows. During network congestion, DiffServ nodes use drop precedence to control variable bit rates and burst sizes that exceed the minimum assured bandwidth. Nortel recommends that you use the Bronze NNSC for noncritical OAM traffic with the CS1 DSCP marking.

Standard NNSC

The switch uses the Standard NNSC for best-effort services. No delay, loss, or jitter guarantees are specified for this NNSC.

Egress queue packet assignment

The Ethernet Routing Switch 8600 assigns packets to egress (transmit) queues based on the ingress mappings and the internal QoS level.

ATTENTION
MPLS can only be used on R and RS modules.

Ingress mappings and queues

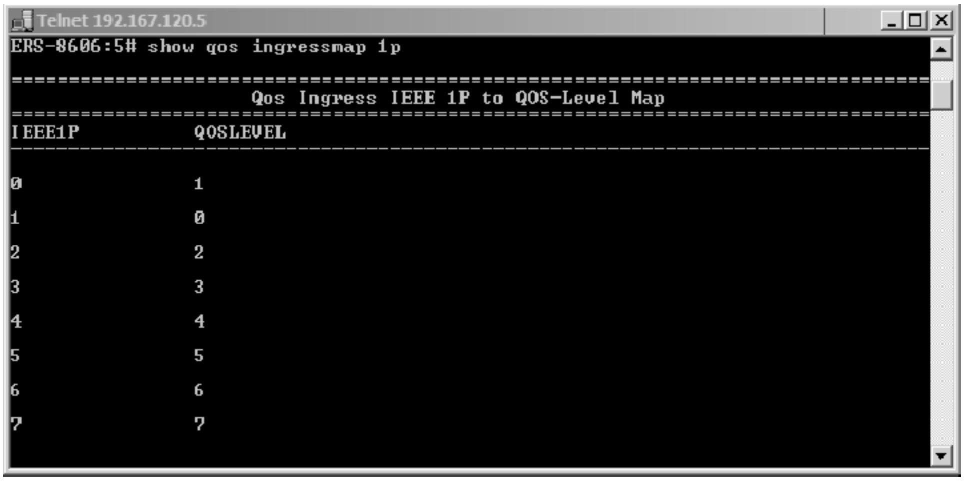
The switch uses ingress maps to translate incoming packet QoS markings to the internal QoS level. Packets are internally classified based on the internal QoS level.

Ingress mappings include:

- 802.1p to (internal) QoS level
- DSCP to (internal) QoS level
- EXP-bit to (internal) QoS level

The following figures show ingress mappings obtained using the CLI command **`show qos ingressmap 1p`**.

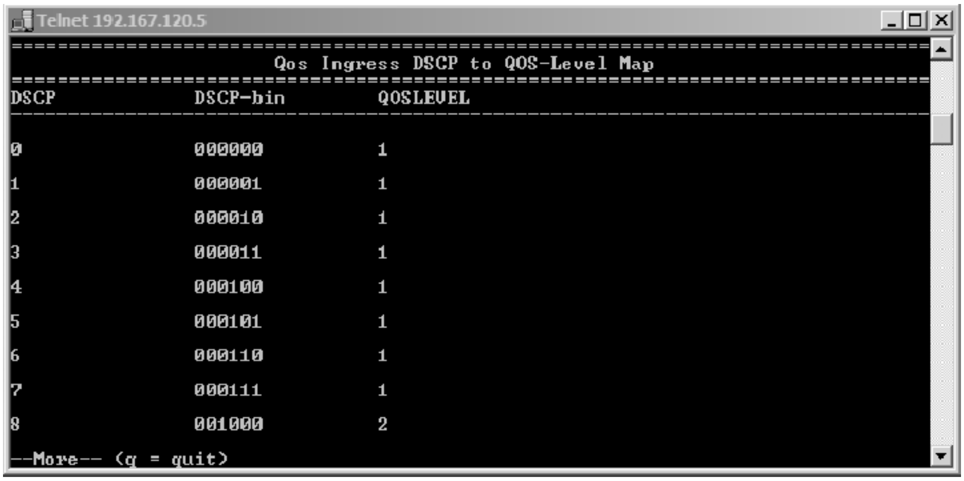
Figure 4
Ingress 802.1p bit to QoS mappings



```
ERS-8606:5# show qos ingressmap 1p

================================================================================
                     Qos Ingress IEEE 1P to QOS-Level Map
================================================================================
IEEE1P          QOSLEVEL
--------------------------------------------------------------------------------

0               1

1               0

2               2

3               3

4               4

5               5

6               6

7               7
```

The following figure shows DSCP to internal QoS level mappings.

Figure 5
Ingress DSCP to QoS mappings (partial)



```
================================================================================
                       Qos Ingress DSCP to QOS-Level Map
================================================================================
DSCP            DSCP-bin        QOSLEVEL
--------------------------------------------------------------------------------

0               000000          1

1               000001          1

2               000010          1

3               000011          1

4               000100          1

5               000101          1

6               000110          1

7               000111          1

8               001000          2

--More-- (q = quit)
```

The following tables describe default ingress and egress mappings.

Table 2
Default ingress 802.1p to QoS to egress queue mappings

802.1 p	Internal QoS	Egress queue		Queue name (Egress Queue Set 2)
		Fast Ethernet	Gigabit Ethernet	
0	1	4	4	Standard (or Default)
1	0	5	55	Custom
2	2	3	3	Bronze
3	3	2	2	Silver
4	4	1	1	Gold
5	5	0	0	Platinum
6	6	6	62	Premium
7	7	7	63	Network (or Critical)

In the following table, TOS denotes Type of Service and Hex denotes hexadecimal.

Table 3
Gigabit Ethernet default ingress DSCP to QoS to egress queue mapping

Ingress			Internal QoS	Egress queue	PHB	Queue name (Egress Queue Set 2)
DSCP	DSCP (Hex)	TOS				
00	00	00	1	4	CS0	Custom
00	00	00	1	4	DE	
08	08	20	2	3	CS1	Bronze
10	A	28	2	3	AF11	
16	10	40	3	2	CS2	Silver
18	12	48	3	2	AF21	
24	18	60	4	1	CS3	Gold
26	1A	68	4	1	AF31	
32	20	80	5	0	CS4	Platinum
34	22	88	5	0	AF41	
40	28	A0	6	62	CS5	Premium
26	2E	B8	6	62	EF	

Table 3
Gigabit Ethernet default ingress DSCP to QoS to egress queue mapping (cont'd.)

Ingress			Internal QoS	Egress queue	PHB	Queue name (Egress Queue Set 2)
DSCP	**DSCP (Hex)**	**TOS**				
48	30	C0	7	63	CS6	Network (or Critical)
56	38	E0	7	63	CS7	

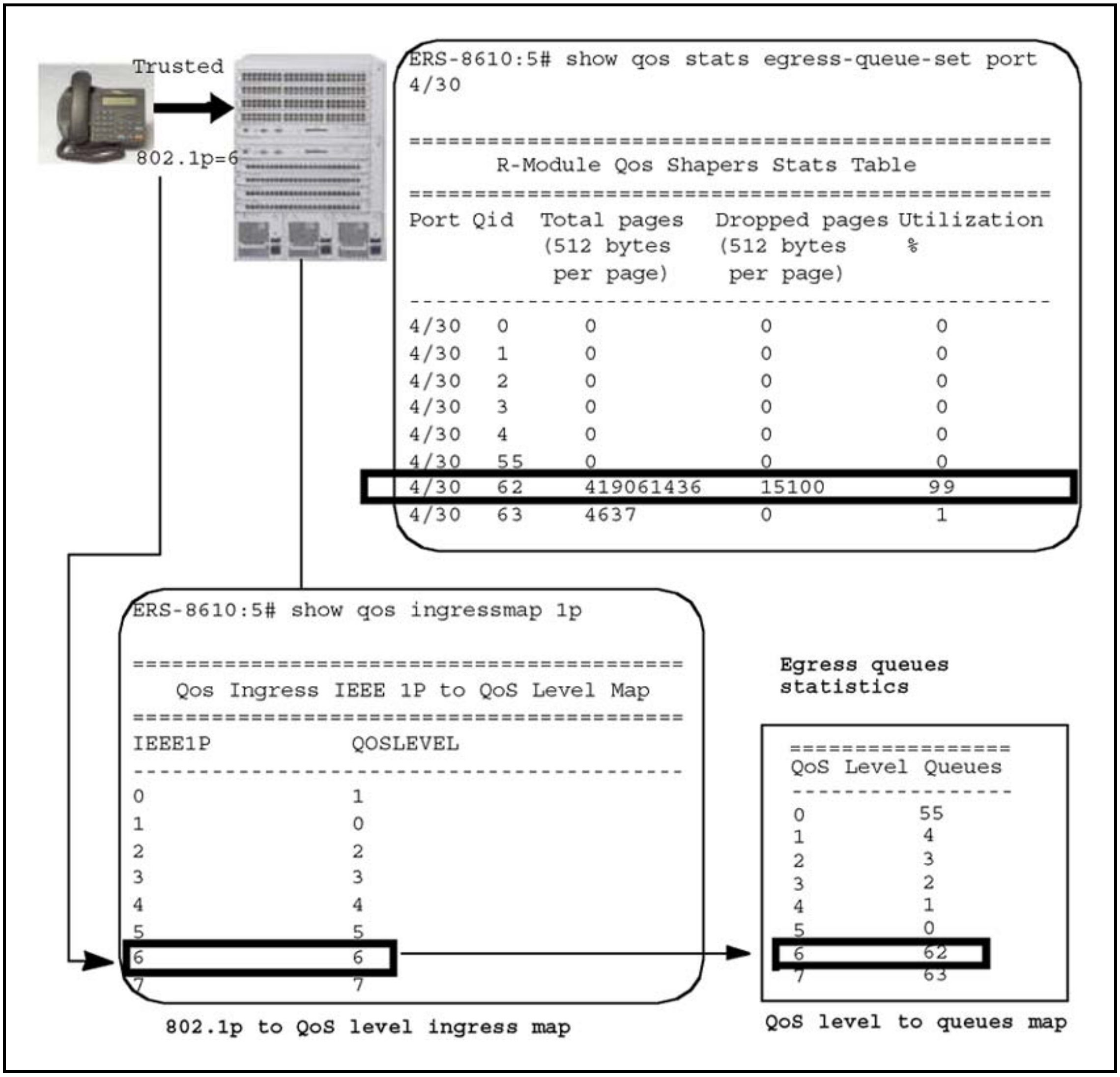
Internal QoS level

The internal QoS level or effective QoS level is a key element in the Ethernet Routing Switch 8600 QoS architecture. The internal QoS level specifies the kind of treatment a packet receives and the transmit queue for its exit (egress) path. Every packet that ingresses the Ethernet Routing Switch 8600 is classified and assigned an internal QoS level.

Internal QoS levels map to the transmit or egress queues on a port. For example, for an access port, the highest value among the port QoS level, VLAN QoS level, and MAC QoS level becomes the internal QoS level (effective QoS level). For Layer 3 trusted (core) ports, incoming DSCP/TOS bits are honored by the switch. The internal QoS level is assigned using the ingress DSCP to QoS level map. If a MAC QoS level is configured on an untrusted port, it takes precedence over the VLAN QoS level and the port QoS level.

The following figure shows a Nortel i2002 VoIP phone that sends packets with a 802.1p value of 6 on a trusted Layer 2 port. The 802.1p-to-QoS level ingress map determines the internal QoS level of the packet. The packet is then placed in the appropriate queue using the QoS level to queue mapping table.

Figure 6
Path from input port to queues



```
ERS-8610:5# show qos stats egress-queue-set port
4/30

================================================
      R-Module Qos Shapers Stats Table
================================================
Port Qid  Total pages   Dropped pages Utilization
          (512 bytes    (512 bytes     %
           per page)     per page)
------------------------------------------------
4/30  0     0             0             0
4/30  1     0             0             0
4/30  2     0             0             0
4/30  3     0             0             0
4/30  4     0             0             0
4/30  55    0             0             0
4/30  62    419061436     15100         99
4/30  63    4637          0             1
```

```
ERS-8610:5# show qos ingressmap 1p

==========================================
   Qos Ingress IEEE 1P to QoS Level Map
==========================================
IEEE1P           QOSLEVEL
------------------------------------------
0                1
1                0
2                2
3                3
4                4
5                5
6                6
7                7
```

```
=================
QoS Level  Queues
-----------------
0          55
1          4
2          3
3          2
4          1
5          0
6          62
7          63
```

Egress queueing and modules

Packets that egress from R series module ports can originate from either another R series module port or from a Classic module port.

The egress queue is determined by the internal QoS level. Queue numbers depend on module port types (Fast Ethernet, 1 Gigabit Ethernet, 10 Gigabit Ethernet). All Classic input/output modules have identical QoS to egress queue mapping, regardless of the port type. The COP (central processor) maintains the table that maps packet QoS level to egress queue, which depends on the port type.

QoS and VoIP

Voice over Internet Protocol (VoIP) traffic requires low latency and jitter. To ensure VoIP traffic is handled appropriately, configure proper QoS for such traffic.

When the Ethernet Routing Switch 8600 is used as a core router, to treat VoIP traffic appropriately, configure ports as core ports (this is the default port setting). In this case, QoS markings applied to VoIP traffic are trusted, and the switch does not re-mark QoS settings. However, if this is not sufficient, you can also apply filters, route policies, or re-mark traffic.

When you use the Ethernet Routing Switch 8600 as a Edge router (access port, or untrusted), proper attention must be paid to how VoIP traffic is marked. Because Power over Ethernet (PoE) is not supported on the Ethernet Routing Switch 8600, and the switch generally operates in the network core, VoIP traffic is not a concern. However, if you are using the Ethernet Routing Switch 8600 as an Edge device and wish to apply QoS to VoIP traffic, you can configure a specific VLAN (for example, a Voice VLAN) to apply a QoS level to VoIP traffic. In this case, Nortel recommends that you assign the VLAN default QoS level to 6 (Premium).

For Release 5.0, the Ethernet Routing Switch 8600 supports a security mechanism called Nortel Secure Network Access (NSNA). NSNA supports the use of special VoIP VLANs; for more information, see *Ethernet Routing Switch 8600 Security* (NN46205-601) .

Priority queuing and servicing

Classic modules support eight output queues for each 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 4 "Traffic service class mapping to QoS levels" (page 36) 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.

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 of traffic has 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 Ethernet Routing Switch 8600, the default queue for all traffic is QoS level 1, or the standard traffic service class.

Table 4
Traffic service class 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 packets are placed in 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 packet transmit opportunity to determine which queue is serviced first.

When a 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 4 "Traffic service class mapping to QoS levels" (page 36) 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.

Traffic filtering fundamentals

Traffic filtering on the Ethernet Routing Switch 8600 is a mechanism that helps you to manage traffic by defining filtering conditions and associating these conditions with specific actions. Filtering blocks unwanted traffic and prioritizes other traffic, which efficiently manages bandwidth and protects your network.

Navigation

Overview

Using traffic filters, you can reduce network congestion and control access to network resources by blocking, forwarding, or prioritizing specified traffic on an interface.

The Ethernet Routing Switch 8600 can use traffic filtering for many purposes. Filtering can provide security, and can help ensure that all traffic is treated according the class of service (COS) required by the application. The Ethernet Routing Switch can drop low-priority traffic under congestion, police incoming traffic, and mark or drop nonconforming traffic. The traffic class (internal to the switch), drop precedence, DSCP markings, and 802.1p bit markings define the COS. DiffServ marking and re-marking are supported using filters.

You do not have to use filters to provide QoS. Filters can override QoS packet operations.

Traffic filters for Classic and R series modules

The Ethernet Routing Switch 8600 uses two different traffic filtering implementations:

- the pre-4.0 implementation that involves E and M modules (Classic modules) to support Layer 3 and Layer 4 filtering.
- a filtering implementation that utilizes R series modules and ACLs to support ingress and egress Layer 2 through Layer 7 filtering.

Classic and R module filters can coexist in the same chassis. Use Classic commands to configure pre-4.0 filters that operate only on Classic modules, and use the 4.0 and later commands to configure filters that operate only on R modules. *Nortel Ethernet Routing Switch 8600 Configuration — QoS and IP Filtering for R and RS Modules* (NN46205-507) describes the R module traffic filtering commands, and this document describes Classic traffic filtering commands.

Rate limiting

Implement rate limiting to perform QoS rate metering every 2.5 milliseconds, in increments of 64 bytes.

Table 5 "10 Mb/s Ethernet line-rate metering" (page 39), Table 6 "100 Mb/s Ethernet line-rate metering" (page 39), and Table 7 "Gigabit Ethernet line rate metering" (page 40) represent the measured line rates, in multiples of 64, for the three Ethernet speeds tested, with the expected results.

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 packet.

The rates were obtained using a source and destination filter.

Table 5
10 Mb/s Ethernet line-rate metering

average-rate <int>										
Packet size in (bytes)	**5** 10%[1]	**10** 20%	**15** 30%	**20** 40%	**25** 50%	**30** 60%	**35** 70%	**40** 80%	**45** 90%	**50** 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
Note 1: Target average percentage of line rate Note 2: Rate in megabits per second										

Table 6
100 Mb/s Ethernet line-rate metering

average-rate <int>										
Packet size in (bytes)	**50** 10%[1]	**100** 20%	**150** 30%	**200** 40%	**250** 50%	**300** 60%	**350** 70%	**400** 80%	**450** 90%	**500** 100%
64	10.25[2]	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	76.19	76.19
256	10.66	20.47	31.14	40.93	51.53	61.18	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

Note 1: Target average percentage of line rate
Note 2: Rate in megabits per second

Table 7
Gigabit Ethernet line rate metering

average-rate <int>										
Packet size in (bytes)	**500** 10%[1]	**1000** 20%	**1500** 30%	**2000** 40%	**2500** 50%	**3000** 60%	**3500** 70%	**4000** 80%	**4500** 90%	**5000** 100%
64	102.50[2]	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

Note 1: Target average percentage of line rate
Note 2: Rate in megabits per second

Rate metering

In the Ethernet Routing Switch 8600, QoS rate metering is accomplished in increments of 64 bytes every 2.5 milliseconds. Table 8 "10 Mb/s Ethernet line rate metering" (page 41), Table 9 "100 Mb/s Ethernet line rate metering" (page 41), Table 10 "Gigabit Ethernet line rate metering" (page 42)and list the throughput in megabits per second (Mb/s) for various traffic flows using different rate-limiting values, and source and destination filters.

All traffic loads are at 100 percent 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 percent of total interface speed.

The following table lists the values for 10 Mb/s Ethernet.

Table 8
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
Note 1:	**target average percentage of line rate**									
Note 2:	**rate in Mb/s**									

The following table lists the values for 100 Mb/s Ethernet.

Table 9
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

The following table lists the values for Gigabit Ethernet.

Table 10
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 you assign QoS levels, note that the following can affect 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 8 "10 Mb/s Ethernet line rate metering" (page 41), at 100 percent 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.

IP filtering

IP filtering manages traffic and, in some cases, provides security. Each filter set defines:

- the conditions that must match for inclusion in the filter set
- the actions that are 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 that are forwarded through the switch on specified ingress port. The filters are applied to the switch ingress port with a default action to forward or drop. All packets not matching any filter are forwarded or dropped, depending on the default action of the port. You can apply two types of filters:

- traffic filters
- global filters

You can apply traffic filters to the following parameters:

- source IP address
- destination IP address
- DiffServ field
- Internet Control Message Protocol (ICMP) request
- IP fragment

Filters are applied to 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.

IP filtering navigation

- "Filter characteristics" (page 44)
- "Source, destination, and global filters" (page 44)
- "Filter configuration" (page 46)
- "Filter actions " (page 46)
- "IP telephony and multimedia default filters" (page 47)
- "Rate limiting " (page 38)

Filter characteristics

Filters on the Ethernet Routing Switch 8600 have the following characteristics and requirements:

- You can define up to 3071 filter IDs among all ports or on a single port, including source and destination and global filters.
- Up to 200 filter sets can be defined for source and destination filters, while up to 100 filter sets can be defined for global filters.
- A collection of source and destination filters is defined in a set, and the set is applied to a port or a group of port. You can assign multiple sets to any port.
- A collection of global filters is defined in a global set (not exceeding eight for each set), and the set is applied to a port or group of port. Multiple sets may be applied to one port or a set of port, but the maximum number of global filters you can enable on a port set is eight.

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

ATTENTION
Nortel recommends that you check and optimize your configuration. Consult the Ethernet Routing Switch 8600 product management team regarding filtering requirements.

Source, destination, and global filters

Classic modules support two different kinds of filters:

- “Source and destination filters” (page 44)
- “Global filters” (page 45)

Source and destination filters

Source and destination filters (traffic filters) instruct a router interface to selectively handle specified IP traffic. Information in the packet headers determines which packets receive special handling. Traffic filters 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 can optionally specify a destination IP address and mask. Destination filters must specify a destination IP address and mask, and can optionally specify a source IP address and mask. Although you can configure source filters with 0.0.0.0/0.0.0.0 as the source address, if you do, the filter connects to all forwarding records. You can configure destination filters with 0.0.0.0/0.0.0.0 as the destination address.

A source and destination filter applies the following actions to a packet that matches the filter record:

- forwards the packet when the filter is applied with a forward action
- drops the packet when the filter is applied with a drop action
- mirrors the packet to the defined mirror port
- forwards the packet to the next hop
- modifies the DS codepoint (only on DiffServ access port)
- modifies IEEE 802.1p
- polices the packet

If you configure source and destination filters for nonlocal routes, corresponding routing entries are created and updated (as needed) in the routing table, thus maintaining the effectiveness of these filters.

ATTENTION
Mask lengths one to seven are not supported; however, the zero mask length is allowed for source filters and destination filters. Use the longest mask to match subnets.

ATTENTION
Zero-mask source-type IP filters are not effective for incoming source IP addresses for which an IP route, Address Resolution Protocol (ARP), or matching non-zero-mask subnet IP source and destination filter does not exist.

ATTENTION
Source Destination IP Filters will not work for Multicast Traffic, only Global Filters can be used to filter on this criteria.

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.
- You can apply up to eight global filters on any set of RaptARU port. A set includes eight 10/100 Mb/s ports or 1 gigabit port, each of which accommodates eight global filters.
- A global filter causes the same actions described for source and destination filters.

Filter configuration

Matching criteria for filters in the Ethernet Routing Switch 8600 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 established bidirectionally
- 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

Filter actions

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

Each filtered port on the Ethernet Routing Switch 8600 has a default action of forward or drop associated with it. When the filter action mode matches the default port action, the default port action is used.

When the port default action is drop, the packets are forwarded only if a matching filter action mode is forward. If a single match occurs with an action mode of forward, the frame is forwarded regardless of how many matching filters are found with an action mode of drop. 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, the packets are dropped only if a matching filter action mode is droped. If a single match occurs with a drop action, the packet is dropped regardless of how many matching filters have forwarding actions. 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 11 "Port actions for filters" (page 47) indicates the forward or drop behavior of a port if filter matches are found for a packet.

Table 11
Port actions for filters

Port mode	Filter mode	Packet action
Forward	Default	Forward all packet 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.

QoS in IP-based networks is essential because of the connectionless nature of IP. A simple IP network provides a best-effort service that makes no guarantees about when, or how much data, it can deliver. Enabling IP technology to offer a transparent service (as compared to more traditional leased-line services or virtual circuit services such as Frame Relay and ATM) requires a QoS strategy that provides 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 traffic prioritization mechanisms. A number of key parameters define QoS in a network, as shown in Table 12 "QoS network parameters" (page 48).

Table 12
QoS network parameters

Parameter	Description
Latency (propagat ion 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 (Kb/s) or megabits per second (Mb/s).
Packet loss	A percentage of the packets that can 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 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.

IP telephony and multimedia default filters navigation

- "QoS implementation" (page 48)
- "IP telephony traffic" (page 49)
- "Signaling and media traffic parameters" (page 50)

QoS implementation

The Ethernet Routing Switch 8600 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 classic 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 quality of 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 stream must be identified and prioritized with better QoS to effectively improve communication quality and experience. The default IP telephony filters also configure this prioritization for some video conference applications and streaming multimedia applications.

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

ATTENTION
The IP telephony filter feature provides a list of supported IP telephony devices and the types of signaling protocols supported by that particular device.

ATTENTION
When using the Device Manager for configuration, the status of DiffServ on a port is modified automatically when you assign or remove an IP telephony media filter only if the check box TelephonyAndMultimediaFilterEnable is enabled. To enable this check box, go to Port, Edit ,TelephonyAndMultimediaFilterEnable. 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.

When you set the IP telephony and multimedia filters, information representing these filters is propagated from the Security, Data Path, Filters dialog box to the following tabs:

- filter
- control
- DiffServs
- source and destination sets

Most of the options are set to defaults. If you configure any options that affect the identification of the telephony traffic, you must tune the Ethernet Routing Switch 8600 IP telephony filters accordingly. Any improper configuration can impact the network. This effect ranges from adverse affects to network stability and quality to giving unpredictable and undesired treatment to some flows. In addition, these filters affect some flows if the configuration is not correct.

The following platforms use IP telephony filters:

- none (default)
- CSE 1000
- CSE 2000
- CSE 3000
- BCM
- MERIDIAN LINE card
- MERIDIAN TRUNK card
- MSL100IP
- VCON
- Minerva
- custom (user-defined)

> **ATTENTION**
> Incorrectly defined filters affect flows.

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 13 "UDP/TCP port parameters for signaling and media traffic" (page 51) provides UDP/TCP port parameters.

Table 13
UDP/TCP port parameters for signaling and media traffic

Platform devices			Streams			
Port	**Platform**	**Device**	**Protocol**	**Port range**	**Option**	**Type**
01	CSE 1000		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	Voice Gateway	UDP	28000-28255	src-dst	media
			TCP	1720-1720	dst	signal
			TCP	1719-1719	src-dst	signal
05	MeridianTrunk	Voice Gateway	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	Voice Gateway	UDP	5000-5000	src-dst	signal

[1] CSE2000 and MSL100IP are the same. CSE3000 is not supported.

Table 13
UDP/TCP port parameters for signaling and media traffic (cont'd.)

Platform devices			Streams			
Port	**Platform**	**Device**	**Protocol**	**Port range**	**Option**	**Type**
			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 the same. CSE3000 is not supported.						

Filtering criteria

This section describes the criteria to consider when you create a filter for the Ethernet Routing Switch 8600.

- "Modifying criteria" (page 52)
- "Action criteria" (page 52)
- "Traffic filters (source and destination)" (page 53)
- "Action modes " (page 53)

Modifying criteria Configure filters to modify the following fields:

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

Action criteria Filtering actions include:

- drop—drops all packets
- forward—forwards all packets that match the filter
- 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 Layer 2 (Ethernet)

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

Traffic filters (source and destination) Source filters must specify a source IP address and mask, and they can optionally specify a destination IP address and mask. Destination filters must specify a destination IP address and mask, and they can 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, after the source filter is configured with 0.0.0.0/0.0.0.0, this filter connects to all forwarding records. You can also configure destination filters with 0.0.0.0/0.0.0.0 as the destination address.

Traffic filters perform the following:

- 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 port on an Ethernet Routing Switch 8600 has a default action mode of forward associated with it. A packet that matches any filter with the action mode of drop is dropped. A packet that matches one filter having the action mode of forward is forwarded if and only if it does not also match a filter with the drop action mode. If a packet matches multiple filters and any one of those filters is drop, the packet is dropped.

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

Table 14
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.

QoS configuration using Device Manager

Configure QoS to ensure that network resources are allocated where they are needed most.

Select a topic:

- “DiffServ configuration” (page 55)
- “QoS levels for nonIP traffic configuration” (page 62)

Navigation

- “DiffServ configuration” (page 55)
- “QoS levels for nonIP traffic configuration” (page 62)

DiffServ configuration

Use DiffServ to implement classification and mapping functions at the network boundary or access points, thus regulating packet behavior.

Select a topic:

- “Configuring DiffServ for a port” (page 56)
- “Editing a service class administrative weight” (page 56)
- “Modifying ingress 802.1p to QoS mappings” (page 57)
- “Modifying ingress DSCP to QoS mappings” (page 58)
- “Modifying egress QoS to 802.1p mappings” (page 59)
- “Modifying egress QoS to DSCP mappings” (page 60)

DiffServ configuration navigation

Configuring DiffServ for a port

Configure DiffServ so that the Ethernet Routing Switch will use DiffServ to provide DiffServ-based QoS on that port.

Procedure 1
Procedure steps

Step	Action
1	From Device Manager menu bar, select **Edit, Port, General - GlobalRouter (vrf 0)**. The Port dialog box appears with the Interface tab displayed.
2	In the **QosLevel** section of the interface tab, select **DiffServ** to enable it.
3	Specify the port type by setting **Layer3Trust** to **access** or **core**.
4	Click **Apply**.

--End--

Editing a service class administrative weight

Edit a service class administrative weight to modify the administrative weight for the corresponding service class.

Procedure steps

Step	Action
1	From Device Manager menu bar, choose **QOS, Mapping Tables** . The QOS dialog box appears with the Mapping Tables tab displayed.
2	In the row of the service class you want to edit, double-click on the **AdminWeight** field and enter the new administrative weight.

3 Click **Apply**.

--End--

For more information, see “Mapping Tables tab fields” (page 57).

Mapping Tables tab fields

Variable definitions

Use the data in the following table to help you use the Mapping Tables tab.

Variable	Value
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).

Modifying ingress 802.1p to QoS mappings

You can modify the ingress mappings to change traffic priorities. However, Nortel recommends that you use the default mappings.

ATTENTION
For bridged and tagged traffic, the switch determines the QoS level based on the IEEE 802.1p bits. The mapping of the bits to QoS levels is through the ingress tag and through the QoS mapping table.

⚠ **CAUTION**
Nortel recommends that you do not change the default values. If you change the values, make sure that the values are consistent on all other Ethernet Routing Switch 8600 and other devices in your network. Inconsistent mapping of table values can result in unpredictable service levels.

Procedure steps

Step Action

1 From Device Manager menu bar, choose **QOS, Mapping Tables**.

The QOS dialog box appears with the Mapping Tables tab displayed.

2 Click the **Ingress 8021p to QoS** tab. The Ingress 8021p to QoS tab appears.

3 Ensure that the configuration is correct.

--End--

For more information, see "Ingress 8021p to QoS tab fields" (page 58).

Ingress 8021p to QoS tab fields

Variable definitions

Use the data in the following table to help you use the Ingress 8021p to QoS tab.

Variable	Value
InIeee8021P	Value of the IEEE 802.1p bit of the incoming packet.
QosLevel	Equivalent egress QoS level (0 to 7).

Modifying ingress DSCP to QoS mappings

You can modify the ingress DSCP to QoS mappings to change traffic priorities. However, Nortel recommends that you use the default mappings.

> **ATTENTION**
> For all routed IP packets, the port maps the DSCP to the QoS level according to the Ingress DscpToQoS table.

> **ATTENTION**
> Changes to the mapping table take effect after you reboot the switch.

Procedure steps

Step **Action**

1 From Device Manager menu bar, choose **QOS, Mapping Tables**.

The QOS dialog box appears with the Mapping Tables tab displayed.

2 Click the **Ingress Dscp To Qos** tab.

3 Modify the mappings as required.

4 Click **Apply**.

--End--

For more information, see "Dscp To Qos tab fields" (page 59).

Dscp To Qos tab fields

Variable definitions

Use the data in the following table to help you use the Dscp To Qos tab.

Variable	Value
InDscp	Value of the DiffServ codepoint (in decimal format) in the IP header of the incoming packet.
InDscpBinaryFormat	Value of the DiffServ codepoint (in binary format) in the IP header of the incoming packet.
QosLevel	Equivalent Quality of Service level.

Modifying egress QoS to 802.1p mappings

You can change the mappings between the QoS levels and the IEEE 802.1p bits.

ATTENTION
If the packet egress is tagged, the appropriate IEEE 802.1p bits are set according to the Egress QoS to 8021p tab.

CAUTION
Nortel recommends that you do not change the default values. If you change the values, make sure that the values are consistent on all other Ethernet Routing switch 8600 and other devices in your network. Inconsistent mapping of table values can result in unpredictable service levels.

Procedure steps

Step **Action**

1 From Device Manager menu bar, choose **QOS, Mapping Tables**.

The QOS dialog box appears with the Mapping Tables tab displayed.

2 Click the **Egress QoS to 8021p** tab. The Egress QoS to 8021p tab appears.

--End--

For more information, see “EgressQoS to 8021p tab fields” (page 60).

See also:

- “Configuring DiffServ for a port” (page 56)
- “Editing a service class administrative weight” (page 56)
- “Modifying ingress 802.1p to QoS mappings” (page 57)
- “Modifying ingress DSCP to QoS mappings” (page 58)
- “Modifying egress QoS to DSCP mappings” (page 60)

EgressQoS to 8021p tab fields

Variable definitions

Use the data in the following table to help you use the Egress QoS to 8021p tab.

Variable	Value
QosLevel	QoS level of the outgoing packet.
Outleee8021P	Equivalent value of the IEEE 802.1p bit.

Modifying egress QoS to DSCP mappings

You can modify the egress QoS to DSCP mappings to change traffic priorities. However, Nortel recommends that you use the default mappings.

ATTENTION
When no traffic filter is used, the DSCP of bridged IP traffic is reset according to the QoS level as the traffic egresses.

ATTENTION
Changes to the mapping table take effect after you reboot the switch.

CAUTION
Nortel recommends that you do not change the default values. If you change the values, make sure that the values are consistent on all other Ethernet Routing switch 8600 and other devices in your network. Inconsistent mapping of table values can result in unpredictable service levels.

Procedure steps

Step **Action**

1 From Device Manager menu bar, choose **QOS, Mapping Tables**.

The QOS dialog box appears with the Mapping Tables tab displayed.

2 Click the **Egress QoS To Dscp** tab.

The Egress QoS To Dscp tab appears.

3 Modify egress QoS to DSCP mappings.

--End--

For more information, see "Egress QoS To Dscp tab fields" (page 61).

See also:

- "Configuring DiffServ for a port" (page 56)
- "Editing a service class administrative weight" (page 56)
- "Modifying ingress 802.1p to QoS mappings" (page 57)
- "Modifying ingress DSCP to QoS mappings" (page 58)
- "Modifying egress QoS to 802.1p mappings" (page 59)

Egress QoS To Dscp tab fields

Variable definitions

Use the data in the following table to help you use the Egress Qos To Dscp tab.

Variable	Value
QosLevel	QoS level of the outgoing packet.
OutDscp	Equivalent value of the DiffServ code point (in decimal format).
OutDscpBinaryFormat	Equivalent value of DiffServ code point (in binary format).

QoS levels for nonIP traffic configuration

This section describes how to assign QoS levels to non-IP traffic.

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

Select a topic:

- "Configuring the VLAN QoS level" (page 62)
- "Viewing and assigning QoS levels by port" (page 63)
- "Configuring the QoS level for specific MAC addresses" (page 63)

QoS levels for nonIP traffic configuration navigation

- "Configuring the VLAN QoS level" (page 62)
- "Viewing and assigning QoS levels by port" (page 63)
- "Configuring the QoS level for specific MAC addresses" (page 63)

Configuring the VLAN QoS level

Use the default VLAN QoS level to assign a default QoS level for all traffic.

Prerequisites

- A VLAN is already configured. If you are configuring a new VLAN, you configure the QoS level as part of that configuration.

Procedure steps

Step	Action
1	From Device Manager menu bar, choose **VLAN, VLANs - GlobalRouter (vrf 0)**. The VLAN - GlobalRouter (vrf 0) dialog box appears with the Basic tab displayed.
2	In the **VLAN - GlobalRouter (vrf 0)** dialog box, click the **Advanced** tab. The VLAN - GlobalRouting (vrf 0) Advanced tab appears.
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.

4	Click **Apply**.

--End--

See also:

- “Viewing and assigning QoS levels by port” (page 63)
- “Configuring the QoS level for specific MAC addresses” (page 63)

Viewing and assigning QoS levels by port

Use this procedure to view and assign QoS levels by port.

Procedure steps

Step	Action
1	From Device Manager menu bar, choose **Edit, Port, General globalRouter (vrf 0)**. The Port - GlobalRouter (vrf 0) dialog box appears with the Interface tab displayed.
2	In the **QosLevel** box, select the QoS level.
3	Click **Apply**.

--End--

See also:

- “Configuring the VLAN QoS level” (page 62)
- “Configuring the QoS level for specific MAC addresses” (page 63)

Configuring the QoS level for specific MAC addresses

Apply a QoS level to traffic from specific VLAN MAC addresses to provide special QoS treatment to the packets.

Procedure steps

Step	Action
1	From Device Manager menu bar, choose **VLAN, VLAN - GlobalRouter (vrf 0)**. The VLAN dialog box appears with the Basic tab displayed.
2	In the dialog box **Basic** tab, select a VLAN. The Bridge button is enabled.

3 Click **Bridge**.

The Bridge, VLAN - GlobalRouter (vrf 0) dialog box appears with the FDB Aging tab displayed.

4 Select the **Static** tab.

The Bridge, VLAN, - GlobalRouter (vrf 0) appears.

5 In the **Static** tab, click **Insert**.

The Bridge, VLAN, - GlobalRouter (vrf 0) Insert Static dialog box appears.

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

7 In the **Port** text box, click the ellipsis button and select the port.

8 In the **QosLevel** area, select the QoS level.

9 Click **Insert**.

--End--

For more information, see "Static tab fields" (page 64).

See also:

- "Configuring the VLAN QoS level" (page 62)
- "Viewing and assigning QoS levels by port" (page 63)

Static tab fields

Variable definitions

Use the data in the following table to help you use the Static tab.

Variable	Value
MacAddress	The MAC address of this entry. This address is used to match the destination address of incoming packets.
Port	The port number.
Monitor	Select to copy packets with a MAC address in the source or destination field. Used with port mirroring.
QoSLevel	The assigned QoS level for all traffic from a VLAN.

Configuring broadcast and multicast rate limiting

Configure rate limiting to limit the amount of broadcast and multicast traffic carried on a port.

Step	Action
1	On the Device view, choose a port.
2	From the Device Manager menu bar, choose **Edit, Port, General - GeneralRouter (vrf 0)**. The Port - GeneralRouter (vrf 0) dialog box appears with the Rate Limiting tab displayed.
3	Click the **Rate Limiting** tab. The Rate Limiting tab appears.
4	Double-click **TrafficType** and select either multicast or broadcast.
5	To edit the rate, double-click**AllowedRate**.
6	Click **Apply**.

--End--

For more information, see "Rate Limiting tab fields" (page 65).

See also:

- "Building global filter sets" (page 99)
- "Building source and destination filter sets" (page 100)
- "Configuring port filter actions" (page 101)
- "Configuring IP telephony and multimedia platform filters " (page 102)
- " Configuring IP telephony and multimedia streams " (page 104)
- "Configuring IP telephony and multimedia filter lists on a port " (page 105)
- "Enabling and disabling an IP telephony and multimedia filter on a port" (page 107)
- "Deleting an IP telephony and multimedia filter list from a port" (page 108)

Rate Limiting tab fields

Variable definitions

Use the information in the following table to help you use the Rate Limiting tab.

Variable	Value
Index	Specifies the port.
TrafficType	Specifies multicast or broadcast traffic.
AllowedRateKbps	Sets the rate limit in kbit/s.
Enable	Enables or disables rate limiting on the port.

QoS configuration using the CLI

Configure QoS to ensure that network resources are allocated where they are needed most. All information about statistics is moved to *Nortel Ethernet Routing Switch 8600 Performance Management* (NN46205-704) .

Navigation

Job aid: Roadmap of QoS CLI commands

The following roadmap lists some of the QoS commands and their parameters. Use this list as a quick reference.

Table 15
Job aid: Roadmap of QoS CLI commands

Command	Parameter
`config ethernet <ports>`	`access-diffserv <true|false>`
	`broadcast-rate-limit <value> [<enable|disable>]`
	`enable-diffserv <true|false>`
	`multicast-rate-limit <value> [<enable|disable>]`
	`qos-level <0...6>`

Table 15
Job aid: Roadmap of QoS CLI commands (cont'd.)

Command	Parameter
`config qos egressmap`	`1p <level> <ieee1p>`
	`ds <level> <dscp>`
	`exp <level> <exp>`
	`info`
`config qos ingressmap`	`1p <ieee1p> <level>`
	`ds <dscp> <level>`
	`exp <exp> <level>`
	`info`
`show qos egressmap`	`1p <level>`
	`ds <level>`
	`exp <level>`
`show qos ingressmap`	`1p [<ieee1p>]`
	`ds [<dscp>]`
	`exp [<exp>]`
`show qos queue <level>`	

DiffServ configuration

Use DiffServ to implement classification and mapping functions at the network boundary or access points, thus regulating packet behavior. With Classic modules, you can configure a port as either a trusted (core) or untrusted (access) port.

DiffServ configuration navigation

- "Enabling Diffserv for a port" (page 68)
- "Configuring Layer 3 trusted/untrusted ports" (page 69)
- "Configuring the port QoS level" (page 70)
- "Configuring the VLAN QoS level" (page 70)
- "Configuring the QoS level for specific MAC addresses" (page 71)

Enabling Diffserv for a port

Enable DiffServ so that the Ethernet Routing Switch will use DiffServ to provide DiffServ-based QoS on that port.

> **ATTENTION**
> When you first enable DiffServ on a port, the port type is set to core by default, which means that the Type of Service (TOS) bits are trusted (IP provides a Type of Service implementation, providing traffic prioritization, and Quality of Service [QoS] attributes).

Procedure steps

Step	Action
1	Enable Diffserv on a port by using the following command:

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

--End--

Variable definitions

The following table describes variables that you enter in the **config ethernet <ports> enable-diffserv <true|false>** command.

Variable	Value
enable-diffserv <true|false>	True enables diffserv for the port or ports selected. When set to true all other QoS parameter values and functions now take affect and are applied. If set to false, these parameters and settings do not apply. By default, enable-diffserv is false.

Configuring Layer 3 trusted/untrusted ports

Configure a port as trusted or untrusted to determine the Layer 3 QoS actions the switch performs. A trusted port honors incoming DSCP markings. An untrusted port overrides DSCP markings.

Procedure steps

Step	Action
1	Ensure DiffServ is enabled.
2	Configure the port as Layer 3 trusted or untrusted:

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

--End--

Variable definitions

The following table describes variables that you enter in the `config ethernet <ports> access-diffserv true` command.

Variable	Value
`access-diffserv <true|false>`	True specifies an access port and overrides incoming DSCP bits; false specifies a core port and honors and services incoming DSCP bits. By default, access-diffserv is false.

The Device Manager field for this parameter is called Layer3Trust. A value of true = access (for Device Manager) and false = core (for Device Manager).

Configuring the port QoS level

Use the default port QoS level to assign a default QoS level for all traffic.

Procedure steps

Step	Action
1	Configure the port QoS level by using the following command: `config ethernet <ports> qos-level <0...6>`

--End--

Variable definitions

The following table describes variables that you enter in the `config ethernet <ports> qos-level <0...6>` command.

Variable	Value
`qos-level <0...6>`	Specifies the default QoS level for the port traffic. QoS level 7 is reserved for network control traffic. By default, the QoS level is set to 1 (one).

Configuring the VLAN QoS level

The default port or VLAN QoS levels can be changed to assign a default QoS level for all traffic.

Procedure steps

Step	Action
1	Configure the VLAN level by using the following commands:

```
config vlan <vlan-id> qos-level <integer>
```

`<vlan-id>` specifies the VLAN ID (1 to 4094) for which you wish to specify the QoS level.

--End--

Variable definitions

The following table describes variables that you enter in the **`config vlan <vlan-id> qos-level <integer>`** command.

Variable	Value
`qos-level <integer>`	Specifies the default QoS level for the VLAN traffic. QoS level 7 is reserved for network control traffic. By default, the QoS level is set to 1 (one).

Configuring the QoS level for specific MAC addresses

Apply a QoS level to traffic from specific VLAN MAC addresses to provide special QoS treatment to the packets.

Procedure steps

Step	Action
1	To set the source MAC QoS level for a dynamically-learned address, enter the following command: **`config vlan <vlan id> fdb-entry qos-level <mac> status <value> <0...6>`**
2	To configure the source MAC QoS level for a static address: **`config vlan <vlan id> fdb-static add <mac> port <value> qos <value>`**

--End--

Variable definitions

The following table describes variables that you enter in the **`config vlan <vlan id> fdb-entry qos-level <mac> status <value> <0...6>`** command.

Variable	Value
`<0...6>`	Specifies the QoS level.

Variable	Value
`<mac>`	`mac` specifies the MAC address in the format 0x00:0x00:0x00:0x00:0x00:0x0 0.
`<vlan id>`	Specifies the VLAN (1 to 4094) for which you wish to specify the QoS level.
`status <value>`	Specifies the FDB status (other|invalid|learned|self|mgmt).

The following table describes optional parameters the you enter after the`config vlan <vid> fdb-static add <mac> port <value> qos <value>` command.

Variable	Value
`info`	Shows current level parameter settings and next level directories.
`remove <mac>`	Removes a static member to a VLAN. `mac` is the MAC address in the format {0x00:0x00:0x00:0x00:0x00:0x00}.

Configuring the QoS egress mapping table

You can modify the QoS egress mapping to change traffic priorities. However, Nortel recommends that you use the default mappings.

Prerequisites

- Changes to this mapping table do not take effect until you save and reboot the switch.

Procedure steps

Step	Action
1	Configure the QoS to 802.1p mappings by using the following command: `config qos egressmap 1p <level> <ieee1p>`
2	Configure the QoS to DSCP mappings by using the following command: `config qos egressmap ds <level> <dscp>`

--End--

Variable definitions

The following table describes variables that you enter in the **`config qos egressmap 1p <level> <ieee1p>`** and **`config qos egressmap ds <level> <dscp>`** commands.

Variable	Value
`1p <level> <ieee1p>`	Maps QoS Level to IEEE 1p priority. • `level` is the QoS level in the range of 1 to 7. • `ieee1p` is the IEEE 1P Priority in the range of 1 to 7.
`ds <level> <dscp>`	Maps QoS Level to DS Byte. • `level` is the QoS level in the range of 1 to 7. • `dscp` is the Diff-Serv Code Point : Hex/Binary/Decimal. The string length is 1 to 6.

The following table describes optional parameters the you enter after the **`config qos egressmap`** and **`config qos egressmap`** commands.

Variable	Value
`1p <level> <ieee1p>`	Maps the QoS level to IEEE 802.1p priority bit level.`<ieee1p>` is the IEEE 802.1p bit level. The value ranges from 0 to 7. `<level>` is the QoS level.
`ds <level> <dscp>`	Maps the QoS level to the DSCP. `<dscp>` ranges from 0 to 63. `<level>` is the QoS level.
`exp <level> <exp>`	Maps the QoS level to EXP bits. <exp> ranges from 0 to 7. `<level>` is the QoS level. Only R and RS modules support MPLS.
`info`	Displays which DSCP and IEEE 802.1p levels are mapped to QoS levels for egress traffic.

Configuring the QoS ingress mapping table

You can modify the ingress QoS mapping table to change traffic priorities. However, Nortel recommends that you use the default mappings.

Procedure steps

Step	Action
1	To configure DSCP to QoS ingress mappings:

```
config qos ingressmap ds <dscp> <level>
```

2 To configure 802.1p bit to QoS ingress mappings:

```
config qos ingressmap 1p <ieee1p> <level>
```

3 Ensure the configuration is correct:

```
show qos ingressmap <1p|ds|exp> [<value>]
```

--End--

Variable definitions

The following table describes variables that you enter in the **config qos ingressmap ds <dscp> <level>** command.

Variable	Value
`ds <dscp> <level>`	Maps the DS byte to QoS level. • `level` configures the QoS level from 0 to 7. • `dscp` configures the DiffServ Code Point (DSCP) as an index from 0 to 63.

Use the data in the following table to help you use the **config qos ingressmap ds <dscp> <level>** command.

Variable	Value
`1p <ieee1p> <level>`	Maps the IEEE 802.1p bit to QoS level. • `level` configures the QoS level from 0 to 7. • `ieee1p` configures the IEEE 1p bit level as an index from 0 to 7.
`exp <exp> <level>`	Maps the MPLS EXP bit to a QoS level with a range from 0 to 7. Only R and RS modules support MPLS.
`info`	Displays information about the QoS ingress mappings.

Showing QoS queue information

Use this procedure to view the QoS queue information for the eight queues on a Classic module.

Procedure steps

Step Action

1 Show QoS queue information by using the following command:

```
show qos queue [<level>]
```

--End--

Variable definitions

The following table describes variables that you enter in the **`show qos queue [<level>]`** command.

Variable	Value
`<level>`	Shows the queue level index in the range of 0 to 7.

Configuring broadcast and multicast rate limiting

Use broadcast and multicast rate limiting to limit the amount of ingress broadcast and multicast traffic on a port. Traffic that violates the rate limit is dropped.

Broadcast and multicast bandwidth limiting is supported on R and RS modules. Broadcast and multicast rate limiting is supported on Classic modules.

Procedure steps

Step	Action
1	Configure broadcast rate limiting by using the following command: **`config eth <ports> broadcast-rate-limit <value> enable`**
2	Configure multicast rate limiting by using the following command: **`config eth <ports> multicast-rate-limit <value> enable`**

--End--

Variable definitions

The following table describes variables that you enter in the **`config eth <ports> broadcast-rate-limit <value> enable`** and **`config eth <ports> multicast-rate-limit <value> enable`** commands.

Variable	Value
`broadcast-rate-limit <value> [<enable|disable>]`	Specifies the rate limit for broadcast traffic from 250 to 2 147 483 647 kbit/s. **`enable|disable`** enables or disables rate limiting.
`multicast-rate-limit <value> [<enable|disable>]`	Specifies the rate limit for multicast traffic from 250 to 2 147 483 647 kbit/s. **`enable|disable`** enables or disables rate limiting.

QoS configuration using the NNCLI

Use the procedures in this section to configure QoS in your Ethernet Routing Switch 8600.

Navigation

Job aid: Roadmap of QoS NNCLI commands

The following roadmap lists some of the QoS commands and their parameters. Use this list as a quick reference.

Table 16
Job aid: Roadmap of QoS NNCLI commands

Command	Parameter
Privileged EXEC mode	
`show vlan mac-address-entry [<1-4094>] [mac <WORD>] [port <portlist>]`	
`show qos 802.1p-override`	`<cr>`
	`fastEthernet <portlist>`
	`gigabitEthernet <portlist>`
	`vlan <1-4094>`

Table 16
Job aid: Roadmap of QoS NNCLI commands (cont'd.)

Command	Parameter
show qos egress-map	<cr>
	1p <0-7>
	ds <0-7>
show qos egress-queue-set [port <portlist>] [<1-386>]	
show qos eq-map <1-10>	
show qos ingress-map	<cr>
	1p <0-7>
	ds <0-63>
show qos policy-config	<cr>
	<1-16383>
	lane <WORD 1-128>
	port <portlist>
show qos queue [<0-7>]	
show qos statistics egress-queue-set	<cr>
	<1-386>
	[detail]
	interface-type {fastEthernet <portlist>|gigabitEthernet <portlist>}
show qos statistics policy	<cr>
	<0-20000>
	lane <WORD 1-128>
	port <portlist>
Global Configuration mode	
qos egressmap	1p <0-7> <0-7>
	ds <0-7> <WORD 1-6>
qos ingressmap	1p <0-7> <0-7>
	ds <0-63> <0-7>
qos policy <1-16383>	lanes <WORD 1-128>
	name <WORD 1-32>
	peak-rate <250-10000000> svc-rate <250-10000000>

Table 16
Job aid: Roadmap of QoS NNCLI commands (cont'd.)

Command	Parameter
`qos threshold <0-3> <0-7>`	`<cr>`
	`<0-63>`
Interface Configuration mode	
`access-diffserv [port <portlist>] [enable]`	
`enable-diffserv [port <portlist>] [enable]`	
`qos`	`802.1p-override [enable]`
	`[port <portlist>] level <0-6>`
`rate-limit [port <portlist>]`	`broadcast <1-65535>`
	`multicast <1-65535>`

DiffServ port configuration

This section describes how to configure a DiffServ port to enable end-to-end QoS for IP traffic.

DiffServ port configuration navigation

- "Enabling Diffserv on a port" (page 79)
- "Configuring Layer 3 trusted/untrusted ports" (page 80)
- "Configuring the port QoS level" (page 70)
- "Configuring the VLAN QoS level" (page 81)
- "Configuring the QoS level for specific MAC addresses" (page 82)

Enabling Diffserv on a port

Enable DiffServ so that the switch uses the DiffServ to provide DiffServ-based QoS on that port.

Prerequisites

- You must log on to the Interface Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Enable Diffserv on a port by using the following command: `enable-diffserv [port <portlist>] [enable]`

--End--

Variable definitions

Use the data in the following table to help you use the **`enable-diffserv`** command.

Variable	Value
`[enable]`	Enables Diffserv on a port.
`[port <portlist>]`	Specifies the ports which are to be changed.

Configuring Layer 3 trusted/untrusted ports

Configure a port as trusted or untrusted to determine the Layer 3 QoS actions the switch performs. A trusted port honors incoming DSCP markings. An untrusted port overrides DSCP markings.

Prerequisites

- You must log on to the Interface Configuration mode in the NNCLI.
- Ensure DiffServ is enabled.

Procedure steps

Step	Action
1	Configure the port as Layer 3 untrusted by using the following command: `access-diffserv [port <portlist>] [enable]`

--End--

Variable definitions

Use the following table to help you use the **`access-diffserv`** command.

Variable	Value
`[enable]`	If enabled, specifies an access port and overrides incoming DSCP bits. If disabled, specifies a core port and honors and services incoming DSCP bits. By default, access-diffserv is false.
`port <portlist>`	Specifies the ports which are to be changed.

Configuring the port QoS level

Use the default port QoS level to assign a default QoS level for all traffic.

Prerequisites

You must log on to the Interface Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure the port QoS level by using the following command: `qos level [port <portlist>] <0-6>`

--End--

Variable definitions

Use the following table to help you use the `qos level` command.

Variable	Value
`<0-6>`	Specifies the default QoS level for the port traffic. QoS level 7 is reserved for network control traffic. By default, the QoS level is set to 1 (one).
`port <portlist>`	Specifies the slot and port, or slot and port list.

Configuring the VLAN QoS level

The default port or VLAN QoS levels can be changed to assign a default QoS level for all traffic.

Prerequisites

- You must log on to the VLAN Interface Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure the VLAN QoS level by using the following command: `qos level [port <portlist>] <0-6>`

--End--

Variable definitions

Use the following table to help you use the `qos level` command.

Variable	Value
`<0-6>`	Specifies the default QoS level for the VLAN traffic. QoS level 7 is reserved for network control traffic. By default, the QoS level is set to 1 (one).
`port <portlist>`	Specifies the ports to be changed.

Configuring the QoS level for specific MAC addresses

Apply a QoS level to traffic from specific VLAN MAC addresses to provide special QoS treatment to the packets.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	To set the source MAC QoS level for a dynamically-learned address, enter the following command: `vlan mac-address-entry <1-4094> qos-level <H.H.H> <0-6> status <other|invalid|learned|self|mgmt>`
2	To configure the source MAC QoS level for a bridge static address: `vlan mac-address-static <1-4094> <H.H.H> <portlist> qos <0-6>`
3	To configure the source MAC QoS level for a bridge filter address:

```
vlan mac-address-filter <1-4094> <H.H.H> <portlist>
<0-6>
```

--End--

Variable definitions

Use the data in the following table to help you use the commands in this procedure.

Variable	Value
`<0-6>`	Specifies the QoS level.
`<1-4094>`	Specifies the VLAN ID.
`<H.H.H>`	Specifies the MAC address in the format 0x00:0x00:0x00:0x00:0x00 :0x00
`<portlist>`	Specifies the slot and port, or slot and port list.
`status <other|invalid|learned|self|mgmt>`	Specifies the FDB status (other|invalid|learned|self|mgmt).

Configuring the QoS egress mapping table

You can modify the egress QoS mapping table to change traffic priorities. However, Nortel recommends that you use the default mappings.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.
- Save and reboot the switch for the mapping table to take effect.

Procedure steps

Step	Action

1 To configure QoS to DSCP egress mappings:

```
qos egressmap ds <0-7> <WORD 1-6>
```

2 To configure QoS to 802.1p bit egress mappings:

```
qos egressmap 1p <0-7> <0-7>
```

3 Ensure the configuration is correct:

```
show qos egress-map
```

--End--

Variable definitions

Use the data in the following table to help you use the `qos egressmap` commands.

Variable	Value
`ds <0-7> <WORD 1-6>`	Maps the QoS level to DS byte. You can specify the DSCP in either hexadecimal, binary, or decimal.
`exp <0-7> <0-7>`	Maps the QoS level to MPLS EXP level. Only R and RS modules support MPLS.
`1p <0-7> <0-7>`	Maps the QoS level to IEEE 802.1p priority in the range of 0 to 7.

Configuring the QoS ingress mapping table

You can modify the ingress mappings to change traffic priorities. However, Nortel recommends that you use the default mappings.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.
- Changes to this mapping table do not take effect until you save and reboot the switch.

Procedure steps

Step	Action

1 To configure QoS to DSCP egress mappings:

```
qos ingressmap ds <0-63> <0-7>
```

2 To configure QoS to 802.1p bit egress mappings:

```
qos ingressmap 1p <0-7> <0-7>
```

3 Ensure the configuration is correct:

```
show qos ingress-map
```

--End--

Variable definitions

Use the data in the following data in table to help you use the **`qos ingressmap`** commands.

Variable	Value
`ds <0-63> <0-7>`	Maps the DS byte to QoS level.
`exp <0-7> <0-7>`	Maps QoS level to EXP bit level on egress in the range of 0 to 7. MPLS is supported on R and RS modules only.
`1p <0-7> <0-7>`	Maps the IEEE 802.1p bit to QoS level.

Showing QoS queue information

Use this procedure to view the QoS queue information on the Ethernet Routing Switch 8600.

Prerequisites

You must log on to the Privileged Exec mode in the NNCLI.

Procedure steps

Step	Action
1	Show the QoS queue information by using the following command: `show qos queue [<0-7>]`

--End--

Variable definitions

Use the data in the following table to help you use the commands in this procedure.

Variable	Value
`<0-7>`	Shows the queue parameters for a specific QoS level.`0-7` is the QoS level.

Configuring broadcast and multicast rate limiting

Use broadcast and multicast rate limiting to limit the amount of ingress broadcast and multicast traffic on a port. Traffic that violates the rate limit is dropped.

Broadcast and multicast bandwidth limiting is supported on R and RS modules. Broadcast and multicast rate limiting is supported on Classic modules.

Prerequisites

- You must log on to the Interface Configuration in the NNCLI.

Procedure steps

Step	Action

1	Configure broadcast and multicast rate limiting by using the following commands:
	`rate-limit [port <portList>] broadcast <1-65535>`
	`rate-limit [port <portList>] multicast <1-65535>`

--End--

Variable definitions

Use the data in the following table to help you use the commands in this procedure.

Variable	Value
`broadcast <1-65535>`	Sets the rate-limit for broadcast traffic from 0 to 65535 packets per second.
`multicast <1-65535>`	Sets the rate-limit for multicast traffic from 0 to 65535 packets per second.
`<portlist>`	Specifies the slot and port.

Traffic filter configuration using Device Manager

Use traffic filtering to provide security by blocking unwanted traffic and to help provide QoS by prioritizing other traffic.

Select a topic:

Navigation

- “Configuring IP telephony and multimedia platform filters ” (page 102)
- “ Configuring IP telephony and multimedia streams ” (page 104)
- “Configuring IP telephony and multimedia filter lists on a port ” (page 105)
- “Enabling and disabling an IP telephony and multimedia filter on a port” (page 107)
- “Deleting an IP telephony and multimedia filter list from a port” (page 108)
- “Rate-limiting traffic profile configuration” (page 110)
- “Configuring traffic filters for DiffServ access ports” (page 108)
- “Configuring broadcast and multicast rate limiting” (page 65)

Filter management

This section describes how to manage filters.

Select a topic:

- “Inserting a global filter” (page 88)
- “Inserting a destination filter” (page 92)
- “Inserting a source filter” (page 94)
- “Editing a filter” (page 96)
- “Controlling filters” (page 97)

Filter management navigation

- “Inserting a global filter” (page 88)
- “Inserting a destination filter” (page 92)
- “Inserting a source filter” (page 94)
- “Editing a filter” (page 96)
- “Controlling filters” (page 97)

Inserting a global filter

Use a global filter to selectively accept, reject, or modify traffic.

Procedure steps

Step **Action**

1 From the Device Manager menu bar, choose **Security, Data Path, Filters**.

The Filter dialog box appears with the Filters tab displayed.

2 Click **Insert**.

The Filters, Insert Filters dialog box appears.

Use this dialog box to select the criteria for global filters and DiffServ filters.

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, udp (optional), ospf, ipsecesp, ipsecah, vrrp, or usrDefined.

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

This step is applicable only if you select a TCP, UDP, or user-defined protocol.

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

This step is applicable only if you select a TCP, UDP, or user-defined protocol.

12 Set the following parameters (optional):

- **Mirror**
- **TcpConnect**

> **ATTENTION**
> TcpConnect is available only if you select a TCP or user-defined protocol.

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

14 In the **StopOnMatch** option box, select **enable** or **disable**.

15 If you want to match ICMP request packets, select **MatchIcmpRequest** .

16 If you want to match ICMP fragmented packets, select **MatchIpFragment** .

17 If you want to enable statistics, select **EnableStatistic** .

18 If you want to modify 802.1p bit markings, select **DiffServModifyIeee8021PEnable**.

> **ATTENTION**
> 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 modified value in the **DiffServModifyIeee8021P** field.

20 If you want to modify DSCP markings, select **DiffServModifyDscpEnable**.

21 In the **DiffServModifyDscp** field, 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 associate with this filter.

23 Click **Insert**.

--End--

For more information, see “Filters tab fields” (page 90).

See also:

- “Inserting a destination filter” (page 92)
- “Inserting a source filter” (page 94)
- “Editing a filter” (page 96)
- “Controlling filters” (page 97)

Filters tab fields

Variable definitions

Use the data in the following table to help you configure the Filters tab.

Variable	Value
Type	Source filter, destination filter, global filter.
DstAddr	Destination IP address.
DstMask	Destination subnet mask.

Variable	Value
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	The TCP/UDP source port number.
SrcOption	The TCP/UDP source port option (ignore, equal, less, greater, or not equal).
DstPort	The TCP/UDP destination port number.
DstOption	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	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 to perform matching on ICMP request packets.
MatchIpFragment	Set to perform matching on fragmented IP packets.
EnableStatistic	Set to enable if you want statistics for this filter.
NextHopForwardIpAddr	Set to enable to apply the filter to the next hop (destination/source filter only).
NextHopUnreachableDropEnable	Set to enable if you want drop action (destination/source filter only).
DiffServMatchDscpEnable	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 (destination/source filter only).

Variable	Value
DiffServMatchDscp	Specifies 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 must not be changed.
DiffServModifyIeee8021PEnable	Set to enable to allow the IEEE 802.1p field to be modified on packets ingressing DiffServ access port only. By default, the IEEE 802.1p field is set to 0.
DiffServModifyIeee8021P	If you do not want the IEEE 802.1p field set to 0, 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 port 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	Specifies which traffic profile is applied to packets matching this filter. A zero value means no traffic profile is applied.

Inserting a destination filter

Use a destination filter to selectively accept, modify, or reject traffic based on destination IP parameters.

Procedure steps

Step	Action
1	From the Device Manager menu bar, choose **Security, Data Path, Filters**. The Filter dialog box appears with the Filters tab displayed.
2	From the **Filters** tab, click **Insert**. The Filter, Insert Filters dialog box appears.
3	In the **Type** field, select **destination**.

4 In the **DstAddr** field, type the destination IP address.

5 In the **DstMask** field, type the destination subnet mask.

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, udp (optional), ipsecesp, ipsecah, ospf, vrrp, or usrDefined.

10 Configure **ProtocolTypeUsrDefined** as required.

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

This step is applicable only if you select a TCP, UDP, or user-defined protocol.

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, UDP, or usrDefined protocol was selected.

13 Set the following parameters (optional):

- **Mirror**
- **TcpConnect**

> **ATTENTION**
> TcpConnect is available only if you select a TCP or user-defined protocol.

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

15 Enable or disable**StopOnMatch** .

16 To match on ICMP request packets, select**MatchIcmpRequest** .

17 To match on fragmented IP packets, select **MatchIpFragment** .

18 To enable statistics for this filter, select**EnableStatistic** .

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

20 Enable or disable **NextHopUnreachableDropEnable** as required.

21 Enable **DiffServMatchDscpEnable** 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 value of **00**.

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

24 To modify the IEEE 802.1p field, enable**DiffServModifyIeee8021PEnable** .

25 If you do not want to use the IEEE 802.1p value automatically assigned based on the QoS table, enter the modified value in the **IEEE 802.1p** field.

> **ATTENTION**
> 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, 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, be to associate with this filter.

29 Click **Insert**.

--End--

See also:

- "Inserting a global filter" (page 88)
- "Inserting a source filter" (page 94)
- "Editing a filter" (page 96)
- "Controlling filters" (page 97)

Inserting a source filter

Use a source filter to selectively accept, modify, or reject traffic based on source IP parameters.

Procedure steps

Step	Action
1	From the Device Manager menu bar, choose **Security, Data Path, Filters**. The Filter dialog box appears with the Filters tab displayed.

2 Click **Insert** tab.

The Filters, Insert Filters dialog box appears.

3 In the **Type** field, select **Source**.

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), ipsecesp, ipsecah, ospf, vrrp, or usrDefined.

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 you select a TCP, UDP, or user-defined protocol.

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

This step is applicable only if you select a TCP, UDP, or user-defined protocol.

13 Set the following parameters (optional):

- **Mirror**
- **TcpConnect**

ATTENTION
TcpConnect is available only if a TCP or usrDefined protocol was selected.

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 To match fragmented IP packets, enable**MatchIpFragment** .

18 To enable statistics, select **EnableStatistic** .

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

20 Enable or disable**NextHopUnreachableDropEnable** as required.

21 To modify the DiffServMatchDscp field, select**DiffServMatchDscpEnable** .

22 To match the DiffServ codepoint field, enter **DiffServMatchDscp** value (in binary format).

23 Leave the **DiffServMatchDscpReserved** field at its default of **00**.

> **ATTENTION**
> When you enable a traffic filter to modify either the DSCP or the IEEE 802.1p bits, the traffic filter also modifies the 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 modified value in the **IEEE 802.1p** field.

26 In the **DiffServModifyDscpEnable** option box, click to enable if you want to modify the DSCP.

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**.

--End--

See also:

- "Inserting a global filter" (page 88)
- "Inserting a destination filter" (page 92)
- "Editing a filter" (page 96)
- "Controlling filters" (page 97)

Editing a filter

Use this procedure to edit the filter parameters.

Procedure steps

Step	Action
1	From the Device Manager menu bar, choose **Security, Data Path, Filters**.

The Filter dialog box appears with the Filters tab displayed.

> **ATTENTION**
> Packets matching a filter match criteria follow the filter action specified in the filter. The options set for DiffServ is seen in the DiffServs tab, not in the Filters tab.

2 Double-click any of the fields with white backgrounds to either select a new value from the pop-up menu or to enter a new value.

3 Click **Apply**.

4 Click **Refresh**.

5 After you edit the filter, reapply the filter set to the port associated with that filter.

--End--

See also:

- "Inserting a global filter" (page 88)
- "Inserting a destination filter" (page 92)
- "Inserting a source filter" (page 94)
- "Controlling filters" (page 97)

Controlling filters

Use this procedure to view and manage filter information.

Procedure steps

Step	Action
1	From Device Manager menu bar choose, **Security, Data Path, Filters**. The Filter dialog box appears with the Filters tab displayed.
2	Click the **Control** tab. The Control tab appears.
3	Click **Refresh**.
4	Configure the parameters you want to modify for each filter.
5	Click **Apply**.
6	Double-click any of the fields with white backgrounds 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 ModifyIeee8021P Enable field to disable.

7 Click **Apply**.

8 Click **Refresh**.

9 After you edit the filter, enable or disable the port.

--End--

For more information, see "Control tab fields" (page 98)

See also:

- "Inserting a global filter" (page 88)
- "Inserting a destination filter" (page 92)
- "Inserting a source filter" (page 94)
- "Editing a filter" (page 96)

Control tab fields

Variable definitions

Use the data in the following table to help you use the Control tab.

Variable	**Value**
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	Set mode to: • UseDefaultAction • Forward • Drop • ForwardToNextHop
StopOnMatch	Set to true to stop on match, the default setting.
MatchIcmpRequest	Set to true to perform matching on ICMP request packets..

Variable	Value
MatchIpFragment	Set to true to perform matching on fragmented IP packets.
EnableStatistic	Set to true if you want statistics for this filter.
NextHopForwardIpAddr	Set to enable to apply the filter to the next hop.
NextHopUnreachableDropEnable	Set to enable if you want drop action.

Building global filter sets

Build global filter sets to group global filters.

Procedure steps

Step	Action
1	From the Device Manager menu bar, choose **Security, Data Path, Filters**. The Filter dialog box appears with the Filters tab displayed.
2	Click the **Global Sets** tab. The Global Sets tab appears.
3	Click **Refresh**.
4	Click **Insert**. The Filter, Insert Global Sets dialog box appears.
5	Type the filter ID, name, and select the filter ID from the **FilterIdList**.
6	Click **Insert**.

--End--

For more information, see "Global Sets tab fields" (page 99).

Global Sets tab fields

Variable definitions

Use the data in the following table to help you use the Global Sets tab.

Variable	Value
Id	A unique value to identify a global filter list.
Name	The name of the filter list.

Variable	Value
FilterIdList	The number of filters that are associated with this filter list.
MemberPorts	The ports on which the filter is used.

Building source and destination filter sets

Build global filter sets to group source or destination filters.

Step	Action
1	From the Device Manager menu bar, choose **Security, Data Path, Filters**. The Filter dialog box appears with the Filters tab displayed.
2	Click the **Source/Destination Sets** tab. The Source/Destination Sets tab appears.
3	Click **Refresh**.
4	Click **Insert**. The Filter, Insert Source/Destination Sets dialog box appears. Use this dialog box to build a list of source and destination filters.
5	Type the filter ID and name, and select the filter ID in the **FilterIdList**.

--End--

For more information, see “Source/Destination Sets tab fields” (page 100).

Source/Destination Sets tab fields

Variable definitions

Use the data in the following table to help you use the Source/Destination Sets tab.

Variable	Value
Id	A unique value to identify a particular global filter list.
Name	The name that is given to the filter list.
FilterIdList	Indicates the number of filters that are associated with this filter list.
MemberPorts	Port on which the filter is used.

Configuring port filter actions

Configure the port filter actions to determine which filters are active on the port, and what actions the port should take for matching filters.

Step	Action
1	From Device Manager menu bar, choose **Security, Data Path, Filters**. The Filter dialog box appears with the Filters tab displayed.
2	Click the **Filtered Ports** tab. The Filtered Ports tab appears.
3	Click **Refresh**.
4	Click **Insert**. The Filter, Insert Filtered ports dialog box appears.
5	In the **Port** field, click the button (...) and select the ports.
6	Click the ellipsis button next to the **FilterSet** field and select a filter set.
7	In the **DefaultAction** option box, set the action mode to **forward**, **drop**, or **none**.
8	Select **Enable** to activate the filter.
9	Click **Insert**.

--End--

For more information, see “Filtered Ports tab fields” (page 102).

See also:

- “Building global filter sets” (page 99)
- “Building source and destination filter sets” (page 100)
- “Configuring IP telephony and multimedia platform filters ” (page 102)
- “ Configuring IP telephony and multimedia streams ” (page 104)
- “Configuring IP telephony and multimedia filter lists on a port ” (page 105)
- “Configuring broadcast and multicast rate limiting” (page 65)
- “Enabling and disabling an IP telephony and multimedia filter on a port” (page 107)
- “Deleting an IP telephony and multimedia filter list from a port” (page 108)

Filtered Ports tab fields

Variable definitions

Use the data in the following table to help you use the Filtered Ports tab.

Variable	Value
IfIndex	The port associated with the filter.
Ports	The ports to which to apply the filter sets. Select physical ports, not logical ports like MLT.
FilterSet	The selection of filter lists, both global and nonglobal.
DefaultAction	This action is forward, drop, or none.
Enable	Activates the filter. When you change a filter parameter, disable the filter on its port and then enable the filter again to reapply the changed filter to the port.
NumGlobalFilters	The number of global filters applied to this port.
NumBaseFilters	The number of base source and destination filters applied to this port.

Configuring IP telephony and multimedia platform filters

Configure IP telephony and multimedia platform filters to provide differentiated service, better network management, flexible call monitoring, and convenient troubleshooting for VoIP calls.

Procedure steps

Step	Action
1	From the Device Manager menu bar, choose **Security, Data Path, Filters**. The Filter dialog box appears with the Filters tab displayed.
2	Click the **Multimedia Platforms** tab. The Multimedia Platforms tab appears.
3	Click **Insert**. The Filter, Insert Multimedia Platforms dialog box appears.
4	Specify a name (optional).
5	Select a platform.
6	Select a device.
7	Specify a gateway IP address (optional).

8 Select **StatisticsEnable** (optional).

9 Click **Insert**.

--End--

For more information, see “Multimedia Platforms tab fields ” (page 103).

See also:

- “Building global filter sets” (page 99)
- “Building source and destination filter sets” (page 100)
- “Configuring port filter actions” (page 101)
- “ Configuring IP telephony and multimedia streams ” (page 104)
- “Configuring IP telephony and multimedia filter lists on a port ” (page 105)
- “Configuring broadcast and multicast rate limiting” (page 65)
- “Enabling and disabling an IP telephony and multimedia filter on a port” (page 107)
- “Deleting an IP telephony and multimedia filter list from a port” (page 108)
-

Multimedia Platforms tab fields

Variable definitions

Use the data in the following table to help you use the Multimedia Platforms tab.

Variable	Value
MediaId	The number assigned to the filter set. The range is from 3000 to 3127.
Name	The name of the multimedia platform.
Platform	The type of multimedia platform used.
Device	The type of multimedia device used.
IpAddress	The IP address of the interface you are specifying.
Stream IDs	Displays the port range ID.
Slot/Ports	Specifies the slot and port.
StatisticEnable	Enables or disables the display of statistics for the filter.

Configuring IP telephony and multimedia streams

Configure IP telephony and multimedia streams to provide differentiated service, better network management, flexible call monitoring, and convenient troubleshooting for VoIP calls, and to prevent multimedia overloading.

Procedure steps

Step	Action
1	From the Device Manager menu bar, choose **Security, Data Path, Filters**. The Filter dialog box appears with the Filters tab displayed.
2	Click the **Multimedia Streams** tab. The Multimedia Streams tab appears.
3	Click **Insert**. The Filter, Insert Multimedia Streams dialog box appears.
4	Click the **MediaId** button (...). The MediaId list box appears.
5	Select a media ID from the list box.
6	Click **OK**.
7	In the **Filter, Insert Multimedia Stream** dialog box, specify a Stream Id.
8	Specify a name (optional).
9	Select a **Protocol** (optional).
10	Specify a **PortMin** (optional).
11	Specify a **PortMax** (optional).
12	Select a **PortOption**.
13	Select a **Type**.
14	Specify **MatchDSCP**.

--End--

For more information, see “Multimedia Streams tab fields” (page 105).

See also:

- “Building global filter sets” (page 99)
- “Building source and destination filter sets” (page 100)
- “Configuring port filter actions” (page 101)

- “Configuring IP telephony and multimedia platform filters ” (page 102)
- “Configuring IP telephony and multimedia filter lists on a port ” (page 105)
- “Configuring broadcast and multicast rate limiting” (page 65)
- “Enabling and disabling an IP telephony and multimedia filter on a port” (page 107)
- “Deleting an IP telephony and multimedia filter list from a port” (page 108)

Multimedia Streams tab fields

Variable definitions

Use the data in the following table to help you use the Multimedia Streams tab.

Variable	Value
MediaId	Displays the Media ID in the Media ID table.
StreamID	Displays the port range ID.
Name	Enter the stream name.
Protocol	Select either TCP or UDP protocol.
PortMin	The TCP/UDP source and destination port to filter on.
PortMax	The TCP/UDP source and destination port to filter on.
PortOption	Select source port, destination port, or both.
Stream Type	Type of stream to filter: signal or media.
RemarkDscp	Specifies if the DSCP is remarked.
MatchDscp	Used to specify what the value of the DSCP is 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

Configure IP telephony and multimedia filter lists on a port to filter IP telephony and multimedia traffic.

Procedure steps

Step **Action**

1 From Device Manager menu bar, choose **Security, Data Path, Filters**.

The Filter dialog box appears with the Filters tab displayed.

2 Click the **Filtered Ports** tab.

The Filtered port tab appears.

3 Click **Insert**.

The Filter, Insert Filtered ports dialog box appears.

4 Click the **Ports** button (...).

The IpFilterPortIfIndex dialog box appears.

5 Select the ports.

6 Click **OK**.

7 Click the **FilterSet** button (...).

8 Select a filter set.

9 Click **OK**.

10 Select **Forward**.

11 Select **Enable**.

12 Click **Insert**.

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

--End--

For more information, see “Filtered Ports tab fields” (page 102).

See also:

- “Building global filter sets” (page 99)
- “Building source and destination filter sets” (page 100)
- “Configuring port filter actions” (page 101)
- “Configuring IP telephony and multimedia platform filters ” (page 102)
- “ Configuring IP telephony and multimedia streams ” (page 104)
- “Configuring broadcast and multicast rate limiting” (page 65)

- “Enabling and disabling an IP telephony and multimedia filter on a port” (page 107)
- “Deleting an IP telephony and multimedia filter list from a port” (page 108)

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

Enable or disable an IP telephony and multimedia filter on a port to activate or deactivate the filter.

Procedure steps

Step	Action
1	From Device Manager menu bar, choose **Security, Data Path, Filters**. The Filter dialog box appears with the Filters tab displayed.
2	Click the **Filtered Ports** tab. The Filtered Ports tab appears.
3	Double-click in the **Enable** column of the filter you want to enable. A list box appears.
4	Select **true** or **false**.
5	Click **Apply**.

--End--

See also:

- “Building global filter sets” (page 99)
- “Building source and destination filter sets” (page 100)
- “Configuring port filter actions” (page 101)
- “Configuring IP telephony and multimedia platform filters ” (page 102)
- “ Configuring IP telephony and multimedia streams ” (page 104)
- “Configuring IP telephony and multimedia filter lists on a port ” (page 105)
- “Configuring broadcast and multicast rate limiting” (page 65)
- “Deleting an IP telephony and multimedia filter list from a port” (page 108)

Deleting an IP telephony and multimedia filter list from a port

Use this procedure to remove an IP telephony and multimedia filter from a port.

Procedure steps

Step	Action
1	From Device Manager menu bar, choose **Security, Data Path, Filters**. The Filter dialog box appears with the Filters tab displayed.
2	Click the **Filtered Ports** tab. The Filtered Ports tab appears.
3	Select the row with the slot and port number of the filter you want to delete.
4	Click **Delete**.

--End--

See also:

- “Building global filter sets” (page 99)
- “Building source and destination filter sets” (page 100)
- “Configuring port filter actions” (page 101)
- “Configuring IP telephony and multimedia platform filters ” (page 102)
- “ Configuring IP telephony and multimedia streams ” (page 104)
- “Configuring IP telephony and multimedia filter lists on a port ” (page 105)
- “Configuring broadcast and multicast rate limiting” (page 65)
- “Enabling and disabling an IP telephony and multimedia filter on a port” (page 107)
-

Configuring traffic filters for DiffServ access ports

Configure the DiffServ parameters to specify the packet actions the DiffServ filter performs.

Procedure steps

Step **Action**

1 From Device Manager menu bar, choose **Security, Data Path, Filters**.

The Filter dialog box appears with the Filters tab displayed.

2 Click the **DiffServs** tab.

The DiffServs tab appears. Packets matching a filter criterion follow the filter action specified in the filter.

> **ATTENTION**
> 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.

3 Click any of the fields with white backgrounds to select a new value.

You can now select either a new value from the pop-up menu or enter a new value.

If you change a value in the **ModifyDscp** or the **ModifyIeee8021P**

4 Set the **ModifyDscpEnable** or **ModifyIeee8021PEnable** field to disable (**false**)

5 Click the **Apply** and the **Refresh** buttons.

6 Set field to enable (**true**).

7 Click **Apply**.

8 Click **Refresh**.

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

10 Click **Apply**.

--End--

For more information, see "DiffServs tab fields" (page 109).

DiffServs tab fields

Variable definitions

Use the data in the following table to help you use the DiffServs tab.

Value	Variable
Id	The unique filter 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	Specifies the match value for the DSCP. The user must enter a 6-bit binary value. By default the value is 000000. If the DSCP in the incoming packet matches this value, 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 must not be changed.
ModifyIeee8021PEnable	Set to enable to allow the IEEE 802.1p field to be modified on the packets ingressing DiffServ access port only. By default, the IEEE 802.1p field is set to zero.
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 the packets ingressing DiffServ access port 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	Specifies which traffic profile is applied to the packets matching this filter. A zero value means no traffic profile is applied.

Rate-limiting traffic profile configuration

This section describes how to create and manage a rate-limiting traffic profile. It also describes how to assign a traffic rate to a microflow or an aggregate flow as it traverses the DiffServ network.

> **ATTENTION**
> 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), then 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 are discarded, based on the action defined in the traffic profile.

Select a topic:

- "Creating a rate-limiting traffic profile" (page 111)
- "Editing a rate-limiting traffic profile" (page 112)

Rate-limiting traffic profile configuration navigation

- "Creating a rate-limiting traffic profile" (page 111)
- "Editing a rate-limiting traffic profile" (page 112)

Creating a rate-limiting traffic profile

Create a traffic profile to specify the handling properties of a traffic flow selected by a classifier. A traffic flow 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.

Step	Action
1	From Device Manager menu bar, choose **QOS, Profile**. The QOSProfile dialog box appears.
2	Click the**Insert** tab. The **QOSProfile, Insert Traffic Profile** dialog box appears.
3	Type information in the appropriate fields.
4	Click **Insert**.

--End--

For more information, see "Traffic Profile tab fields" (page 111).

See also:

- "Editing a rate-limiting traffic profile" (page 112)

Traffic Profile tab fields

Variable definitions

Use the data in the following table to help you use the Traffic Profile tab.

Variable	Value
Id	Profile ID.
Name	Profile name.
Enable	Enables (true) or disables (false) the profile.
TranslateDscpEnable	Specifies whether translation of the DSCP needs to be performed. If true is selected, packets that fall within the traffic profile are remarked with the InProfileDscp value. Packets that fall outside the traffic profile are remarked 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 the packets that fall outside the traffic profile must be discarded.
AverageRate	Average rate is accomplished in increments of 64 bytes every 2.5 milliseconds.

Editing a rate-limiting traffic profile

Edit a traffic profile to add or delete the properties of a traffic flow selected by a classifier.

Procedure steps

Step	Action
1	From Device Manager menu bar, choose **QOS, Profile**. The QOSProfile dialog box appears with the Traffic Profile tab displayed.
2	To change the name of a traffic profile, double-click on the **Name** field and enter a new name.
3	To enable or disable a traffic profile feature, double-click on the desired field and select **enable** (true) or **disable** (false) from the list.

4 Click **Apply**.

--End--

For more information, see “Traffic Profile tab fields” (page 111).

Traffic filter configuration using the CLI

Use traffic filtering to provide security by blocking unwanted traffic and to help provide QoS by prioritizing other traffic.

Navigation

- “Job aid: Roadmap of IP filter CLI commands” (page 115)
- “IP traffic filter configuration” (page 119)
- “Ethernet IP traffic filter commands configuration” (page 132)
- “IP traffic filter show commands” (page 134)

Job aid: Roadmap of IP filter CLI commands

The following roadmap lists some of the IP filter commands and their parameters. Use this list as a quick reference.

Table 17
Job aid: Roadmap of IP filter CLI commands

Command	Parameter
`config ethernet <ports> ip traffic-filter`	`add set <value>`
	`create`
	`delete`
	`disable`
	`enable`
	`info`
	`remove set <value>`

Table 17
Job aid: Roadmap of IP filter CLI commands (cont'd.)

Command	Parameter
config ethernet <ports> ip traffic-filter default-action	drop
	forward
	info
	none
config ethernet <ports> multimedia	disable
	enable
	info
	select <select>
config ip traffic-filter	clear-stats [<fid>]
	info
config ip traffic-filter create	destination dst-ip <value> [src-ip <value>] [id <value>]
	global [src-ip <value>] [dst-ip <value>] [id <value>]
	info
	source src-ip <value> [dst-ip <value>] [id <value>]
	traffic-profile <pid>
config ip traffic-filter filter <fid>	delete
	info
	name <name>
config ip traffic-filter filter <fid> action	info
	mirror <enable|disable>
	mode <default|forward|drop|forward-to-next-hop>
	statistic <enable|disable>
	stop-on-match <true|false>
	tcp-connect <enable|disable>
	traffic-profile <integer>

Table 17
Job aid: Roadmap of IP filter CLI commands (cont'd.)

Command	Parameter
`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`	`ds-field <6-bit dscp> <2-bit reserved>`
	`ds-field-enable <enable|disable>`
	`dst-port <port> [dst-option <value>]`
	`icmp-request <true|false>`
	`info`
	`ip-fragment <true|false>`
	`protocol <protocoltype> [<pid>]`
	`src-port <port> [src-option <value>]`
`config ip traffic-filter filter <fid> modify`	`dscp <6-bit dscp>`
	`dscp-enable <enable|disable>`
	`ieee8021p <integer>`
	`ieee8021p-enable <enable|disable>`
	`info`
`config ip traffic-filter global-set <gsetid>`	`add-filter <fid>`
	`create [name <value>]`
	`delete`
	`info`
	`remove-filter <fid>`
`config ip traffic-filter media <mediaId>`	`create [platform <value>] [device <value>]`
	`delete`
	`gateway-ip <ipaddr>`
	`info`
	`name <name>`
	`statistic <enable|disable>`

Table 17
Job aid: Roadmap of IP filter CLI commands (cont’d.)

Command	Parameter
`config ip traffic-filter media <mediaId> stream <streamId>`	`create`
	`delete`
	`info`
	`match-dscp <6-bit dscpVal>`
	`name <name>`
	`port-option <src|dst|src-dst>`
	`ports min <value> [max <value>]`
	`protocol <udp|tcp>`
	`stream-type <signal|media>`
`config ip traffic-filter set <setid>`	`add-filter <fid>`
	`create [name <value>]`
	`delete`
	`info`
	`name <value>`
	`remove-filter <fid>`
`config ip traffic-filter traffic-profile <pid>`	`average-rate <int>`
	`delete`
	`discard-out-profile <enable|disable>`
	`enable <true|false`
	`in-dscp <value>`
	`info`
	`name <name>`
	`out-dscp <value>`
	`translate-dscp <enable|disable>`
`show ip traffic-filter active`	
`show ip traffic-filter destination [<fid>]`	
`show ip traffic-filter disabled [<port>]`	
`show ip traffic-filter enabled [<port>]`	

Table 17
Job aid: Roadmap of IP filter CLI commands (cont'd.)

Command	Parameter
`show ip traffic-filter global [<fid>]`	
`show ip traffic-filter interface <ports>`	
`show ip traffic-filter media [mediaid]`	
`show ip traffic-filter show-all [file <value>]`	
`show ip traffic-filter source [<fid>]`	
`show ip traffic-filter stats [<fid>]`	
`show ip traffic-filter stream [<mediaid>] [<streamid>]`	
`show ip traffic-filter info`	`global-set [<id>]`
	`set [<id>]`
`show ip traffic-filter traffic-profile info [<id>]`	

IP traffic filter configuration

This section describes how to configure the IP traffic filters to manage traffic and, in some cases, provide security.

IP traffic filter configuration navigation

- "Creating traffic filters" (page 120)
- "Creating traffic filters" (page 120)
- "Creating destination traffic filters" (page 121)
- "Creating source traffic filters" (page 121)
- "Viewing a specific traffic filter" (page 122)
- "Configuring traffic filter action parameters" (page 123)
- "Configuring the traffic filter next-hop IP address" (page 124)
- "Configuring traffic filter match settings" (page 125)
- "Configuring traffic filters for DiffServ access ports" (page 126)
- "Configuring a global filter set" (page 127)
- "Configuring multimedia traffic filters" (page 128)
- "Configuring a media stream traffic filter" (page 129)

- “Configuring a source and destination filter set ” (page 130)
- “Configuring traffic filter rate-limiting profiles” (page 131)

Creating traffic filters

Use traffic filters to selectively accept, reject, or modify traffic.

Procedure steps

Step	Action
1	Create traffic filters by using the following command along with the parameters in the variable definitions table: **`config ip traffic-filter create destination dst-ip <value> [src-ip<value>] [id <value> ]`**

--End--

Variable definitions

The following table describes variables that you enter in the **`config ip traffic-filter create destination dst-ip <value> [src-ip<value>] [id <value> ]`** command.

Variable	Value
`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}.

The following table describes optional parameters the you enter after the **`config ip traffic-filter create destination dst-ip <value> [src-ip<value>] [id <value> ]`** command.

Variable	Value
`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}.

Variable	Value
`info`	Displays the destination, source, and global filters that have been created.
`source 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}.
`traffic-profile <pid>`	Specifies a traffic profile to use with this traffic filter. • `pid` is the profile number in the range 1 to 64.

Creating destination traffic filters

Create a destination filter to selectively accept, modify, or reject traffic based on destination IP parameters.

Procedure steps

Step	Action
1	Create the destination traffic filter by using the following command: `config ip traffic-filter create destination dst-ip <value> [src-ip <value>] [id <value> ]`

--End--

Variable definitions

The following table describes variables that you enter in the **`config ip traffic-filter create destination dst-ip <value> [src-ip <value>] [id <value> ]`** command.

Variable	Value
`destination dst-ip <value> [src-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}.

Creating source traffic filters

Create a source filter to selectively accept, modify, or reject traffic based on source IP parameters.

Procedure steps

Step	Action
1	Create the source traffic filters by using the following command: `ip traffic-filter create source src-ip <value> [dst-ip <value>] [id <value>]`

--End--

Variable definitions

The following table describes variables that you enter in the `ip traffic-filter create source src-ip <value> [dst-ip <value>] [id <value>]` command.

Variable	Value
`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}.

Viewing a specific traffic filter

You can view information about a specific filter and name or delete the filter.

Procedure steps

Step	Action
1	View a specific traffic filter by using the following command along with the following variable definitions table: `config ip traffic-filter filter <fid>`

--End--

Variable definitions

The following table describes optional parameters the you enter after the `config ip traffic-filter filter <fid>` command.

Variable	Value
`action`	Specifies the action commands.

Variable	Value
`delete`	Deletes the specified traffic filter.
`info`	Displays the settings for the specified filter.
`match`	Matches commands.
`modify`	Modifies commands.
`name`	Sets the filter name.

Configuring traffic filter action parameters

Configure the port filter actions to determine which filters are active on the port, and what actions the port should take for matching filters.

Procedure steps

Step	Action
1	Configure the traffic along with the parameters in the variable definitions table: `config ip traffic-filter filter <fid> action`

--End--

Variable definitions

The following table describes optional parameters the you enter after the `config ip traffic-filter filter <fid> action` command.

Variable	Value
`info`	Displays configure actions for the filter.
`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.
`next-hop-forward info`	Displays information about the next-hop-forward filter settings.

Variable	Value
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), packet that match the filter are forwarded normally unless the next-hop-unreachable-drop option is enabled.
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 displays zero 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.
traffic-profile <integer>	Sets the IP traffic profile. The valid options are 0 to 64.

Configuring the traffic filter next-hop IP address

Configure traffic filter action parameters to specify the IP address of the next-hop router.

Procedure steps

Step	Action
1	Configure the traffic filter next-hop IP address by using the following command: **config ip traffic-filter filter <fid> action next-hop-forward ip-address <ipaddr>**

--End--

Variable definitions

The following table describes variables that you enter in the **config ip traffic-filter filter <fid> action next-hop-forward ip-address <ipaddr>** command.

Variable	Value
`ip-address <ipaddr>`	Specifies 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

Configure traffic filter match parameters to specify the match criteria for filters.

Procedure steps

Step	Action
1	Configure the traffic filter match settings by using the following command with the options in the variable definitions table: `config ip traffic-filter filter <fid> match`

--End--

Variable definitions

The following table describes variables that you enter in the **`config ip traffic-filter filter <fid> match ds-field <6-bit dscp> <2-bit reserved>`** command.

Variable	Value
`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 is applied to the packet. • `6-bit dscp` is a binary number • `2-bit reserved` is a binary number

The following table describes optional parameters the you enter after the**`config ip traffic-filter filter <fid> match ds-field <6-bit dscp> <2-bit reserved>`** command.

Variable	Value
`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 or UDP destination port option. {ignore|equal|less|greater|notequal}.
`icmp-request <true|false>`	Enables or disables the traffic filter to match ICMP requests.
`info`	Displays the match settings for the filter.
`ip-fragment <true|false>`	Enables or disables the traffic filter to allow IP fragments to be filtered.
`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}.

Configuring traffic filters for DiffServ access ports

Use traffic filters on DiffServ access ports to modify untrusted DSCP or 802.1p bit markings.

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

Procedure steps

Step	Action
1	Configure the traffic filter for DiffServ access port using the following command, along with the variables in the following table: **config ip traffic-filter filter <fid> modify dscp <6-bit dscp>**

--End--

Variable definitions

The following table describes variables that you enter in the **config ip traffic-filter filter <fid> modify dscp <6-bit dscp>** command.

Variable	Value
dscp <6-bit dscp>	If you want the DS codepoint (DSCP) modified to a nonzero value, use this command to specify the value for the DSCP. After entering the binary number, you must disable and then enable the traffic filter to ensure that it takes effect. **6-bit dscp** is a binary number.

The following table describes optional parameters the you enter after the **config ip traffic-filter filter <fid> modify dscp <6-bit dscp>** command.

Variable	Value
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>	Modifies IEEE 802.1p bits to a nonzero value. Use this field to specify the value for the IEEE 802.1p bits. Disable and enable the filter for changes to take effect.
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.
info	Displays the modify settings for the filter.

Configuring a global filter set

Configure global traffic filter sets to group global filters.

Procedure steps

Step	Action
1	Configure the global traffic filter settings by using the following command: `config ip traffic-filter global-set <gsetid> add-filter <fid>`

--End--

Variable definitions

The following table describes variables that you enter in the **`config ip traffic-filter global-set <gsetid> add-filter <fid>`** command.

Variable	Value
`add-filter <fid>`	Adds a global filter to a global filter set. `fid` is the traffic filter ID in the range of 1–4000.

The following table describes optional parameters the you enter after the **`config ip traffic-filter global-set <gsetid> add-filter <fid>`** command.

Variable	Value
`create [name <value>]`	Creates a global filter set. • `name <value>` sets a name to the filter.
`delete`	Deletes a global filter set.
`info`	Displays the global filter set characteristics.
`remove-filter <value>`	Removes a global filter from a global filter set. `fid` is the traffic filter ID in the range of 1–4000.

Configuring multimedia traffic filters

Configure multimedia platform filters to provide differentiated service, better network management, flexible call monitoring, and convenient troubleshooting for VoIP calls.

Procedure steps

Step	Action
1	Configure the multimedia traffic filter by using the following command:

```
config ip traffic-filter media <mediaId> create
[platform <value> [device <value>]
```

--End--

Variable definitions

The following table describes variables that you enter in the **`config ip traffic-filter media <mediaId> create [platform <value> [device <value>]`** command.

Variable	Value
`create [platform <value> [device <value>]`	Creates a multimedia filter for a platform or a device. • `[platform <value>]` • `[device <value>]`

The following table describes optional parameters the you enter after the **`config ip traffic-filter media <mediaId> create [platform <value> [device <value>]`** command.

Variable	Value
`delete`	Deletes a multimedia filter.
`gateway-ip <ipaddr>`	Specifies the IP address of the gateway.
`info`	Displays information about the traffic filter media.
`name`	Specifies the name of the selected media device.
`statistic <enable|disable>`	Enables or disables the display of statistics about the filter.
`stream`	Configures multimedia filter stream.

Configuring a media stream traffic filter

Configure media stream traffic filter to provide differentiated service, better network management, flexible call monitoring, and convenient troubleshooting for VoIP calls, and to prevent multimedia overloading.

Procedure steps

Step	Action
1	Configure the media stream traffic filter by using the following command:

```
config ip traffic-filter media <mediaId> stream
<streamId> create
```

--End--

Variable definitions

The following table describes variables that you enter in the `config ip traffic-filter media <mediaId> stream <streamId> create` command.

Variable	Value
`create`	Creates a multimedia stream.

The following table describes optional parameters the you enter after the`config ip traffic-filter media <mediaId> stream <streamId> create` command.

Variable	Value
`delete`	Deletes an IP media traffic filter.
`info`	Displays information about the multimedia traffic filter.
`match-dscp <6-bit dscpVal>`	Specifies a 6-bit binary value for the stream.
`name`	Specifies the name of the selected media device.
`port-option <src|dst|src-dst>`	Specifies a port option, either src, dest, or srcDest.
`ports min <value> [max <value>]`	Specifies the minimum port number.
`protocol <udp|tcp>`	Specifies either the TCP or UDP protocol.
`stream-type <signal|media>`	Specifies the type of stream. The valid options are signal and media.

Configuring a source and destination filter set

You can use a source and destination filter set to group source and destination filters. You cannot add global filters to this set.

Procedure steps

Step Action

1 Create a source and destination filter set by using the following command, along with the parameters in the variable definitions table:

```
config ip traffic-filter set <setid>
```

--End--

Variable definitions

The following table describes optional parameters the you enter after the `config ip traffic-filter set <setid>` command.

Variable	Value
`add-filter`	Adds a source or destination filter to a filter set.
`create [name <value>]`	Creates a filter set.
`delete`	Deletes a filter set.
`info`	Displays the filter set characteristics.
`name`	Changes the name of a filter set.
`remove-filter`	Removes a filter from a filter set.

Configuring traffic filter rate-limiting profiles

Configure a traffic profile to specify the handling properties of a traffic flow selected by a classifier. A traffic flow 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.

Procedure steps

Step	Action
1	Configure the traffic filter rate-limiting profiles by using the following commands:

```
config ip traffic-filter traffic-profile <pid>
```

--End--

Variable definitions

The following table describes optional parameters the you enter after the `config ip traffic-filter traffic-profile <pid>` commands.

Variable	Value
`average-rate <int>`	Sets the traffic profile's average rate. See for more information. `int` is the rate {0 to 65535}, which is expressed in 64-byte segments of data allowed in a 2.5 millisecond timeslot.

Variable	Value
`delete`	Deletes the traffic profile.
`discard-out-profie <enable|disable>`	Enables or disables the ability to discard the traffic that violates the traffic profile's average rate.
`emable <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.
`info`	Displays the traffic profile settings.
`name <name>`	Names the traffic profile. `name` is a string of 0–32 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.

Ethernet IP traffic filter commands configuration

This section describes how to manage IP traffic filters.

Ethernet IP traffic filter configuration navigation

- "Applying filters to a port" (page 132)
- "Configuring the default action for a filter" (page 133)
- "Applying a multimedia traffic filter to a port" (page 134)

Applying filters to a port

Apply traffic filters on a port to manage traffic.

Each filter set includes match conditions and actions to perform when a match condition occurs.

Procedure steps

Step	Action
1	Configure the traffic filters on a port by using the following command:

```
config ethernet <ports> ip traffic-filter
```

--End--

Variable definitions

The following table describes optional parameters the you enter after the `config ethernet <ports> ip traffic-filter` command.

Variable	Value
`add set <value>`	Adds a filter set to a port. `value` is the global or source and destination filter set ID (1–1000).
`create`	Creates a traffic filtering entity on a port.
`delete`	Removes filtering from a port.
`disable`	Disables filtering on a port. Whenever you change a filter parameter, disable the filter on its filter port and then enable the filter again to reapply the changed filter to the port.
`enable`	Enables filtering on a port. Whenever you change a filter parameter, you must disable the filter on its filter port and then enable the filter again to reapply the changed filter to the port.
`info`	Displays the traffic filters applied to the port.
`remove set <value>`	Removes a filter set from a port. `value` is the filter set ID in the range 1 to 1000.

Configuring the default action for a filter

Configure the port filter default action for a filter to forward or drop packets that match filter criteria.

Procedure steps

Step	Action
1	Configure the default action on a port traffic filter by using the following command: `config ethernet <ports> ip traffic-filter default-action`

--End--

Variable definitions

The following table describes optional parameters the you enter after the **`config ethernet <ports> ip traffic-filter default-action`** command.

Variable	Value
`drop`	Sets the port filter default action to drop.
`forward`	Sets the port filter default action to forward.
`info`	Displays the port default action configuration.
`none`	Does not apply any policy to the port.

Applying a multimedia traffic filter to a port

Assign a multimedia filter to a port to manage port traffic.

Procedure steps

Step	Action
1	Assign a multimedia traffic filter to a port by using the following command: **`config ethernet <ports> multimedia select <select>`**

--End--

Variable definitions

The following table describes optional parameters the you enter after the **`config ethernet <ports> multimedia`** command.

Variable	Value
`disable`	Disables a multimedia filter on a port.
`enable`	Enables a multimedia filter on a port.
`info`	Displays information about the multimedia Ethernet port.
`select <select>`	Selects the multimedia filter.

IP traffic filter show commands

This section describes the IP traffic filter show commands.

Showing IP traffic filter commands navigation

- “Showing the active traffic filters” (page 135)
- “Showing destination filter information” (page 136)

- “Showing disabled traffic filters” (page 136)
- “Showing enabled traffic filters” (page 135)
- “Showing global traffic filters” (page 136)
- “Showing traffic filter interface information” (page 137)
- “Showing multimedia traffic filter information” (page 137)
- “Showing source traffic filter information” (page 136)
- “Showing multimedia stream traffic filter information” (page 137)
- “Showing all traffic filter information” (page 138)
- “Showing traffic filter global set information” (page 138)
- “Showing source and destination traffic filter set information” (page 138)
- “Showing traffic filter traffic profile information” (page 139)

Showing the active traffic filters

Use this procedure to learn which filters are active.

Procedure steps

Step	Action
1	View the active traffic filters by using the following command: `show ip traffic-filter active`

--End--

Showing enabled traffic filters

Use this procedure to view information about enabled filters on the Ethernet Routing Switch 8600 or on a specified port.

Procedure steps

Step	Action
1	Show enabled traffic filters by using the following command: `show ip traffic-filter enabled [<port>]`

--End--

Showing disabled traffic filters

Use this procedure to learn which filters are disabled.

Procedure steps

Step	Action
1	View the disabled traffic filters by using the following command: `show ip traffic-filter disabled [<port>]`

--End--

Showing global traffic filters

Use this procedure to view global filters for the Ethernet Routing Switch 8600 or for the specified filter IDs.

Procedure steps

Step	Action
1	View the global traffic filters by using the following command: `show ip traffic-filter global [<fid>]`

--End--

Showing destination filter information

Use this procedure to view to view information about active destination filters.

Procedure steps

Step	Action
1	View destination traffic filters by using the following command: `show ip traffic-filter destination [<fid>]`

--End--

Showing source traffic filter information

Use this procedure to view information about active source traffic filters.

Procedure steps

Step	Action
1	View active source traffic filter information by using the following command: `show ip traffic-filter source [<fid>]`

--End--

Showing traffic filter interface information

Use this procedure to learn which filters are applied to a port.

Procedure steps

Step	Action
1	View the traffic filter interface information by using the following command: `show ip traffic-filter interface <port>`

--End--

Showing multimedia traffic filter information

Use this procedure to view multimedia platform and device filters by filter ID.

Procedure steps

Step	Action
1	View filter information by using the following command: `show ip traffic-filter media`

--End--

Showing multimedia stream traffic filter information

You can view information about multimedia stream traffic filters.

Procedure steps

Step	Action
1	Show stream traffic filters by using the following command:

```
show ip traffic-filter stream
```

--End--

Showing all traffic filter information

Use this procedure to view all traffic filter information.

Procedure steps

Step	Action
1	View all the traffic filter information `show ip traffic-filter show-all [file <value>]`

--End--

Showing traffic filter global set information

Use this procedure to view information about the specified global filter set or all global filter lists configured on the Ethernet Routing Switch 8600.

Procedure steps

Step	Action
1	Show the global traffic filter set information by using the following command: `show ip traffic-filter info global-set [<id>]`

--End--

Showing source and destination traffic filter set information

Use this procedure to view information for the specified source and destination filter list or all source and destination filter lists.

Procedure steps

Step	Action
1	Show the traffic filter set information by using the following command:

```
show ip traffic-filter info set [<id>]
```

--End--

Showing traffic filter traffic profile information

Use this procedure to view the traffic profile settings.

Procedure steps

Step	Action
1	Show traffic filter traffic-profile information by using the following command: `show ip traffic-filter traffic-profile info [<id>]`

--End--

Traffic filter configuration using the NNCLI

This chapter describes how to configure IP traffic filters to provide traffic control and basic security by using the Nortel Command Line Interface (NNCLI).

Navigation

Job aid: Roadmap of traffic filter NNCLI commands

The following roadmap lists some of the IP filter commands and their parameters. Use this list as a quick reference.

Table 18
Job aid: Roadmap of traffic filter NNCLI commands

Command	Parameter
PrivEXEC mode	
`clear ip traffic-filter-statistics`	
`show ip traffic-filter`	`<cr>`
	`<1-4096>`
	`<portlist>`
`show ip traffic-filter active`	
`show ip traffic-filter destination [<1-4096>]`	
`show ip traffic-filter enabled [<portlist>]`	

Table 18
Job aid: Roadmap of traffic filter NNCLI commands (cont'd.)

Command	Parameter
show ip traffic-filter global [<1-4096>]	
show ip traffic-filter global-set [<1-100>]	
show ip traffic-filter interface	fastEthernet <portlist>
	gigabitEthernet <portlist>
	pos <portlist>
show ip traffic-filter media [<3000-3127>]	
show ip traffic-filter profile [<1-64>]	
show ip traffic-filter set [<300-1000>]	
show ip traffic-filter source [<1-4096>]	
show ip traffic-filter statistics [<1-3071>]	
show ip traffic-filter stream [<3000-3127>]	
Global Configuration mode	
ip traffic-filter action <1-4096>	mirror
	mode <default|forward|drop|forward-to-next-hop>
	next-hop-forward [next-hop-unreachable-drop] [<A.B.C.D>]
	statistic
	stop-on-match
	tcp-connect
	traffic-profile <0-64>
ip traffic-filter destination dst-ip <A.B.C.D> <A.B.C.D> [<1-4096>] [src-ip <A.B.C.D> <A.B.C.D>]	
ip traffic-filter filter <1-4096> name <WORD 0-15>	

Table 18
Job aid: Roadmap of traffic filter NNCLI commands (cont'd.)

Command	Parameter
ip traffic-filter global	<cr>
	<1-4096>
	dst-ip <A.B.C.D> <A.B.C.D>
	src-ip <A.B.C.D> <A.B.C.D>
ip traffic-filter global-set <1-100>	<cr>
	filter <1-4096>
	name <WORD 1-15>
ip traffic-filter match <1-4096>	ds-field <WORD 1-6> <WORD 1-2>
	ds-field-enable
	dst-port <0-65535> [dst-option <equal |notequal|greater|less|ignore>]
	icmp-request
	ip-fragment
	protocol <ignore|icmp|tcp|udp|vrrp|ospf|ipsec_esp|ipsec_ah|usrDefined> [<0-255>]
	src-port <0-65535> [src-option <equal |notequal|greater|less|ignore>]
ip traffic-filter media <3000-3127>	<cr>
	device <0-6>
	gateway <A.B.C.D>
	name <WORD 0-63>
	platform <0-10>
	statistic
ip traffic-filter media-stream <3000-3127> <1-4>	<cr>
	match-dscp <WORD 1-6>
	name <WORD 0-31>
	port-option <dst|src|src-dst>
	ports min <0-65535>
	protocol <tcp|udp>
	stream-type <media|signal>
ip traffic-filter modify <1-4096>	<cr>
	dscp <WORD 1-6>

Table 18
Job aid: Roadmap of traffic filter NNCLI commands (cont'd.)

Command	Parameter
	`dscp-enable`
	`ieee8021p <0-7>`
	`ieee8021p-enable`
`ip traffic-filter profile <1-64>`	`<cr>`
	`average-rate <0-65535>`
	`discard-out-profile`
	`enable`
	`in-dscp <WORD 1-6>`
	`name <WORD 0-2>`
	`out-dscp`
	`translate-dscp`
`ip traffic-filter set <300-1000>`	`<cr>`
	`filter <1-4096>`
	`name <WORD 0-15>`
`ip traffic-filter source src-ip <A.B.C.D> <A.B.C.D>`	`<cr>`
	`<1-4096>`
	`dst-ip <A.B.C.D> <A.B.C.D>`
Interface Configuration mode	
`ip traffic-filter`	`<cr>`
	`default-action <drop|forward>`
	`enable`
	`set <1-3127>`
`multimedia`	`enable`
	`select <WORD 0-63>`

Traffic filter configuration

This section describes how to configure an IP traffic filter, manage traffic, and, in some cases, provide security.

Traffic filter configuration navigation

- "Creating traffic filters" (page 145)
- "Creating destination traffic filters" (page 121)
- "Creating source traffic filters" (page 147)

- “Viewing a specific traffic filter” (page 147)
- “Configuring traffic filter action parameters” (page 148)
- “Configuring the traffic filter next-hop IP address” (page 149)
- “Configuring traffic filter match settings” (page 150)
- “Configuring traffic filters for DiffServ access ports” (page 151)
- “Configuring a global filter set” (page 152)
- “Configuring multimedia traffic filters” (page 153)
- “Configuring a media stream traffic filter” (page 154)
- “Configuring a source and destination filter set ” (page 155)
- “Configuring traffic filter rate-limiting profiles” (page 156)

Creating traffic filters

Use traffic filters to selectively accept, reject, or modify traffic.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step **Action**

1 Create global traffic filters by using the following command:

```
ip traffic-filter global [<1-4096>] [dst-ip <A.B.C.D>
<A.B.C.D>] [src-ip <A.B.C.D> <A.B.C.D>]
```

2 Create source traffic filters by using the following command:

```
ip traffic-filter source src-ip <A.B.C.D> <A.B.C.D>
[<1-4096>] [dst-ip <A.B.C.D> <A.B.C.D>]
```

3 Create destination traffic filters by using the following command:

```
ip traffic-filter destination dst-ip <A.B.C.D>
<A.B.C.D> [<1-4096>] [src-ip <A.B.C.D> <A.B.C.D>]
```

--End--

Variable definitions

Use the data in the following table to help you use the `ip traffic-filter` command.

Variable	Value
`destination dst-ip <A.B.C.D> <A.B.C.D> [<1-4096>] [src-ip <A.B.C.D> <A.B.C.D>]`	Creates a destination filter: • `dst-ip <A.B.C.D> <A.B.C.D>` is the destination IP address and mask. • `src-ip <A.B.C.D> <A.B.C.D>` is the source IP address and mask. • `<1-4096>` is the traffic filter ID.
`global [<1-4096>] [dst-ip <A.B.C.D> <A.B.C.D>] [src-ip <A.B.C.D> <A.B.C.D>]`	Creates a global filter: • `src-ip <A.B.C.D> <A.B.C.D>` is the source IP address and mask. • `dst-ip <A.B.C.D> <A.B.C.D>` is the source IP and mask. • `<1-4096>` is the traffic filter ID.
`source src-ip <A.B.C.D> <A.B.C.D> [<1-4096>] [dst-ip <A.B.C.D> <A.B.C.D>]`	Creates a source filter: • `src-ip <A.B.C.D> <A.B.C.D>` is the source IP address and mask. • `dst-ip <A.B.C.D> <A.B.C.D>` is the destination IP address and mask. • `<1-4096>` is the traffic filter ID.

Creating destination traffic filters

Create a destination filter to selectively accept, modify, or reject traffic based on destination IP parameters.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Create destination traffic filters by using the following command: `ip traffic-filter destination dst-ip <A.B.C.D> <A.B.C.D> [<1-4096>] [src-ip <A.B.C.D> <A.B.C.D>]`

--End--

Variable definitions

Use the data in the following table to help you configure destination filters.

Variable	Value
`<1-4096>`	Specifies the filter ID.
`dst-ip <A.B.C.D> <A.B.C.D>`	Specifies the source IP address and mask.
`src-ip <A.B.C.D> <A.B.C.D>`	Specifies the source IP address and mask.

Creating source traffic filters

Create a source filter to selectively accept, modify, or reject traffic based on source IP parameters.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Create a source traffic filters by using the following command:

```
ip traffic-filter source src-ip <A.B.C.D> <A.B.C.D>
[<1-4096>] [dst-ip <A.B.C.D> <A.B.C.D>]
```

--End--

Variable definitions

Use the data in the following table to help you configure source filters.

Variable	Value
`<1-4096>`	Specifies the filter ID.
`dst-ip <A.B.C.D> <A.B.C.D>`	Specifies the source IP address and mask.
`src-ip <A.B.C.D> <A.B.C.D>`	Specifies the source IP address and mask.

Viewing a specific traffic filter

You can view information about a specific filter and name or delete the filter.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	View a specific traffic filter by using the following command: `ip traffic-filter filter <1-4096>`
2	Rename a specific traffic filter by using the following command: `ip traffic-filter filter <1-4096> name <WORD 0-15>`

--End--

Variable definitions

Use the data in the following table to help you use the `ip traffic-filter filter` command.

Variable	Value
`<1-4096>`	Specifies the traffic filter ID.
`name <WORD 0-15>`	Names the traffic filter.

Configuring traffic filter action parameters

Configure the port filter actions to determine which filters are active on the port, and what actions the port should take for matching filters.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure the traffic filter action parameters by using the following command with the options in the variable definitions table: `ip traffic-filter action <1-4096>`

--End--

Variable definitions

Use the data in the following table to help you use the `ip traffic-filter action <1-4096>` command.

variable	Value
`mirror`	Enables 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.
`next-hop-forward [next-hop-unreachable-drop] [<A.B.C.D>]`	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), packet that match the filter are forwarded normally unless the next-hop-unreachable-drop option is enabled .
`statistic`	Enables statistics collection on the traffic filter. The default setting is disable. If disabled, the show ip traffic-filter stats command displays zero for this filter.
`stop-on-match`	Stops further filtering if the current filter is applied.
`tcp-connect`	Enables 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.
`traffic-profile <0-64>`	Sets the IP traffic profile. The valid options are 0–64.

Configuring the traffic filter next-hop IP address

Configure traffic filter action parameters to specify the IP address of the next-hop router.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure the traffic filter next-hop IP address by using the following command: `ip traffic-filter action <1-4096> next-hop-forward [next-hop-unreachable-drop] [<A.B.C.D>]`

--End--

Variable definitions

Use the data in the following table to help you configure the next hop.

Variable	Value
`<1-4096>`	Specifies the filter ID.
`<A.B.C.D>`	Sets the IP address of next hop.
`next-hop-unreachable-drop`	Specifies that if the next-hop address is unreachable, the packet is dropped.

Configuring traffic filter match settings

Configure traffic filter match parameters to specify the match criteria for filters.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure the traffic filter match settings by using the following command with the options in the following table: `ip traffic-filter match <1-4096>` `<1-4096>` specifies the filter ID.

--End--

Variable definitions

Use the data in the following table to help you use the `ip traffic-filter match <1-4096>` command.

Variable	Value
ds-field <WORD 1-6> <WORD 1-2>	Sets the traffic match DSCP 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 is applied to the packet. • **<WORD 1-6>** is the DSCP as a binary number. • **<WORD 1-2>** is the reserved field as a binary number.
ds-field-enable	Enables or disables the traffic filter to match on the DS field set for the traffic filter.
dst-port <0-65535> [dst-option <equal|notequal|greater|less|ignore>]	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	Enables the traffic filter to match ICMP requests.
ip-fragment	Enables the traffic filter to allow IP fragments to be filtered.
protocol <ignore|icmp|tcp|udp|vrrp|ospf|ipsec_esp|ipsec_ah|usrDefined> [<0-255>]	Sets the protocol type for the filter. • The protocol is ignore, ICMP, TCP, UDP, vrrp, ospf, ipsec_esp, ipsec_ah, or usrDefined. • **<0-255>** is the PID in decimal format that you assign.
src-port <0-65535> [src-option <equal|notequal|greater|less|ignore>]	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}.

Configuring traffic filters for DiffServ access ports

Use traffic filters on DiffServ access ports to modify untrusted DSCP or 802.1p bit markings.

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

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure the traffic filter for DiffServ access port using the following command with the options in the following table: `ip traffic-filter modify <1-4096>`

--End--

Variable definitions

Use the data in the following table to help you use the **`ip traffic-filter modify <1-4096>`** command.

Variable	Value
`dscp <WORD 1-6>`	Modifies the DSCP. If you want the DS codepoint (DSCP) modified to a nonzero value, use this command to specify the value for the DSCP. After entering the binary number, you must disable and then enable the traffic filter to ensure that it takes effect. `<WORD 1-6>` is a binary number.
`dscp-enable`	Enables or disables the traffic filter to modify the DSCP to zero on packet ingressing a DiffServ access port only.
`ieee8021p <0-7>`	Modifies IEEE 802.1p bits to a nonzero value. Use this field to specify the value for the IEEE 802.1p bits. Disable and enable the filter for changes to take effect.
`ieee8021p-enable`	Enables or disables the traffic filter to modify the IEEE 802.1p bits to zero on packets ingressing a DiffServ access port only.

Configuring a global filter set

Configure global traffic filter sets to group global filters.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Create a global filter set by using the following command: `ip traffic-filter global-set <1-100>`
2	Add global filters to the filter set: `ip traffic-filter global-set <1-100> filter <1-4096>`
3	Name the global filter set: `ip traffic-filter global-set <1-100> name <WORD 1-15>`

--End--

Variable definitions

Use the data in the following table to help you use the **ip traffic-filter global-set <1-100>** command.

Variable	Value
`<cr>`	Creates the set.
`filter <1-4096>`	Adds a global filter to a global filter set.
`name <WORD 1-15>`	Assigns a name for the global filter set.

Configuring multimedia traffic filters

Configure multimedia platform filters to provide differentiated service, better network management, flexible call monitoring, and convenient troubleshooting for VoIP calls.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Create the filter by using the following command: `ip traffic-filter media <3000-3127>`

2 Use the following table to configure other filter parameters as required.

--End--

Variable definitions

Use the data in the following table to help you use the `ip traffic-filter media <3000-3127>` command.

Variable	Value
`device <0-6>`	Device identifier or the type.
`gateway <A.B.C.D>`	Sets the gateway IP address.
`name <WORD 0-63>`	Sets the media name of the selected device.
`platform <0-10> [device <0-6>]`	Creates IP traffic filter media for a platform or a device.
`statistic`	Enables the display of statistics about the filter.

Configuring a media stream traffic filter

Configure multimedia platform filters to provide differentiated service, better network management, flexible call monitoring, and convenient troubleshooting for VoIP calls.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step Action

1 Create the media stream filter by using the following command:

```
ip traffic-filter media-stream <3000-3127> <1-4>
```

2 Use the following table to configure other parameters as required.

--End--

Variable definitions

Use the data in the following table to help you use the `ip traffic-filter media-stream <3000-3127> <1-4>` command.

Variable	Value
`<cr>`	Creates the filter. `<3000-3127>` is the filter ID. `<1-4>` specifies the stream ID.
`match-dscp <WORD 1-6>`	Specifies a 6-bit binary value for the stream.
`name <WORD 0-31>`	Specifies the name of the selected media device.
`port-option <src|dst|src-dst>`	Specifies a port option, either src, dest, or srcDest.
`ports min <0-65535> [max <0-65535>]`	Specifies the minimum port number in the range of 0 to 65535
`protocol <udp|tcp>`	Specifies either a TCP or UDP protocol.
`stream-type <signal|media>`	Specifies the type of stream. The valid options are signal and media.

Configuring a source and destination filter set

You can use a source and destination filter set to group source and destination filters. You cannot add global filters to this set.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step **Action**

1 Create the set by using the following command:

```
ip traffic-filter set <300-1000>
```

2 Add filters to the set:

```
ip traffic-filter set <300-1000> filter <1-4096>
```

--End--

Variable definitions

Use the data in the following table to help you use the `ip traffic-filter set <300-1000>` command.

Variable	Value
`<cr>`	Creates the set.

Variable	Value
filter <1-4096>	Adds a filter to a filter set. **<1-4096>** is the traffic filter ID.
[name <WORD 0-15>]	Configures the set name.

Configuring traffic filter rate-limiting profiles

Configure a traffic profile to specify the handling properties of a traffic flow selected by a classifier. A traffic flow 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.

Prerequisites

- You must log on to the Global Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure traffic filter rate-limiting profiles by using the following command: **ip traffic-filter profile <1-64>**

--End--

Variable definitions

Use the data in the following table to help you use the **ip traffic-filter profile <1-64>** commands.

Variable	Value
<cr>	Creates the profile, where **<1-64>** is the profile ID.
average-rate <0-65535>	Sets the traffic profile average rate, which is expressed in 64-byte segments of data allowed in a 2.5 millisecond timeslot.
discard-out-profile	Enables the ability to discard traffic that violates the traffic profile average rate.
enable	Enables the filter traffic-profile.

Variable	Value
`in-dscp <WORD 1-6>`	Marks traffic that conforms to the average rate in the traffic profile. `<WORD 1-6>` is the DSCP expressed in the format Binary- xxxxxx 6-bit (MSB...LSB), Hex, or Decimal.
`name <WORD 0-32>`	Specifies the IPF filter traffic profile name.
`out-dscp <WORD 1-6>`	Marks traffic that falls outside the traffic profile's average rate. `<WORD 1-6>` is the DSCP expressed in the format Binary- xxxxxx 6-bit (MSB...LSB), Hex, or Decimal.
`translate-dscp`	Enables the profile translate for DSCP. This command must be enabled for any traffic to be marked.

Ethernet IP traffic filter commands configuration

This section describes how to configure the Ethernet IP traffic filter commands so that you can manage an IP traffic filter.

Ethernet IP traffic filter configuration navigation

- "Applying filters to a port" (page 157)
- "Configuring the default action on a port filter" (page 158)
- "Applying a multimedia traffic filter to a port" (page 159)

Applying filters to a port

Apply traffic filters on a port to manage traffic.

Each filter set includes match conditions and actions to perform when a match condition occurs.

Prerequisites

- You must log on to the Interface Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Configure filters to apply to the port by using the following command: `ip traffic-filter set <1-3127>`

2 Configure the default action, if required:

```
ip traffic-filter default-action <drop|forward>
```

3 Enable the filter:

```
ip traffic-filter enable
```

--End--

Variable definitions

Use the data in the following table to help you use the **ip traffic-filter** command.

Variable	Value
`<cr>`	Creates the filter instance on the port.
`default-action <drop|forward>`	Sets the default action for the interface.
`enable`	Enables the filter on the port.
`set <1-3127>`	Adds a filter to a port. **value** is the global or source and destination filter set ID

Configuring the default action on a port filter

Configure the port filter default action for a filter to forward or drop packets that match filter criteria.

Prerequisites

- You must log on to the Interface Configuration mode in the NNCLI.

Procedure steps

Step **Action**

1 Configure the forward or drop action on a port traffic filter by using the following command:

```
ip traffic-filter default-action <drop|forward>
```

--End--

Variable definitions

Use the data in the following table to help you use the **ip traffic-filter default-action** command.

Variable	Value
`forward`	Sets the port filter default action to forward.
`drop`	Sets the port filter default action to drop.

Applying a multimedia traffic filter to a port

Assign a multimedia filter to a port to manage port traffic.

Prerequisites

- You must log on to the Interface Configuration mode in the NNCLI.

Procedure steps

Step	Action
1	Specify the filter to use on the port by using the following command: `multimedia select <WORD 0-63>`
2	Enable the filter: `multimedia enable`

--End--

Variable definitions

Use the data in the following table to help you use the **`multimedia`** command.

Variable	Value
`enable`	Enables a multimedia Ethernet filter on the port.
`select <WORD 0-63>`	Selects a multimedia device for the port by name.

Show IP traffic filter commands

This section describes IP traffic filter commands.

Show IP traffic filter commands navigation

- “Showing the active traffic filters” (page 160)
- “Showing enabled traffic filters” (page 160)
- “Showing disabled traffic filters” (page 161)
- “Showing global traffic filters” (page 162)
- “Showing destination filter information” (page 162)

Showing the active traffic filters

Use this procedure to learn which filters are active.

Prerequisites

- You must log on to the Privileged Exec mode in the NNCLI.

Procedure steps

Step	Action
1	View the active traffic filters by using the following command: `show ip traffic-filter active`

--End--

Showing enabled traffic filters

Use this procedure to view information about enabled filters on the switch or on a specified port.

Prerequisites

- You must log on to the Privileged Exec mode in the NNCLI.

Procedure steps

Step	Action
1	View the enabled traffic filters by using the following command:

```
show ip traffic-filter enabled [<portlist>]
```

--End--

Variable definitions

Use the data in the following table to help you use the **`show ip traffic-filter enabled`** command.

Variable	Value
`<cr>`	Shows enabled filter information for all ports.
`<portlist>`	Specifies the ports for which to show enabled filter information.

Showing disabled traffic filters

Use this procedure to learn which filters are disabled.

Prerequisites

- You must log on to the Privileged Exec mode in the NNCLI.

Procedure steps

Step	Action
1	View the disabled traffic filters by using the following command: `show ip traffic-filter [<portlist>]`

--End--

Variable definitions

Use the data in the following table to help you use the **`show ip traffic-filter`** command.

Variable	Value
`<cr>`	Shows disabled filter information for all ports.
`<portlist>`	Specifies the ports for which to show disabled filter information.

Showing global traffic filters

Use this procedure to view the global filters for the Ethernet Routing Switch 8600 or for the specified filter IDs.

Prerequisites

- You must log on to the Privileged Exec mode in the NNCLI.

Procedure steps

Step	Action
1	View the global traffic filters by using the following command: `show ip traffic-filter global [<1-4096>]`

--End--

Variable definitions

Use the data in the following table to help you use the **`show ip traffic-filter global`** command.

Variable	Value
`<cr>`	Shows global traffic filter information.
`<1-4096>`	Shows information for the filter ID in the range of 1–4096.

Showing destination filter information

Use this procedure to display active destination traffic filters.

Prerequisites

- You must log on to the Privileged Exec mode in the NNCLI.

Procedure steps

Step	Action
1	View the traffic filter source and destinations by using the following command: `show ip traffic-filter destination [<1-4096>]`

--End--

Variable definitions

Use the data in the following table to help you use this command.

Variable	Value
`<1-4096>`	Filter identification number in the range of 1 to 4096.

Showing source traffic filter information

Use this procedure to view information about active source traffic filters.

Prerequisites

- You must log on to the Privileged Exec mode in the NNCLI.

Procedure steps

Step	Action
1	View active source-traffic filter information by using the following command: `show ip traffic-filter source [<1-4096>]`

--End--

Variable definitions

Use the data in the following table to help you use this command.

Variable	Value
`<1-4096>`	Specifies the filter ID in the range of 1 to 4096.

Showing traffic filter interface information

Use this procedure to learn which filters are applied to a port.

Prerequisites

- You must log on to the Privileged Exec mode in the NNCLI.

Procedure steps

Step	Action
1	View the traffic filter interface information by using the following command:

```
show ip traffic-filter interface {fastEthernet|gigabit
Ethernet|pos} <portlist>
```

--End--

Variable definitions

Use the data in the following table to help you use the **`show ip traffic-filter interface {fastEthernet|gigabitEthernet|pos}`** command.

Variable	Value
`<portlist>`	Specifies the ports for which to show enabled filter information.

Showing multimedia traffic filter information

Use this procedure to view multimedia platform and device filters by filter ID.

Prerequisites

- You must log on to the Privileged Exec mode in the NNCLI.

Procedure steps

Step	Action
1	View traffic filter media information by using the following command: `show ip traffic-filter media [<3000-3127>]`

--End--

Variable definitions

Use the data in the following table to help view multimedia filters.

Variable	Value
`<3000-3127>`	Specifies the filters for which to show information.

Showing multimedia stream traffic filter information

Use this procedure to view the media platforms and devices by filter ID.

Prerequisites

- You must log on to the Privileged Exec mode in the NNCLI.

Procedure steps

Step	Action
1	View traffic filter streams by using the following command: `show ip traffic-filter stream [<3000-3127>]`

--End--

Variable definitions

Use the data in the following table to help view stream filters.

Variable	Value
<3000-3127>	Specifies the filter for which to show information.

Showing traffic filter global set information

Show traffic filter global set information to display information about the specified global filter set or all global filter lists configured on the switch.

Prerequisites

- You must log on to the Privileged Exec mode in the NNCLI.

Procedure steps

Step	Action
1	Show traffic filter global-set information by using the following command: `show ip traffic-filter global-set [<1-100>]`

--End--

Variable definitions

Use the data in the following table to help you use this command.

Variable	Value
`<1-100>`	Shows information about a specific global set by set ID in the range 1 to 100.

Showing source and destination traffic filter set information

Display the traffic filter set information to view information for the specified source and destination filter list or all source and destination filter lists.

Prerequisites

- You must log on to the Privileged Exec mode in the NNCLI.

Procedure steps

Step	Action
1	Show the traffic filter set information by using the following command: `show ip traffic-filter set [<300-1000>]`

--End--

Variable definitions

Use the data in the following table to help you use this command.

Variable	Value
`<300-1000>`	Specifies the filter set by ID.

Showing traffic filter traffic profile information

Display the traffic filter traffic-profile information to view the traffic-profile settings.

Prerequisites

- You must log on to the Privileged Exec mode in the NNCLI.

Procedure steps

Step	Action
1	Show traffic filter traffic-profile information by using the following command:

```
show ip traffic-filter profile [<1-64>]
```

--End--

Variable definitions

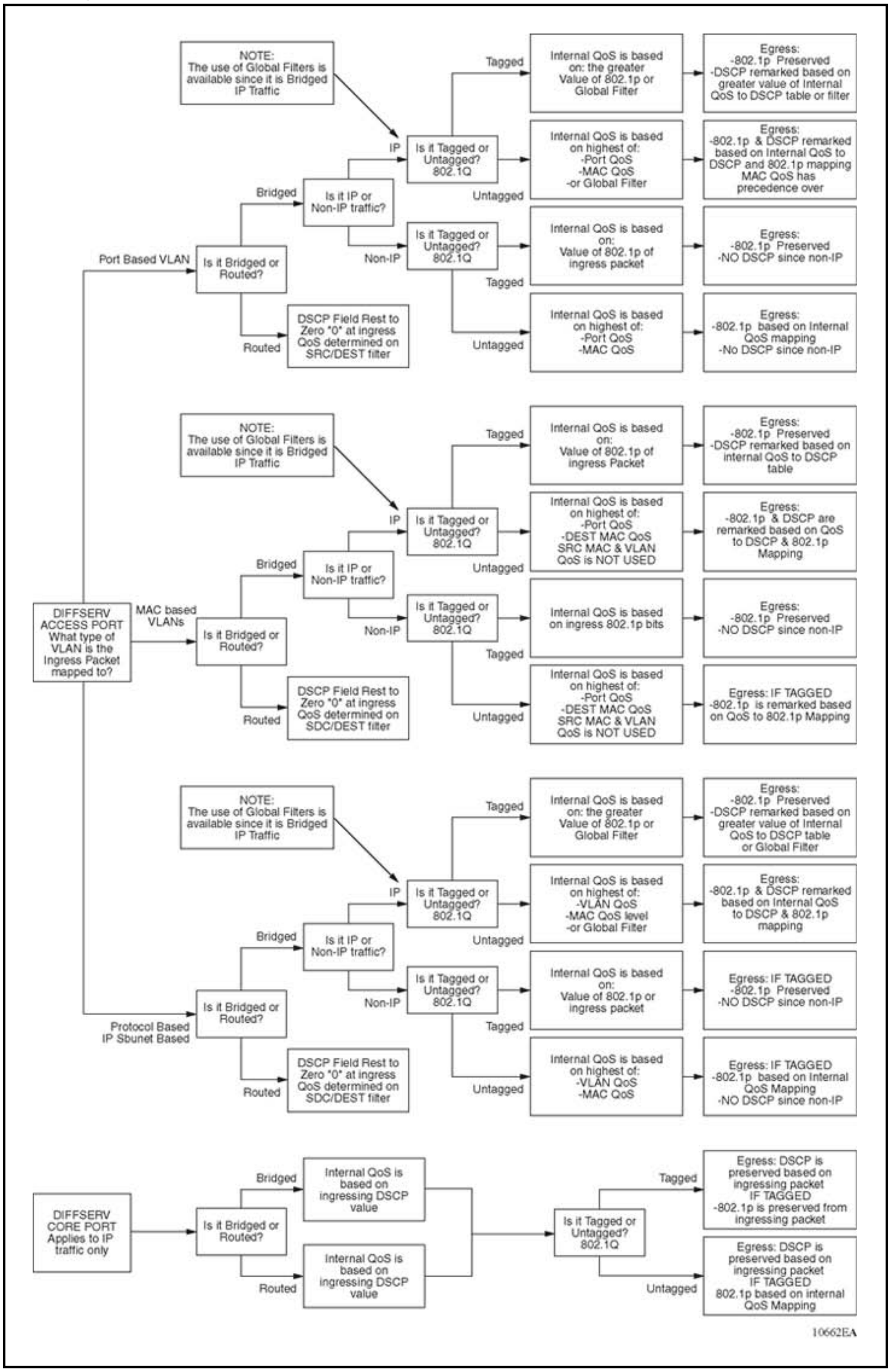
Use the data in the following table to help you use this command.

Variable	Value
`<1-64>`	Specifies the profile ID. The value ranges from 1 to 64.

Appendix
QoS algorithm for Classic modules

The following figure provides an illustration of the QoS algorithm and the decision-making process it encompasses.

Figure 7
QoS algorithm


DIFFSERV ACCESS PORT What type of VLAN is the Ingress Packet mapped to?
Port Based VLAN
MAC based VLANs
Protocol Based IP Sbunet Based
NOTE: The use of Global Filters is available since it is Bridged IP Traffic
Is it Bridged or Routed?
Bridged
Routed
Is it IP or Non-IP traffic?
IP
Non-IP
Is it Tagged or Untagged? 802.1Q
Tagged
Untagged
DSCP Field Rest to Zero "0" at ingress QoS determined on SRC/DEST filter
Internal QoS is based on: the greater Value of 802.1p or Global Filter
Egress: -802.1p Preserved -DSCP remarked based on greater value of Internal QoS to DSCP table or filter
Internal QoS is based on highest of: -Port QoS -MAC QoS -or Global Filter
Egress: -802.1p & DSCP remarked based on Internal QoS to DSCP and 802.1p mapping MAC QoS has precedence over
Internal QoS is based on: Value of 802.1p of ingress packet
Egress: -802.1p Preserved -NO DSCP since non-IP
Internal QoS is based on highest of: -Port QoS -MAC QoS
Egress: -802.1p based on Internal QoS mapping -No DSCP since non-IP
NOTE: The use of Global Filters is available since it is Bridged IP Traffic
Internal QoS is based on: Value of 802.1p of ingress Packet
Egress: -802.1p Preserved -DSCP remarked based on internal QoS to DSCP table
Internal QoS is based on highest of: -Port QoS -DEST MAC QoS SRC MAC & VLAN QoS is NOT USED
Egress: -802.1p & DSCP are remarked based on QoS to DSCP & 802.1p Mapping
Internal QoS is based on ingress 802.1p bits
Egress: -802.1p Preserved -NO DSCP since non-IP
Internal QoS is based on highest of: -Port QoS -DEST MAC QoS SRC MAC & VLAN QoS is NOT USED
Egress: IF TAGGED -802.1p is remarked based on QoS to 802.1p Mapping
DSCP Field Rest to Zero "0" at ingress QoS determined on SDC/DEST filter
NOTE: The use of Global Filters is available since it is Bridged IP Traffic
Internal QoS is based on: the greater Value of 802.1p or Global Filter
Egress: -802.1p Preserved -DSCP remarked based on greater value of Internal QoS to DSCP table or Global Filter
Internal QoS is based on highest of: -VLAN QoS -MAC QoS level -or Global Filter
Egress: -802.1p & DSCP remarked based on Internal QoS to DSCP & 802.1p mapping
Internal QoS is based on: Value of 802.1p or ingress packet
Egress: IF TAGGED -802.1p Preserved -NO DSCP since non-IP
Internal QoS is based on highest of: -VLAN QoS -MAC QoS
Egress: IF TAGGED -802.1p based on Internal QoS Mapping -NO DSCP since non-IP
DSCP Field Rest to Zero "0" at ingress QoS determined on SDC/DEST filter
DIFFSERV CORE PORT Applies to IP traffic only
Is it Bridged or Routed?
Bridged
Routed
Internal QoS is based on ingressing DSCP value
Internal QoS is based on ingressing DSCP value
Is it Tagged or Untagged? 802.1Q
Tagged
Untagged
Egress: DSCP is preserved based on ingressing packet IF TAGGED -802.1p is preserved from ingressing packet
Egress: DSCP is preserved based on ingressing packet IF TAGGED 802.1p based on internal QoS Mapping
10662EA

Index

Nortel Ethernet Routing Switch 8600

Configuration — QoS and IP Filtering for Classic Modules

Printed in Canada, India, and the United States of America
Release: 5.0
Publication: NN46205-508
Document revision: 01.04
Document release date: 21 April 2009

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

www.nortel.com
LEGAL NOTICE

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

ATTENTION

For information about the safety precautions, read "Safety messages" in this guide.

For information about the software license, read "Software license" in this guide.