Part No. 209570-D
November 2002

4655 Great America Parkway
Santa Clara, CA 95054

Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5

NORTEL NETWORKS™

USA requirements only

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

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

European requirements only

EN 55 022 statement

This is to certify that the Nortel Networks Business Policy Switch 2000 is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class A (CISPR 22).

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

Achtung: Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Attention: Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l’utilisateur de prendre les mesures spécifiques appropriées.

AEC Declaration of Conformity

This product conforms (or these products conform) to the provisions of the R&TTE Directive 1999/5/EC.

Japan/Nippon requirements only

Voluntary Control Council for Interference (VCCI) statement

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

Taiwan requirements

Bureau of Standards, Metrology and Inspection (BSMI) Statement

警告使用者:

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

Canada requirements only

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Business Policy Switch 2000) does not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (Business Policy Switch 2000) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

Nortel Networks Inc. software license agreement

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

“Software” is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no

rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

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

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

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

4. General

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

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

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

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

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

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

Contents

Figures

Tables

Preface

Welcome to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*. This document provides instructions on configuring and managing the Business Policy Switch 2000* through the World Wide Web.

The Web-based management interface is one of many tools specifically designed to assist the network manager in creating complex standalone or network configurations. In addition to the Web-based management system discussed in this book, you can manage the BPS 2000 using SNMP, the Command Line Interface (CLI), Device Manager (DM), or the console interface (CI) menus. Refer to the documents listed "Related publications" on page 26 for information on using and managing the BPS 2000.

This guide describes how to use the Web-based management user interface to configure and maintain your BPS 2000 and the devices connected within its framework.

Before you begin

This guide is intended for network managers who are responsible for configuring BPS 2000. Consequently, this guide assumes prior knowledge and understanding of the terminology, theories, and practices and specific knowledge about the networking devices, protocols, and interfaces that comprise your network.

You should have working knowledge of the Windows* operating system, graphical user interfaces (GUIs), and Web browsers.

Text conventions

This guide uses the following text conventions:

italic text	Indicates new terms and book titles.
separator (>)	Shows menu paths. Example: Configuration > Port Management identifies the Port Management option on the Configuration menu.

Related publications

For more information about using the Web-based management user interface and the BPS 2000, refer to the following publications:

- *Release Notes for the Business Policy Switch 2000 Software Version 2.5* (part number 210676-T)

  Documents important changes about the software and hardware that are not covered in other related publications.

- *Using the Business Policy Switch 2000 Software Version 2.5* (part number 208700-D)

  Describes how to use the BPS 2000.

- *Business Policy Switch 2000 Installation Instructions* (part number 209319-A)

  Describes how to install the BPS 2000.

- *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5* (part number 212160-C)

  Describes how to use the Command Line Interface (CLI) to configure and manage the BPS 2000.

- *Reference for the Business Policy Switch 2000 Management Software Version 2.5* (part number 209322-D)

Describes how to use the Java Device Manager to configure and manage the BPS 2000.

- *Installing Media Dependent Adapters (MDA)s* (part number 302403-H)

  Describes how to install optional MDAs in your Business Policy Switch 2000.

- *Installing Gigabit Interface Converters and Small Form Factor Pluggable Interface Converters* (part number 312865-B)

  Describes how to install optional GBICs and SFP GBICs into the optional MDA in your Business Policy Switch 2000.

- *Installing Optivity Policy Services* (part number 306972-E Rev 00)

  Describes how to install Optivity Policy Services*.

- *Managing Policy Information in Optivity Policy Services* (part number 306969-F Rev 00)

  Describes how to configure and manage Optivity Policy Services.

- *Release Notes for Optivity Policy Services Version 3.0* (part number 306975-F Rev 00)

  Documents important Optivity Policy Services changes that are not covered in other related publications.

- *Task Map - Installing Optivity Policy Services Product Family* (part number 306976-E Rev 00)

  Provides a quick map to installing Optivity Policy Services.

- *Known Anomalies for Optivity Policy Services Version 3.0* (part number 306974-E Rev 00)

  Describes known anomalies with Optivity Policy Services.

More information on Optivity Policy Services is available at the OPS 3.0 evalution site, located at the www.nortelnetworks.com/products/01/unifiedmanagement/policy/eval/register.html URL.

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. (The product family for the BPS 2000 is Data and Internet.) Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

Additionally, you can obtain printed books from Vervante.com. Contact Vervante.com to order a printed book at http://www.vervante.com/nortel.

How to get help

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

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

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

Additional information about the Nortel Networks Technical Solutions Centers is available from the www.nortelnetworks.com/help/contact/global URL.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www130.nortelnetworks.com/cgi-bin/eserv/common/essContactUs.jsp URL.

Chapter 1
Using the Web-based management interface

This chapter describes the requirements for using the Web-based management interface and how to use it as a tool to configure your BPS 2000. This chapter covers:

New features

The following new features that you can access through Web-based management have been introduced to the BPS 2000 software since version 1.0:

- Introduced with software version 2.5
  - Per VLAN egress tagging (refer to Chapter 7)
  - QoS enhancements
    - Number of available Layer 2 filters increased to 24 (refer to Chapters 8 and 9)
    - QoS In/Out Profile statistics improved (refer to Chapter 9)

- Introduced with software version 2.0
  - Support for BPS 2000-1GT, BPS 2000-2GT, and BPS 2000-2GE MDAs (refer to *Installing Media Dependent Adapters (MDA)s* and *Installing Gigabit Interface Converters and Small Form Factor Pluggable Interface Converters*)
  - Ability to view CPU and memory utilization (refer to Chapter 2)
  - Ability to set per port spanning tree path cost and priority (refer to Chapter 7)
  - Shaping for QoS networks (refer to Chapters 8 and 9)
  - Improved QoS Wizard (refer to Chapter 8**)**
  - QoS Quick Config (refer to Chapter 8)
  - Port naming (refer to Chapter 4)
  - MAC address-based filtering (refer to Chapter 4)
  - Individual IP addresses for each unit in the stack (refer to Chapter 4)
  - Configurable VID for tagged BPDU with multiple spanning tree groups (refer to Chapter 7)
  - Specifying multiple VLANs in a QoS single filter (refer to Chapters 8 and 9)
- Introduced with software version 1.2
  - VLANS increased to 256
  - Support for multiple spanning tree groups (refer to Chapter 7)
  - IP manager list (refer to Chapter 4)
- Introduced with software version 1.1
  - QoS metering added to policy-enabled networks (refer to Chapter 8)
  - Support for the BayStack 450-1GBIC MDA
  - EAPOL-based security (refer to Chapter 4)
  - Automatic PVID (refer to Chapter 5)
  - Table of port statistics (refer to Chapter 6)

Note: To access the software version 2.5 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Stacking compatibility

You can stack the BPS 2000 up to 8 units high. There are two types of stacks:

- Pure BPS 2000—This stack has *only* BPS 2000 switches. It is sometimes referred to as a pure stack. The stack operational mode for this type of stack is Pure BPS 2000 Mode.
- Hybrid—This stack has a combination of BPS 2000 switches *and* BayStack* 450 and/or BayStack 410 switches. It is sometimes referred to as a mixed stack. The stack operational mode for this type of stack is Hybrid Mode.

When you work with the BPS 2000 in standalone mode, you should ensure that the stack operational mode shows Pure BPS 2000 Mode, and does not show Hybrid Mode.

All BPS 2000 switches in the stack must be running the identical version of software, and all the BayStack switches must be running the identical version of software.

When you are working with a mixed stack, you *must* ensure that the Interoperability Software Version Numbers (ISVN) are identical. That is, the ISVN number for the BayStack 450 switch and BayStack 410 switch must have the same ISVN as the BPS 2000. If the ISVNs are not the same, the stack does not operate.

In sum, the stacking software compatibility requirements are as follows:

- Pure BPS 2000 stack—All units must be running the same software version.
- Pure BayStack 450 stack—All units must be running the same software version.
- Hybrid stack:
  - All BPS 2000 units must be running the same software version.
  - All BayStack 410 units must be running the same software version.
  - All BayStack 450 units must be running the same software version.
  - All software versions must have the identical ISVN.

Refer to Appendix B of *Using the Business Policy Switch 2000 Software Version 2.5* for complete information on interoperability and compatibility between the BPS 2000 and BayStack switches.

Software version 2.5 compatibility with BayStack 450 switches

The BPS 2000 software version 2.5 is compatible with BayStack 450 software version 4.1.

When you are using a local console to access the BPS 2000 software version 2.5 features with a Hybrid, or mixed, stack (BPS 2000 and BayStack 450 and 410 switches in the same stack), you must plug your local console into a BPS 2000 unit.

To find out which version of the BPS 2000 software is running, use the console interface (CI) menus or the Web-based management system:

- CI menus—From the main menu of the console, choose Systems Characteristics menu. The software currently running is displayed in sysDescr.
- Web-based management system—Open the System Information page, which is under Administration on the main menu. The software currently running is displayed in the sysDescription field.

You can use 256 port-, protocol-, and MAC SA-based VLANs for the stack with a Pure BPS 2000 stack running software version 1.2. (The maximum number of MAC SA-based VLANs available is 48). If you are working with a mixed, or Hybrid, stack, you can use 64 VLANs for the entire stack. When you change from a Pure BPS 2000 Stack mode to a Hybrid Stack mode:

- If you have up to 64 VLANs on the Pure BPS 2000 Stack, they will be retained when you change to a Hybrid Stack.
- If you have more than 64 VLANs on the Pure BPS 2000 Stack, you will lose them all. The Hybrid Stack will return to the default VLAN configuration.

Also, a mixed, or Hybrid, stack does not support multiple Spanning Tree Groups (STG). You have a single instance of STG when working with a mixed stack.

- If you have up to 64 VLANs on the Pure BPS 2000 Stack, they will be retained when you change to a Hybrid Stack.
- If you have more than 64 VLANs on the Pure BPS 2000 Stack, you will lose them all. The Hybrid Stack will return to the default VLAN configuration.

Also, a mixed, or Hybrid, stack does not support multiple Spanning Tree Groups (STG). You have a single instance of STG when working with a mixed stack.

Note: Refer to *Using the Business Policy Switch 2000 Software Version 2.5* for complete information on upgrading software for a Pure BPS2000 stack and for a Hybrid stack.

Requirements

To use the Web-based management interface, you need the following items:

- A recent computer connected to any of the network ports
- One of the following Web browsers installed on the computer (check the memory requirements):
  - Microsoft Internet Explorer*, version 4.0 or later (Windows 95/98/NT)
  - Netscape Navigator*, version 4.51 or later (Windows 95/98/NT & Unix)
- The IP address of the BPS 2000
- A web browser optimized for 800 by 600 pixel screen size

Note: The Web-based management interface Web pages may load at different speeds depending on the Web browser you use.

Port numbering syntax

When you enter a port number in a stack configuration, you must specify a unit/port number. A unit/port number consists of the unit number, a slash (/), and the port number. For example, 1/1 is the unit number 1 and port number 1, and 3/11 is unit number 3 and port number 11.

In some cases, you can use a list of ports, or a port list. In this case, the same unit/port number notation applies. In addition, you can use hyphens to specify ranges of ports. For example, 1/1-7,2/1-7,2/9,3/1-4,4/12 is a valid unit/port number list. It represents the following port order:

- Unit 1: ports 1 to 7
- Unit 2: ports 1 to 7 and port 9
- Unit 3: ports 1 to 4
- Unit 4: port 12

Logging in to the Web-based management interface

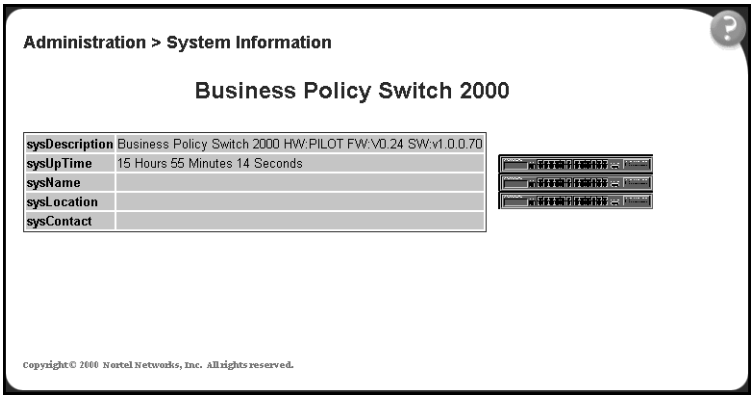
Before you log in to the Web-based management interface, use the console interface to verify the VLAN port assignments and to ensure that your switch CPU and your computer are assigned to the same VLAN. If the devices are not connected to the same VLAN, you cannot access the Web-based management system.

To log in to the Web-based management interface, follow these steps:

1. Start your Web browser.
2. In the Web address field, enter the IP address for your host switch or stack, for example, http://10.30.31.105, and press [Enter].

   The home page opens (Figure 1).

Figure 1 Web-based management interface home page

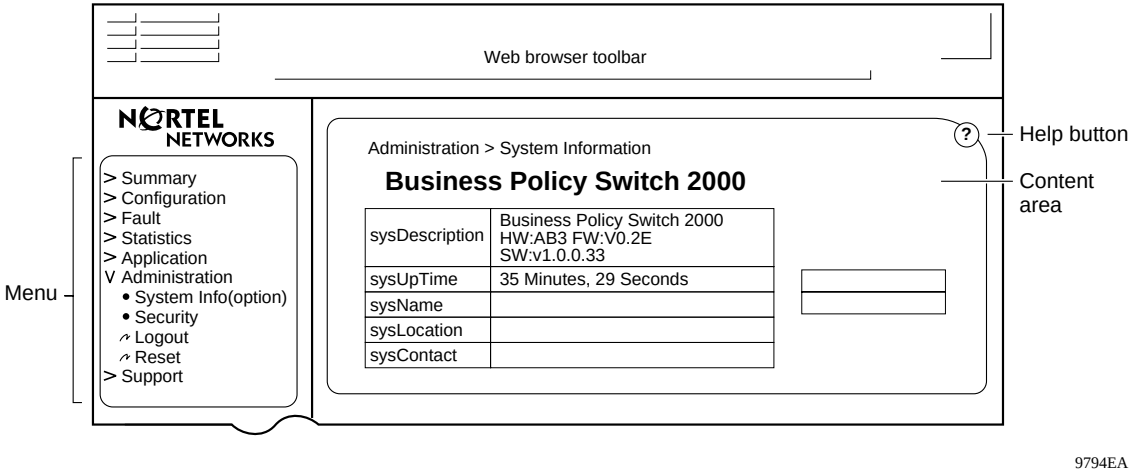


Network security does not yet exist the first time you access the Web-based management user interface. As the system administrator, you must create access parameters and passwords to protect the integrity of your network configuration(s). For more information on setting access parameters and system passwords, refer to Chapter 4.

Web page layout

The home Web page (Figure 2) and all successive Web pages have a common layout. Each is divided into two sections: the menu and the management page. All Web pages are optimized for a 800 x 600 pixel screen size.

Figure 2 Web page layout



Menu

The menu, as shown in Figure 2, contains a list of seven main titles and their corresponding options.

To navigate the Web-based management interface menu, click a menu title and then click one of its options. When you click an option, the corresponding page opens.

Table 1 lists the main headings in the Web-based management user interface and their associated options.

Table 1 Main headings and options

Main menu titles	Options
Summary	Stack Information (stack mode only) Switch Information Identify Unit Numbers (stack mode only) Stack Numbering (stack mode only)
Configuration	IP System Remote Access SNMPv1 SNMPv3* SNMP Trap MAC Address Table Find MAC Address Port Management High Speed Flow Control Software Download Configuration File Console/Comm Port Stack Operational Mode
Fault	RMON Threshold RMON Event Log System Log
Statistics	Port* Port Error Summary Interface* Ethernet Errors* Transparent Bridging* RMON Ethernet* RMON History*
Application	Port Mirroring Rate Limiting EAPOL Security MAC Address Security* IGMP* VLAN* Spanning Tree* Multilink Trunk* QoS* COPS*
Administration	System Information Security* Logout Reset Reset to Defaults
Support	Help Release Notes Manuals Upgrades
*Has additional menus.	

Tools are provided in the menu to assist you in navigating the Web-based management interface.

Caution: Web browser capabilities such as page bookmarking, refresh, and page forward and page back, function as they would in any other Web site. However, these capabilities do not enhance the functionality of the Web-based management interface. Nortel Networks recommends that you use only the navigation tools provided in the management interface.

Table 2 describes the icons that appear on the menu.

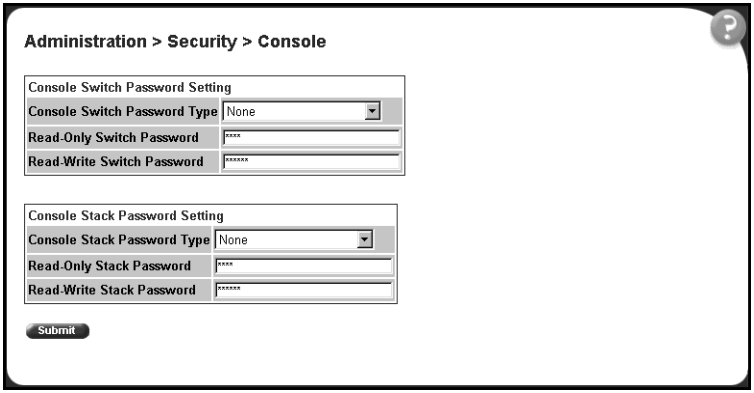
Table 2 Menu icons

Button or icon	Description
	This icon identifies a menu title. Click this icon to display its options.
	This icon identifies a menu title option. Click this icon to display the corresponding page.
	This icon identifies a menu title option with a hyperlink to related pages.
	This icon is linked an action, for example, logout, reset, or reset to system defaults.
NORTEL NETWORKS	Clicking on the Nortel Networks logo opens the corporate home page in a new Web browser.

Management page

When you click a menu option, the corresponding management page opens. Figure 3 shows the page displayed for the Administration > Security > Console option.

Figure 3 Console page



A page is composed of one or more of the following elements:

- Tables and input forms

  The gray cells in a page are display only, and white cells are input fields.

- Check boxes

  You enable or disable a selection by clicking a check box. When a check mark is displayed in the box, that selection is enabled. You disable a selection by clicking the checked box.

- Icons and buttons

  Icons and buttons perform an action concerning the displayed page or the switch. Some pages include a button that opens another page or updates the values shown on the current page. Other pages include icons that initiate an action, such as reformatting the current displayed data as a bar or pie chart.

Table 3 describes the icons that may appear on a pages to assist you in navigation.

Table 3 Page buttons and icons

Icon	Name	Description
	Modify	Accesses a modification page for the selected row.
	View	Accesses a view only statistics page for the selected row.
	Delete	Deletes a row.
	Bar Graph	Displays statistics information in a bar graph format.
	Help	Accesses the Help menu in a new Web browser.
	Item-Specific Help	Accesses the item-specific Help menu in a new Web browser.
		Note: Text within a table that is highlighted blue and underlined is a hyperlink to a related management page.

Chapter 2
Administering the switch

The administrative options available to you are:

For more information on the feature discussed in this chapter, refer to *Using the Business Policy Switch 2000 Software Version 2.5*. This book also has instructions using the Console Interface (CI) menus to configure and manage the switch. Refer to *Reference for the Command Line Interface for the Business Policy Switch 2000 Management Software Version 2.5* for instructions on managing the BPS 2000 using the CLI and to *Reference for the Business Policy Switch 2000 Management Software Version 2.5* for instructions on managing the switch using the Device Manager.

Note: The software version 2.5 features are available in a mixed stack if you access the stack through a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Viewing general information

You can view an image of the BPS 2000 switch or an image of your entire stack configuration, as information on use of the BPS 2000 CPU and memory capacity.

Viewing system information

You can view an image of the BPS 2000 switch or an image of your entire stack configuration, information about the host device (or stack) and, if provided, the contact person or manager for the switch. The System Information page is also the Web-based management interface home page.

To view system information:

➨ From the main menu, choose Administration > System Information.

The System Information page opens (Figure 4).

Note: You create or modify existing system information parameters on the System page. For more information on configuring system information, refer to Chapter 2.

Figure 4 System Information home page

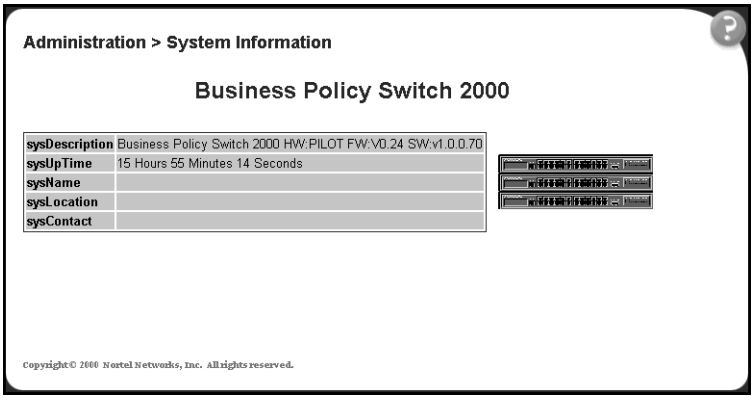


Table 4 describes the items on the System Information page.

Table 4 System Information page items

Item	Description
sysDescription	The default description of the Business Policy Switch 2000, including the hardware, firmware, software, and ISVN version numbers.
sysUpTime	The elapsed time since the last network management portion of the system was last re-initialized.
sysName	The name created by the network administrator to identify the switch, for example Finance Group.
sysLocation	The location name created by the network administrator to identify the switch location, for example, first floor.
sysContact	The name and email contact information of the administratively assigned person to contact regarding switch operation.

Configuring system security

This section describes the steps you use to build and manage security using the Web-based management interface. For more information on setting security systems, refer to setting EAPOL, MAC security, and IP manager list in Chapter 4.

Setting console, Telnet, and Web passwords

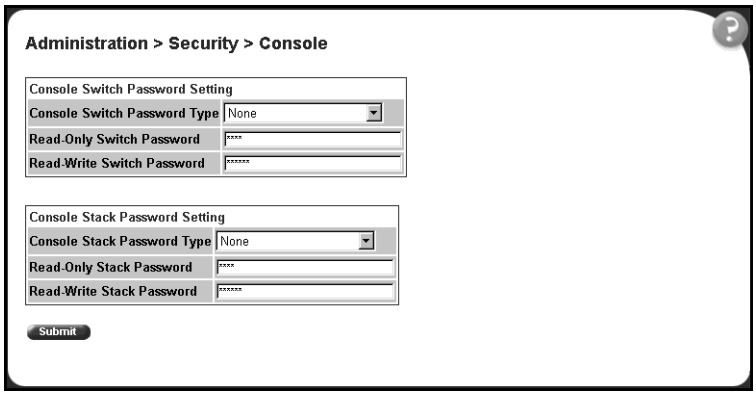
To set console, Telnet, and Web passwords:

1. From the main menu, choose Administration > Security and Console, Telnet, or Web.

   The selected password page opens (Figure 5).

Note: The title of the page corresponds to the menu selection you choose. In Figure 5, the network administrator selected Administration > Security > Console.

Figure 5 Console password setting page



Note: Console, Telnet, and Web settings share the same switch and stack password type and password.

Table 5 describes the items on the Console page.

Table 5 Console page items

Section	Item	Setting	Description
Console Switch Password Setting	Console Switch Password Setting Type	(1) None (2) Local Password (3) RADIUS Authentication	Displays the switch password types. Note: The default is None.
	Read-Only Switch Password	1..15 alphanumeric string	Type the read-only password setting for the read-only access user.
	Read-Write Switch Password	1..15 alphanumeric string	Type the read-write password setting for the read-write access user.
Console Stack Password Setting	Console Stack Password Setting Type	(1) None (2) Local Password (3) RADIUS Authentication	Displays the stack password types. Note: The default is None.
	Read-Only Stack Password	1..15 alphanumeric string	Type the read-only password setting for the read-only access user.
	Read-Write Stack Password	1..15 alphanumeric string	Type the read-write password setting for the read-write access user.

2 Type the information, or make a selection from the list.

3 Click Submit.

Configuring RADIUS security

To configure RADIUS security parameters:

1 From the main menu, choose Administration > Security > RADIUS.

The RADIUS page opens.

Figure 6 RADIUS page

Table 6 describes the items on the RADIUS page.

Table 6 RADIUS page items

Item	Setting	Description
Primary RADIUS Server	XXX.XXX.XXX.XXX	Type a Primary RADIUS server IP address in the appropriate format.
Secondary RADIUS Server	XXX.XXX.XXX.XXX	Type a Secondary RADIUS server IP address in the appropriate format.
UDP RADIUS Port	Integer	Type the UDP RADIUS port number.
RADIUS Shared Secret	1..16	Type a unique character string to create a secret password.

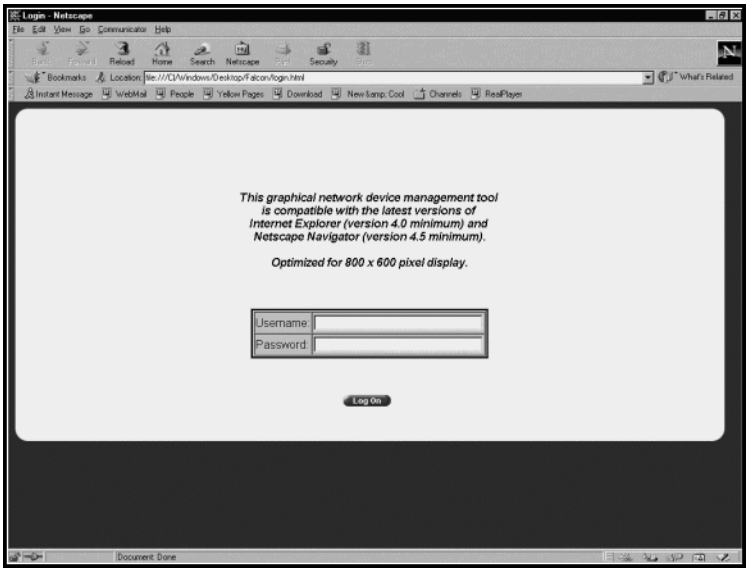
2 Type the information.

3 Click Submit.

Logging on to the management interface

Once switch and stack passwords and RADIUS authentication settings are integrated into the Web-based management user interface, anyone who attempts to use the application is presented with a log on page (Figure 7).

Figure 7 Web-based management interface log on page

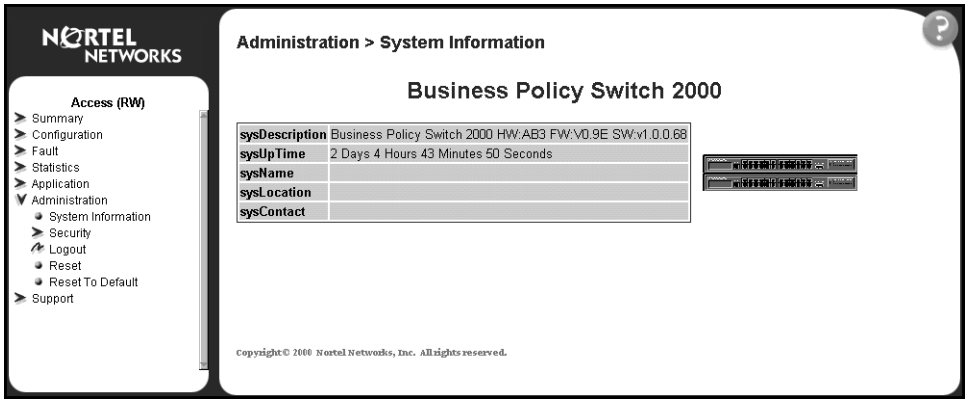


To log on to the Web-based management interface:

1. In the Username text box, type **RO** for read-only access or **RW** for read-write access.
2. In the Password text box, type your password.
3. Click Log On.

   The System Information home page opens (Figure 8).

Figure 8 System Information home page



With Web access enabled, the switch can support up to four concurrent Web page users. Two predefined user levels are available, and each user level has a corresponding username and password.

Table 7 shows an example of the two predefined user levels available and their access level within the Web-based management user interface.

Table 7 User levels and access levels

User level	User name for each level	Password for each user level	Access Level
Read-only	RO	XXXXXXXX	Read only
Read-write	RW	XXXXXXXX	Full read/write access

Resetting the BPS 2000

You can reset a standalone switch, a specific unit in a stack configuration, or an entire stack without erasing any configured switch parameters. While resetting, the switch initiates a self-test that comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress. (Resetting means rebooting in this context.)

To reset the BPS 2000 without making changes (since your last Submit request):

1 From the main menu, choose Administration > Reset.

The Reset page opens (Figure 9).

Note: When you are working on a single (nonstacked) switch, the system returns the message:
`Are you sure your want to reset the switch?`
When you press OK, the switch resets.

Figure 9 Reset page

2 From the list, choose to reset the switch only, or the entire stack.

3 Click Submit.

Note: If you have not configured system password security, a reset returns you to the home page, as shown in Figure 1 on page 35. If you have configured system password security, a reset returns you to a log on page, as shown in Figure 7 on page 46.

Resetting the BPS 2000 to system defaults

You can reset a standalone switch, a specific unit in a stack configuration, or an entire stack, replacing all configured switch parameters with the factory default values.

Caution: If you choose reset to default settings, all configured settings are replaced with factory default settings when you click Submit (Stack Operational Mode is not reset to factory default}. For more information on factory default settings, see *Using the Business Policy Switch 2000 Software Version 2.5*.

During the reset process, the switch initiates a self-test that comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

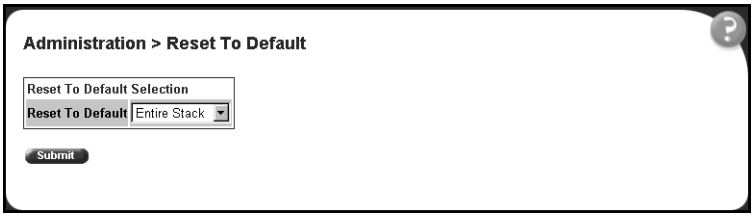
To reset the BPS 2000 to system defaults:

1 From the main menu, choose Administration > Reset to Default.

The Reset to Default page opens (Figure 10).

Note: When you are working on a single (nonstacked) switch, the system returns the message:
`Are you sure your want to reset the switch?`
When you press OK, the switch resets.

Figure 10 Reset to Default page



2 From the list, choose to reset the switch only to system defaults, or the entire stack.

3 Click Submit.

Note: If you have not configured system password security, a reset returns you to the home page, as shown in Figure 1 on page 35. If you have configured system password security, a reset returns you to a log on page, as shown in Figure 7 on page 46.

Logging out of the management interface

To log out of the Web-based management interface:

1 From the main menu, choose Administration > Logout.

A message opens prompting you to confirm your request

2 Do one of the following:

- Click OK to logout of the Web-based management interface.
- Click Cancel to return to the Web-based management interface home page.

Chapter 3
Viewing summary information

The summary information options are:

Note: To access the software version 2.5 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Viewing stack information

You can view a summary of your stack framework, for example, the current version of the running software and the IP address of the Web-based management interface.

Note: The Web-based management user interface automatically detects the operational mode of your system. If the system is in standalone mode, the Stack Information page is not an option listed in the menu. For information on how to set system operational modes, see "Setting system operational modes" on page 122.

To view stack information:

1 From the main menu, choose Summary > Stack Information.

The Stack Information page opens (Figure 11).

Figure 11 Stack Information page

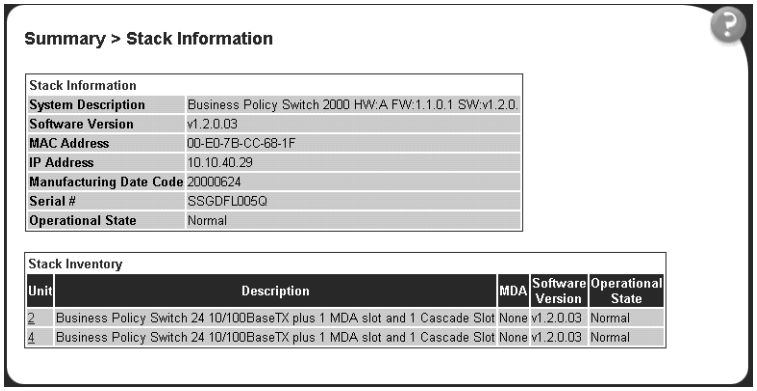


Table 8 describes the fields on the Stack Information and Stack Inventory sections of the Stack Information page.

Table 8 Stack Information page fields

Section	Fields	Description
Stack Information	System Description	The name created in the configuration process to identify the stack.
	Software Version	The version of the running software.
	MAC Address	The MAC address of the stack.
	IP Address	The IP address of the stack.
	Manufacturing Date Code	The date of manufacture of the board in ASCII format: YYYYMMDD.
	Serial Number	The serial number of the base unit.
	Operational State	The current operational state of the device. The operational states are: Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured
Stack Inventory	Unit	The unit number assigned to the device by the network manager. For more information on stack numbering, see page 54.
	Description	The description of the device or its subcomponent.
	MDA	The media dependent adapter (MDA) connected to the switch.

Table 8 Stack Information page fields (continued)

Section	Fields	Description
	Software Version	The current running software version.
	Operational State	The current operational state of the stack. The operational states are: Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured.

2 In the upper-left corner of the Stack Information page, click the number of the device you want to view.

The Stack Information page is updated with information about the selected switch.

Viewing summary switch information

You can view summary information about the switch, for example, the unit number and its corresponding physical description and serial number.

To view summary switch information:

1 From the main menu, choose Summary > Switch Information.

The Switch Information page opens (Figure 12).

Figure 12 Switch Information page

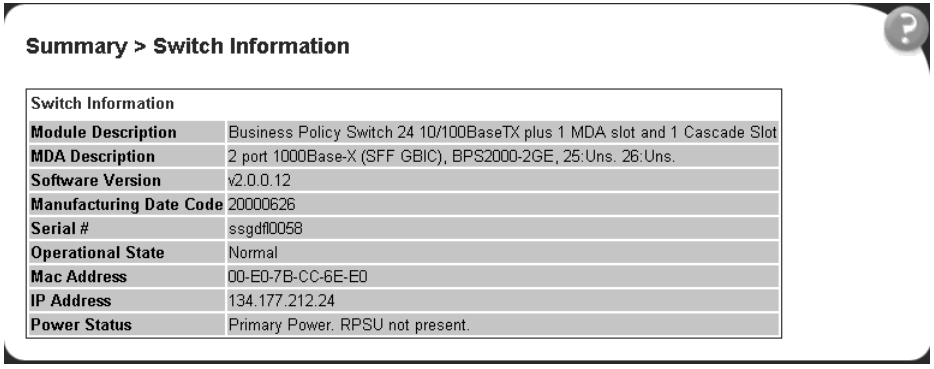


Table 9 describes the fields on the Switch Information page.

Table 9 Switch Information page fields

Item	Description
Unit	Select the number of the device on which to view summary information. The page is updated with information about the selected switch. For more information on stack numbering, see page 54.
Module Description	The factory set description of the policy switch.
MDA Description	The factory set description of the sub-component/MDA.
Software Version	The version of the running software.
Manufacturing Date Code	The date of manufacture of the board in ASCII format.
Serial Number	The serial number of the policy switch.
Operational State	The current operational state of the device. The operational states are: Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured.
Mac Address	The MAC address of the device.
IP Address	The IP address of the device.
Power Status	The current power status of the device: • Primary Power. RPSU not present • Primary Power. RPSU present • Redundant Power. Primary power failed • Unavailable

2 In the upper-left corner of the Switch Information page, click the number of the device you want to view.

The Switch Information page is updated with information about the selected switch.

Changing stack numbering

If your system is set to “stack” operational mode, you can view existing stack numbering information and renumber the devices in your stack framework. For information on how to set your system’s operational mode, see “Setting system operational modes” on page 122.

Note: The unit number does not affect the base unit designation.

To view or renumber devices within the stack framework:

1 From the main menu, choose Summary > Stack Numbering.

The Stack Numbering Setting page opens (Figure 13).

Figure 13 Stack Numbering Setting page

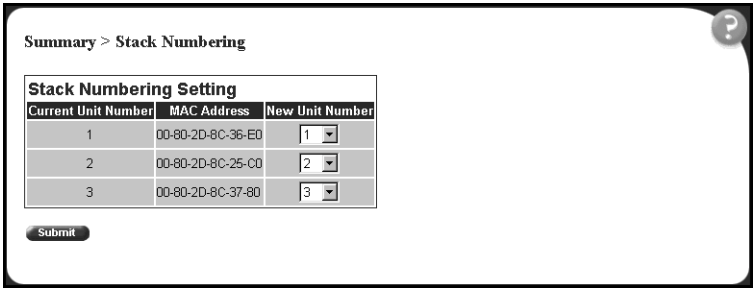


Table 10 describes the fields on the Stack Numbering Setting page.

Table 10 Stack Numbering Setting page fields

Item	Range	Description
Current Unit Number	1..8	Unit number previously assigned to the policy switch. The entries in this column are displayed in order of their current physical cabling with respect to the base unit, and can show nonconsecutive unit numbering if one or more units were previously moved or modified. The entries can also include unit numbers of units that are no longer participating in the stack (not currently active).
MAC Address	XX.XX.XX.XX.XX.XX	MAC address of the corresponding unit listed in the Current Unit Number field.
New Unit Number	1..8, None	Choose a new number to assign to your selected policy switch. Note: If you leave the field blank, the system automatically selects the next available number.

2 Choose the new number to assign to your switch.

3 Click Submit.

A message opens prompting you to confirm your request.

4 Do one of the following:

- Click OK to renumber the stack.

- Click Cancel to return to the Stack Numbering page without making changes.

Identifying unit numbers

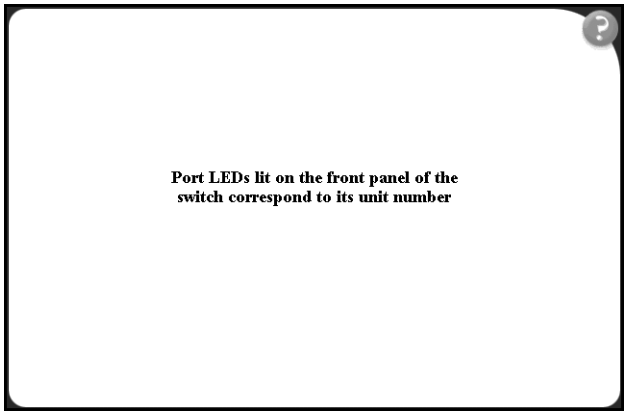
You can identify the unit numbers of the switches participating in a stack configuration by viewing the LEDs on the front panel of each switch.

To identify unit numbers in your configuration:

1 From the main menu, choose Summary > Identify Unit Numbers.

The Identify Unit Numbers page opens (Figure 14).

Figure 14 Identify Unit Numbers page



2 To continue viewing summary information or to start the configuration process, choose another option from the main menu.

Chapter 4
Configuring the switch

The switch configuration options available to you are:

Note: To access the software version 2.5 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Configuring BootP, IP, and gateway settings

You can configure your BootP mode settings, create and modify your in-band stack and in-band switch IP addresses and in-band subnet mask parameters, and configure the IP address of your default gateway. Beginning with software version 2.0, you can configure IP addresses for individual units in a stack.

Note: Settings take effect immediately when you click Submit.

To configure BootP, IP, and gateway settings:

1 From the main menu, choose Configuration > IP.

The IP page opens (Figure 15).

Figure 15 IP page for a standalone BPS 2000

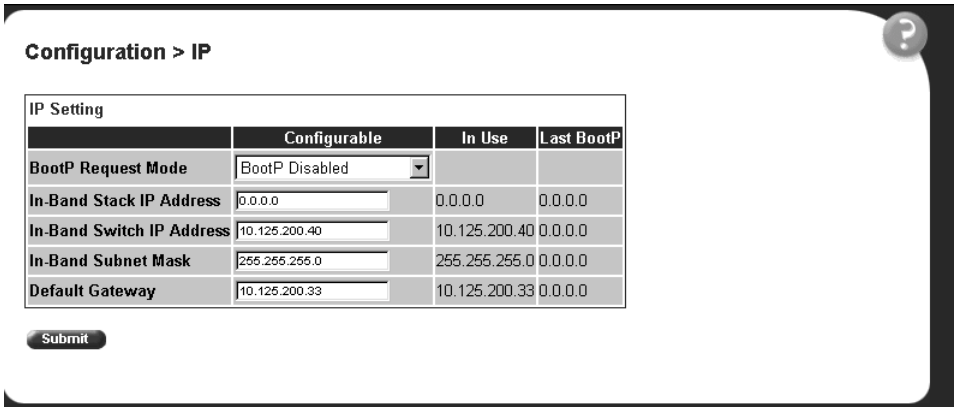
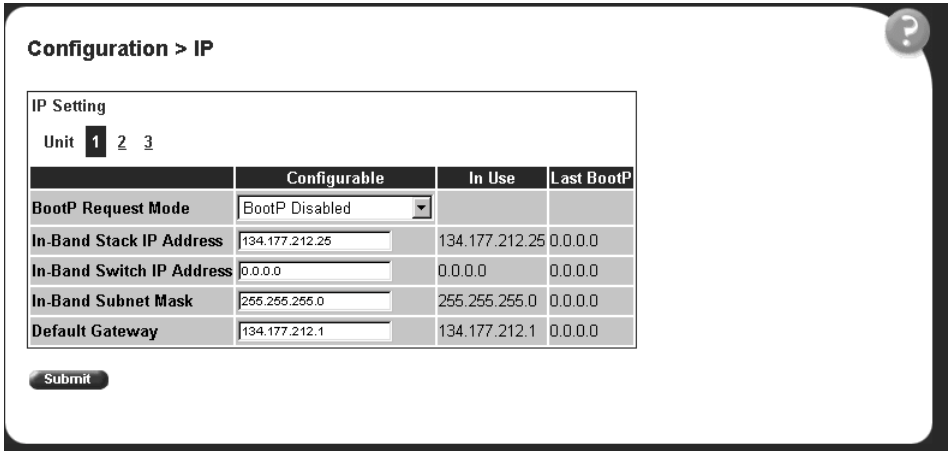


Figure 16 IP page for a stack



Note: To change the IP information for a specific unit in the stack, choose that unit and enter the desired IP information into the In-Band Switch IP address field.

Table 11 describes the items on the IP page.

Table 11 IP page items

Section	Item	Range	Description
Boot Mode Setting	BootP Request Mode	BootP When Needed	Choose this mode to inform the switch to send a BootP request when the switch IP address stored in nonvolatile memory is the factory default value. If the stored IP address differs from the factory default value, the switch uses the stored network parameters. If the switch cannot find a BootP server, it tries five more times to find one and then defaults to the factory settings
		BootP Always	Choose this mode to inform the switch, each time the switch boots, to ignore any stored network parameters and send a BootP request. If the BootP request fails, the switch boots with the factory default IP configuration. This setting disables remote management if no BootP server is set up for the switch, but it allows the switch to boot normally.
		BootP Disabled	Choose this mode to inform the switch, each time the switch boots, to use the IP configuration parameters stored in non-volatile memory. If a BootP configuration is in progress when you issue this command, the BootP configuration stops.

Table 11 IP page items

Section	Item	Range	Description
		BootP or Last Address	Choose this mode to inform the switch, at each startup, to obtain its IP configuration using BootP. If the BootP request fails, the switch uses the network parameters stored in its non-volatile memory. Note: Valid parameters obtained in using BootP always replace current information stored in the non-volatile memory.
		Note: Whenever the switch is broadcasting BootP requests, the BootP process times out if a reply is not received within (approximately) 7 minutes. When the process times out, the BootP request mode automatically changes to BootP Disabled mode. To restart the BootP process, change the BootP request mode to any of the three following modes: BootP When Needed, BootP Always, or to BootP or Last Address.	
IP Setting	In-Band Stack IP Address	XXX.XXX.XXX.XXX	Type a new stack IP address in the appropriate format.
	In-Band Switch IP Address	XXX.XXX.XXX.XXX	Type a new switch IP address in the appropriate format. Note: When the IP address is entered in the In-Band IP Address field, and the In-Band Subnet Mask field value is not present, the software provides an *in-use* default value for the In-Band Subnet Mask field that is based on the class of the IP address entered in the In-Band IP Address field.
	In-Band Subnet Mast	XXX.XXX.XXX.XXX	Type a new subnet mask in the appropriate format.
	In-Use		The column header for the read-only fields in this screen. The data displayed in this column represents data that is currently in use.
	Last BootP		The column header for the read-only fields in this screen. The read-only data displayed in this column represents data obtained from the last BootP reply received.
Gateway Setting	Default Gateway	XXX.XXX.XXX.XXX	Type an IP address for the default gateway in the appropriate format.

2 Type information in the text boxes, or select from a list.

3 Click Submit.

Modifying system settings

You can create or modify the system name, system location, and network manager contact information.

Note: The configurable parameters on the System page are displayed in a read only-format on the Web-based management user interface System Information home page (see Figure 1 on page 35).

To configure system settings:

1 From the main menu, choose Configuration > System.

The System page opens (Figure 17).

Figure 17 System page

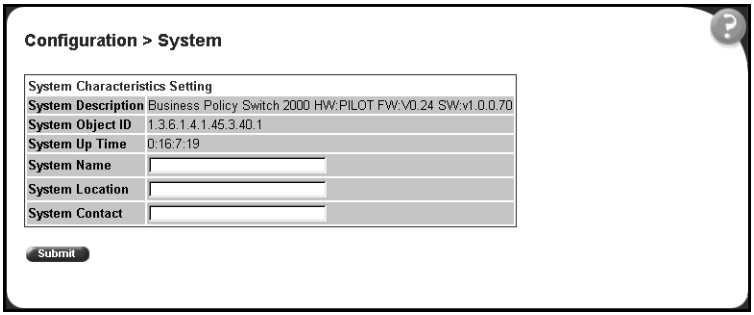


Table 12 describes the items on the System page.

Table 12 System page items

Item	Range	Description
System Description		The factory set description of the hardware and software versions.
System Object ID		The character string that the vendor created to uniquely identify this device.
System Up Time		The elapsed time since the last network management portion of the system was last re-initialized. Note: This field is updated only when the screen is redisplayed.
System Name	0..255	Type a character string to create a name to identify the switch, for example Finance Group.
System Location	0..255	Type a character string to create a name for the switch location, for example, First Floor.
System Contact	0..255	Type a character string to create the contact information for the network manager or the selected person to contact regarding switch operation, for example, mcarlson@company.com Note: To operate correctly with the Web interface, the system contact should be an e-mail address.

2 Type information in the text boxes.

3 Click Submit.

About SNMP

Simple Network Management Protocol (SNMP) is the standard for network management that uses a common software agent to manage local and wide area network equipment from different vendors; part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite and defined in RFC1157. SNMPv1 is version one, or the original standard protocol. SNMPv3 is a combination of proposal updates to SNMP, most of which deal with security.

Configuring SNMPv1

You can configure SNMPv1 read-write and read-only community strings, enable or disable trap mode settings, and/or enable or disable the Autotopology feature. The Autotopology feature, when enabled, performs a process that recognizes any device on the managed network and defines and maps its relation to other network devices in real time.

To configure the community string, trap mode, and Autotopology settings and features:

1 From the main menu, choose Configuration > SNMPv1.

The SNMPv1 page opens (Figure 18).

Figure 18 SNMPv1 page

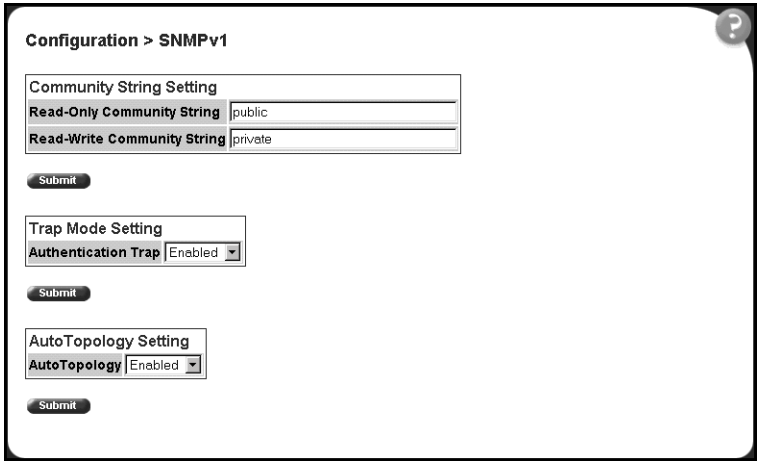


Table 13 describes the items on the SNMPv1 page.

Table 13 SNMPv1 page items

Section	Item	Range	Description
Community String Setting	Read-Only Community String	1..32	Type a character string to identify the community string for the SNMPv1 read-only community, for example, public or private. The default value is public.
	Read-Write Community String	1..32	Type a character string to identify the community string for the SNMPv1 read-write community, for example, public or private. The default value is private.
Trap Mode Setting	Authentication Trap	(1) Enable (2) Disable	Choose to enable or disable the authentication trap.
AutoTopology Setting	AutoTopology	(1) Enable (2) Disable	Choose to enable or disable the autotopology feature.

2 Type information in the text boxes, or select from a list.

3 Click Submit in any section to save your changes.

Configuring SNMPv3

This section describes the steps to build and manage SNMPv3 in the Web-based management user interface.

Viewing SNMPv3 system information

You can view information about the SNMPv3 engine that exists and the private protocols that are supported in your network configuration. You can also view information about packets received by the system having particular errors, such as unavailable contexts, unknown contexts, decrypting errors, or unknown user names.

To view SNMPv3 system information:

1 From the main menu, choose Configuration > SNMPv3 > System Information.

The System Information page opens (Figure 19).

Figure 19 System Information page

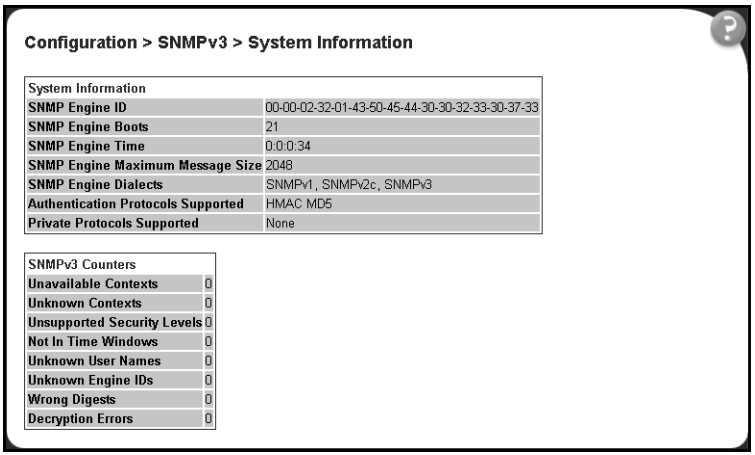


Table 14 describes the fields on the System Information section of the SNMPv3 System Information page.

Table 14 System Information section fields

Item	Description
SNMP Engine ID	The SNMP engine's identification number.
SNMP Engine Boots	The number of times that the SNMP engine has re-initialized itself since its initial configuration.
SNMP Engine Time	The number of seconds since the SNMP engine last incremented the snmpEngineBoots object.
SNMP Engine Maximum Message Size	The maximum length, in octets, of an SNMP message which this SNMP engine can send or receive and process determined as the minimum of the maximum message size values supported among all transports available to and supported by the engine.
SNMP Engine Dialects	The SNMP dialect the engine recognizes. The dialects are:SNMP1v1, SNMPv2C, and SNMPv3.
Authentication Protocols Supported	The registration point for standards-track authentication protocols used in SNMP Management Frameworks. The registration points are: None, HMAC MD5. Note: The Business Policy Switch 2000 supports only the MD5 authentication protocol.
Private Protocols Supported	The registration point for standards-track privacy protocols used in SNMP Management Frameworks. The registration points are: None or CBC-DES. Note: The Business Policy Switch 2000 does not support privacy protocols.

Table 15 describes the fields on the SNMPv3 Counters section of the SNMPv3 System Information page.

Table 15 SNMPv3 Counters section fields

Item	Description
Unavailable Contexts	The total number of packets dropped by the SNMP engine because the context contained in the message was unavailable.
Unknown Contexts	The total number of packets dropped by the SNMP engine because the context contained in the message was unknown.
Unsupported Security Levels	The total number of packets dropped by the SNMP engine because they requested a security level that was unknown to the SNMP engine or otherwise unavailable.
Not in Time Windows	The total number of packets dropped by the SNMP engine because they appeared outside of the authoritative SNMP engine's window.
Unknown User Names	The total number of packets dropped by the SNMP engine because they referenced an unknown user.
Unknown Engine IDs	The total number of packets dropped by the SNMP engine because they referenced an snmpEngineID that was not known to the SNMP engine.
Wrong Digests	The total number of packets dropped by the SNMP engine because they did not contain the expected digest value.
Decryption Errors	The total number of packets dropped by the SNMP engine because they could not be decrypted.

Configuring user access to SNMPv3

You can view a table of all current SNMPv3 user security information such as authentication/privacy protocols in use, and create or delete SNMPv3 system user configurations.

Creating an SNMPv3 system user configuration

To create an SNMPv3 system user configuration:

1 From the main menu choose Configuration > SNMPv3 > User Specification.

The User Specification page opens (Figure 20).

Figure 20 User Specification page

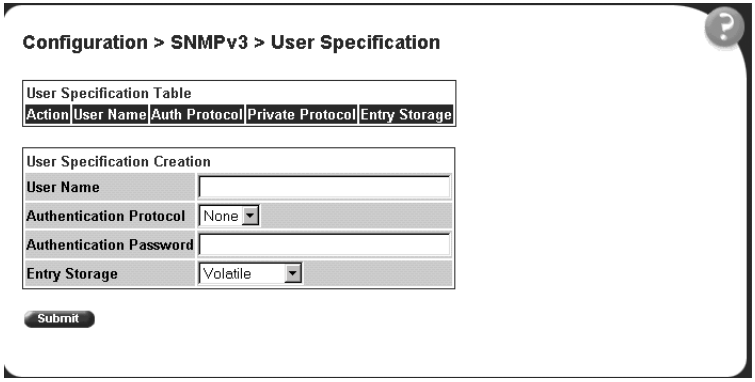


Table 16 describes the items on the User Specification Table section of the User Specification page.

Table 16 User Specification Table section items

Item and MIB association	Description
	Deletes the row.
User Name (usmUserSecurityName)	The name of an existing SNMPv3 user.
Authentication Protocol (usmUserAuthProtocol)	Indicates whether the message sent on behalf of this user to/from the SNMP engine identified UserEngineID can be authenticated by the MD5 authentication protocol. Note: The Business Policy Switch 2000 supports only the MD5 authentication protocol.
Private Protocol (usmUserPrivProtocol)	Displays whether or not messages sent on behalf of this user to or from the SNMP engine identified by usmUserEngineID can be protected from disclosure, and if so, the type of privacy protocol which is used.
Entry Storage	The current storage type for this row. If “Volatile” is displayed, information is dropped (lost) when you turn the power off. If non-volatile is displayed, information is saved in NVRAM when you turn the power off

Table 17 describes the items on the User Specification Creation section of the User Specification page.

Table 17 User Specification Creation section items

Item and MIB association	Range	Description
User Name	1..32	Type a string of characters to create an identity for the user.
Authentication Protocol (usmUserAuthProtocol)	None MD5	Choose whether or not the message sent on behalf of this user to/from the SNMP engine identified UserEngineID can be authenticated with the MD5 protocol. Note: The Business Policy Switch 2000 supports only the MD5 authentication protocol.
Authentication Password (usmUserAuthPassword)	1..32	Type a string of character to create a password to use in conjunction with the authorization protocol.
Entry Storage (usmUserStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the User Specification Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new configuration is displayed in the User Specification Table (Figure 20).

Deleting an SNMPv3 system user configuration

To delete an existing SNMPv3 user configuration:

1. From the main menu, choose Configuration > SNMPv3 > User Specification.

   The User Specification page opens (Figure 20).

2. In the User Specification Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the SNMPv3 user configuration.
   - Click Cancel to return to the User Specification page without making changes.

Configuring an SNMPv3 system user group membership

You can view a table of existing SNMPv3 group membership configurations and map or delete an SNMPv3 user to group configuration.

Mapping an SNMPv3 system user to a group

To map an SNMPv3 system user to a group:

1. From the main menu, choose Configuration > SNMPv3 > Group Membership.

   The Group Membership page opens (Figure 21).

Figure 21 Group Membership page

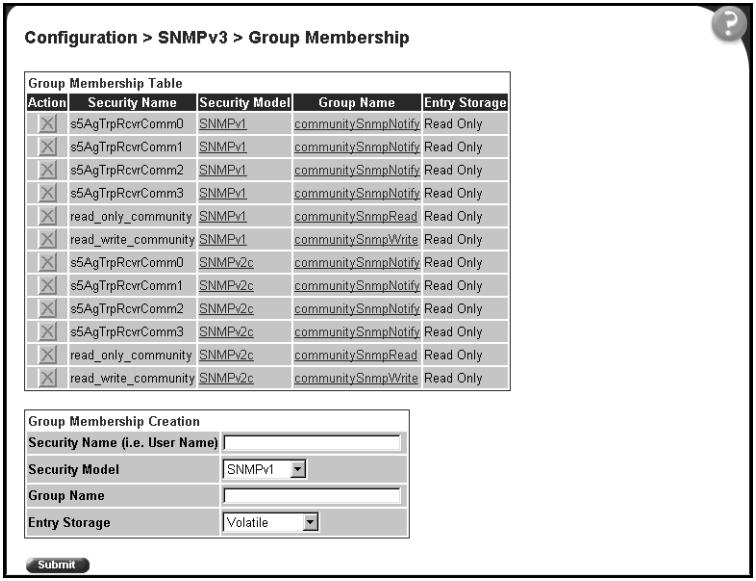


Table 18 describes the items on the Group Membership page.

Table 18 Group Membership page items

Item and MIB association	Range	Description
		Deletes the row.
Security Name (vacmSecurityToGroupStatus)	1..32	Type a string of character to create a security name for the principal which is mapped by this entry to a group name.
Security Model (vacmSecurityToGroupStatus)	(1) SNMPv1 (2) SNMPv2c (3) USM	Choose the security model within which the security name to group name mapping is valid.
Group Name (vacmGroupName)	1..32	Type a string of character to specify the group name.
Entry Storage (vacmSecurityToGroupStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the Group Membership Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Group Membership Table.

Deleting an SNMPv3 group membership configuration

To delete an SNMPv3 group membership configuration:

1 From the main menu, choose Configuration > SNMPv3 > Group Membership.

The Group Membership page opens (Figure 21).

2 In the Group Membership Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the group membership configuration.
- Click Cancel to return to the Group Membership page without making changes.

Note: This Group Membership Table section of the Group Membership page contains hyperlinks to the SNMPv3 User Specification and Group Access Rights pages. For more information on these pages, see "Configuring user access to SNMPv3" on page 66 and "Configuring SNMPv3 group access rights" on page 72.

Configuring SNMPv3 group access rights

You can view a table of existing SNMPv3 group access rights configurations, and you can create or delete a group's SNMPv3 system-level access rights.

Creating an SNMPv3 group access rights configuration

To create a group's SNMPv3 system-level access right configuration:

1 From the main menu, choose Configuration > SNMPv3 > Group Access Rights.

The Group Access Rights page opens (Figure 22).

Figure 22 Group Access Rights page

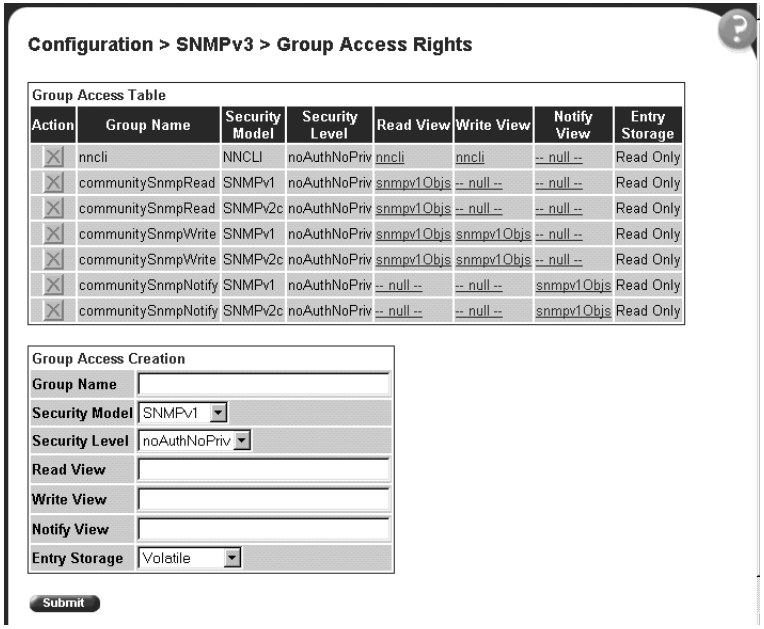


Table 19 describes the items on the Group Access Rights page.

Table 19 Group Access Rights page items

Item and MIB association	Range	Description
		Deletes the row.
Group Name (vacmAccessToGroupStatus)	1..32	Type a character string to specify the group name to which access is granted.
Security Model (vacmAccessSecurityModel)l	(1) SNMPv1 (2) SNMPv2c (3) USM	Choose the security model to which access is granted.
Security Level (vacmAccessSecurityLevel)	(1) noAuthNoPriv (2) authNoPriv	Choose the minimum level of security required in order to gain the access rights allowed to the group.
Read View (vacmAccessReadViewName)	1..32	Type a character string to identify the MIB view of the SNMP context to which this entry authorizes read access.
Write View (vacmAccessWriteViewName)	1..32	Type a character string to identify the MIB view of the SNMP context to which this entry authorizes write access.
Notify View (vacmAccessNotifyViewName)	1..32	Type a character string to identify the MIB view to which this entry authorizes access to notifications.
Entry Storage (vacmSecurityToGroupStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the Group Access Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Group Access Table.

Deleting an SNMPv3 group access rights configuration

To delete a n SNMPv3 group access configuration:

1 From the main menu, choose Configuration > SNMPv3 > Group Access Rights.

The Group Access Rights page opens (Figure 22).

2 In the Group Access Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the group access configuration.
- Click Cancel to return to the Group Access Rights page without making changes.

Note: This Group Access Table section of the Group Access Rights page contains hyperlinks to the Management Information View page. For more information, see "Configuring an SNMPv3 management information view" on page 74.

Configuring an SNMPv3 management information view

You can view a table of existing SNMPv3 management information view configurations, and you can create or delete SNMPv3 management information view configurations.

Note: A view may consist of multiple entries in the table, each with the same view name, but a different view subtree.

Creating an SNMPv3 management information view configuration

To create an SNMPv3 management information view configuration:

1 From the main menu, choose Configuration > SNMPv3 > Management Info View.

The Management Information page opens (Figure 23).

Figure 23 Management Information View page

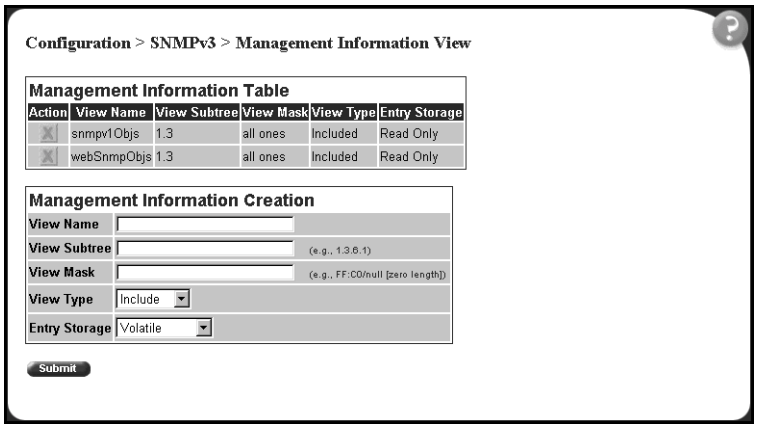


Table 20 describes the items on the Management Information View page.

Table 20 Management Information View page items

Item and MIB association	Range	Description
		Deletes the row.
View Name (vacmViewTreeFamilyViewName)	1..32	Type a character string to create a name for a family of view subtrees.
View Subtree (vacmViewTreeFamilySubtree)	X.X.X.X.X...	Type an object identifier (OID) to specify the MIB subtree which, when combined with the corresponding instance of vacmViewTreeFamilyMask, defines a family of view subtrees. Note: If no OID is entered and the field is blank, a default mask value consisting of “1s” is recognized.
View Mask (vacmViewTreeFamilyMask)	Octet String (0..16)	Type the bit mask which, in combination with the corresponding instance of vacmViewFamilySubtree, defines a family of view subtrees.
View Type (vacmViewTreeFamilyType)	(1) Included (2) Excluded	Choose to include or exclude a family of view subtrees.
Entry Storage (vacmSecurityToGroupStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the Management Information Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Management Information Table (Figure 23).

Deleting an SNMPv3 management information view configuration

To delete an existing SNMPv3 management information view configuration:

1 From the main menu, choose Configuration > SNMPv3 > Management Info View.

The Management Information page opens (Figure 23).

2 In the Management Information Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the management information view configuration.
- Click Cancel to return to the table without making changes.

Configuring an SNMPv3 system notification entry

You can view a table of existing SNMPv3 system notification configurations, and you can configure specific SNMPv3 system notification types with particular message recipients and delete SNMPv3 notification configurations.

Creating an SNMPv3 system notification configuration

To create an SNMPv3 system notification configuration:

1 From the main menu, choose Configuration > SNMPv3 > Notification.

The Notification page opens (Figure 24).

Figure 24 Notification page

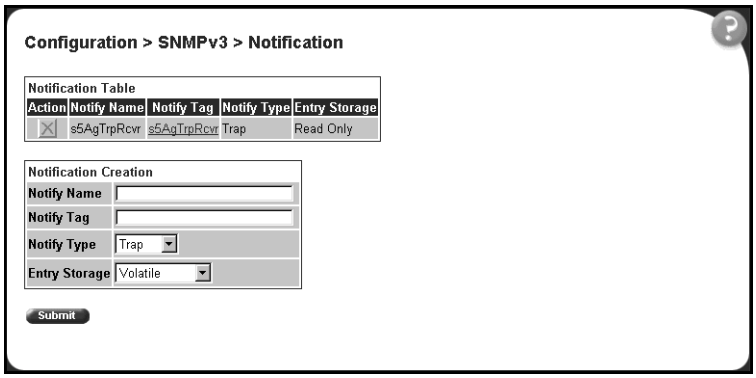


Table 21 describes the items on the Notification page.

Table 21 Notification page items

Item and MIB association	Range	Description
		Deletes the row.
Notify Name (snmpNotifyRowStatus)	1..32	Type a character string to identify the entry.
Notify Tag (snmpNotifyTag)	1..32	Type a value which to use to select entries in the snmpTargetAddrTable. Any entry in the snmpTargetAddrTable which contains a tag value which is equal to the value of an instance of this object is selected. If this object carries a zero length, no entries are selected
Notify Type (snmpNotifyType)	(1) Trap (2) Inform	Choose the type of notification to generate.
Entry Storage (snmpNotifyStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the Notification Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Notification Table (Figure 24).

Note: This Notification Table section of the Notification page contains hyperlinks to the Target Parameter page. For more information, see "Configuring an SNMPv3 management target parameter" on page 81.

Deleting an SNMPv3 system notification configuration

To delete an SNMPv3 notification configuration:

1 From the main menu, choose Configuration > SNMPv3 > Notification.

The Notification page opens (Figure 24).

2 In the Notification Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the notification configuration.
- Click Cancel to return to the table without making changes.

Configuring an SNMPv3 management target address

You can view a table of existing SNMPv3 management target configurations, create SNMPv3 management target address configurations that associate notifications with particular recipients and delete SNMPv3 target address configurations.

Creating an SNMPv3 target address configuration

To create an SNMPv3 target address configuration:

1 From the main menu, choose Configuration > SNMPv3 > Target Address.

The Target Address page opens (Figure 25).

Figure 25 Target Address page

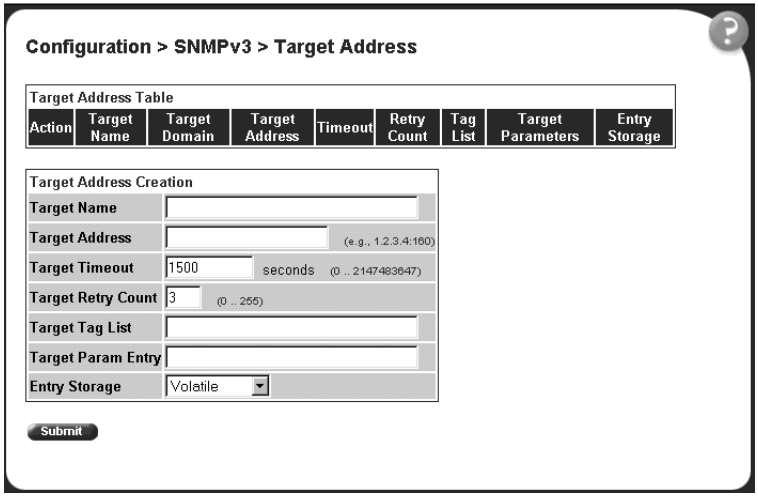


Table 22 describes the items on the Target Address page.

Table 22 Target Address page items

Item and MIB association	Range	Description
✕		Deletes the row.
Target Name (snmpTargetAddrName)	1..32	Type a character string to create a target name.
Target Domain (snmpTargetAddrTDomain)	1..32	The transport type of the address contained in the snmpTargetAddrTAddress object.
Target Address (snmpTargetAddrTAddress)	XXX.XXX.XXX.XXX:XXX	Type a transport address in the format of an IP address, colon, and UDP port number. For example: 10.30.31.99:162 (see Figure 25 on page 79).
Target Timeout (snmpTargetAddrTimeout)	Integer	Type the number, in seconds, to designate as the maximum time to wait for a response to an inform notification before re-sending the “Inform” notification.
Target Retry Count (snmpTargetAddrRetryCount)	0..255	Type the default number of retires to be attempted when a response is not received for a generated message. An application may provide its own retry count, in which case the value of this object is ignored.
Target Tag List (snmpTargetAddrTagList)	1..20	Type the space-separated list of tag values to be used to select target addresses for a particular operation.
Target Parameter Entry (snmpTargetAddr)	1..32	Type a numeric string to identify an entry in the snmpTargetParamsTable. The identified entry contains SNMP parameters to be used when generated messages to be sent to this transport address
Entry Storage	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the Target Address Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Target Address Table (Figure 25).

Note: This Target Address Table section of the Target Address page contains hyperlinks to the Target Parameter page. For more information, see “Configuring an SNMPv3 management target parameter” on page 81.

Deleting an SNMPv3 target address configuration

To delete an SNMPv3 target address configuration:

1. From the main menu, choose Configuration > SNMPv3 > Target Address.

   The Target Address page opens (Figure 25).

2. In the Target Address Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the target address configuration.
   - Click Cancel to return to the table without making changes.

Configuring an SNMPv3 management target parameter

SNMPv3 management target parameters are used during notification generation to specify the communication parameters used for exchanges with notification recipients.

You can view a table of existing SNMPv3 target parameter configurations, create SNMPv3 target parameters that associate notifications with particular recipients, and delete existing SNMPv3 target parameter configurations.

Creating an SNMPv3 target parameter configuration

To create an SNMPv3 target parameter configuration:

1. From the main menu, choose Configuration > SNMPv3 > Target Parameter.

   The Target Parameter page opens (Figure 26).

Figure 26 Target Parameter page

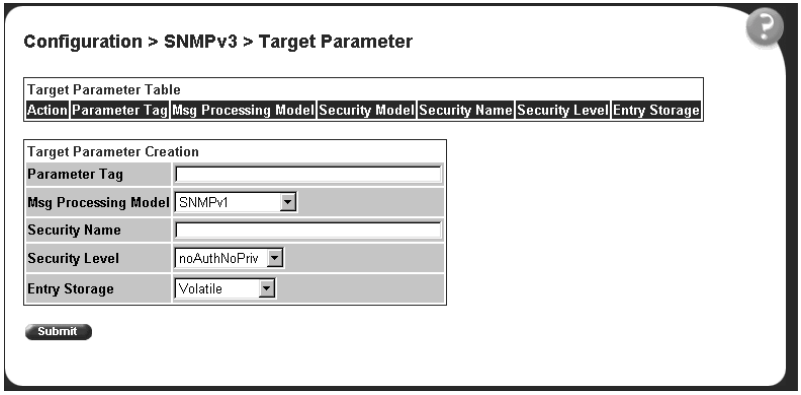


Table 23 describes the items on the Target Parameter page.

Table 23 Target Parameter page items

Item	Range	Description
✕		Deletes the row.
Parameter Tag (snmpTargetParamsRowStatus)	1..32	Type a unique character string to identify the parameter tag.
Msg Processing Model (snmpTargetParamsMPModel)	(0) SNMPv1 (1) SNMPv2c (2) SNMPv2* (3) SNMPv3 /USM	Choose the message processing model to be used when generating SNMP messages using this entry.
Security Name (snmpTargetParamsSecuirtyName)	1..32	Type the principal on whose behalf SNMP messages are generated using this entry
Security Level (snmpTargetParamsSecuirtyLevel)	(1) noAuthNoPriv (2) authNoPriv	Choose the level of security to be used when generating SNMP messages using this entry
Entry Storage (snmpTargetParamsStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the Target Parameter Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Target Parameter Table (Figure 26).

Deleting an SNMPv3 target parameter configuration

To delete an SNMPv3 target parameter configuration:

1. From the main menu, choose Configuration > SNMPv3 > Target Address.

   The Target Address page opens (Figure 25).

2. In the Target Parameter Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the target parameter configuration.
   - Click Cancel to return to the table without making changes.

Configuring SNMP traps

You can configure the IP address and community string for a new SNMP trap receiver, view a table of existing SNMP trap receiver configurations, or delete an existing SNMP trap receiver configuration(s).

Note: The SNMP Trap Receiver Table is an alternative to using the SNMPv3 Target Table and SNMPv3 Parameter Table. However, only SNMPv1 traps are configurable using this table.

Creating an SNMP trap receiver configuration

To create an SNMP trap receiver configuration:

1. From the main menu, choose Configuration > SNMP Trap.

   The SNMP Trap Receiver page opens (Figure 27).

Figure 27 SNMP Trap Receiver page

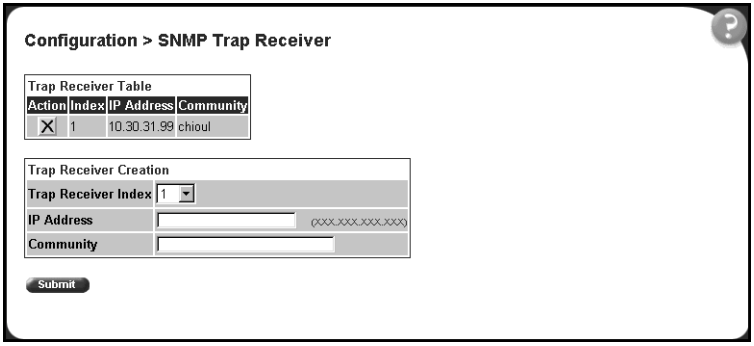


Table 24 describes the items on the Trap Receiver Table and Trap Receiver Creation sections of the SNMP Trap Receiver page.

Table 24 SNMP Trap Receiver page items

Items	Range	Description
✕		Deletes the row.
Trap Receiver Index	1..4	Choose the number of the trap receiver to create or modify.
IP Address	XXX.XXX.XXX.XXX	Type the network address for the SNMP manager that is to receive the specified trap.
Community	0..32	Type the community string for the specified trap receiver.

2 In the Trap Receiver Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Trap Receiver Table (Figure 27).

Deleting an SNMP trap receiver configuration

To delete SNMP trap receiver configurations:

1 From the main menu, choose Configuration > SNMP Trap.

The SNMP Trap Receiver page opens (Figure 27).

2 In the Trap Receiver Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the SNMP trap receiver configuration.
- Click Cancel to return to the table without making changes.

Configuring EAPOL-based security

Beginning with software version 1.1, you can configure security based on the Extensible Authentication Protocol over LAN (EAPOL) protocol. Refer to *Using the Business Policy Switch 2000 Software Version 2.5*, for more information EAPOL-based security.

To configure EAPOL:

1 From the main menu, choose Application > EAPOL Security.

The EAPOL Security Configuration page opens (Figure 28 and Figure 29). Use the scroll bar on the right to move down the page and the scroll bar on the bottom to move across the page.

Figure 28 EAPOL Security Configuration page (1 of 2)

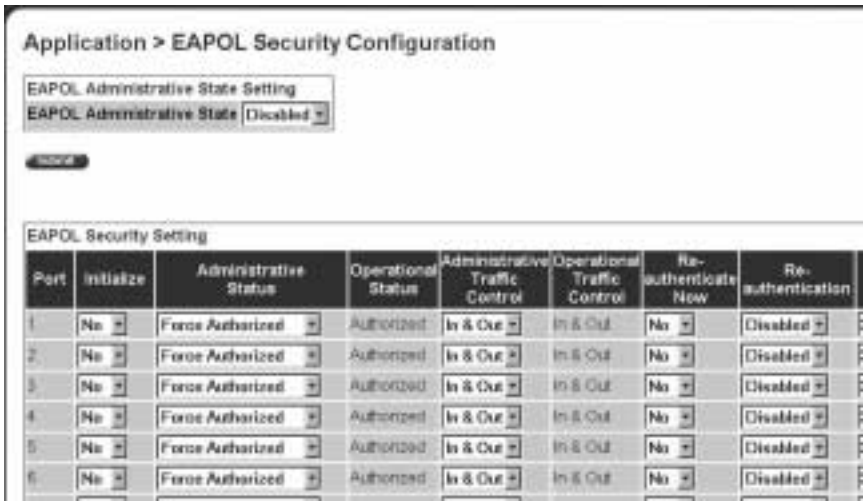


Figure 29 EAPOL Security Configuration page (2 of 2)

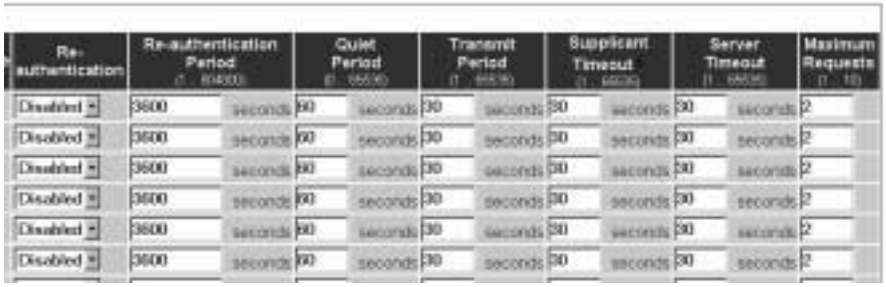


Table 25 describes the fields on the EAPOL Security Configuration page.

Table 25 EAPOL Security Configuration page fields

Section	Item	Range	Description
EAPOL Administrative State Setting	EAPOL Administrative State	(1) Enabled (2) Disabled	Enables or disables EAPOL-based security.
EAPOL Security Setting	Unit		Displays the unit you are viewing.
	Port	1 to 28	Displays the port number.
	Initialize	(1) Yes (2) No	Activates EAPOL state on this port.
	Administrative Status	(1) Force Unauthorized (2) Auto (3) Force Authorized	Allows you to set the EAPOL authorization status: • Force Unauthorized—Always unauthorized • Auto—Status depends on EAP authentication results • Force Authorized—Always authorized
	Operational Status	(1) Authorized (2) Unauthorized	Displays the current authorization status.
	Administrative Traffic Control	(1) In & Out (2) In Only	Allows you to set EAPOL authentication either for incoming and outgoing traffic or for incoming traffic only.
	Operational Traffic Control	(1) In & Out (2) In Only	Displays the current administrative traffic control setting.
	Re-authenticate Now	(1) Yes (2) No	Allows you to activate EAPOL authentication immediately, without waiting for the re-authentication period to expire.
	Re-authentication	(1) Enabled (2) Disabled	Allows you to repeat EAPOL authentication according to the time value specified in Re-authentication Period field.
	Re-authentication Period	1..604800	With Re-authentication enabled, allows you to specify the time period between successive EAPOL authentications.
	Quiet Period	0..65535	Allows you to specify the time interval between an authentication failure and the start of a new authentication attempt.
	Transmit Period	1..65535	Allows you to specify how long the switch waits for the supplicant to respond to EAP Request/Identity packets.
	Supplicant Timeout	1..65535	Allows you to specify how long the switch waits for the supplicant to respond to all EAP packets, except EAP Request/Identity packets.
	Server Timeout	1..65535	Allows you to specify how long the switch waits for the RADIUS server to respond to all EAP packets.
	Maximum Requests	1..10	Allows you to specify the number of times the switch attempts to resend EAP packets to a supplicant.

2. Complete fields as described in the table.
3. Click Submit.

Managing remote access by IP address

Beginning with software version 1.2, you can configure the remote access you allow. You can specify up to 10 IP addresses to allow Web access, SNMP access, or Telnet access to the BPS 2000.

To configure remote access using the Web-based management system:

1. From the main menu of the Business Policy Switch 2000 Web-based Manager, choose Configuration > Remote Access.

   The Remote Access page opens (Figure 30).

Figure 30 Remote Access page

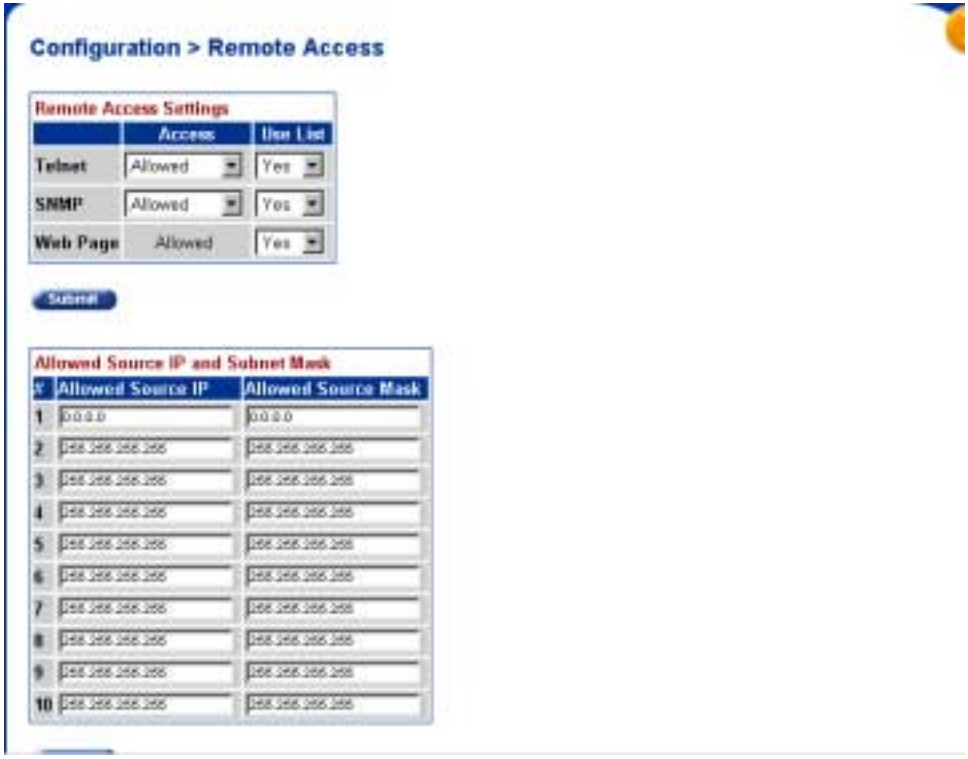


Table 26 describes the fields on the Remote Access page.

Table 26 Remote Access page fields

Section	Item	Range	Description
Remote Access Settings	Telnet/Access	(1)Allowed (2) Disallowed	Allows Telnet access.
	Telnet/Use List	(1) Yes (2) No	Restricts Telnet access to the specified 10 source IP addresses.
	SNMP/Access	(1)Allowed (2) Disallowed	Allows SNMP access.
	SNMP/Use List	(1) Yes (2) No	Restricts SNMP access to the specified 10 source IP addresses.
	Web Page/Access		Displays allowed Web access.

Table 26 Remote Access page fields (continued)

Section	Item	Range	Description
	Web/Use List	(1) Yes (2) No	Restricts Web access to the specified 10 source IP addresses.
Allowed Source IP and Subnet Mask	Allowed Source IP	XXX.XXX.XXX.XXX	Enter the source IP address you want to allow switch access.
	Allowed Source Mask	XXX.XXX.XXX.XXX	Enter the source IP mask you want to allow switch access.

2 Complete fields as described in the table.

3 Click Submit.

Configuring MAC address-based security

Beginning with software version 1.1, the MAC address-based security system allows you to specify a range of system responses to unauthorized network access to your switch with the Web-based management system.

The system response can range from sending a trap to disabling the port. The network access control is based on the MAC source addresses (SAs) of the authorized stations. You can specify a list of up to 448 MAC SAs that are authorized to access the switch. You can also specify the ports that each MAC SA is allowed to access. The options for allowed MAC SA port access include: NONE, ALL, and single or multiple ports that are specified in a list, for example, 1-4, 6, 9, and so forth. You must also include the MAC SA of any router connected to any secure ports.

When the switch software detects an SA security violation, the response can be to send a trap, turn on destination address (DA) filtering for all SAs, disable the specific port, or any combination of these three options.

Beginning with software version 2.0, you can configure the BPS 2000 to drop all packets having a specified MAC destination address (DA). You can create a list of up to 10 MAC DAs you want to filter.The packet with the specified MAC DA will be dropped regardless of the ingress port, source address (SA) intrusion, or VLAN membership.

Note: Ensure that you do not enter the MAC address of the switch or stack you are working on.

This feature is available only with BPS2000 software version 2.0 and higher. Also, this feature is unavailable on the BayStack 450 or 410 switches. In a Hybrid stack, only the BPS 2000 will filter the specified MAC DAs.

Note: After configuring the switch for MAC address-based security, you must enable the ports you want, using the Port Configuration page.

Configuring MAC address-based security

To configure MAC address-based security using the Web-based management system:

1. From the main menu, choose Application > MAC Address Security > Security Configuration.

   The Security Configuration page opens (Figure 31).

Figure 31 Security Configuration page

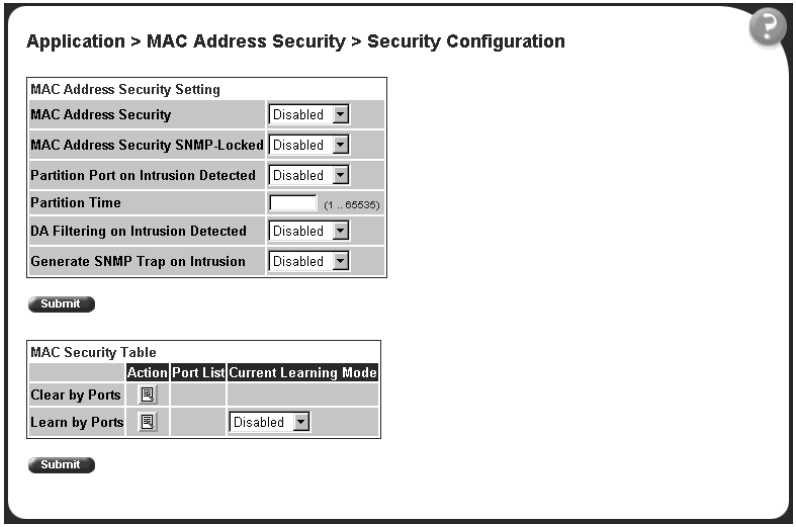


Table 27 describes the items on the Security Configuration page.

Table 27 Security Configuration page items

Section	Item	Range	Description
MAC Address Security Setting	MAC Address Security	(1) Enabled (2) Disabled	Enables the MAC address security features.
	MAC Address Security SNMP-Locked	(1) Enabled (2) Disabled	Enables locking SNMP, so that you cannot use SNMP to modify the MAC address security features.
	Partition Port on Intrusion Detected	(1) Forever (2) Enabled (3) Disabled	Configures how the switch reacts to an intrusion event: • Forever—The port is disabled and remains disabled (partitioned) until reset. The port does not reset after the Partition Time elapses. • Enabled—The port is disabled, then automatically reset to enabled after the time specified in the Partition Time field elapses. • Disabled—The port remains enabled, even if an intrusion event is detected.

Table 27 Security Configuration page items (continued)

Section	Item	Range	Description
	Partition Time	1 to 65535	Sets the time to partition a port on intrusion. Note: Use this field only if the Partition Port on Intrusion Detected field is set to Enabled.
	DA Filtering on Intrusion Detected	(1) Enabled (2) Disabled	Enables you to isolate the intruding node (discard) the packets.
	Generate SNMP Trap on Intrusion	(1) Enabled (2) Disabled	Enables generation of an SNMP when an intrusion is detected.
MAC Security Table/ Clear by Ports	Action		Allows you to clear specific ports from participation in the MAC address security features.
	Port List		Will be blank.
	Current Learning Mode		Will be blank.
MAC Security Table/ Learn by Ports	Action		Allows you to identify ports that will learn incoming MAC addresses. All source MAC addresses of any packets received on a specified port(s) are added to the MAC Security Table (maximum of 448 MAC addresses allowed).
	Port List		Displays all the ports that will learn incoming MAC address to detect intrusions (unallowed MAC addresses).
	Current Learning Mode	(1) Enabled (2) Disabled	Enables learning.

2 On the Security Configuration page, type information in the text boxes, or select from a list.

3 Click Submit.

Configuring ports

In this section, you create a list of ports, and you can add ports to or delete ports from each list.

To activate an entry or add or delete ports to a list:

1 From the main menu, choose Application > MAC Address Security > Port Lists.

The Port Lists page opens (Figure 32).

Figure 32 Port Lists page

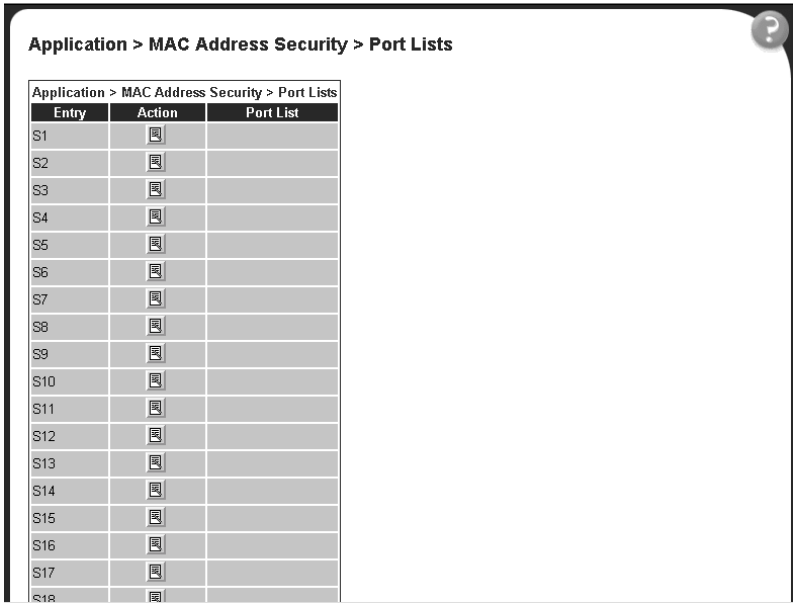


Table 28 describes the items on the Ports Lists page.

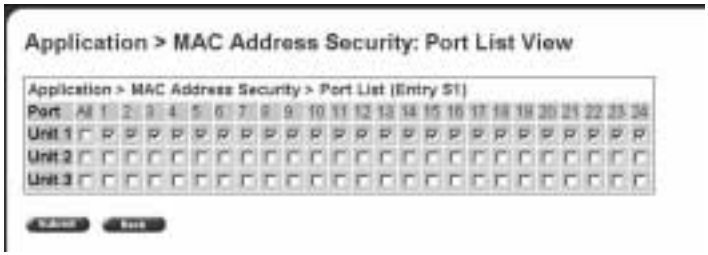
Table 28 Ports Lists page items

Item	Range	Description
Entry		These are the lists of ports.
Action		Allows you to add or delete ports to the lists.
Port List		Displays which ports are associated with each list.

2 To add or delete ports to a list, click the icon in the Action column in the list row you want.

The Port List View, Port List page opens (Figure 33).

Figure 33 Port List View, Port List page



a Click the ports you want to add to the selected list or click None.

b To delete a port from a list, uncheck the box by clicking it.

c Click Submit.

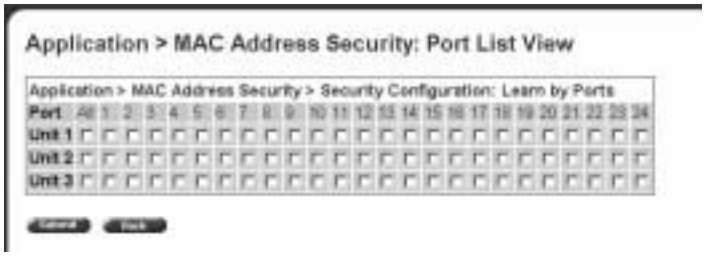
3 From the main menu, choose Application > MAC Address Security > Security Configuration.

The Security Configuration page opens (Figure 31).

4 In the MAC Security Table section, click the icon in the Action column of the Learn By Ports row.

The Port List View, Learn by Ports page opens (Figure 34).

Figure 34 Port List View, Learn by Ports page



a Click the ports through which you want the switch to learn MAC addresses or click None.

b If you want that port to no longer learn MAC addresses, click the checked box to uncheck it.

c Click Submit.

5 In the MAC Security Table section, choose Enabled in the Current Learning Mode column of the Learn By Ports row.

6 Click Submit.

Note: You cannot include any of the port values you have chosen for the secure ports field.

Adding MAC addresses

To add MAC address to the MAC address-based security system:

1 In the main menu, choose Applications > MAC Address Security > Security Table.

It may take awhile for the required addresses to be learned. Then, the Security Table page opens (Figure 35).

Figure 35 Security Table page

Note: Using this page, you instruct the switch to allow the specified MAC address access *only* through the specified port or port list.

Table 29 describes the items on the Security Table page.

Table 29 Security Table page items

Section	Item	Range	Description
MAC Address Security Table	Action		Allows you to delete a MAC address.
	Address		Displays the MAC address.
	Allowed Source	(1) Unit/Port (2) Entry	Displays the entry through which the MAC address is allowed.
MAC Address Security Table Entry Creation	MAC Address		Enter the MAC address you want to allow to access the switch.
	Allowed Source		Select the unit and port through which the MAC address is allowed.
	Entry		Select the port list through which the MAC address is allowed.

2 Complete fields as described in the table.

Note: If you choose an Entry as the Allowed Source, you must have configured that specific entry on the Port View List, Port List page.

3 On the Security Table page, type information in the text boxes, or select from a list.

4 Click Submit.

Note: Be certain to include the MAC address for the default LAN router as an allowed source MAC address.

Clearing ports

You can clear all information from the specified port(s) for the list of ports that learn MAC addresses. If Learn by Ports is enabled, the specified ports will begin again to learn the MAC addresses.

To clear information from selected ports:

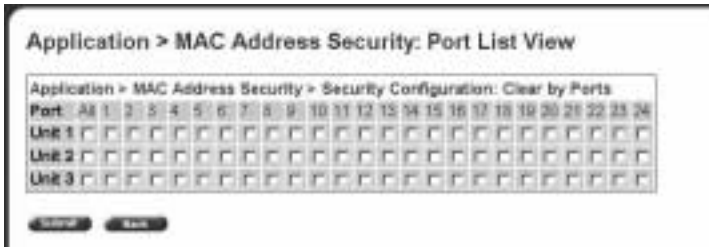
1 From the main menu, choose Application > MAC Address Security > Security Configuration.

   The Security Configuration page opens (Figure 31).

2 In the MAC Security Table section, click the icon in the Action column of the Clear By Ports row.

   The Port List View, Clear by Ports page opens (Figure 36).

Figure 36 Port List View, Clear by Ports page



3 Select the ports you want to clear or click None.

4 Click Submit.

Note: When you specify a port (or ports) to be cleared using this field, the specific port (or ports) will be cleared for each of the entries listed in the MAC Address Security Table. If you totally clear the allowed Source Port(s) field (leaving a blank field) for an entry, the associated MAC address for that entry is also cleared.

Enabling security on ports

To enable or disable MAC address-based security on the port:

1 From the main menu, choose Application > MAC Address Security > Port Configuration.

   The Port Configuration page opens (Figure 37).

Figure 37 Port Configuration page

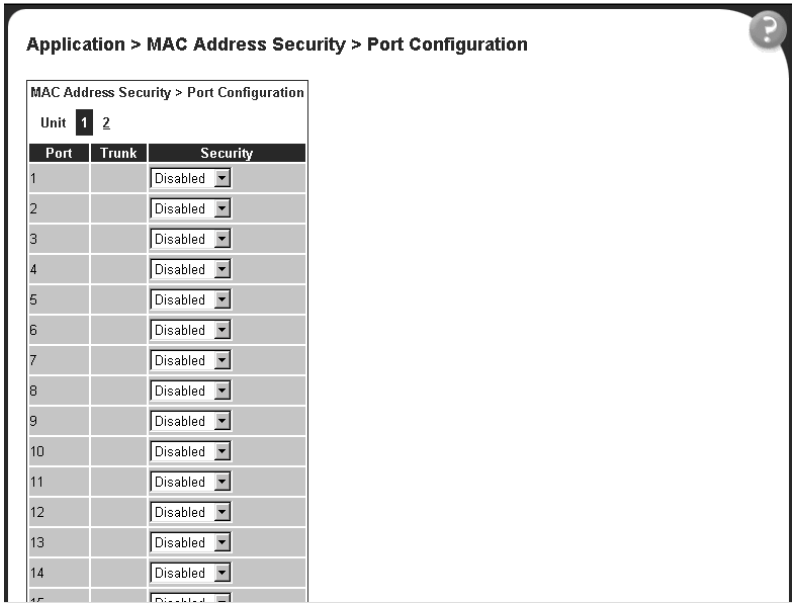


Table 30 describes the items on the Port Configuration page.

Table 30 Port Configuration page items

Item	Range	Description
Unit	1 to 8	Displays the unit number of the ports shown in the table.
Port	1 to 28	Lists each port on the unit.
Trunk	Blank, 1 to 6	Displays the MultiLink Trunk that the port belongs to.
Security	(1) Enabled (2) Disabled	Enables MAC address-based security on that port. Note: You must configure the port for MAC address-based security before enabling the security.

Deleting ports

You can delete ports from the security system in a variety of ways:

- In the Ports List View, Port List page (Figure 33), click on the checkmark of a selected port to delete that port from the specified port list.

- In the Ports List View, Learn by Ports page (Figure 34), click on the checkmark of a selected port to remove that port from those that learn MAC addresses.
- In the Port Configuration page (Figure 37), click Disabled to remove that port from the MAC address-based security system; it will disable all MAC address-based security on that port.

Filtering MAC destination addresses

To drop all packets from a specified MAC destination address (DA):

1 From the main menu, choose Application > MAC Address Security > DA MAC Filtering.

The DA MAC Filtering page opens (Figure 38).

Figure 38 DA MAC Filtering page

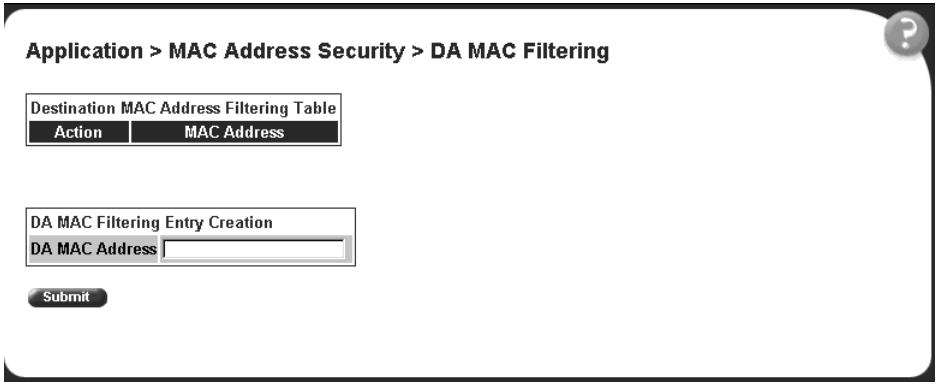


Table 31 describes the items on the DA MAC Filtering page.

Table 31 DA MAC Filtering page items

Section	Item	Range	Description
Destination MAC Address Filtering Table	Action		Allows you to delete a MAC DA you are filtering.

Table 31 DA MAC Filtering page items

Section	Item	Range	Description
	MAC Address	1 -10	Displays list of MAC DAs you want filtered.
DA MAC Filtering Entry Creation	DA MAC Address	XX:XX:XX:XX:XX:XX	Enter the MAC DA you want to filter.

Note: Ensure that you do not enter the MAC address of the management station.

2 In the DA MAC Filtering Entry Creation area, enter the MAC DA you want to filter.

You can list up to 10 MAC DAs to filter.

3 Click Submit.

The system returns you to the DA MAC FIltering page (Table 38) with the new DA listed in the table.

Deleting MAC DAs

To delete a MAC DA:

1 From the main menu, choose Application > MAC Address Security > DA MAC Filtering.

The DA MAC Filtering page opens (Figure 38).

2 In the Destination MAC Address Filtering Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the target parameter configuration.
- Click Cancel to return to the table without making changes.

Viewing learned MAC addresses by VLAN

You can view MAC addresses and their associated port or trunk that the switch or stack configuration has learned, based on the VLAN you select.

To view learned MAC addresses and their associated port or trunk:

1 From the main menu, choose Configuration > MAC Address Table.

The MAC Address Table page opens (Figure 39).

Figure 39 MAC Address Table page

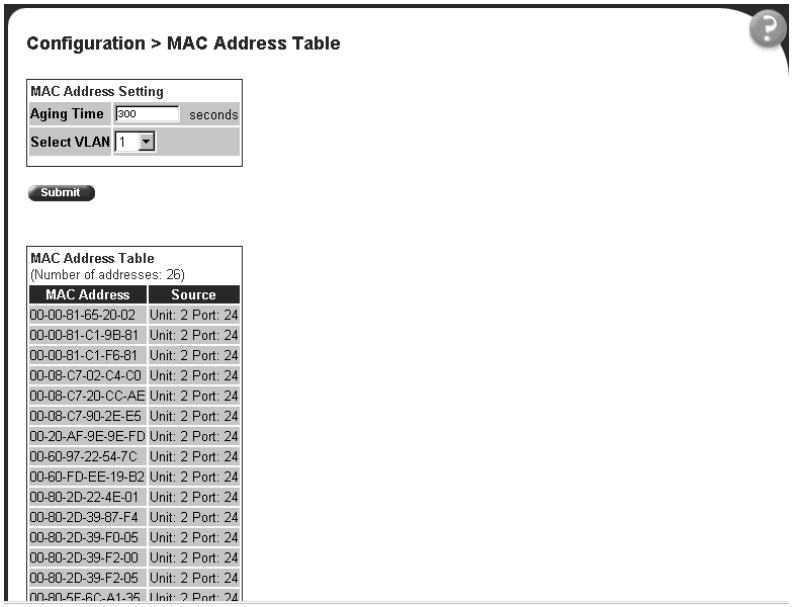


Table 32 describes the items on the MAC Address Table page.

Table 32 MAC Address Table page items

Section	Item	Range	Description
MAC Address Setting	Aging Time	10..1000000	Type the timeout period, in seconds, for aging out dynamically learned forwarding information. If the entry is inactive for a period of time that exceeds the specified aging time, the address is removed. Note: Nortel Networks recommends that you use the default value of 300 seconds.
	Select VLAN	1..256	Choose the VLAN on which to view learned MAC addresses.
MAC Address Table	MAC Address		The unicast MAC address for which the bridge has forwarding and/or filtering information.
	Source		The source of the discovered MAC address.

2 In the MAC Address Setting section, choose the aging time and VLAN you want to view learned MAC addresses on.

3 Click Submit.

Your request is displayed in the MAC Address Table (Figure 39).

Locating a specific MAC address

You can search for a specific MAC address among all the MAC addresses learned from all the VLANs. This is a useful tool for finding whether or not a switch has learned a particular address.

To locate a specific MAC addresses:

1 From the main menu, choose Configuration > Find MAC Address.

The Find MAC Address page opens (Figure 40).

Figure 40 Find MAC Address Table page

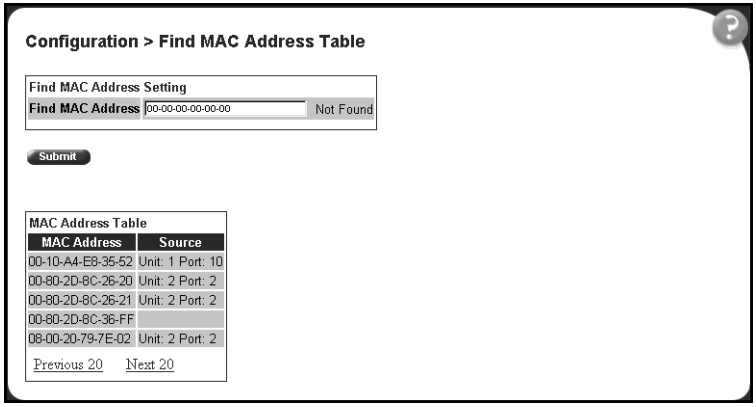


Table 32 on page 103 describes the items on the Find MAC Address Table page.

2 In the MAC Address Setting section, type the MAC address you want to search for.

3 Click Submit to enter the request.

If the address is located, it is shown in the first row in the MAC Address Table section. If the address is not located, the system response “Not Found” is shown to the right of the Find MAC Address input field.

Configuring port's autonegotiation, speed, duplex, status, and alias

You can configure a specific switch port or all switch ports to autonegotiate for the highest available speed of the connected station or you can set the speed for selected switch ports. Autonegotiation is not supported on fiber optic ports.

Note: You cannot *disable* autonegotiation using the BPS2000-1GT or BPS2000-2GT MDA ports; you cannot *enable* autonegotiation using the BPS2000-2GE MDA ports.Use the High Speed Flow control page to work with autonegotiation and gigabit ports.

With software version 2.0, you can name each port, or assign an alias to it, using 27 alphanumeric characters.

To configure a switch port's alias, status, autonegotiation and speed/duplex:

1 From the main menu, choose Configuration > Port Management.

The Port Management page opens (Figure 41).

Figure 41 Port Management page

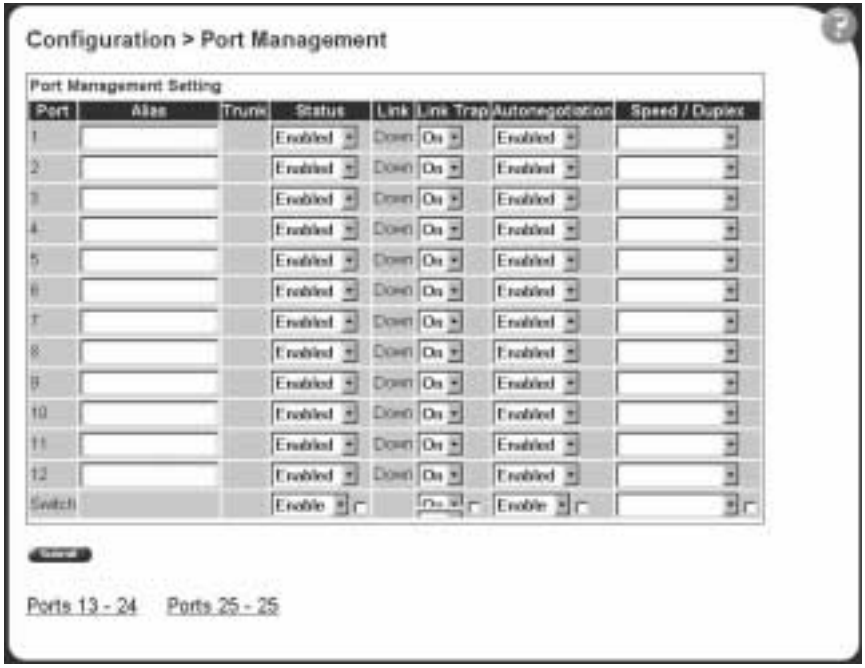


Table 33 describes the items on the Port Management page.

Table 33 Port Management page items

Item	Range	Description
Port		The switch port number of the corresponding row. To select the switch row, click the check box to the right. The values that you set in each switch row affect all switch ports and, when the switch is part of a stack, the values that set in the stack row affect all ports in the entire stack (except the gigabit media dependent adaptor (MDA) ports or fiber optic ports when installed). For information on setting high speed flow control for MDAs, see "Configuring high speed flow control" on page 108.
Alias	27 alphanumeric characters	Displays the name, or alias, you assigned the port. To assign a name or to change the name, enter up to 26 alphanumeric characters.
Trunk		The trunk group that the switch port belongs to as specified in the Trunk Member fields on the MultiLink Trunk page. For more information, see "Configuring MultiLink Trunk (MLT) members" on page 192.
Status	(1) Enabled (2) Disabled	Choose to enable or disable the port. You can also use this field to control access to any switch port. The default setting is Enabled.
Link		The current link state of the corresponding port as follows: • Up: The port is connected and operational • Down: The port is not connected or is not operational.
Link/Trap	(1) On (2) Off	Choose to control whether link up/down traps are sent to the configured trap sink from the switch. The default setting is On.
Autonegotiation	(1) Enabled (2) Disabled	Choose to enable or disable the autonegotiation feature. Choosing to enable autonegotiation sets the corresponding port speed to match the best service provided by the connected station, up to 100Mb/s in full-duplex mode. **NOTE**: This field is disabled for all fiber optic ports. Additionally, you cannot disable this field for the ports on the BPS2000-1GT and BPS2000-2GT MDAs. Use the High Speed Flow Control Configuration screen (next) to set autonegotiation for all gigabit ports. The default setting is Enabled.

Table 33 Port Management page items

Item	Range	Description
Speed / Duplex	(1) 10Mbs / Half (2) 10Mbs / Full (3) 100Mbs / Half (4) 100Mbs / Full (5) 1000Mbs / Full	Choose the Ethernet speed you want the port to support. **NOTE**: 100BASE-FX ports can only be set to 100 Mb/s/Half or 100 Mb/s/Full. Use the High Speed Flow Control Configuration screen (next) to set autonegotiation for all gigabit ports. The default setting is 100Mbs/Half when autonegotiation is disabled and 1000 Mb/s full-duplex for gigabit ports only.
	Note: Disabling ports that are trunk members automatically disables all ports within that trunk.	

2 In the upper-left hand corner, click on the unit number of the policy switch to manage.

The page is updated with the information for the selected switch.

3 In the port row of your choice, select from the lists.

4 Click Submit.

Configuring high speed flow control

You can set switch port parameters for gigabit Ethernet media dependent adapters (MDAs). Use this screen to set autonegotiation for all gigabit ports.

To configure high speed flow control:

1 From the main menu, choose Configuration > High Speed Flow Control.

The High Speed Flow Control page opens (Figure 42).

Figure 42 High Speed Flow Control page

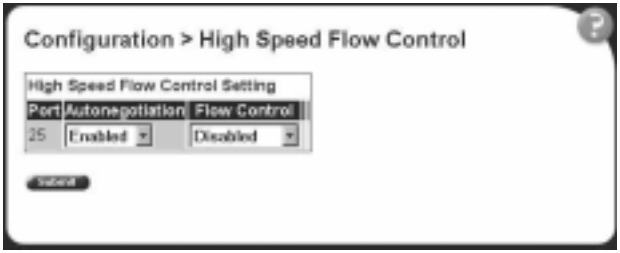


Table 34 describes the items on the High Speed Flow Control page.

Note: The display will change depending on the MDA installed. Table 34 describes all of the possible page items.

Table 34 High Speed Flow Control page items

Item	Range	Description
Autonegotiation	(1) Enabled (2) Disabled	Choose to enable or disable the autonegotiation feature. **NOTE**: Autonegotiation can be enabled on every supported gigabit fiber optic MDA except the BPS 2000-2GE MDA. You cannot disable this field for the ports on the BPS2000-1GT and BPS2000-2GT MDAs. When enabled, the port advertises support for flow control autonegotiation.
Flow Control	(1) Enabled (2) Symmetric (3) Asymmetric	Choose your flow control preference to control traffic and avoid congestion on the gigabit MDA port. Note: Ensure that the settings are the same for both sides of the link.
Preferred Phy	(1) Left (2) Right	Choose the preferred physical port. The port not selected automatically reverts to a backup physical port. **NOTE**: This field may not appear, depending on the MDA you are using.
Active Phy		The current operating physical port. The physical port options are left or right. **NOTE**: This field may not appear, depending on the MDA you are using.

2 In the upper-left hand corner, click on the unit number of the gigabit MDA to configure.

3 Select from the lists.

4 Click Submit.

Downloading switch images

You can download the BPS 2000 software image that is located in non-volatile flash memory. To download the BPS 2000 software image, a properly configured Trivial File Transfer Protocol (TFTP) server must be present in your network, and the policy switch must have an IP address. To learn how to configure the switch or stack IP address, refer to "Configuring BootP, IP, and gateway settings" on page 58.

Caution: Do not interrupt power to the device during the software download process. A power interruption can corrupt the firmware image.

In addition to downloading switch images, this section covers the following topics:

- "Observing LED indications," next
- "Upgrading software" on page 113

To download a switch image:

1 From the main menu, choose Configuration > Software Download.

The Software Download page opens (Figure 43 and Figure 44).

Figure 43 Software Download page for a Pure BPS 2000 stack

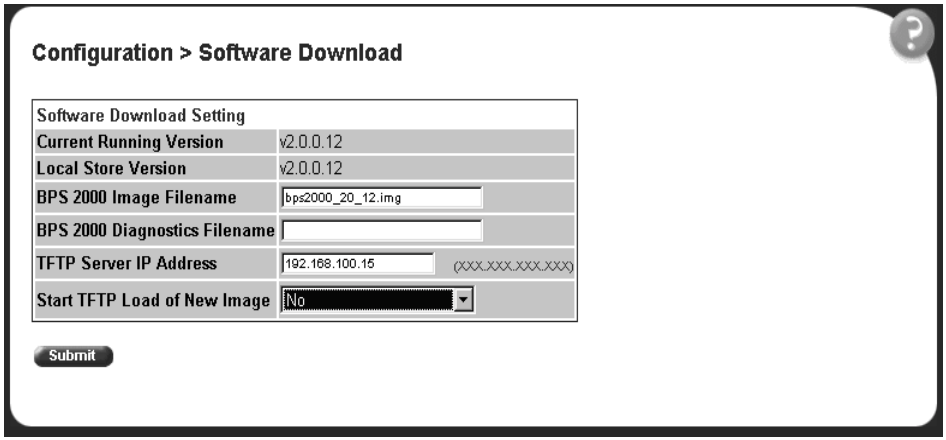


Figure 44 Software Download page for a Hybrid stack

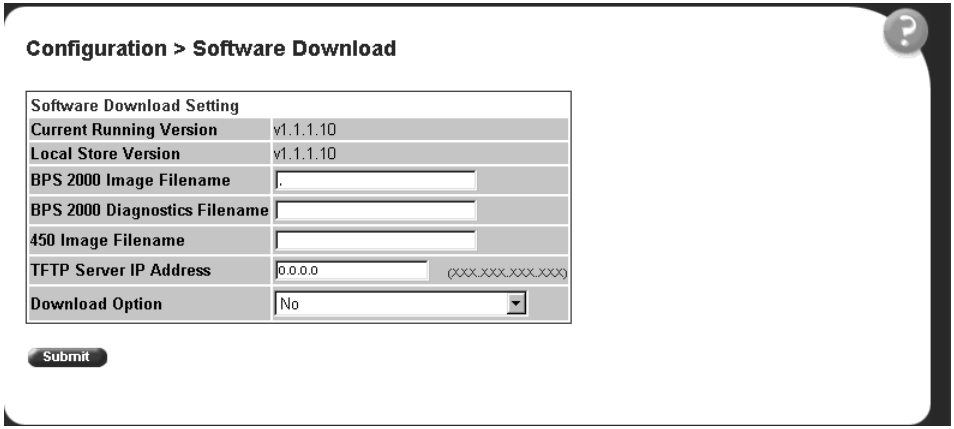


Table 35 describes the items on the Software Download page.

Table 35 Software Download page items

Item	Range	Description
Current Running Version		The version of the current running software.
Local Store Version		The local version of the software in the flash memory.
BPS 2000 Image Filename	1..30	Type the software image load filename.
BPS 2000 Diagnostics Filename	1..30	Type the diagnostics filename.
450 Image Filename	1..30	Type the 450 image filename.
TFTP Server IP Address	XXX.XXX.XXX.XXX	Type the IP address of your TFTP load host.
Start TFTP Load of New Image (in Pure BPS2000 mode) Download Option (in Hybrid mode)	(1) No (2) BPS 2000 Image (3) BPS 200 Diagnostics (4) 450/410 Image (5) BPS 2000 and 450/410 Images (6) BPS 2000 Image If Newer	Choose the software image to load.

2 Type information in the text boxes, or select from a list. (Refer to "Upgrading software" on page 113 for instructions.)

3 Click Submit.

The software download process automatically completes without user intervention. The process erases the contents of flash memory and replaces it with a new software image. Take care not to interrupt the download process until after it runs to completion (the process can take up to 10 minutes, depending on network conditions).

When the download process is complete, the switch automatically resets and the new software image initiates a self-test.

During the download process, the Business Policy Switch is not operational. You can monitor the progress of the download process by observing the LED indications.

Observing LED indications

Table 36 describes the LED indications during the software download process.

Note: The LED indications described in Table 36 apply to a 24-port switch model. Although a 12-port switch provides *similar* LED indications, the LED indication sequence is associated within the 12-port range.

Table 36 LED Indications during the software download process

Phase	Description	LED Indications
1	The switch downloads the new software image.	**100 Mb/s port status LEDs (ports 18 to 24 only):** The LEDs begin to turn on in succession beginning with port 24, which indicates the progress of the download process. When LEDs 18 to 24 are all on, the switch has received the new software image successfully.
2	The switch erases the flash memory.	**100 Mb/s port status LEDs (ports 1 to 12 only):** The LEDs begin to turn on in succession beginning with port 1, which indicates that various sectors of the switch's flash memory are being erased. When LEDs 1 to 12 are all on, the switch's flash memory has been erased.

Table 36 LED Indications during the software download process (continued)

Phase	Description	LED Indications
3	The switch programs the new software image into the flash memory.	**100 Mb/s port status LEDs (ports 1 to 8 only):** The LEDs begin to turn on in succession beginning with port 1, which indicates that the new software image is being programmed into the switch's flash memory. When LEDs 1 to 8 are all on, the new software image has been programmed successfully into the switch's flash memory.
4	The switch resets automatically.	After the reset completes, the new software image initiates the switch self-test, which comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

Note: You may see an incorrect LED display when downloading the image on a mixed, or Hybrid, stack. All the BU (Base Unit) LEDs may turn on or blink on all BPS 2000 units, as if the stack has failed. However, the stack is operational and the upgrade should complete without problems.

Upgrading software

You follow a different procedure depending if you are using a Pure BPS 2000 stack or a Hybrid stack.

The stacking software compatibility requirements are as follows:

- Pure BPS 2000 stack—All units must be running the same software version.
- Pure BayStack 450 stack—All units must be running the same software version.
- Hybrid stack:
  - All BPS 2000 units must be running the same software version.
  - All BayStack 410 units must be running the same software version.
  - All BayStack 450 units must be running the same software version.
  - All software versions must have the identical ISVN.

This section discusses the following topics:

- "Upgrading software in a Pure BPS 2000 stack or a standalone BPS 2000," next
- "Upgrading software in a Hybrid stack" on page 115

Upgrading software in a Pure BPS 2000 stack or a standalone BPS 2000

To download, or upgrade, software in a Pure BPS 2000 stack or a standalone BPS 2000 unit:

1. From the main menu, choose Configuration > Software Download.

   The Software Download page opens (Figure 43).

2. In the BPS 2000 Image Filename field, enter the image file name.
3. In the TFTP Server IP Address, enter the IP address of your TFTP load host.
4. Choose BPS 2000 Image in the Start TFTP Load of New Image field.
5. Click Submit.

   The system resets, which may take a few minutes. The system opens to the System Information page (Figure 4).

6. From the main menu, choose Configuration > Software Download.
7. In the BPS 2000 Diagnostics Filename field, enter the name of the BPS 2000 diags file.
8. In the TFTP Server IP Address, enter the IP address of your TFTP load host.
9. In the Start TFTP Load of New Image field, choose BPS 2000 Diagnostics.
10. Click Submit.

    The system resets, which may take a few minutes. The system opens to the System Information page (Figure 4).

However, if you are currently using software version 1.0, 1.0.1, or 1.1, you must upgrade to software version 1.1.1 before upgrading to version 2.5.

Upgrading software in a Hybrid stack

The physical order of the units and the unit numbering in the Hybrid stack does not affect the upgrading process at all. In addition, the cabling order regarding upstream/downstream neighbors does not affect the process.

Before you attempt to download new software (or upgrade software) to a Hybrid (mixed) stack, you *must* ensure that the Interoperability Software Version Numbers (ISVN) are identical. That is, the ISVN number for the BayStack 450 switch and BayStack 410 switch must have the same ISVN as the BPS 2000. If the ISVNs are not the same, the stack does not operate. The ISVNs and the accompanying software release are:

- ISVN 1
  - BayStack 410 or Bay Stack 450—version 3.1
  - BPS 2000—versions 1.0 and 1.0.1
- ISVN 2
  - BayStack 410 or BayStack 450—versions 4.0 and 4.1
  - BPS 2000—versions 1.1, 1.1.1, 1.2, 2.0, and 2.5

This section describe the steps for the following software upgrades:

- "Upgrading software when ISVN is 2," next
- "Upgrading software when ISVN is 1" on page 116

Upgrading software when ISVN is 2

If you are currently using BPS 2000 software version 1.0, 1.0.1, or 1.1, you must upgrade to software version 1.1.1 before upgrading to BPS 2000 version 2.5.

To upgrade a Hybrid stack to BPS 2000 software version 2.5 when the ISVN numbers of the units are 2:

1 Choose Configuration > Software Download from the main menu.

The Software Download screen appears (Figure 44).

2 In the BPS 2000 Image Filename field, enter the name of the BPS 2000 image file.

3. In the TFTP Server IP Address, enter the IP address of your TFTP load host.
4. In the Start TFTP Load of New Image field, choose BPS 2000 Image in the Start TFTP Load of New Image field.
5. Click Submit.

   The system resets, which may take a few minutes. The system opens to the System Information page (Figure 4).

6. From the main menu, choose Configuration > Software Download.
7. In the BPS 2000 Diagnostics Filename field, enter the name of the BPS 2000 diags file.
8. In the TFTP Server IP Address, enter the IP address of your TFTP load host.
9. In the Start TFTP Load of New Image field, choose BPS 2000 Diagnostics.
10. Click Submit.

    The system resets, which may take a few minutes. The system opens to the System Information page (Figure 4).

11. From the main menu, choose Configuration > Software Download.

Refer to the documentation for the BayStack 450 and BayStack 410 switches to upgrade the software on those switches.

Upgrading software when ISVN is 1

To upgrade a Hybrid stack to BPS 2000 software version 2.5 when the ISVN numbers of the units are 1:

1. Choose Configuration > Software Download from the main menu.

   The Software Download screen appears (Figure 44).

2. In the BPS 2000 Image Filename field, enter the name of the BPS 2000 image file.
3. In the 450 Image Filename field, enter the name of the BayStack 450/410 image file.
4. In the TFTP Server IP Address, enter the IP address of your TFTP load host.

5 In the Start TFTP Load of New Image field, choose Both BPS 2000 and 450 Image.

Note: If you do not download both the BPS 2000 and BayStack 410/450 images simultaneously, the stack may not form.

6 Click Submit.

The system resets, which may take a few minutes. The system opens to the System Information page (Figure 4).

7 From the main menu, choose Configuration > Software Download.

8 In the 450 Image Filename field, enter the name of the other 450 image file.

9 In the TFTP Server IP Address, enter the IP address of your TFTP load host.

10 In the Start TFTP Load of New Image field, choose 450 Image.

11 Click Submit.

The system resets, which may take a few minutes. The system opens to the System Information page (Figure 4).

12 From the main menu, choose Configuration > Software Download.

13 In the BPS 2000 Diagnostics Filename field, enter the name of the BPS 2000 diags file.

14 In the TFTP Server IP Address, enter the IP address of your TFTP load host.

15 In the Start TFTP Load of New Image field, choose BPS 2000 Diagnostics.

16 Click Submit.

The system resets, which may take a few minutes. The system opens to the System Information page (Figure 4).

17 From the main menu, choose Configuration > System.

The System page opens (Figure 17).

18 Validate that the ISVN on both the BPS 2000 and the BayStack are 2.

Refer to *Using the Business Policy Switch 2000 Software Version 2.5* for further information on downloading software and upgrading software in standalone BPS 2000 units, in pure BPS 2000 stacks, and in mixed (Hybrid) stacks.

Storing and retrieving a switch configuration file from a TFTP server

You can store switch and stack configuration parameters on a Trivial File Transfer Protocol (TFTP) server. You can retrieve the configuration parameters of a standalone switch or an entire stack and use the retrieved parameters to automatically configure a replacement switch or stack.

To store a switch or stack configuration, you must set up the file on your TFTP server and set the filename read/write permission to enabled.

To download the BPS 2000 configuration file, a properly configured TFTP server must be present in your network, and the policy switch must have an IP address. To learn how to configure the switch or stack IP address, refer to "Configuring BootP, IP, and gateway settings" on page 58.

To store or retrieve a switch or stack configuration file:

1 From the main menu, choose Configuration > Configuration File.

The Configuration File Download/Upload page opens (Figure 45).

Figure 45 Configuration File Download/Upload page

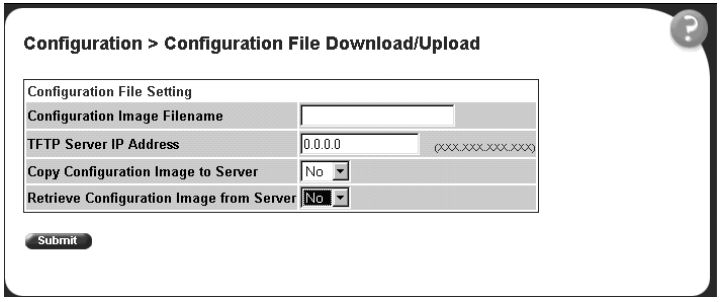


Table 37 describes the items on the Configuration File page.

Table 37 Configuration File page items

Item	Range	Description
Configuration Image Filename	1..32	Type the configuration file name.
TFTP Server IP Address	XXX.XXX.XXX.XXX	Type the IP address of the TFTP load host.
Copy Configuration Image to Server	(1) Yes (2) No	Choose whether or not to copy the configuration image to the server.
Retrieve Configuration Image from Server	(1) Yes (2) No	Choose whether or not to retrieve the configuration image from a server. If you choose Yes, the download process begins immediately and, when completed, causes the switch or stack to reset with the new configuration parameters.

2 Type information in the text boxes, or select from a list.

3 Click Submit.

Table 38 describes the requirements for storing or retrieving configuration parameters on a TFTP server.

Table 38 Requirements for storing or retrieving configuration parameters on a TFTP server

Requirements
• The Configuration File feature can only be used to copy *standalone switch configuration parameters to other standalone switches* or to copy *stack configuration parameters to other stack configurations*. For example, you cannot duplicate the configuration parameters of a unit in a *stack* configuration and use it to configure a *standalone* switch.
• A configuration file obtained from a standalone switch can only be used to configure other standalone switches that have the same firmware revision and model type as the donor standalone switch.
• A configuration file obtained from a stack unit can only be used to configure other stacks that have the same number of switches, firmware version, model types, and physical IDs as the stack the donor stack unit resides in.
• Reconfigured stacks are configured according to the unit order number of the donor unit. For example, the configuration file parameters from a donor unit with physical ID *x* are used to reconfigure the unit with physical ID *x*.
• The configuration file also duplicates any settings that exist for any MDA that is installed in the donor switch. If you use the configuration file to configure another switch that has the same MDA model installed, the configuration file settings will also apply to and override the existing MDA settings.

Table 39 describes the parameters that are not saved to the configuration file.

Table 39 Parameters not saved to the configuration file

These parameters are not saved:	**Used in this screen:**	**See page:**
In-Band Stack IP Address	IP Configuration/Setup	58
In-Band Switch IP Address		
In-Band Subnet Mask		
Default Gateway		
Configuration Image Filename	Configuration File Download/Upload	118
TFTP Server IP Address		
Console Read-Only Switch Password	Console/Comm Port Configuration	121
Console Read-Write Switch Password		
Console Read-Only Stack Password		
Console Read-Write Stack Password		

Configuring port communication speed

You can view the current console/communication port settings and configure the console port baud rate to match the baud rate of the console terminal.

To view current console/communication port settings and configure console port speed:

1 From the main menu, choose Configuration > Console/Comm Port.

The Console/Communication Port page opens (Figure 46).

Figure 46 Console/Communication Port page

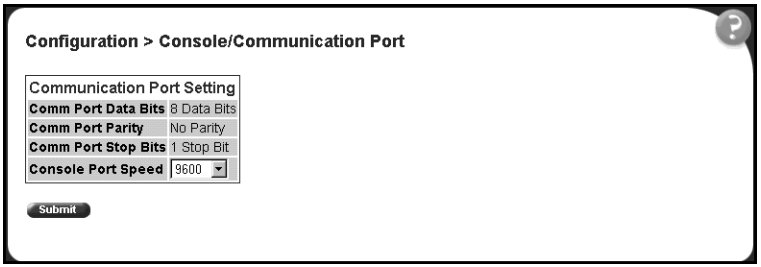


Table 40 describes the items on the Console/Communication Port page.

Table 40 Console/Communication Port Setting page items

Item	Range	Description
Comm Port Data Bits		The current console communication port data bit setting.
Comm Port Parity		The current console communication port parity setting.
Comm Port Stop Bits		The current console communication port stop bit setting.
Console Port Speed	2400 4800 9600 19200 38400	Choose the console port speed baud rate. Note: The default setting is 9600.
		Caution: If you choose a baud rate that does not match your console terminal baud rate, you will lose communication with the configuration interface when you click Submit.

2 Select from the list.

3 Click Submit.

Setting system operational modes

You can set the next stack mode operation of either a stack of BPS 2000 only, or a mixed stack of BPS 2000 and BayStack 450 and 410 switches.

To set the next stack mode operation:

1 From the main menu, choose Configuration > Stack Operational Mode.

The Stack Operational Mode Setting page opens (Figure 47).

Figure 47 Stack Operational Mode page

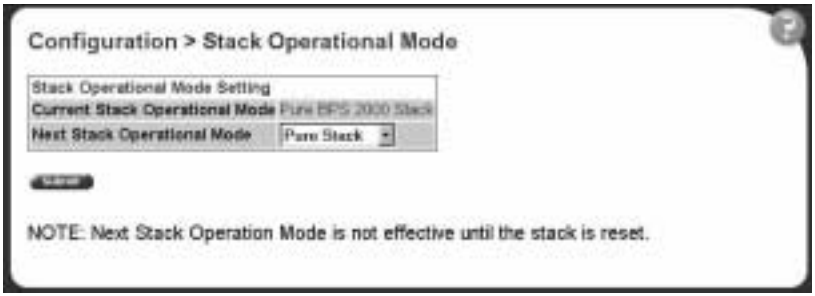


Table 41 describes the items on the Stack Operational Mode Setting page.

Table 41 Stack Operational Mode page items

Item	Range	Description
Current Stack Operational Mode		Current stack operational mode. The options are Pure BPS 2000 Stack or Hybrid Stack.
Next Stack operational Mode	(1) Pure Stack (2) Hybrid Stack	Choose whether your stack is BPS 2000 only, or a mixed stack of BayStack 450 and BPS 2000 (Hybrid Stack).

2 Select from the list.

3 Click Submit.

Chapter 5
Configuring remote network monitoring (RMON)

The RMON management information base (MIB) is an interface between the RMON agent on a BayStack 450 switch or Business Policy Switch 2000 and RMON management applications such as the Web-based management user interface. It defines objects that are suitable for the management of any type of network. Some groups are specifically targeted for Ethernet networks.

The RMON agent continuously collects statistics and proactively monitors the switch.

This RMON options available to you are:

Note: To access the software version 2.5 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Configuring RMON fault threshold parameters

Alarms are useful when you need to know when the value of some variable goes out of range. RMON alarms can be defined on any MIB variable that resolves to an integer value. String variables (such as system description) cannot be used as alarm variables.

Creating an RMON fault threshold

You can create the RMON threshold parameters for fault notification (alarms).

To create an RMON threshold:

1 From the main menu, choose Fault > RMON Threshold.

The RMON Threshold page opens (Figure 48).

Figure 48 RMON Threshold page

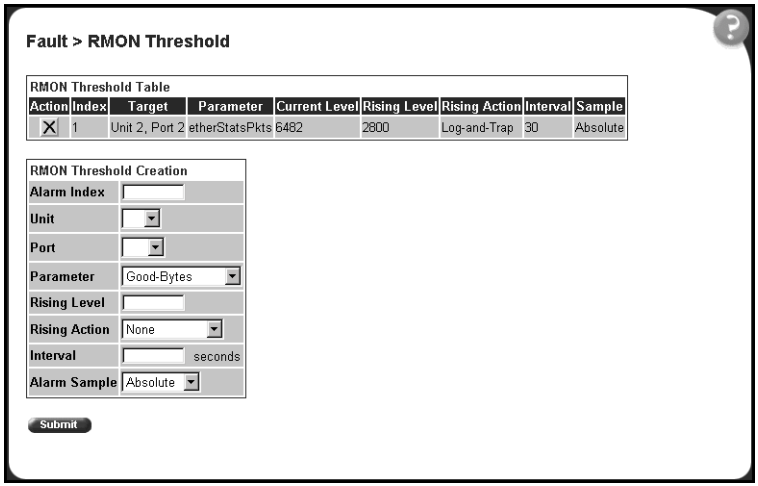


Table 42 describes the items on the RMON Threshold page.

Table 42 RMON Threshold page items

Item	Range	Description
		Deletes the row.
Index/Alarm Index	1..10	Type the unique number to identify the alarm entry.
Target	Integer	The unit number and port number.
Unit	1..8	Choose the switch on which to configure port alarms.
Port	1..28	Choose the port on which to set an alarm.
Parameter	(1) Good-Bytes (2) Good-Packets (3) Multicast (4) Broadcast (5) CRC-Errors (6) Runts (7) Fragments (8) Frame-Too-Long (9) Collisions	Choose the sampled statistic.
Current Level	Integer	The value of the statistic during the last sampling period. Note: If the sample type is Delta, the value is the difference between the samples at the *beginning and end* of the period. If the sample type is Absolute, the value is the sampled value at the *end* of the period.
Rising Level	Integer	Type the event entry to be used when a rising threshold is crossed. Note: When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated. After a rising event is generated, another such event is not generated until the sampled value falls below this threshold and reaches the Falling Threshold.
Rising Action	(1) None (2) Log (3) SNMP-Trap (4) Log-and-Trap	Choose the type of notification for the event. Selecting Log generates an entry in the RMON Event Log table for each event. Selecting SNMP Trap sends an SNMP trap to one or more management stations.

Table 42 RMON Threshold page items (continued)

Item	Range	Description
Interval		Type the time period (in seconds) to sample data and compare the data to the rising and falling thresholds.
Sample/Alarm Sample	(1) Absolute (2) Delta	Choose the sampling method: Absolute: *Absolute* alarms are defined on the current value of the alarm variable. An example of an alarm defined with absolute value is card operating status. Because this value is not cumulative, but instead represents states, such as card up (value 1) and card down (value 2), you set it for absolute value. Therefore, an alarm could be created with a rising value of 2 and a falling value of 1 to alert a user to whether the card is up or down. Delta: Most alarm variables related to Ethernet traffic are set to *delta* value. Delta alarms are defined based on the difference in the value of the alarm variable between the start of the polling period and the end of the polling period. Delta alarms are sampled twice per polling period. For each sample, the last two values are added together and compared to the threshold values. This process increases precision and allows for the detection of threshold crossings that span the sampling boundary. Therefore, if you keep track of the current values of a given delta-valued alarm and add them together, the result is twice the actual value. (This result is not an error in the software.)

2 In the RMON Threshold Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new configuration is displayed in the RMON Threshold Table (Figure 48).

Note: RMON threshold configurations are not modifiable. They must be deleted and the information recreated.

Deleting an RMON threshold configuration

To delete an existing RMON threshold configuration:

1 From the main menu, choose Fault > RMON Threshold.

The RMON Threshold page opens (Figure 48).

2 In the RMON Threshold Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the RMON threshold configuration.
- Click Cancel to return to the RMON Threshold page without making changes.

Viewing the RMON fault event log

RMON events and alarms work together to notify you when values in your network go out of a specified range. When values pass the specified ranges, the alarm is triggered and “fires.” The event specifies how the activity is recorded.

An event specifies whether a trap, a log, or a trap and a log are generated to view alarm activity. When RMON is globally enabled, two default events are generated:

- Rising Event
- Falling Event

Default events specify that when an alarm goes out of range, the firing of the alarm is tracked in both a trap and a log. For example, when an alarm fires at the rising threshold, the rising event specifies that this information be sent to both a trap and a log. The RMON Event Log page works in conjunction with the RMON Threshold page to enable you to view a history of RMON fault events.

To view a history of RMON fault events:

➨ From the main menu, choose Fault > RMON Event Log.

The RMON Event Log page opens (Figure 49).

Figure 49 RMON Event Log page

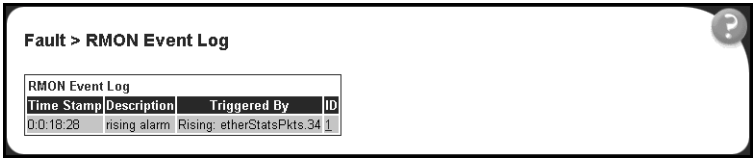


Table 43 describes the fields on the RMON Event Log page.

Table 43 RMON Event Log page fields

Item	Description
Time Stamp	The time the event occurred.
Description	An implementation dependent description of the event that activated this log entry.
Triggered By	A comment describing the source of the event.
ID	The event that generated this log entry.

Viewing the system log

You can view a display of messages contained in non-volatile random access memory (NVRAM) or dynamic random access memory (DRAM) and NVRAM.

To open the System Log page:

1 From the main menu, choose Fault > System Log.

The System Log page opens (Figure 50).

Figure 50 System Log page

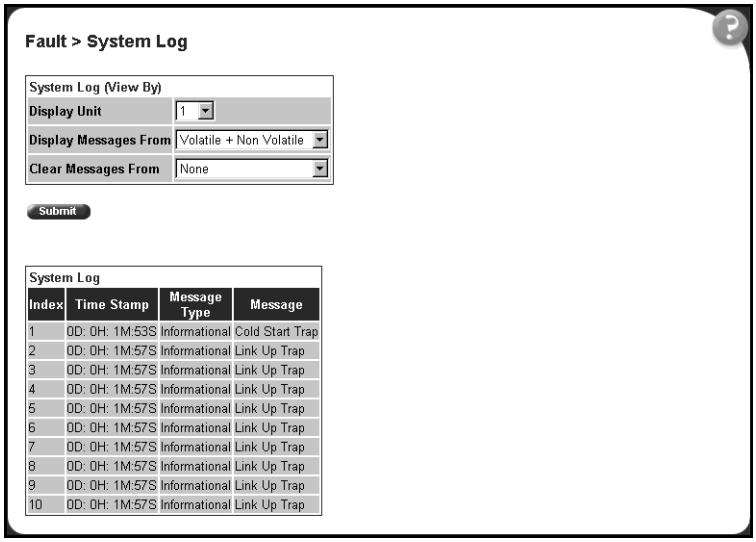


Table 44 describes the fields on the System Log page.

Table 44 System Log page fields

Section	Item	Range	Description
System Log (View By)	Display Unit	1..8	Choose the unit on which to display messages or clear messages.
	Display Messages From	(1) Non Volatile (2) Volatile + Non Volatile	Choose to display messages from Non Volatile memory (NVRAM) or Volatile (DRAM) and Non Volatile memory. The default settings is Non Volatile.
	Clear Messages From	(1) Volatile (2) Volatile + Non Volatile (3) None	Choose to clear messages from Volatile memory or Volatile and Non Volatile memory. The default settings is None (do not clear messages)
System Log	Index		The number of the event.
	Time Stamp		The time, in hundreths of a second, between system initialization and the time the log messages entered the system.
	Message Type		The type of message. The options are (1) Critical, (2) Serious, and (3) Informational.
	Message		A character string that identifies the origin of the message and the reason why the message was generated.

2 In the System Log (View By) section do one or more of the following:

- Choose the number of the unit from which to display messages.
- Choose where to display messages from.
- Choose to clear messages from Volatile or Non Volatile memory.

3 Click Submit.

The results of your request are displayed in the System Log section (Figure 50).

Viewing RMON Ethernet statistics

You can gather and graph RMON Ethernet statistics in a variety of formats.

To gather and graph RMON Ethernet statistics:

1 From the main menu, choose Statistics > RMON Ethernet.

The RMON Ethernet page opens (Figure 51).

Figure 51 RMON Ethernet page

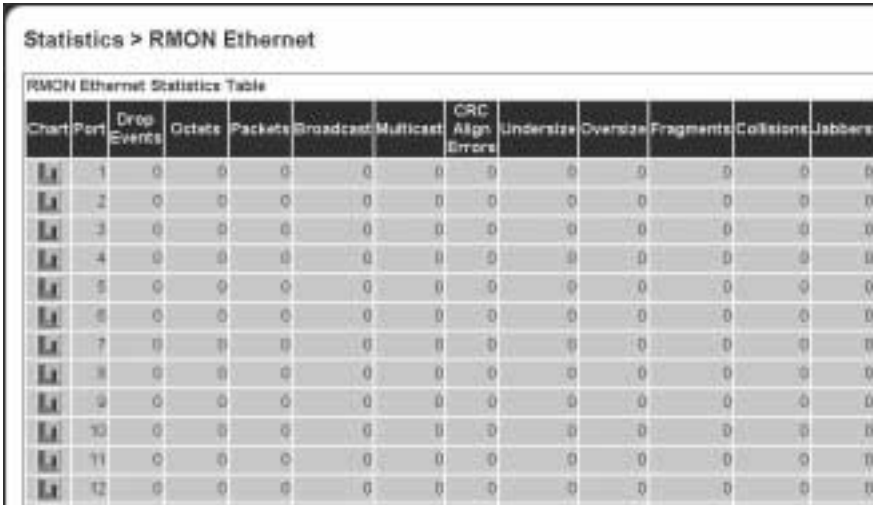


Table 45 describes the items on the RMON Ethernet page.

Table 45 RMON Ethernet page items

Item	Description
	Displays statistics as a bar graph.
Port	The port number that corresponds to the selected switch.
Drop Events	The number of events in which packets were dropped by the interface due to a lack of resources.
Octets	The number of octets of data (including those in bad packets) received on the network (excluding framing bits, but including Frame Check Sequence (FCS) octets).
Packets	The number of good packets received that were directed to the broadcast address. This *does not* include multicast packets.

Table 45 RMON Ethernet page items (continued)

Item	Description
Broadcast	The number of good packets received that were directed to the broadcast address. This *does not* include multicast packets.
Multicast	The number of good packets received that were directed to the multicast address. This *does not* include packets sent to the broadcast address.
CRC Align Errors	The number of packets received that had a length (excluding and 1518 octets, inclusive, but had either a bad Frame FCS with an integral number of octets (FCS errors) with a non-integral number of octets (alignment error).
Undersize	The number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.
Oversize	The number of packets received that were longer than 1518 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.
Fragments	The number of packets received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Collisions	The “best estimate” number of collisions on this Ethernet segment.
Jabbers	The number of packets received that were longer than 1518 octets in length (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Packets < = 64 bytes 65-127 bytes 128-255 bytes 256-511 bytes 512-1023 bytes 1024-1518 bytes	The number of octets received (including bad packets) in length (excluding framing bits, but including FCS octets).

2 In the upper-left hand corner, click on the unit number of the device to monitor.

3 Click Submit.

The RMON Ethernet Statistics Table is updated with information about the selected device (Figure 51).

Viewing RMON Ethernet statistics in a bar graph format

To view RMON Ethernet statistics in a bar graph format:

1 From the main menu, choose Statistics > RMON Ethernet.

The RMON Ethernet page opens (Figure 51).

2 In the port row of your choice, click the bar graph icon.

The RMON Ethernet: Chart page appears in a bar graph format (Figure 52).

Figure 52 RMON Ethernet: Chart in a bar graph format

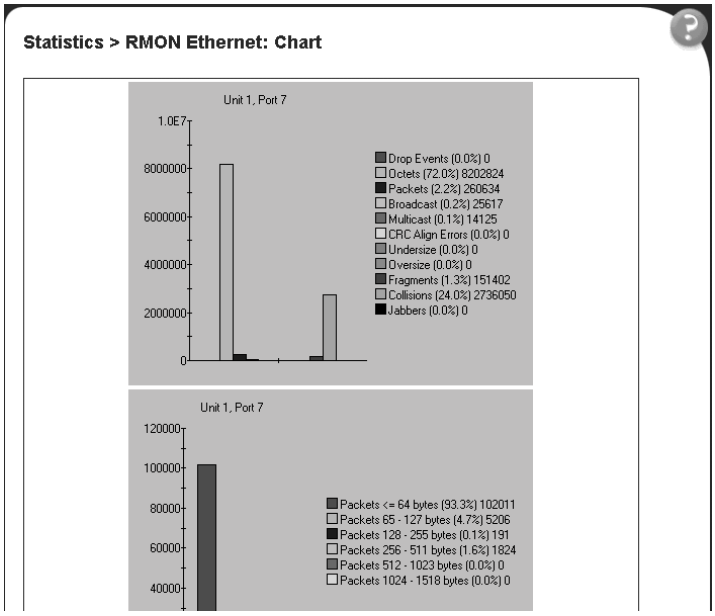


Table 45 describes the items on the RMON Ethernet: Chart page.

3 To refresh statistical information, go to the bottom of the page and click Update, or click Back to return to the Ethernet Statistics page.

Viewing RMON history

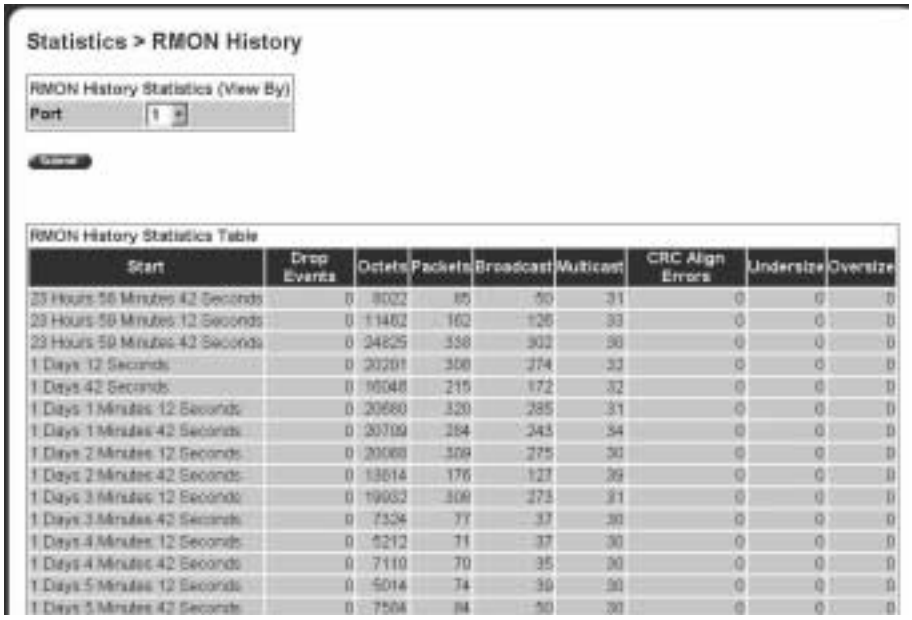
You can view a periodic statistical sampling of data from various types of networks.

To view periodic statistical data:

1 From the main menu, choose Statistics > RMON History.

The RMON History page opens (Figure 53).

Figure 53 RMON History page



Statistics > RMON History

RMON History Statistics (View By)

Port 1

RMON History Statistics Table

Start	Drop Events	Octets	Packets	Broadcast	Multicast	CRC Align Errors	Undersize	Oversize
23 Hours 58 Minutes 42 Seconds	0	8022	85	50	31	0	0	0
23 Hours 59 Minutes 12 Seconds	0	11462	162	126	33	0	0	0
23 Hours 59 Minutes 42 Seconds	0	24825	338	302	30	0	0	0
1 Days 12 Seconds	0	20201	308	274	33	0	0	0
1 Days 42 Seconds	0	16048	215	172	32	0	0	0
1 Days 1 Minutes 12 Seconds	0	20660	320	285	31	0	0	0
1 Days 1 Minutes 42 Seconds	0	20709	284	243	34	0	0	0
1 Days 2 Minutes 12 Seconds	0	20068	309	275	30	0	0	0
1 Days 2 Minutes 42 Seconds	0	13614	176	127	39	0	0	0
1 Days 3 Minutes 12 Seconds	0	19002	308	273	31	0	0	0
1 Days 3 Minutes 42 Seconds	0	7324	77	37	30	0	0	0
1 Days 4 Minutes 12 Seconds	0	6212	71	37	30	0	0	0
1 Days 4 Minutes 42 Seconds	0	7110	70	35	30	0	0	0
1 Days 5 Minutes 12 Seconds	0	6014	74	39	30	0	0	0
1 Days 5 Minutes 42 Seconds	0	7504	84	50	30	0	0	0

Table 46 describes the items on the RMON History page.

Table 46 RMON History page items

Section	Item	Description
RMON History Statistics (View By)	Unit	Choose the unit number to be monitored.
	Port	Choose the port number to be monitored.
RMON History Statistics Table	Start	The value of the sysUPTime at the start of the interval over which this sample was measured.
	Drop Events	The number of events in which packets were dropped by the interface due to a lack of resources.
	Octets	The number of octets of data (including those in bad packets) received on the network (excluding framing bits, but including Frame Check Sequence (FCS) octets).
	Packets	The number of good packets received that were directed to the broadcast address. This *does not* include multicast packets.
	Broadcast	The number of good packets received that were directed to the broadcast address. This *does not* include multicast packets.
	Multicast	The number of good packets received that were directed to the multicast address. This *does not* include packets sent to the broadcast address.
	CRC Align Errors	The number of packets received that had a length (excluding and 1518 octets, inclusive, but had either a bad Frame FCS with an integral number of octets (FCS errors) with a non-integral number of octets (alignment error).
	Undersize	The number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.
	Oversize	The number of packets received that were longer than 1518 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.

2 In the RMON History Statistics section, choose the unit and port number to be monitored.

3 Click Submit.

The RMON History Statistics Table is updated with information about the selected device and port (Figure 53).

Chapter 6
Viewing system statistics

The options available to monitor system statistical data are:

Note: To access the software version 2.5 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Viewing port statistics

You can view detailed statistics about a selected switch port in a stacked or standalone configuration. Both received and transmitted statistics are displayed so that you can compare throughput or other port parameters.

To view statistical data about a selected switch port:

1 From the main menu, choose Statistics > Port.

The Port page opens (Figure 54).

Figure 54 Port page

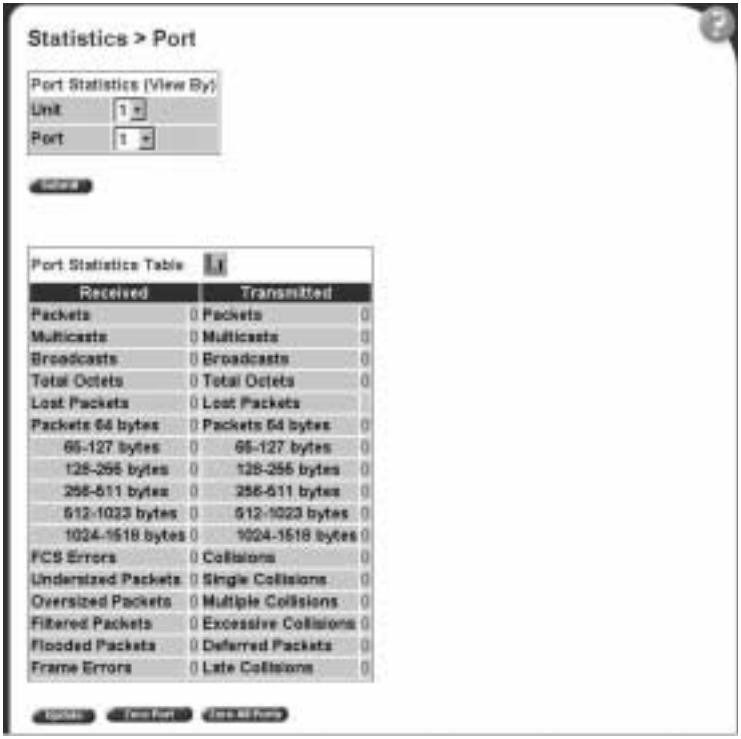


Table 47 describes the items on the Port page.

Table 47 Port page items

Section	Item	Description
Port Statistics (View By)	Unit	Choose the number of the switch to monitor.
	Port	Choose the switch's port number to monitor.
		Displays statistics in a bar graph format.
Port Statistics Table	Packets	The number of packets received/transmitted on this port, including bad packets, broadcast packets, and multicast packets.
	Multicast	The number of good multicast packets received/transmitted on this port, excluding broadcast packets.
	Broadcasts	The number of good broadcast packets received/transmitted on this port.
	Total Octets	The number of octets of data received/transmitted on this port, including data in bad packets and FCS octets, and framing bits.

Table 47 Port page items (continued)

Section	Item	Description
	Lost Packets	The number of packets discarded on this port when the capacity of the port transmit buffer was exceeded.
	Packets = 64 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 65-127 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 128-255 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 256-511 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 512-1023 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 1024-1518 bytes	The number of packets this size received/transmitted successfully on this port.
	FCS Errors	The number of valid-size packets received on this port with proper framing but discarded because of cyclic redundancy check (CRC) errors.
	Undersized Packets	The number of packets received on this port with fewer than 64 bytes and with proper CRC and framing (also known as short frames or runts).
	Oversized Packets	The number of packets that were received on this port with proper CRC and framing that meet the following requirements: • 1518 bytes if no VLAN tag exists • 1522 bytes if a VLAN tag exists
	Filtered Packets	The number of packets filtered, but not forwarded on this port.
	Flooded Packets	The number of packets flooded (forwarded) through this port because the destination address was not recognized in the address database.
	Frame Errors	The number of valid-size packets received on this port but discarded because of CRC errors and improper framing.
Port Statistics Table, cont.	Collisions	The number of collisions detected on this port.
	Single Collisions	The number of packets that were transmitted successfully on this port after a single collision.
	Multiple Collisions	The number of packets that were transmitted successfully on this port after more than one collision.
	Excessive Collisions	The number of packets lost on this port due to excessive collisions.
	Deferred Packets	The number of frames that were delayed on the first transmission attempt, but never incurred a collision.
	Late Collisions	The number of packets collisions that occurred after a total length of time that exceeded 512 bit-times of packet transmission.

2 In the Port Statistics section, choose the unit number and its port number.

3 Click Submit.

The Port Statistics Table is updated with information about the selected device and port (Figure 54).

4 To update the statistical information, click Update.

Zeroing ports

To clear the statistical information for the currently displayed port:

➨ Click Zero Port.

To clear the statistical information for all ports in a switch or stack configuration:

➨ Click Zero All Ports.

Viewing port statistics in a bar graph format

You can view port statistics in a bar graph format.

Note: If you choose to install the BPS 2000 software version 2.5 that supports Secure Shell, you will not be able to view port statistics in a bar graph format. The bar graph icon will not appear in the Port Statistics Table.

To view the displayed statistical information in a bar graph format:

1 In the Port Statistics Table, click the bar graph icon.

The Port: Chart page opens in a bar graph format (Figure 55).

Figure 55 Port: Chart page in a bar graph format

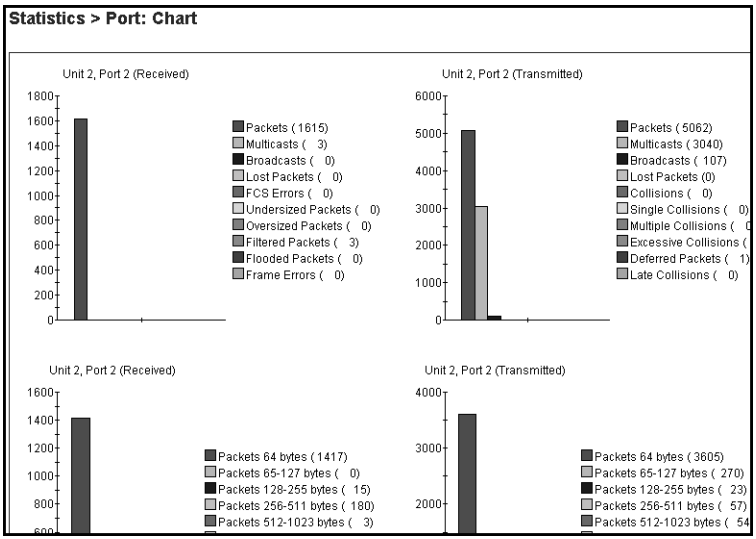


Table 47 describes the items on the Port: Chart page.

2 Click Back to return to the Port page.

Viewing all port errors

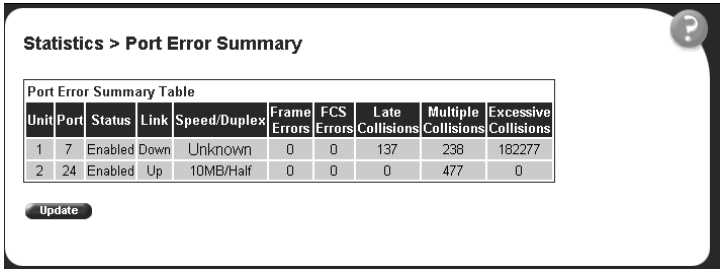
Beginning with software version 1.1, you can view all ports in the entire stack that have an error. If a particular port has no errors, it will not be displayed.

To view a summary of the port errors for the BPS 2000:

1 From the main menu, choose Statistics > Port Error Summary.

The Port Error Summary page opens (Figure 56).

Figure 56 Port Error Summary page



Unit	Port	Status	Link	Speed/Duplex	Frame Errors	FCS Errors	Late Collisions	Multiple Collisions	Excessive Collisions
1	7	Enabled	Down	Unknown	0	0	137	238	182277
2	24	Enabled	Up	10MB/Half	0	0	0	477	0

Table 48 describes the read-only information displayed in the Port Error Summary Table.

Table 48 Port Error Summary Table fields

Item	Description
Unit	Displays the unit number in the stack.
Port	Displays the port number of the unit.
Status	Displays the status of the port (Enabled/Disabled).
Link	Displays the link status of the port (Up/Down).
Speed/Duplex	Displays the speed at which the port is operating, as well as whether it is in half- or full-duplex mode.
Frame Errors	Displays the number of frame errors received on this port.
FCS Errors	Displays the number of frame check sequence (FCS) errors received on this port.
Late Collisions	Displays the number of late collisions errors received on this port.
Multiple Collisions	Displays the number of multiple collisions errors received on this port.
Excessive Collisions	Displays the number of excessive collisions errors received on this port.

2 To view the latest port statistics, click the Update button at the bottom of the page.

Viewing interface statistics

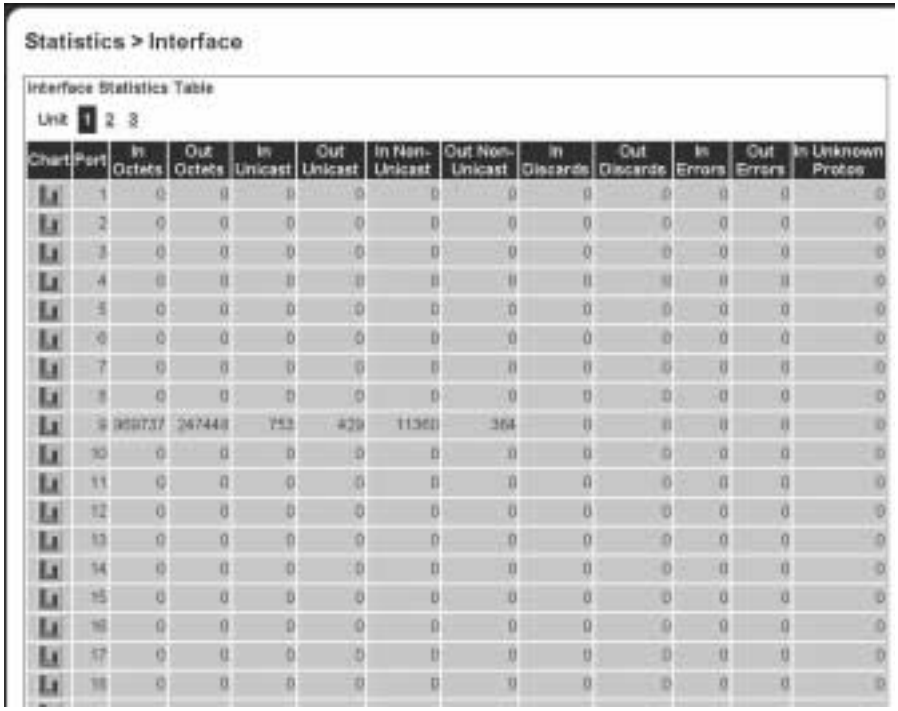
You can view selected switch interface statistics.

To view an interface's statistical information:

1 From the main menu, choose Statistics > Interface.

The Interface page opens (Figure 57).

Figure 57 Interface page



Statistics > Interface

Interface Statistics Table

Unit 1 2 3

Chart	Port	In Octets	Out Octets	In Unicast	Out Unicast	In Non-Unicast	Out Non-Unicast	In Discards	Out Discards	In Errors	Out Errors	In Unknown Protos
Lg	1	0	0	0	0	0	0	0	0	0	0	0
Lg	2	0	0	0	0	0	0	0	0	0	0	0
Lg	3	0	0	0	0	0	0	0	0	0	0	0
Lg	4	0	0	0	0	0	0	0	0	0	0	0
Lg	5	0	0	0	0	0	0	0	0	0	0	0
Lg	6	0	0	0	0	0	0	0	0	0	0	0
Lg	7	0	0	0	0	0	0	0	0	0	0	0
Lg	8	0	0	0	0	0	0	0	0	0	0	0
Lg	9	969737	247448	753	429	11360	364	0	0	0	0	0
Lg	10	0	0	0	0	0	0	0	0	0	0	0
Lg	11	0	0	0	0	0	0	0	0	0	0	0
Lg	12	0	0	0	0	0	0	0	0	0	0	0
Lg	13	0	0	0	0	0	0	0	0	0	0	0
Lg	14	0	0	0	0	0	0	0	0	0	0	0
Lg	15	0	0	0	0	0	0	0	0	0	0	0
Lg	16	0	0	0	0	0	0	0	0	0	0	0
Lg	17	0	0	0	0	0	0	0	0	0	0	0
Lg	18	0	0	0	0	0	0	0	0	0	0	0

Table 49 describes the items on the Interface page.

Table 49 Interface page items

Item	Description
	Displays statistics in a bar graph format.
Port	The port number corresponding to the selected switch.
In Octets	The number of octets received on the interface, including framing characters.
Out Octets	The number of octets transmitted out of the interface, including framing characters.
In Unicast	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Out Unicast	The number of packets that higher-layer protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
In Non-Unicast	The number of non-unicast packets, for example, subnetwork-broadcast or subnetwork-multicast packets, delivered to a higher protocol.
Out Non-Unicast	The number of packets that higher-level protocols requested be transmitted to a non-unicast address. For example, a subnetwork-broadcast or a subnetwork multicast address, including those that were discarded or not sent.
In Discards	The number of inbound packets which were selected to be discarded even though no errors were detected to prevent their being delivered to a higher-layer protocol. Packet discarding is not arbitrary. One reason for discarding packets is to free buffer space.
Out Discards	The number of outbound packets which were selected to be discarded even though no errors were detected to prevent their being transmitted. Packet discarding is not arbitrary. One reason for discarding packets is to free buffer space.
In Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Out Errors	The number of outbound packets that could not be transmitted because of errors.
In Unknown Protos	The number of packets received through the interface that were discarded because of an unknown or unsupported protocol.

2 In the upper-left hand corner, click on the unit number of the device to monitor.

The page is updated with the information for the selected device (Figure 57).

3 To update the statistical information, click Update.

Viewing interface statistics in a bar graph format

You can view interface statistics in a bar graph format.

Note: If you choose to install the BPS 2000 software version 2.5 that supports Secure Shell, you will not be able to view interface statistics in a bar graph format. The bar graph icon will not appear in the Interface page.

To view interface statistics in a bar graph format:

1. From the main menu, choose Statistics > Interface.

   The Interface page opens (Figure 57).

2. In the port row of your choice, click the bar graph icon.

   The Interface: Chart page opens in a bar graph format (Figure 58).

Figure 58 Interface: Chart in a bar graph format

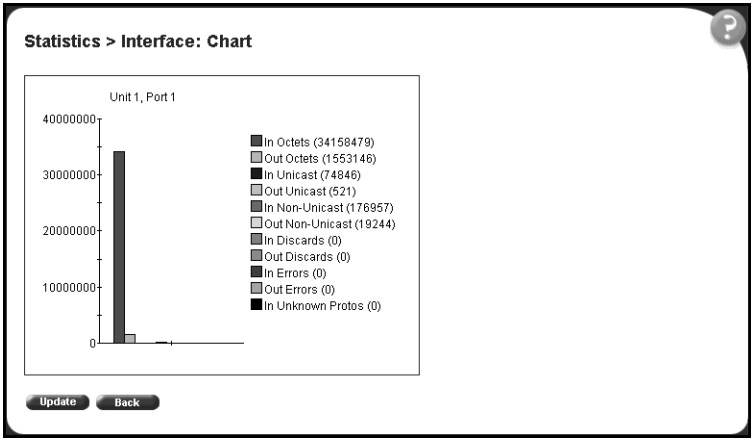


Table 49 describes the items on the Interface: Chart page.

3. To update the statistical information, click Update, or click Back to return to the Interface page.

Viewing Ethernet error statistics

You can view Ethernet error statistics for each monitored interface linked to the Business Policy Switch 2000.

To view Ethernet error statistics:

1 From the main menu, choose Statistics > Ethernet Errors.

The Ethernet Errors page opens (Figure 59).

Figure 59 Ethernet Errors page

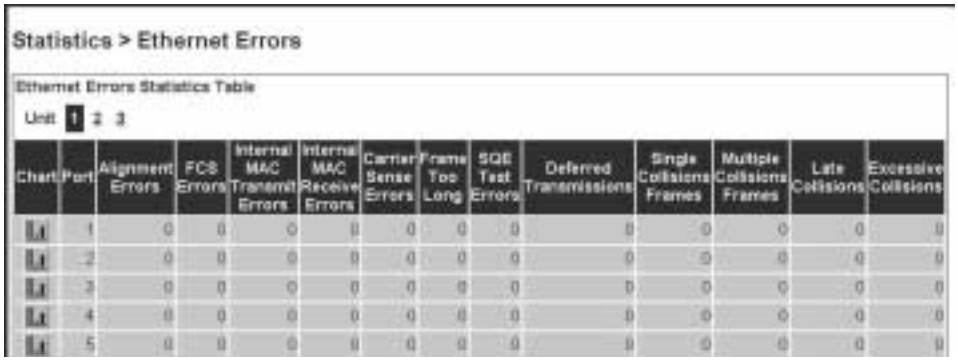


Table 50 describes the items on the Ethernet Errors page.

Table 50 Ethernet Errors page items

Item	Description
	Displays statistics in a bar graph format.
Port	The port number corresponding to the selected switch.
Alignment Errors	The number of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check.
FCS Errors	The number of frames received on a particular interface that are an integral number of octets in length, but do not pass the FCS check.
Internal MAC Transmit Errors	The number of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame only is counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object.
Internal MAC Receive Errors	The number of frames for which reception on a particular interface fails due to an internal MAC sublayer transmit error. A frame only is counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object.

Table 50 Ethernet Errors page items (continued)

Item	Description
Carrier Sense Errors	The number of times that the carrier sense conditions was lost or never asserted when attempting to transmit a frame on a particular interface.
Frame Too Long	The number of frames received on a particular interface that exceed the maximum permitted frame size.
SQE Test Errors	The number of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985, and its generation is described in section 7.2.4.6 of the same document.
Deferred Transmissions	The number of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy.
Single Collision Frames	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Multiple Collision Frames	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by a single collision.
Late Collisions	The number of times a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.
Excessive Collisions	The number of frames for which transmission on a particular interface fails due to excessive collisions.

2 In the upper-left hand corner, click on the unit number of the device to monitor.

The table is updated with the information for the selected device.

3 To refresh the statistical information, click Update.

Viewing Ethernet error statistics in a bar graph format

You can view Ethernet Errors statistics in a bar graph format.

Note: If you choose to install the BPS 2000 software version 2.5 that supports Secure Shell, you will not be able to view Ethernet error statistics in a bar graph format. The bar graph icon will not appear in the Ethernet Errors page.

To view Ethernet errors statistics in a bar graph format:

1 From the main menu, choose Statistics > Ethernet Errors.

The Ethernet Errors page opens (Figure 57).

2 In the port row of your choice, click the bar graph icon.

The Ethernet Errors: Chart page opens in a bar graph format (Figure 60).

Figure 60 Ethernet Error: Chart in a bar graph format

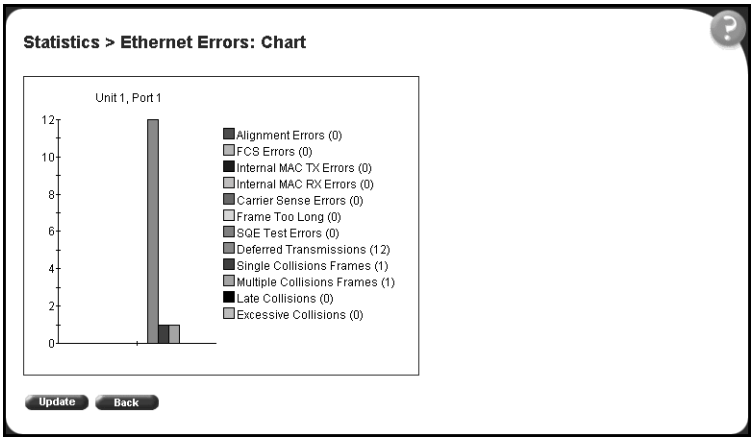


Table 50 describes the items on the Ethernet Errors: Chart page.

3 To update the statistical information, click Update, or click Back to return to the Ethernet Errors page.

Viewing transparent bridging statistics

You can view the transparent bridging statistics measured for each monitored interface on the device.

To view transparent bridging statistics:

1 From the main menu, choose Statistics > Transparent Bridging.

The Transparent Bridging page opens (Figure 61).

Figure 61 Transparent Bridging page

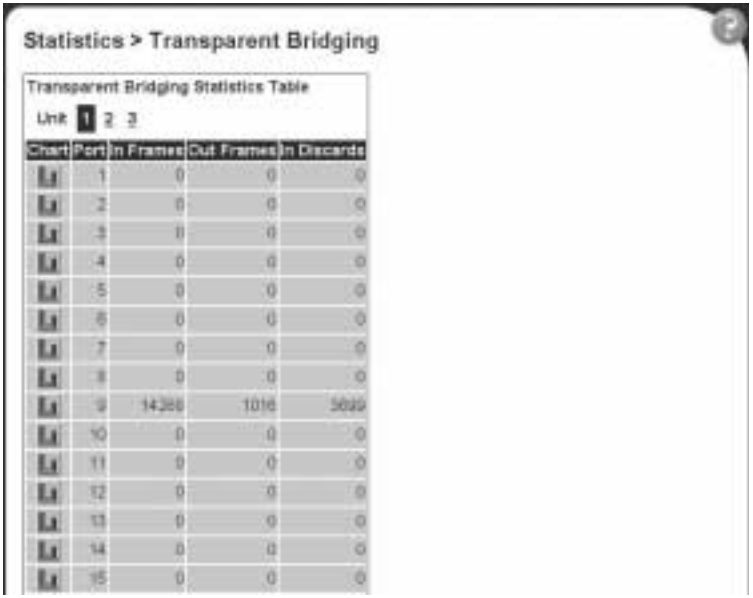


Table 51 describes the items on the Transparent Bridging page.

Table 51 Transparent Bridging page items

Item	Description
	Displays statistics in a bar graph format.
Port	The port number that corresponds to the selected switch.
In Frames (dot1dTpPortInFrames)	The number of frames that have been received by this port from its segment. A frame received on the interface corresponding to this port is counted only if it is for a protocol being processed by the local bridging function, including bridge management errors.
Out Frames (dot1dTpPortOutFrames)	The number of frames that have been transmitted by this port from its segment. A frame received on the interface corresponding to this port is counted only if it is for a protocol being processed by the local bridging function, including bridge management errors.
In Discards (dot1dTpPortInDiscards)	The number of valid frames received which were discarded by the forwarding process.

2 In the upper-left hand corner, click on the unit number of the device to monitor.

The page is updated with statistics about the selected device and its corresponding port number.

3 To refresh the statistical information, click Update.

Viewing transparent bridging statistics in a bar graph format

You can view measured transparent bridging statistics in a bar graph format.

Note: If you choose to install the BPS 2000 software version 2.5 that supports Secure Shell, you will not be able to view transparent bridging statistics in a bar graph format. The bar graph icon will not appear in the Transparent Bridging page.

To view transparent bridging statistics in a bar graph format:

1 From the main menu, choose Statistics > Transparent Bridging.

The Transparent Bridging page opens (Figure 57).

2 In the port row of your choice, click the bar graph icon.

The Transparent Bridging: Chart page opens in a bar graph format (Figure 62).

Figure 62 Transparent Bridging: Chart in a bar graph format

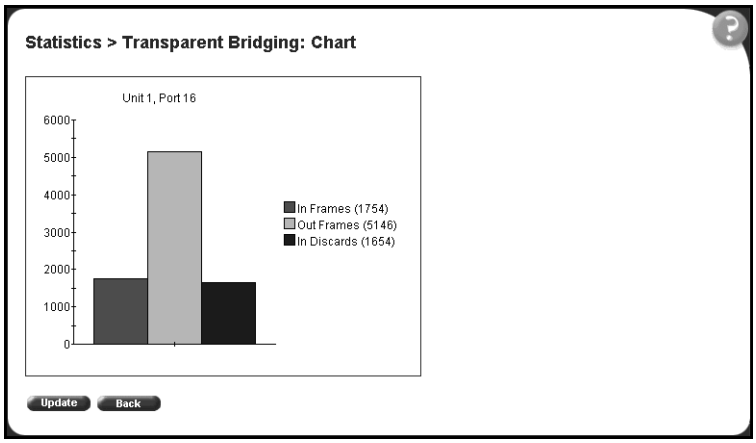


Table 51 describes the items on the Transparent Bridging: Chart page.

3 To update the statistical information, click Update, or click Back to return to the Transparent Bridging page.

Chapter 7
Configuring application settings

The options available to configure application settings are:

Note: To access the software version 2.5 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Configuring port mirroring

The BPS 2000 supports port mirroring to analyze traffic. You can view existing port mirroring activity and you can configure a specific switch port to mirror up to two specified ports or two MAC addresses. When you configure port mirroring, you have the option to specify either port-based monitoring or address-based monitoring. Refer to *Using the Business Policy Switch 2000 Software Version 2.5* for configuration guidelines for port-mirroring.

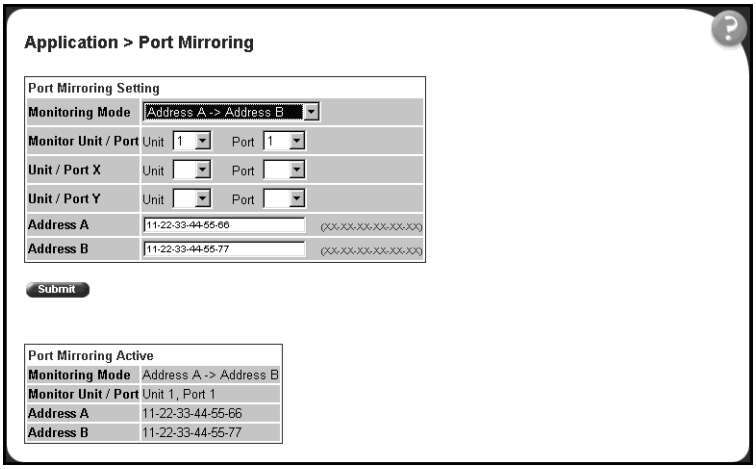
In a stack configuration, you can monitor ports that reside on different units within the stack. For more information, see *Using the Business Policy Switch 2000 Software Version 2.5*.

To configure port mirroring:

1 From the main menu, choose Application > Port Mirroring.

The Port Mirroring page opens (Figure 63).

Figure 63 Port Mirroring page



Note: The Port Mirroring Active section of this only displays those port mirroring configurations you set. If you set no port mirroring configurations, the area will not show rows.

Note: If the port which is monitored is in full duplex, only unicast packets which are addressed to the device that is connected to the port are monitored. If the port which is monitored is half duplex, all the packets which are addressed to the device that is connected to the port are monitored.

Table 52 describes the items on the Port Mirroring page.

Table 52 Port Mirroring page items

Item	Range	Description
Monitoring Mode	(1) Disabled (2) --> Port X (3) Port X --> (4)<-- --> Port X (5) -->Port X or Port Y --> (6) -->Port X and Port Y --> (7) <-- --> Port X and <-- --> Port Y (8) Address A --> any Address (9) any Address --> Address A (10) <-- --> Address A (11) Address A --> Address B (12) Address A <-- --> Address B	Choose any one of the six port-based monitoring modes or any one of the five address-based monitoring modes. For more information on selecting one of the six port-based modes that activates the port X and port Y screen fields, where you can choose up to two ports to monitor, see Table 53 on page 154. For more information on selecting one of the five address-based modes that activates the Address A and Address B screen fields, where you can specify MAC addresses to monitor, see Table 54 on page 154. The default setting is Disabled.
Port-based monitoring		
Monitor Port	1..28	Choose the switch port to designate as the monitor port.
Port X	1..28	Choose the first switch port to be monitored by the designated monitor port. This port is monitored according to the value “X” in the Monitoring Mode field.
Port Y	1..28	Choose the second switch port to be monitored by the designated monitor port. This port is monitored according to the value “Y” in the Monitoring Mode field.
Address-based monitoring		
Address A	XX-XX-XX-XX-XX-XX	Type the MAC address to monitor by the designated monitor port. This address is monitored according to the value “Address A” in the Monitoring Mode field.
Address B	XX-XX-XX-XX-XX-XX	Type the MAC address to monitor by the designated monitor port. This address is monitored according to the value “Address B” in the Monitoring Mode field.

2 Type information in the text boxes, or select from a list.

3 Click Submit.

Selecting one of the port-based monitoring modes activates the port X and/or the port Y screen fields, where you can choose up to two ports to monitor.

Table 53 describes the port-based monitoring modes.

Table 53 Port-based monitoring modes

Item	Description
Disabled	Choose this option to disable port-based monitoring. The default setting is Disabled.
--> Port X	Choose this option to monitor all traffic received by port X.
Port X -->	Choose this option to monitor all traffic transmitted by port X.
<-- --> Port X	Choose this option to monitor all traffic received and transmitted by port X.
--> Port X or Port Y -->	Choose this option to monitor all traffic received by port X or transmitted by port Y. Note: Do not use this mode for multicast and broadcast traffic.
--> Port X and Port Y -->	Choose this option to monitor all traffic received by port X (destined to port Y) and then transmitted by port Y (one way conversation steering). Note: Do not use this mode for multicast and broadcast traffic
<-- --> Port X and Port Y <-- -->	Choose this option to monitor all traffic received by port X and then transmitted by port Y or transmitted by port X and received by port Y (two way conversation steering). Note: Do not use this mode for multicast and broadcast traffic

Selecting any one of the address-based monitoring modes activates the Address A and Address B screen fields, where you can specify MAC addresses to monitor.

Table 54 describes the address-based monitoring modes.

Table 54 Address-based monitoring modes

Item	Description
Disabled	Choose this option to disable port-based monitoring. The default setting is Disabled.
Address A --> any Address	Choose this option to monitor all traffic transmitted from Address A to any address.
any Address --> Address A	Choose this option to monitor all traffic received by Address A from any address.
<-- --> Address A	Choose this option to monitor all traffic received by or transmitted by Address A.
Address A --> Address B	Choose this option to monitor all traffic transmitted by Address A that goes to Address (one way conversation steering).
Address A <-- --> Address B	Choose this option to monitor all traffic received by Address A and then transmitted by Address B or transmitted by Address A and received by Address B (two way conversation steering).

Configuring rate limiting

You can view the current forwarding rate of broadcast and/or multicast packets, and configure the BPS 2000 to limit the forwarding rate of broadcast and multicast packets on each interface. When you configure rate limiting, you are setting the percentage of port bandwidth allowed for a packet type. When the threshold is exceeded, additional packets are discarded.

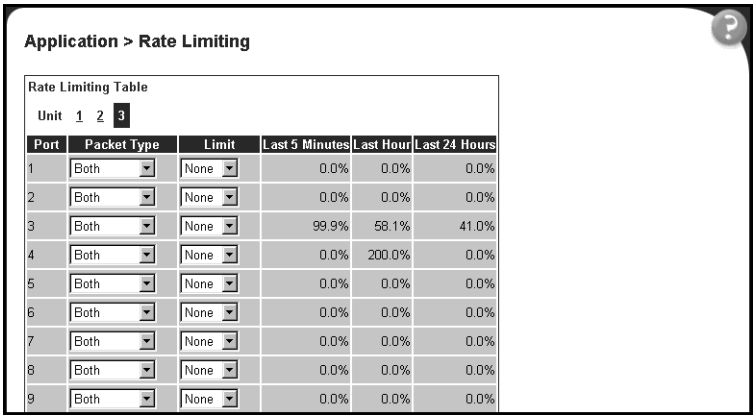
Note: If a port is configured for rate limiting, and it is a MultiLink trunk member, all trunk member ports implement rate limiting. If the port becomes disabled, all trunk members become disabled.

To configure rate limiting:

1 From the main menu, choose Application > Rate Limiting.

The Rate Limiting page opens (Figure 64).

Figure 64 Rate Limiting page



Port	Packet Type	Limit	Last 5 Minutes	Last Hour	Last 24 Hours
1	Both	None	0.0%	0.0%	0.0%
2	Both	None	0.0%	0.0%	0.0%
3	Both	None	99.9%	58.1%	41.0%
4	Both	None	0.0%	200.0%	0.0%
5	Both	None	0.0%	0.0%	0.0%
6	Both	None	0.0%	0.0%	0.0%
7	Both	None	0.0%	0.0%	0.0%
8	Both	None	0.0%	0.0%	0.0%
9	Both	None	0.0%	0.0%	0.0%

Table 55 describes the items on the Rate Limiting page.

Table 55 Rate Limiting page items

Item	Range	Description
Port	1..28	The selected unit's port number. The normal port range is 1 to 28. Note: A standard unit with MDA has a normal range of 25, 26, 28.
Packet Type	(1) Multicast (2) Broadcast (3) Both	Choose the packet type to view on the table. The default setting is Both.
Limit	None, 1-10%	Choose the percentage, if any, of bandwidth allowed for forwarding the packet type specified in the Packet Type field. When the threshold is exceeded, any additional packets are discarded. Note: Rate limiting is disabled if this field is set to none. This allows you to select and view the percentage of specific packet types present in the network, without inadvertently limiting the forwarding rate. The default setting is None.
Last 5 Minutes	0..100%	The percentage of packets received by the port in the last five minutes. This field provides a running average of network activity and is updated every 15 seconds.
Last Hour	0..100%	The percentage of packets received by the port in the last hour. This field provides a running average of network activity and is updated every five minutes.
Last 24 Hours	0..100%	The percentage of packets received by the port in the last 24 hours. This field provides a running average of network activity and is updated every hour.
		Note: The Last 5 Minutes, Last Hour, and Last 24 Hours fields indicate the receiving port's view of network activity regardless of the rate limiting setting.
		Note: When the volume of broadcast and multicast packets is high, placing severe strain on the network (often referred to as a "storm"), you can set the forwarding rate of those packet types to *not exceed* a specified percentage of the total available bandwidth.

2 In the upper-left hand corner, click on the unit number of the device to monitor.

3 Type information in the text boxes, or select from a list.

4 Click Submit.

Note: To avoid broadcast storms (when the volume of a particular packet type is extreme, placing severe strain on the network), set the forwarding rate of the packet type to not exceed a lower percentage of the total available bandwidth.

Configuring IGMP

You can configure a VLAN's switch ports to optimize IP multicast packets in a bridged Ethernet environment, and you can view a table of existing IGMP configurations. For more information about IGMP configuration, see *Using the Business Policy Switch 2000 Software Version 2.5* (208700-C).

To configure IGMP:

1 From the main menu, choose Application > IGMP > IGMP Configuration.

The IGMP Configuration page opens (Figure 65).

Figure 65 IGMP Configuration page

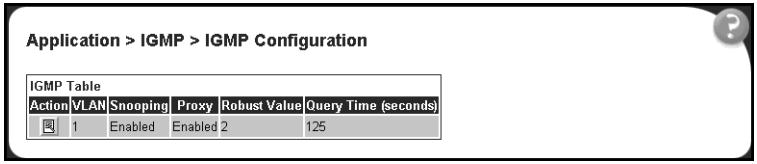


Table 56 describes the items on the IGMP Configuration page.

Table 56 IGMP Configuration page items

Item	Description
	Displays a modification page for the selected VLAN.
VLAN	The number assigned to the VLAN when the VLAN was created. For more information on creating VLANs, see "Creating and managing virtual LANs (VLANs)" on page 161.
Snooping	The operational status for the IGMP snooping feature.
Proxy	If enabled, this feature allows the switch to consolidate IGMP Host Membership Reports received on its downstream ports and to generate a consolidated proxy report for forwarding to its upstream neighbor. Note: This field affects *all* VLANs.

Table 56 IGMP Configuration page items

Item	Description
Robust Value	The predetermined value set by the administrator to offset expected packet loss on a subnet. If packet losses on a subnet are unacceptably high, the Robust Value field can be increased to a higher value. Note: This field affects *only* the VLAN specified in the page's VLAN field.
Query Time	The query interval (the interval between general queries sent by the multicast router).

2 In the VLAN row of your choice, click the Modify icon.

The IGMP: VLAN Configuration page opens (Figure 66).

Figure 66 IGMP: VLAN Configuration page

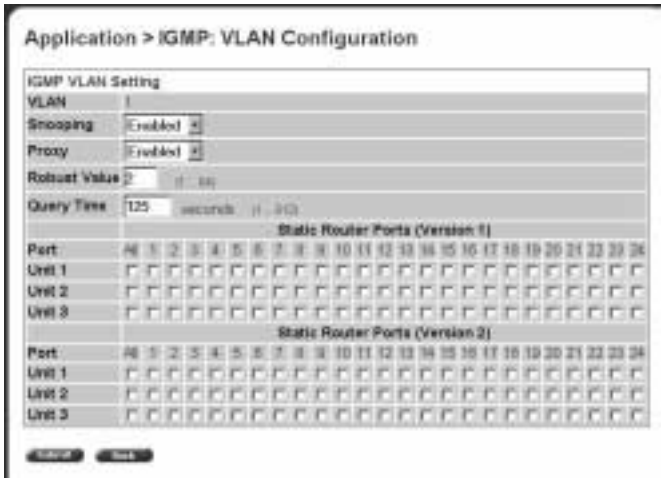


Table 57 describes the items on the IGMP: VLAN Configuration page.

Table 57 IGMP: VLAN Configuration page items

Item	Range	Description
VLAN	1..4094	The number assigned to the VLAN when the VLAN was created. For more information on creating VLANs, see "Creating and managing virtual LANs (VLANs)" on page 161.
Snooping	(1) Enabled (2) Disabled	Choose to enable or disable the IGMP snooping feature. Note: This field affects *all* VLANs. The default setting is Enabled.

Table 57 IGMP: VLAN Configuration page items (continued)

Item	Range	Description
Proxy	(1) Enabled (2) Disabled	Choose to enable or disable the proxy feature. This feature allows the switch to consolidate IGMP Host Membership Reports received on its downstream ports and to generate a consolidated proxy report for forwarding to its upstream neighbor. Note: This field affects *all* VLANs. The default setting is Enabled.
Robust Value	1..64	Type the robust value in the appropriate format. This feature allows you to set the switch to offset expected packet loss on a subnet. If packet losses on a subnet are unacceptably high, the Robust Value field can be increased to a higher value. Note: This field affects *only* the VLAN specified in the page's VLAN field. The default settings is 2.
Query Time	1..512	Type the query time (in seconds) in the appropriate format. This feature allows you to control the number of IGMP messages allowed on the subnet by varying the Query Interval (the interval between general queries sent by the multicast router). Note: This field affects *only* the VLAN specified in the page's VLAN field. The default settings is 125 seconds.
Static Router Ports (Version 1 and Version 2)		Click the check boxes of the router ports to associate with the VLAN (alternatively, click the check box to deselect a selected router port). Note: This field affects *all* VLANs.

3 Type information in the text boxes, or select from a list.

4 In the Static Router Ports section(s), click the check boxes of the router ports to associate with the VLAN.

5 Do one of the following:

- Click Submit.
- Click Back to return to the IGMP page without making changes.

The new configuration is displayed in the IGMP Table (Figure 65).

Viewing Multicast group membership configurations

You can view a table configured IP multicast group addresses for a selected VLAN.

To view multicast group membership configurations for a selected VLAN:

1 From the main menu, choose Application > IGMP > IGMP Multicast Group.

The IGMP Multicast Group Membership page opens (Figure 67).

Figure 67 IGMP Multicast Group Membership page

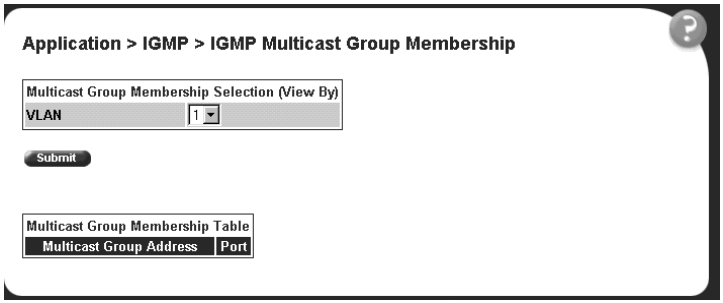


Table 58 describes the items on the IGMP Multicast Group Membership page.

Table 58 IGMP Multicast Group Membership page items

Section	Item	Description
Multicast Group Membership Selection (View By)	VLAN	Choose the VLAN on which to view configured IP addresses.
Multicast Group Membership Table	Multicast Group Address	The IP multicast group addresses that are currently active on the associated port.
	Port	The port numbers associated with the IP multicast group addresses displayed in the IP Multicast Group Address field.

2 In the Multicast Group Membership Selection section, choose the number of VLAN on which to view configured IP addresses.

3 Click Submit.

The results are displayed in the Multicast Group Membership Table (Figure 67).

Creating and managing virtual LANs (VLANs)

A VLAN is a collection of switch ports that make up a single broadcast domain. You can configure a VLAN for a single switch, or for multiple switches. When you create a VLAN, you can control traffic flow and ease the administration of moves, adds, and changes on the network, by eliminating the need to change physical cabling.

Note: For guidelines on configuring VLANs, refer to *Using the Business Policy Switch 2000 Software Version 2.5*.

You can configure three types of VLAN in the Web-based management interface:

- Port-based
- Protocol-based
- MAC SA-based

Beginning with software version 1.2, you can use 256 port-, protocol-, and MAC SA-based VLANs for the stack with a Pure BPS 2000 Stack. (The maximum number of MAC SA-based VLANs available is 48). If you are working with a mixed, or Hybrid, stack, you can use 64 VLANs for the entire stack. When you change from a Pure BPS 2000 Stack mode to a Hybrid Stack mode:

- If you have up to 64 VLANs on the Pure BPS 2000 Stack, they will be retained when you change to a Hybrid Stack.
- If you have more than 64 VLANs on the Pure BPS 2000 Stack, you will lose them all. The Hybrid Stack will return to the default VLAN configuration.

Note: To access 256 VLANs, you must be working in Pure BPS 2000 Stack mode. To view and change the stack operational mode, refer to Chapter 3, “Setting system operational modes.”

Port-based VLANs

A port-based VLAN is a VLAN in which the ports are explicitly configured to be in the VLAN. When you create a port-based VLAN on a switch, you assign a VLAN identification number (VLAN ID) and specify which ports belong to the VLAN. The VLAN ID is used to coordinate VLANs across multiple switches.

With software version 1.1 and higher, the automatic PVID feature automatically sets the PVID when you configure a port-based VLAN. The PVID value will be the same value as VLAN. The user can also manually change the PVID value. The default setting for AutoPVID is Off; you must enable this feature.

Protocol-based VLANs

Beginning with software version 1.2, you can configure as many as 255 protocol-based VLANs, with up to 14 different protocols.

A protocol-based VLAN is a VLAN in which the switch ports are configured as members of a broadcast domain, based on the protocol information within a packet. A protocol-based VLAN can localize broadcast traffic and assure that only the protocol-based VLAN ports are flooded with the specified protocol-type packets.

For protocol-based VLANS, the VLAN classification of the frame is dependent on the protocol of the incoming untagged frame. The frame is forwarded only if that VLAN is registered at the egress port.

MAC SA-based VLANs

A MAC source address (SA)-based VLAN is a VLAN whose frame classification is dependent on the MAC SA of the incoming untagged frame. The frame is forwarded only if that VLAN is registered at the egress port.

Configuring VLANs

You can create VLANs by assigning switch ports, MAC SA, and protocols as VLAN members and you can designate an existing VLAN to act as the management VLAN.

Note: To access the software version 2.5 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

To open the VLAN Configuration page:

➨ From the main menu, choose Application > VLAN > VLAN Configuration.

The VLAN Configuration page opens (Figure 68).

Figure 68 VLAN Configuration page

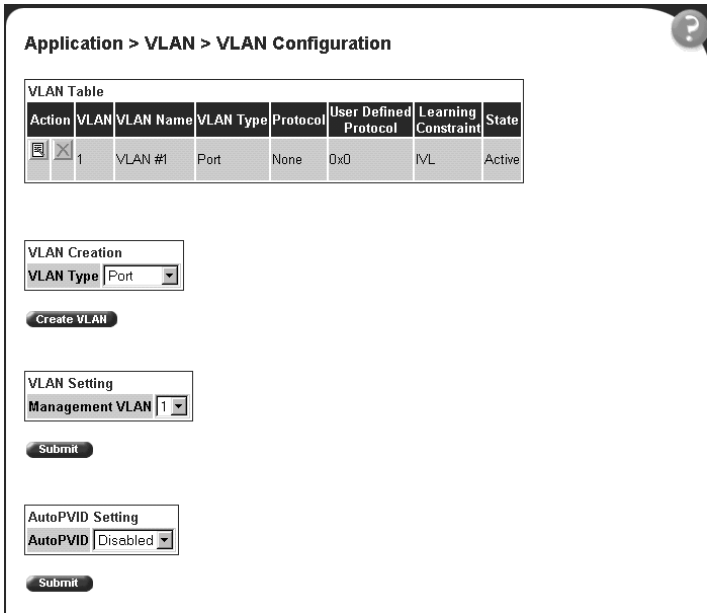


Table 59 describes the items on the VLAN Configuration page.

Table 59 VLAN Configuration page items

Section	Item	Description
VLAN Table		Displays a modification page.
		Deletes the row.
	VLAN	The number assigned to the VLAN when the VLAN was created.
	VLAN Name	The name assigned to the VLAN when the VLAN was created.
	VLAN Type	The base-type assigned when the VLAN was created. The base types are: Port-based, IP Subnet-based, Protocol-based, and MAC SA-based.
	Protocol	The protocol assigned when the VLAN was created. The protocol types are: IP, IPX 802.2, 1PX 802.3, IPX Snap, IPX Ethernet II, Apple Talk, DEC Lat, SNA 802.2, SNA Ethernet II, Net Bios, XNS, Vines, Ipv6, User Defined, and RARP. For more information, see Table 63 on page 170.
	User Defined Protocol	The user-defined protocol assigned when the VLAN was created.
	Learning Constraint	The type of learning constraint selected when the VLAN was created. The choices are IVL and SVL. Note: If you select IVL, the VLAN uses an independent filtering database from all other VLANs. If you select SVL, the VLAN shares the same filtering database as all other VLANs with SVL. Note: When the stack mode is set to “Pure BPS 2000,” the default setting is IVL; IVL is available *only* with a Pure BPS 2000 stack mode. When the stack mode is set to “Hybrid,” the default setting is SVL.
	State	The current operational state of the VLAN.
VLAN Creation	VLAN Type	Choose the type of VLAN to create and click Create VLAN. Your options are: port-based (page 165), protocol-based (page 168), and MAC SA-based (page 173).
VLAN Setting	Management VLAN	Choose the VLAN to designate as the management VLAN.
AutoPVID Setting	AutoPVID	Choose Enabled to activate the Automatic PVID feature and click Submit. Note: Use this *only* with port-based VLANs.

Creating a port-based VLAN

To create a port-based VLAN:

1. From the main menu choose Application > VLAN > VLAN Configuration.

   The VLAN Configuration page opens (Figure 68).

2. In the VLAN Creation section, choose Port.
3. Click Create VLAN.

   The VLAN Configuration: Port Based setting page opens (Figure 69).

Figure 69 VLAN Configuration: Port Based setting page

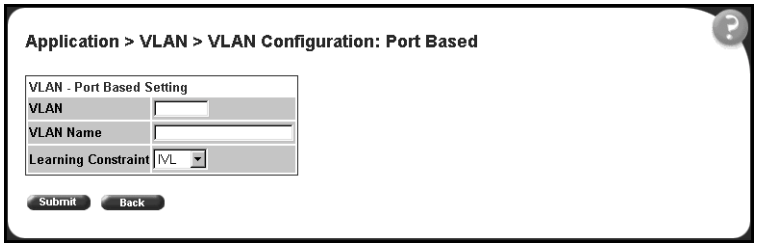


Table 60 describes the items on the VLAN Configuration: Port Based setting page.

Table 60 VLAN Configuration: Port Based setting page items

Item	Range	Description
VLAN	1..4094	The number assigned to the VLAN when the VLAN was created.
VLAN Name	1..16	Type a character string to create a unique name to identify the VLAN, for example, VLAN1.
Learning Constraint	(1) IVL (2) SVL	Choose your learning constraint type. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. If SVL is selected, the VLAN shares the same filtering database as all other VLANs with SVL. Note: If the stack is set to a “pure” operational mode, the default setting is IVL; IVL is available *only* with Pure BPS 2000 stack operational mode. If the stack is set to a “hybrid” operational mode, the default setting is SVL. For more information on setting your stack operational mode, see “Setting system operational modes” on page 122.

4 Type information in the text boxes, or select from a list.

5 Do one of the following:

- Click Submit.
- Click Back to return to the VLAN Configuration page without making changes.

The new port-based VLAN configuration appears in the VLAN Table on the VLAN Configuration page (Figure 68).

Modifying a port-based VLAN

To modify an existing port-based VLAN:

1 From the main menu, choose Application > VLAN > VLAN Configuration.

The VLAN Configuration page opens (Figure 68).

2 In the VLAN Table section, in the port-based VLAN row of your choice, click the Modify icon.

The VLAN Configuration: Port Based modification page opens (Figure 70).

Figure 70 VLAN Configuration: Port Based modification page

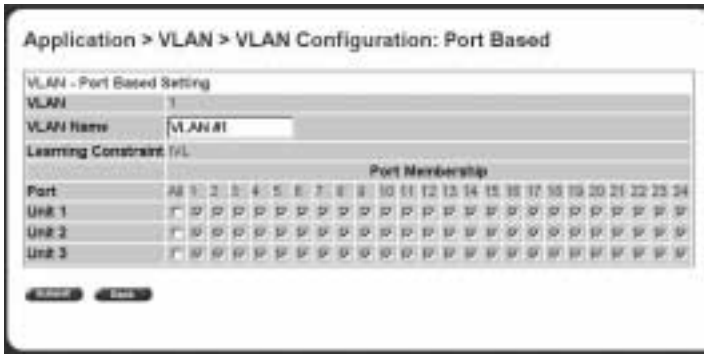


Table 61 describes the items on the VLAN Configuration: Port Based modification page.

Table 61 VLAN Configuration: Port Based modification page items

Item	Description
VLAN	The number assigned to the VLAN when the VLAN was created.
VLAN Name	(Re)name the VLAN.
Learning Constraint	The type of learning constraint selected when the VLAN was created. The learning constraint choices are IVL and SVL. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. IVL is available *only* in the Pure BPS 2000 stack operational mode. If SVL is selected, the VLAN shares the same filtering database as all other VLANs with SVL.
Port/Port Membership	Click the check boxes of *standalone or stacked unit* ports to associate it with the VLAN or, if the port is already a member, click the check box to deselect the it as a member of the VLAN. A port can be configured in one or more VLANs. This field is dependent on the Tagging field value in the VLAN Port Configuration screen. For example: • When the Tagging field is set to *Untagged Access*, you can set the Port Membership field as an untagged port member or as a non-VLAN port member. • When the Tagging field is set to *Tagged Trunk*, you can set the Port Membership field as a tagged port member or as a non-VLAN port member.

3 Type information in the text boxes, or click the check box of a port to associate it with the VLAN or, if the port is already a member, click the check box to deselect it as a member of the VLAN.

4 Do one of the following:

- Click Submit.
- Click Back to return to the VLAN Configuration page without making changes.

The modified VLAN configuration is displayed in the VLAN Table (Figure 68).

Creating a protocol-based VLAN

To create a protocol-based VLAN:

1. From the main menu, choose Application > VLAN > VLAN Configuration.

   The VLAN Configuration page opens (Figure 68).

2. In the VLAN Creation section, choose Protocol.
3. Click Create VLAN.

   The VLAN Configuration: Protocol Based setting page opens (Figure 71).

Figure 71 VLAN Configuration: Protocol Based setting page

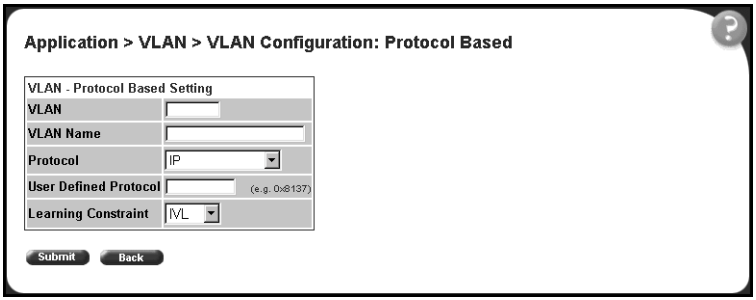


Table 62 describes the items on the VLAN Configuration: Protocol Based setting page.

Note: Beginning with software version 1.2, there are 14 available protocols.

Table 62 VLAN Configuration: Protocol Based setting page items

Item	Range	Description
VLAN	1..4094	Type a unique number to identify the VLAN.
VLAN Name	1..16	Type a unique name to identify the VLAN.
Protocol	IP, IPX 802.2, 1PX 802.3, IPX Snap, IPX Ethernet II, Apple Talk, DEC Lat, SNA 802.2, SNA Ethernet II, Net Bios, XNS, Vines, Ipv6, User Defined, and RARP.	Choose the supported protocol for the VLAN. For more information, see Table 63 on page 170.
User Defined Protocol		If you selected "User Defined" from the Protocol pulldown list, specify the protocol identifier for the VLAN. Note: Any frames that match the specified PID, in any of the following ways are assigned to that user defined VLAN: • The ethertype for Ethernet type 2 frames • The PID in Ethernet SNAP frames • The DSAP or SSAP value in Ethernet 802.2 frames. For a list of rereserved PIDs that are unavailable for user-defined PIDs, see Table 64 on page 171.
Learning Constraint	(1) IVL (2) SVL	Choose your learning constraint type. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. If SVL is selected, the VLAN shares the same filtering database as all other VLANs with SVL. Note: If the stack is set to a "pure" operational mode, the default setting is IVL; IVL is available *only* in Pure BPS 2000 stack operational mode. If the stack is set to a "hybrid" operational mode, the default setting is SVL. For more information on setting your stack operational mode, see "Setting system operational modes" on page 122.

4 Type information in the text boxes, or select from a list.

5 Do one of the following:

- Click Submit.
- Click Back to return to the VLAN Configuration page without making changes.

The new protocol-based VLAN configuration appears in the VLAN Table on the VLAN Configuration page (Figure 68).

Caution: BayStack 450-!GBIC, 450-1SR, 450-1SX, 450-1LR, 450-LX MDA ports and BayStack 410 ports do not have the ability to assign incoming untagged frames to a protocol-based VLAN. To allow gigabit ports and BayStack 410 ports to participate in protocol-based VLANs, set the tagging field value to "Tagged Trunk" (see "Configuring broadcast domains" on page 178).

Table 63 defines the standard protocol-based VLANs and PID types that are supported by the Business Policy Switch and BayStack 450 and 410 switches. See Table 64 for a list of rereserved PIDS that are not available for user-defined PIDs.

Table 63 Standard protocol-based VLANs and PID types

PID Name	Encapsulation	PID Value (hex)	VLAN Type
IP Ether2	Ethernet type 2	0800, 0806	Standard IP on Ethernet Type 2 frames
Ipx 802.3	Ethernet 802.2	FF FF	Novell IPX on Ethernet 802.3 frames
Ipx 802.2	Ethernet 802.0	E0 E0	Novell IPX on Ethernet 802.2 frames
Ipx Snap	Ethernet Snap	8137, 8138	Novell IPX on Ethernet SNAP frames
Ipx Ethernet II	Ethernet type 2	8137, 8138	Novell IPX on Ethernet Type 2 frames
Apple Talk	Ethernet type 2 or Ethernet Snap	809B, 80F3	AppleTalk on Ethernet Type 2 and Ethernet Snap frames
DEC Lat	Ethernet type 2	6004	DEC LAT protocol
DEC Other	Ethernet type 2	6000 - 6003, 6005 - 6009, 8038	Other DEC protocols
Sna 802.2	Ethernet 802.2	04**, **04	IBM SNA on IEEE 802.2 frames
Sna Ethernet II	Ethernet type 2	80D5	IBM SNA on Ethernet Type 2 frames
NetBios	Ethernet type 2	F0**, **F0	NetBIOS protocol
XNS	Ethernet type 2	0600, 0807	Xerox XNS
Vines	Ethernet type 2	0BAD	Banyan VINES
IPv6	Ethernet type 2	86DD	IP version 6

Table 63 Standard protocol-based VLANs and PID types (continued)

PID Name	Encapsulation	PID Value (hex)	VLAN Type
RARP	Ethernet type 2	8035	Reverse Address Resolution Protocol (RARP): RARP is a protocol used by some old diskless devices to obtain IP addresses by providing the MAC layer address. When you create a VLAN based on RARP, you can limit the RARP broadcasts to the ports that lead to the RARP server.
User-Defined	Ethernet type 2, Ethernet 802.2, or Ethernet Snap	User-defined 16 bit value	If you select “User Defined” from the Protocol pulldown list, specify the protocol identifier for the VLAN. Note: Any frames that match the specified PID, in any of the following ways are assigned to that user defined VLAN: The ethertype for Ethernet type 2 frames The PID in Ethernet SNAP frames The DSAP or SSAP value in Ethernet 802.2 frames. For a list of rereserved PIDs that are unavailable for user-defined PIDs, see Table 63 on page 170

Table 64, describes the PIDS that are reserved and not available for user-defined PIDs.

Table 64 Predefined Protocol Identifier (PID)

PID Name	Encapsulation	PID Value (hex)	VLAN Type
IP Ether2	Ethernet type 2	0800, 0806	Standard IP on Ethernet Type 2 frames
Ipx 802.3	Ethernet 802.2	FF FF	Novell IPX on Ethernet 802.3 frames
Ipx 802.2	Ethernet 802.0	E0 E0	Novell IPX on Ethernet 802.2 frames
Ipx Snap	Ethernet Snap	8137, 8138	Novell IPX on Ethernet SNAP frames
Ipx Snap2	Ethernet type 2	8137, 8138	Novell IPX on Ethernet Type 2 frames
AplTk Ether2 Snap	Ethernet type 2 or Ethernet Snap	809B, 80F3	AppleTalk on Ethernet Type 2 and Ethernet Snap frames
Declat Ether2	Ethernet type 2	6004	DEC LAT protocol
DecOther Ether2	Ethernet type 2	6000 - 6003, 6005 - 6009, 8038	Other DEC protocols
Sna 802.2	Ethernet 802.2	04**, **04	IBM SNA on IEEE 802.2 frames
Sna Ether2	Ethernet type 2	80D5	IBM SNA on Ethernet Type 2 frames
NetBios 802.2	Ethernet type 2	F0**, **F0	NetBIOS protocol
Xns Ether2	Ethernet type 2	0600, 0807	Xerox XNS

Table 64 Predefined Protocol Identifier (PID) (continued)

Vines Ether2	Ethernet type 2	0BAD	Banyan VINES
Ipv6 Ether2	Ethernet type 2	86DD	IP version 6
User-Defined	Ethernet type 2, Ethernet 802.2, or Ethernet Snap	User-defined 16 bit value	User-defined protocol-based VLAN. For a list of rereserved PIDs that are unavailable for user-defined PIDs, see Table 64 on page 171.

Modifying a protocol-based VLAN

To modify an existing protocol-based VLAN:

1 From the main menu, choose Application > VLAN > VLAN Configuration.

The VLAN Configuration page opens (Figure 68).

2 In the VLAN Table section, in the protocol-based VLAN row of your choice, click the Modify icon.

The VLAN Configuration: Protocol Based modification page opens (Figure 72).

Figure 72 VLAN Configuration: Protocol Based modification page

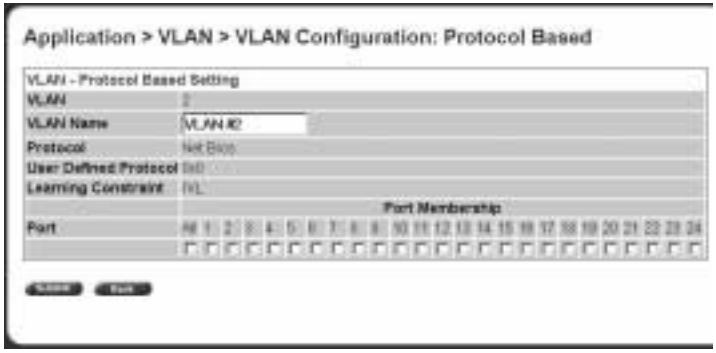


Table 65 describes the items on the VLAN Configuration: Protocol Based modification page.

Table 65 VLAN Configuration: Protocol Based modification page items

Item	Description
VLAN	The number assigned to the VLAN when the VLAN was created.
VLAN Name	(Re)name the VLAN.
Learning Constraint	The type of learning constraint selected when the VLAN was created. The learning constraint choices are IVL and SVL. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. IVL is available *only* in Pure BPS 2000 stack operational mode.If SVL is selected, the VLAN shares the same filtering database as all other VLANs with SVL.
Port/Port Membership	Click the check boxes beneath a port to associate the port with the VLAN or, if the port is already selected click the check box to deselect the port as a member of the VLAN.

3 Type information in the text boxes, or click the check box of a port to associate it with the VLAN or, if the port is already a member, click the check box to deselect it as a member of the VLAN.

4 Do one of the following:

- Click Submit.
- Click Back to return to the VLAN Configuration page without making changes.

The modified VLAN configuration is displayed in the VLAN Table (Figure 68).

Creating a MAC SA-based VLAN

To create a MAC SA-based VLAN:

1 From the main menu, choose Application > VLAN > VLAN Configuration.

The VLAN Configuration page opens (Figure 68).

2 In the VLAN Creation section, choose MAC SA.

3 Click Create VLAN.

The VLAN Configuration: MAC SA Based setting page opens (Figure 73).

Figure 73 VLAN Configuration: MAC SA Based setting page

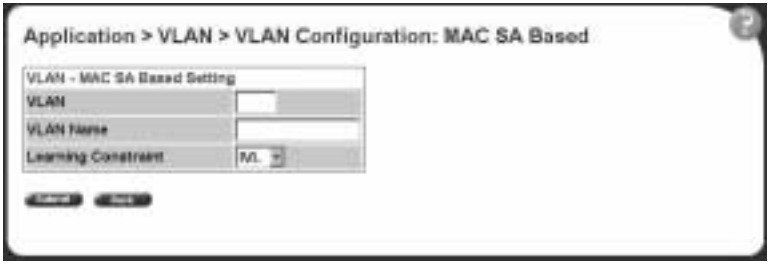


Table 66 describes the items on the VLAN Configuration: MAC SA Based setting page.

Table 66 VLAN Configuration: MAC SA Based setting page items

Item	Range	Description
VLAN	1..4094	Type a unique number to identify the VLAN.
VLAN Name	1..16	Type a unique name to identify the VLAN, for example *.
Learning Constraint	(1) IVL (2) SVL (default)	Choose your learning constraint type. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. If SVL is selected, the VLAN shares the same filtering database as all other VLANs with SVL. Note: If the stack is set to a “pure” operational mode, the default setting is IVL; IVL is available *only* in Pure BPS 2000 mode. If the stack is set to a “hybrid” operational mode, the default setting is SVL. For more information on setting your stack operational mode, see “Setting system operational modes” on page 122.

4 Type information in the text boxes, or select from a list.

5 Do one of the following:

- Click Submit.
- Click Back to return to the VLAN Configuration page without making changes.

The new MAC SA-based VLAN configuration appears in the VLAN Table on the VLAN Configuration page (Figure 68).

Modifying a MAC SA-based VLAN

To modify an existing MAC SA-based VLAN:

1 From the main menu, choose Application > VLAN > VLAN Configuration.

The VLAN Configuration page opens (Figure 68).

2 In the VLAN Table section, in the MAC SA-based VLAN row of your choice, click the Modify icon.

The VLAN Configuration: MAC SA Based modification page opens (Figure 74).

Figure 74 VLAN Configuration: MAC SA Based modification page

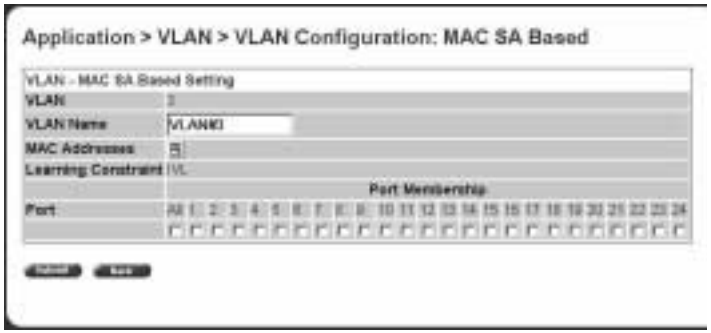


Table 67 describes the items on the VLAN Configuration: MAC SA Based modification page.

Table 67 VLAN Configuration: MAC SA Based modification page items

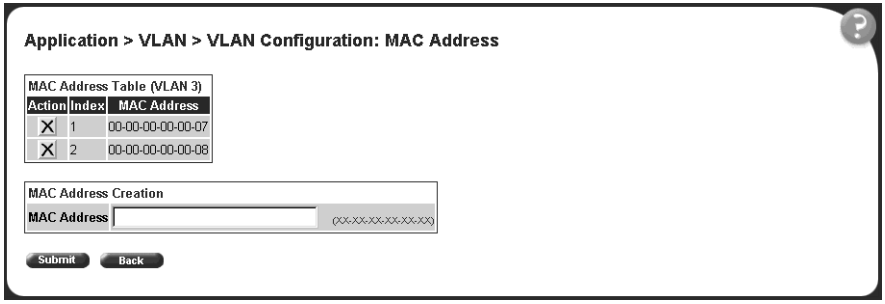
Item	Description
VLAN	The number assigned to the VLAN when the VLAN was created.
VLAN Name	(Re)name the VLAN.
	Opens the VLAN Configuration: MAC Address page (Figure 75).
Learning Constraint	The type of learning constraint selected when the VLAN was created. The learning constraint choices are IVL and SVL. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. IVL is available *only* in the Pure BPS 2000 stack operational mode. If SVL is selected, the VLAN shares the same filtering database as all other VLANs with SVL.

3 Type information in the text boxes, or click the check box of a port to associate it with the VLAN or, if the port is already a member, click the check box to deselect it as a member of the VLAN.

4 To create MAC address associations, click the modify icon.

The VLAN Configuration: MAC Address page opens (Figure 75).

Figure 75 VLAN Configuration: MAC Address page



5 In the MAC Address Creation section, type the MAC address to associate with the VLAN.

The MAC address appears in the MAC Address Table (Figure 75).

Note: You can delete an existing MAC address by clicking the delete icon in the row of the MAC address you want to delete.

6 Do one of the following:

- Click Submit to save your changes and return to the VLAN Configuration: MAC SA Based setting page.
- Click Back to return to the VLAN Configuration: MAC SA Based setting page without making changes.

7 On the VLAN Configuration: MAC SA Based setting page, do one of the following:

- Click Submit.
- Click Back to return to the VLAN Configuration page without making changes.

The modified VLAN configuration is displayed in the VLAN Table (Figure 68).

Selecting a management VLAN

You can select any VLAN to perform as the management VLAN. VLAN 1 is the default management VLAN for the switch. To set this field, the VLAN State field value must be active.

To select a VLAN as the management VLAN:

1 From the main menu, choose Application > VLAN > VLAN Configuration.

The VLAN Configuration page opens (Figure 68).

2 In the VLAN Setting section, choose the VLAN to assign as your management VLAN.

3 Click Submit.

Deleting a VLAN configuration

To delete a VLAN configuration:

1. From the main menu, choose Application > VLAN > VLAN Configuration.

   The VLAN Configuration page opens (Figure 68).

2. In the VLAN Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the VLAN configuration.
   - Click Cancel to return to the VLAN Configuration page without making changes.

Note: You cannot delete VLAN 1.

Configuring broadcast domains

You can configure specified VLAN switch ports with the appropriate PVID/VLAN association that enables the creation of broadcast domains. If you have enabled automatic PVID, you can change the PVID number on this screen. You can configure specified switch ports to filter (discard) all received tagged frames, untagged frames, or unregistered frames. You can also prioritize the order in which the switch forwards untagged packets, on a per-port basis.

To configure broadcast domains:

1. From the main menu, choose Application > VLAN > Port Configuration.

   The Port Configuration page opens (Figure 76).

Figure 76 Port Configuration page

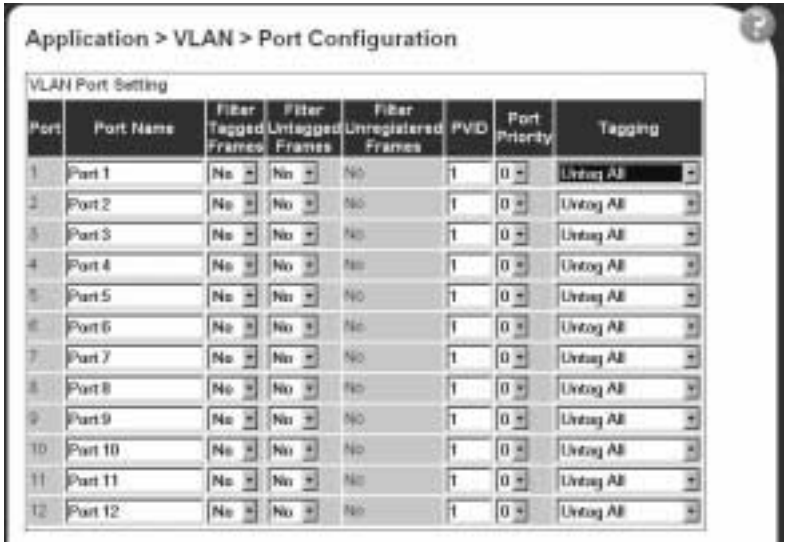


Table 68 describes the items on the Port Configuration page.

Table 68 Port Configuration page items

Item	Range	Description
Port	1..28	The port number.
Port Name	1..16	Type character string to create a unique port name, for example, Unit 1, Port 1.
Filter Tagged Frames	(1) Yes (2) No	Choose how to process filter tagged frames. When a flag is set (Yes), the frames are discarded by the forwarding process. When the flag is reset, the frames are processed normally. The default setting is No (frames are not discarded).
Filter Untagged Frames	(1) Yes (2) No	Choose how to process filter untagged frames. When a flag is set, the frames are discarded by the forwarding process. The default setting is No (no frames discarded).
Filter Unregistered Frames	(1) Yes (2) No	Displays yes/no if a flag is set. If yes, unregistered frames are discarded by the forwarding process. When the flag is reset, unregistered frames are processed normally. The default settings is No.

Table 68 Port Configuration page items (continued)

Item	Range	Description
PVID	1..4094	Type the number of the VLAN ID to assign to untagged frames received on this trunk port. For example, a port with a PVID of 3 assigns all untagged frames received on this port to VLAN 3. The default setting is 1. Note: If AutoPVID is enabled and you want another PVID, enter the desired PVID here.
Port Priority	0-7	Choose the level of priority for each port.
Tagging	(1) Untag All (2) Tag All (3) Untag PVID Only (4) Tag PVID Only	Choose the egress tagging for each port.

2 In the upper-left hand corner, click on the unit number of the switch to monitor.

3 Type information in the text boxes, or select from a list.

4 Click Submit.

Viewing VLAN port information

You can view VLAN information about a selected switch port.

To view VLAN port information:

1 From the main menu, choose Application > VLAN > Port Information.

The Port Information page opens (Figure 77).

Figure 77 Port Information page

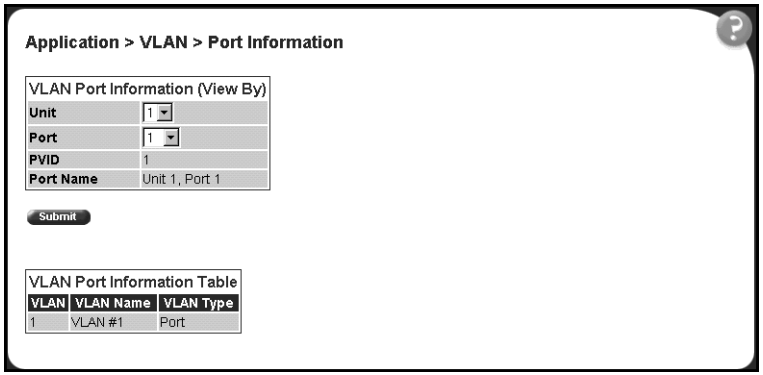


Table 69 describes the items on the Port Information page.

Table 69 Port Information page items

Section	Item	Range	Description
VLAN Port Information (View By)	Unit	1..8	Choose the number of the switch to view.
	Port	1..28	Choose the number of the switch's port to view.
	PVID		The PVID assigned when the VLAN port was created.
	Port Name		The port name assigned when the VLAN port was created.
VLAN Port Information Table	VLAN		The number assigned to the VLAN when it was created.
	VLAN Name		The name assigned to the VLAN when it was created.
	VLAN Type		The VLAN type assigned to the VLAN when it was created.

2 In the VLAN Port Information (View By) section, enter the unit and port number of the VLAN you want to view.

3 Click Submit.

The results of your request are displayed in the VLAN Port Information Table (Figure 77).

Managing spanning tree groups

You can configure system parameters for Spanning Tree Protocol, the industry standard for avoiding loops in switched networks. You can configure individual switch ports or all switch ports for participation in the spanning tree algorithm (STA).

Note: STP resolves duplicate paths in networks and is not necessary for ports that have workstations directly attached to the switch. When STP is enabled on these ports (the default), workstations are unable to attach to servers for a few seconds while STP stabilizes.

With software version 1.2 and higher, the BPS 2000 supports multiple instances (8) of spanning tree groups (STGs) running simultaneously, either all in one standalone switch or across a Pure BPS 2000 Stack. Each STG sends its own Bridge Protocol Data Units (BPDUs), and each STG must be independently configured.

With software version 2.0 and higher, you can choose which VLAN in the STG will send the tagged BPDU.

Note: You must be in Pure BPS 2000 Stack mode in the Stack Operational Mode screen to enable more than 1 STG. If you change to Hybrid mode, you lose all but the default STG.

In the default configuration of the BPS 2000, a single STG with the ID of 1 includes all ports on the switch. It is called the Default STG and sends only untagged BPDUs in order to operate with all devices that support only one instance of STP. Although ports can be added to or deleted from the Default STG, the Default STG itself **cannot** be deleted from the system. All other STGs, except the Default STG, must be created by the user.

Note: To become active, each STG must be enabled by the user after creation. For guidelines on configuring, refer to *Using the Business Policy Switch 2000 Software Version 2.5*.

Beginning with software version 2.0, you can set the spanning tree priority and path cost for each individual port. Beginning with software version 2.0.5, you can set the STG Multicast MAC address.

Creating spanning tree groups

To configure spanning tree groups:

1 From the main menu, choose Application > Spanning Tree > Group Configuration.

The Group Configuration page opens (Figure 78).

Figure 78 Spanning Tree Group Configuration page

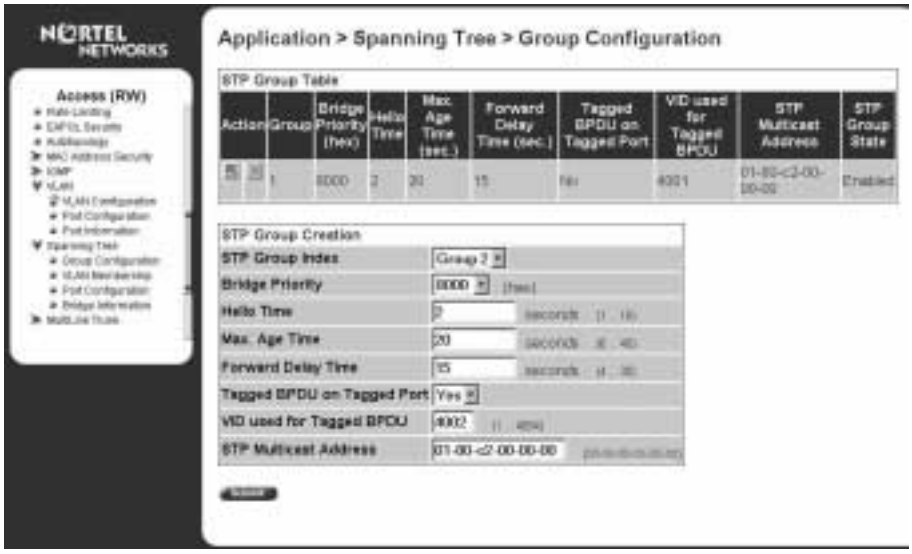


Table 70 describes the items on the Spanning Tree Group Configuration page.

Table 70 Spanning Tree Group Configuration page items

Section	Item	Description
STP Group Table		Deletes the group.
	Group	The number assigned to the spanning tree group when the group was created.
	Bridge Priority	For the STP Group, indicates the management-assigned priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. The spanning tree algorithm uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values.
	Hello Time	For the STP Group, indicates the Hello Interval (the amount of time between transmissions of BPDUs) specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge. Note that, although you can set the Hello Interval for a bridge using bridge management software, once the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network.
	Max. Age time (sec.)	For the STP Group, specifies the maximum age (in seconds) that a Hello message can attain before it is discarded. This parameter, specified by management for this bridge, takes effect only when the bridge becomes the root bridge. Note that, if this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network.
	Forward Delay Time (sec.)	For the STP Group indicates the Forward Delay parameter value specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge. The Forward Delay parameter value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. Note that all bridges participating in the spanning tree network use the root bridge's Forward Delay parameter value.
	Tagged BPDU on Tagged Port	Displays whether you are sendin]g either tagged or untagged BPDUs from a tagged port.
	VID used for Tagged BPDU	Displays the VLAN ID you are sending the tagged BPDUs for the specified STG to.
	STPG State	The current operational state of the spanning tree group: Enabled or Disabled.

Table 70 Spanning Tree Group Configuration page items (continued)

Section	Item	Description
STP Group Creation	STP Group Index	Choose the group number you want to create.
	Bridge Priority	Enter the priority you want.
	Hello Time	Enter the hello time you want for this STG in seconds; range is 1 to 10.
	Max. Age time (sec.)l	Enter the maximum age time you want for this STG in seconds; range is 6 to 40.
	Forward Delay Time (sec.)	Enter the forward delay time you want for this STG in seconds; range is 4 to 30.
	Tagged BPDU on Tagged Port	Set the frames as tagged (Yes) or untagged (No) on tagged ports.
	VID used for Tagged BPDU	Enter the VLAN ID you want to send the tagged BPDUs for the specified STG. Note: The default VIDs are 4001 through 4008 for STG 1 through 8, respectively.
	STP Multicast Address	Enter the STP Multicast MAC address.

2 Complete the fields as shown.

3 Click Submit.

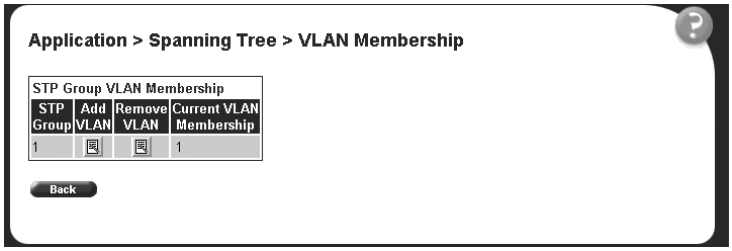
Associating STG with VLAN membership

To add a VLAN to an STG:

1 From the main menu, choose, Application > Spanning Tree > VLAN Membership.

The Spanning Tree VLAN Membership page opens (Figure 79).

Figure 79 Spanning Tree VLAN Membership page



The table displays the spanning tree group and the current VLAN membership.

You can add or remove one or more VLANs to an STG.

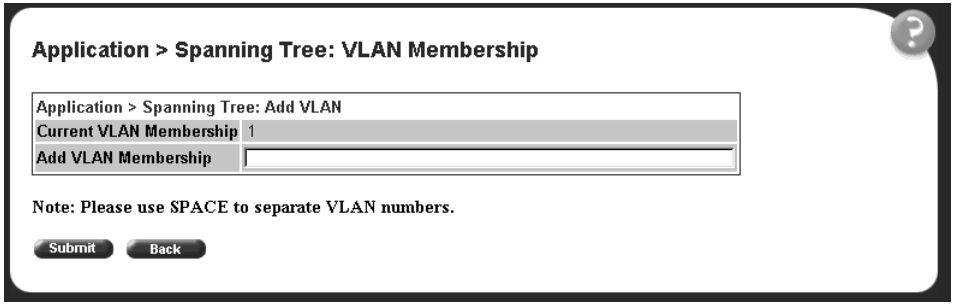
Note: Beginning with software version 2.0, you can move a VLAN from one STG to another by simply adding the VLAN to the specified STG. You no longer must remove the VLAN from the previous STG first.

2 To add a VLAN:

a Click the modification icon in the Add VLAN column.

The Spanning Tree VLAN Membership Add VLAN page opens (Figure 80).

Figure 80 Spanning Tree Add VLAN page



b Enter the number of the VLAN(s) you want to add to the STG.

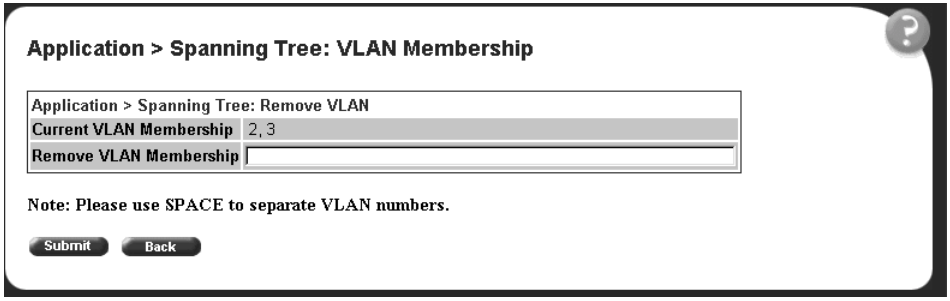
c Click Submit.

3 To remove a VLAN:

a Click the modification icon in the Remove VLAN column.

The Spanning Tree VLAN Membership Remove VLAN page opens (Figure 81).

Figure 81 Spanning Tree Remove VLAN page



b Enter the number of the VLAN(s) you want to remove to the STG.

c Click Submit.

Note: You cannot delete VLAN 1 from STG 1.

Configuring ports for spanning tree

To configure switch ports for Spanning Tree participation:

1 From the main menu, choose Application > Spanning Tree > Port Configuration.

The Spanning Tree Port Configuration page opens (Figure 82).

Figure 82 Spanning Tree Port Configuration page

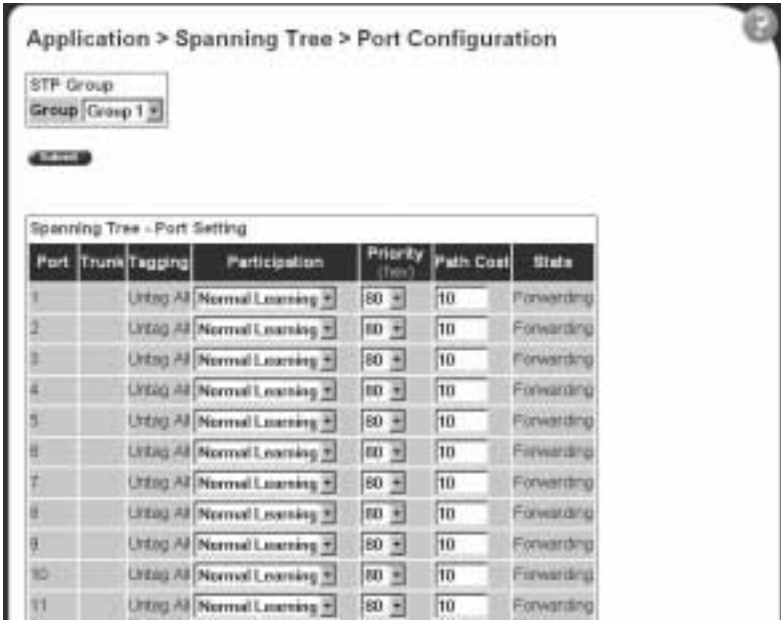


Table 71 describes the items on the Spanning Tree Port Configuration page.

Table 71 Spanning Tree Port Configuration page items

Section	Item	Description
STP Group	Group	Choose the STG Group you want to view.
Spanning Tree - Port Setting	Port	The port number of the currently displayed unit.
	Trunk	The trunk that corresponds to the switch ports specified as MLT members.
	Tagging	Displays the egress tagging settings for the port.
	Participation	Choose any (or all) of the switch ports for Spanning Tree participation.Your options are: (1) Normal Learning (2) Fast Learning (3) Disabled Note: When an individual port is a trunk member, changing this setting for one of the trunk members changes the setting for all members of that trunk. Consider the effect changing this value has in your network topology before making changes. The default settings is Normal Learning.

Table 71 Spanning Tree Port Configuration page items

Section	Item	Description
	Priority	The bridge spanning tree parameter that prioritizes the port's lowest path cost to the root. When one or more ports have the same path cost, the STA selects the path with the highest priority (lowest numerical value).
	Path Cost	The bridge spanning tree parameter that determines the lowest path cost to the root.
	State	The current state of the port as defined by application of the Spanning Tree Protocol. This state controls what action a port takes on reception of a frame. Note: If the bridge has detected a port that is malfunctioning, it will place that port into the broken (6) state. For ports which are disabled, this object will have a value of disabled (1).

2. Using the Spanning Tree - Port Settings fields, in the port row(s) of your choice, choose to enable STP (normal learning or fast learning) or disable STP.
3. Enter the spanning tree priority value for the specified port.

   You do not have to enter a value if you want to use the default priority of 128.
4. Enter the spanning tree path cost value for the specified port.

   You do not have to enter a value if you want to use the default path cost of 10.
5. Click Submit.

Changing spanning tree bridge switch settings

You can view and configure existing Spanning Tree switch settings.

To configure Spanning Tree switch settings:

1. From the main menu, choose Application > Spanning Tree > Bridge Information.

   The Spanning Tree Bridge Information page opens (Figure 83).

Figure 83 Spanning Tree Bridge Information page

Table 72 describes the items on the Spanning Tree Bridge Information page.

Table 72 Spanning Tree Bridge Information page items

Section	Item	Range	Description
STP Group	Group		Choose the STP Group you want to work with.
Spanning Tree - Bridge Information	Bridge Priority	0..0xFFFF	Type the priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. The Spanning Tree Algorithm uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values compared first, followed by the hardware addresses. The default setting is 8000.
	Designated Root	XXXXXXX XXXXXXX	The bridge ID of the root bridge, as determined by the Spanning Tree Algorithm.
	Root Port	1..28	The port number of the port which offers the lowest cost past from this bridge to the root bridge.
	Root Path Cost	Integer	The cost of the path to the root as seen from this bridge.

Table 72 Spanning Tree Bridge Information page items

Section	Item	Range	Description
	Hello Time	1..10 seconds	The actual Hello Interval, the amount of time between transmissions of configuration Bridge Protocol Data Units (BPDUs) that the root bridge is currently using. Note: Bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. See also Bridge Hello Time.
	Maximum Age Time	6..40 seconds	The Maximum Age Time parameter value that the root bridge is currently using. This value specifies the maximum age that a Hello message can attain before it is discarded. Note: The root bridge's Maximum Age Time parameter value becomes the actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. See also Bridge Maximum Age Time.
	Forward Delay	4..30 seconds	The Forward Delay parameter value that the root bridge is currently using. This value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. Note: The root bridge's Forward Delay parameter value becomes the actual Forward Delay parameter value for all bridges participating in the spanning tree network. See also Bridge Forward Delay.
	Bridge Hello Time	1..10 seconds	The Hello Interval (the amount of time between transmissions of BPDUs) specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge. Note: Although you can set the Hello Interval for a bridge using bridge management software, once the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network. See also Hello Time. The default setting is 2 seconds.
	Forward Delay	4..30 seconds	The Forward Delay parameter value that the root bridge is currently using. This value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. Note: The root bridge's Forward Delay parameter value becomes the actual Forward Delay parameter value for all bridges participating in the spanning tree network. See also Bridge Forward Delay.

Table 72 Spanning Tree Bridge Information page items

Section	Item	Range	Description
	Bridge Hello Time	1..10 seconds	The Hello Interval (the amount of time between transmissions of BPDUs) specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge. Note: Although you can set the Hello Interval for a bridge using bridge management software, once the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network. See also Hello Time. The default setting is 2 seconds.
	Tagged BPDU on Tagged Port	(1) Yes (2) No	Displays whether you are sendin]g either tagged or untagged BPDUs from a tagged port.
	VID used for Tagged BPDU	1-4094	Displays the VLAN ID you are sending the tagged BPDUs for the specified STG to.

2 Type information in the text boxes, or select from a list.

3 Click Submit.

Configuring MultiLink Trunk (MLT) members

You can configure groups of links between the BPS 2000 and another switch or a server to provide higher bandwidth with active redundant links. Trunked ports can span multiple units of the stack for fail-safe connectivity to mission-critical servers and the network center.

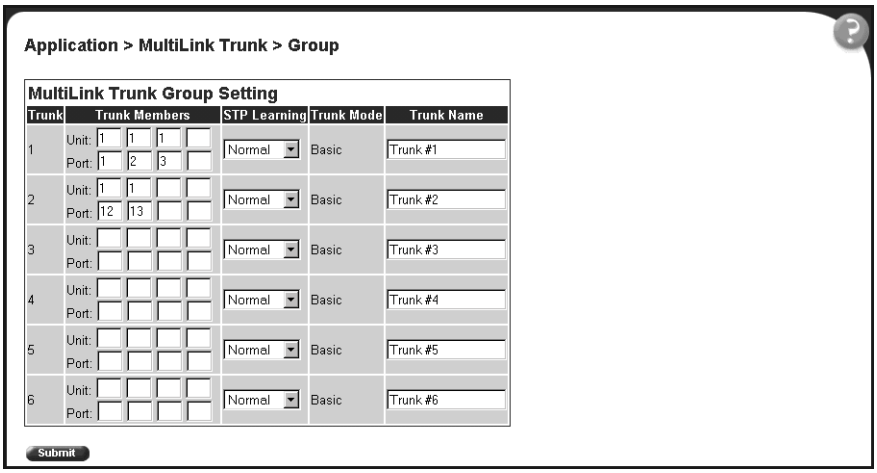
You can configure two to four switch ports together as members of a trunk to a maximum of six trunks.

To configure MultiLink Trunk members:

1 From the main menu, choose Application > MultiLink Trunk > Group.

The Group page opens (Figure 84).

Figure 84 Group page



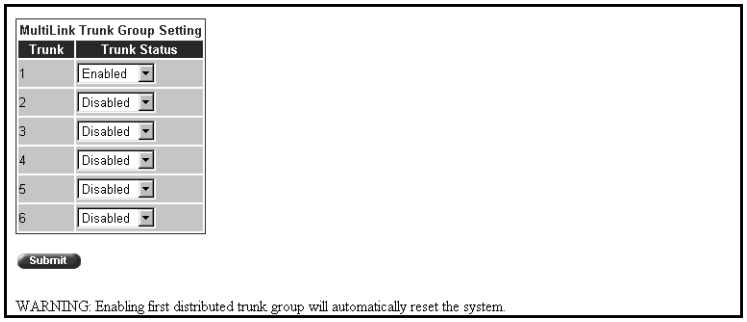


Table 73 describes the items on the Group page.

Table 73 Group page items

Section	Item	Range	Description
MultiLink Trunk Group Setting	Trunk	1..6	This column contains fields in each row that can be configured to create the corresponding trunk. The Unit value in the (Unit/Port) field is configurable only when the switch (unit) is part of a stack configuration. It indicates that the trunk members in this row are associated with the specified unit number configured in the Unit field. Each switch port can only be a member of a single trunk. The appropriate trunk number for each trunk member configured within this field is shown adjacent to the corresponding switch port on the following management pages: Port Configuration (see Figure 41 on page 106) and Spanning Tree Configuration (see Figure 76 on page 179). There are no default settings.
	Trunk Port Members	Unit: 1..8 Port: 1..28	Type the switch and port numbers to associate with the corresponding trunk. Note: You can configure two to four switch ports together as members of a trunk to a maximum of six trunks. Switch ports can only be assigned a member of a single trunk. There are no default settings.
	STP Learning	(1) Normal (2) Fast (3) Disabled	Choose the parameter that allows the specified trunk to participate in the spanning tree. This setting overrides those of the individual trunk members. Selecting Fast shortens the state transition timer by two seconds. The default setting is Normal.
	Trunk Mode	Basic	The default operating mode of the switch. When in Basic mode, source MAC addresses are dynamically assigned to specific trunk members for flooding and forwarding. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.
	Trunk Name	1..20	Type a character string to create a unique name to identify the trunk, for example, Trunk1. The name, if chosen carefully, can provide meaningful information to you. For example, S1:T1 to FS2 indicates that Trunk1, in Switch1 connects to File Server 2.
MultiLink Trunk Group Setting	Trunk Status	(1) Enabled (2) Disabled	Choose to enable or disable any of the existing MultiLink Trunks. Note: When a trunk is not active (Trunk Status field set to Disabled), configuration changes do not take effect until you set the Trunk Status field to enabled.

2 Type information in the text boxes, or select from a list.

3 Click Submit in any section to save your changes.

Monitoring MLT traffic

You can monitor the bandwidth usage for the MultiLink Trunk member ports within each trunk in your configuration by selecting the traffic type to monitor.

To monitor MultiLink Trunk traffic:

1 From the main menu, choose Application > MultiLink Trunk > Utilization.

The Utilization page opens (Figure 85).

Figure 85 Utilization page

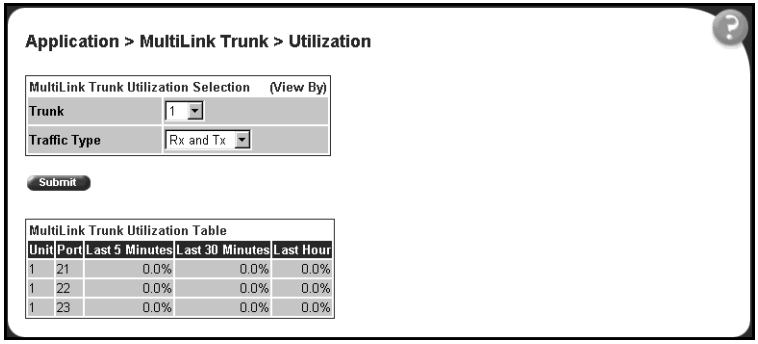


Table 74 describes the items on the Utilization page.

Table 74 Utilization page items

Section	Item	Range	Description
MultiLink Trunk Utilization Selection (View By)	Trunk	1..6	Choose the trunk to be monitored.
	Traffic Type	(1) RX and TX (2) RX (3) TX	Choose the traffic type to be monitored for percentage of bandwidth utilization.

Table 74 Utilization page items (continued)

Section	Item	Range	Description
MultiLink Trunk Utilization Table	Unit/Port		A list of the trunk member switch ports that correspond to the trunk specified in the Trunk column.
	Last 5 Minutes%		The percentage of packets (of the type specified in the Traffic Type field) used by the port in the last five minutes. This field provides a running average of network activity, and is updated every 15 seconds.
	Last 30 Minutes%		The percentage of packets (of the type specified in the Traffic Type field) used by the port in the last 30 minutes. This field provides a running average of network activity, and is updated every 15 seconds.
	Last Hour%		The percentage of packets (of the type specified in the Traffic Type field) used by the port in the last 60 minutes. This field provides a running average of network activity, and is updated every 15 seconds.

2 In the MultiLink Trunk Utilization Selection section, type the Trunk number and traffic type to be monitored.

3 Click Submit.

The results of your request are displayed in the MultiLink Trunk Utilization Table (Figure 85).

Chapter 8
Implementing QoS Using QoS Wizard and QoS Quick Config

You can configure Quality of Service (QoS) features in your network by using the Web-based QoS Wizard, using the QoS Quick Config pages, or using the Advanced QoS configuration pages available in the Web-based management user interface.

This chapter shows how to use the QoS Wizard and QoS Quick Config pages to configure QoS parameters for the BPS 2000. (Refer to Chapter 9 for information on configuring QoS using the Advanced QoS Web pages.)

This chapter covers the following topics:

Note: To configure the features introduced with software version 1.2 and higher in a mixed stack, you must access a BPS 2000 unit.

Using QoS Wizard

The QoS Wizard provides a set of Web pages that allows you to specify common QoS settings for the BPS 2000.

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

This section discusses the following topics:

Note: All the settings you configure with QoS Wizard are actually set when you click the final Finish and see the Session Confirmation page.

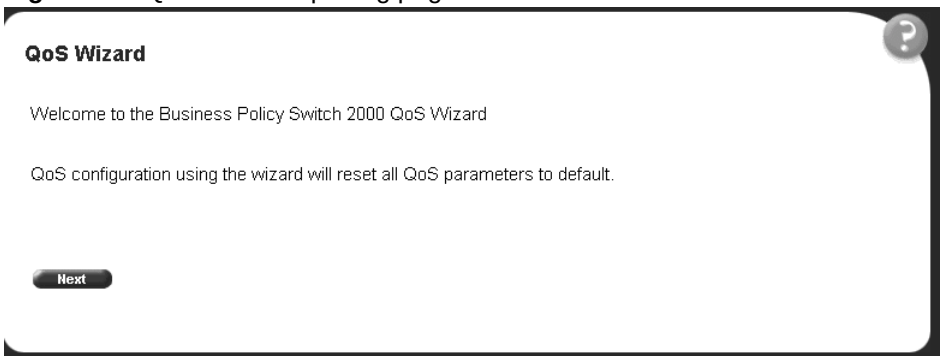
Configuring Standard traffic with the QoS Wizard

To use the QoS Wizard to configure Standard traffic:

1 From the main menu, choose Application > QoS > QoS Wizard.

The QoS Wizard opens (Figure 86).

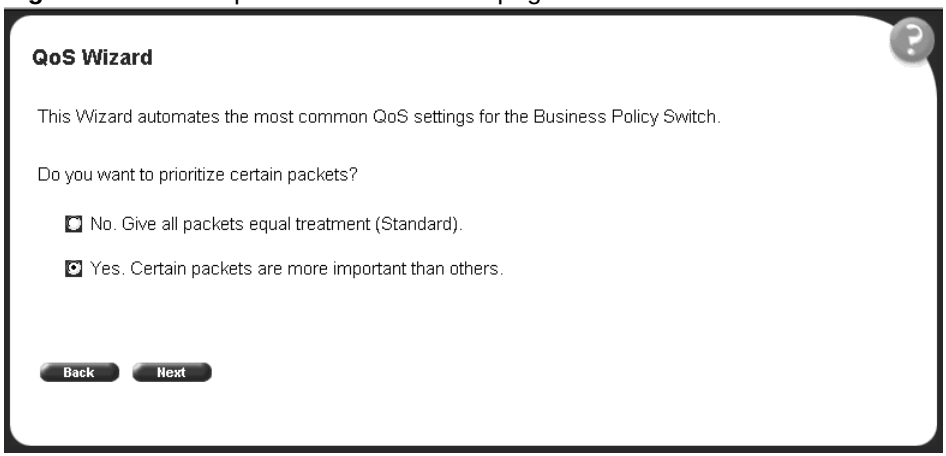
Figure 86 QoS Wizard opening page



2 To continue the configuration process, click Next.

A packet prioritization selection page opens (Figure 87).

Figure 87 Packet prioritization selection page



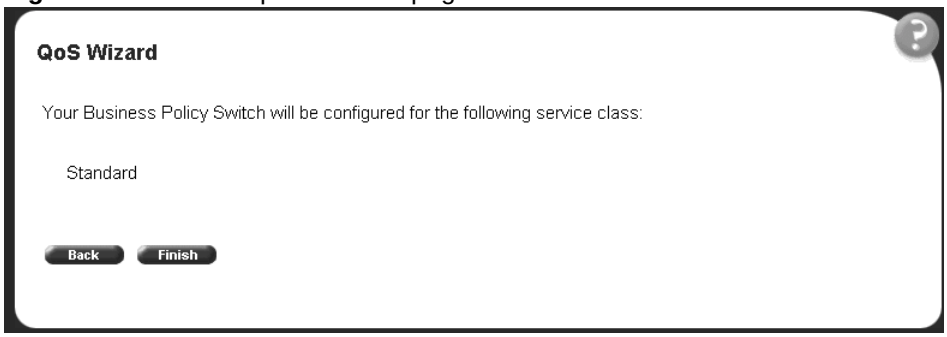
3 Select No.

4 Click Next.

A Standard prioritization page opens (Figure 88).

Note: If you want to prioritize traffic, skip this step and continue the steps outlined in "Prioritizing traffic with the QoS Wizard."

Figure 88 Standard prioritization page



5 To complete the configuration process, click Finish.

The session confirmation page appears (Figure 89).

Figure 89 Session confirmation page

Prioritizing traffic with the QoS Wizard

You can specify that different types of traffic in your network configuration be marked with different priority levels.

The QoS Wizard allows you to prioritize traffic flows by:

- VLAN
- IP application
- User defined flow

Using the QoS Wizard, you can prioritize traffic by one of these categories, by two categories, or by all three. Also, you can define more than one flow in each category. The QoS Wizard leads you through the following four general steps in defining each flow you want to prioritize:

- Step 1 is setting the category of prioritized traffic flow—VLAN, IP Application, or User defined flow.

  The User defined flow has two steps in classifying the flow:

  — Policy Label

  — Policy Definition
- Step 2/3 is setting a Meter for the flow, if you want
- Step 3/4 is choosing the Service Class or Drop for the flow

  If you are metering traffic within the flow, you choose two separate Service Classes: one for In-Profile traffic, and one for Out-of-Profile traffic. If you are not metering traffic within the flow, you choose only one Service Class.
- Step 4/5 is setting a Shaper, or shaping criteria, for the flow, if you want

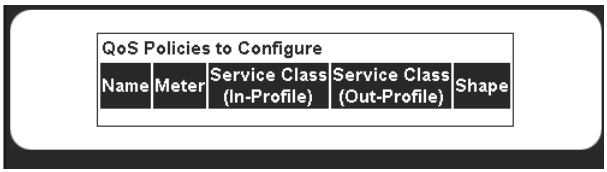
Note: You must be using either the BPS2000-1GT, BPS2000-2GT, or BPS2000-2GE MDA with the Business Policy Switch in order to implement the QoS shaping features.

The QoS Wizard automatically steps you through each of these four steps for each flow you want to prioritize. You can prioritize flows within three different categories and more than one flow per category. When you fill the resources of one category, you will not be prompted again, and you see a check mark next to that category if there are some flows to be configured or an X mark next to that category if there are no flows to be configured in the packet prioritization screen (Figure 91). You will be unable to configure more flows for that category. Should you fill the QoS Wizard resources, you will not be prompted again.The QoS Wizard automatically presents screens to configure each prioritized traffic flow.

Additionally, the packet prioritization screen has a Status button that displays a QoS Policies to Configure in a pop-up window (Figure 90). As you finish configuring each type of flow, this pop-up window displays with the configured flows you configure using the QoS Wizard listed. When you completely finish the QoS Wizard, the policies are implemented.

Note: The system configures the QoS parameters you configure using the QoS Wizard only when you click Finish.

Figure 90 QoS Policies to Configure window



The QoS Policies to Configure table has the following fields:

— Name—Displays the name of the policy.

— Meter—Displays whether you are metering the data in the flow associated with the policy.

— Service Class (In-Profile)—Displays the service class of the flow associated with the policy. If you are metering the data, this is the service class for the data that fits the metered profile.

— Service Class (Out-Profile)—Displays the service class of metered data that falls outside the profile.

— Shape—Displays whether you are shaping the data in the flow associated with the policy.

To assign priority levels to different types of network traffic:

1 From the main menu, choose Application > QoS > QoS Wizard.

The QoS Wizard opens (Figure 86).

2 To continue the configuration process, click Next.

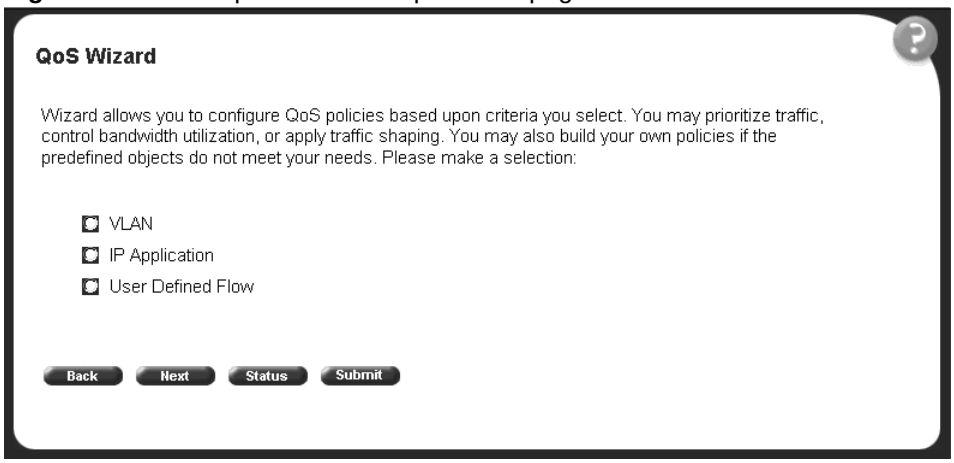
A packet prioritization selection page opens (Figure 87).

3 Select Yes.

4 Click Next.

A packet prioritization explanation page opens (Figure 91).

Figure 91 Packet prioritization explanation page



a To see the policies you have configured, click Status.

The QoS Policies to Configure table opens in a pop-up window (Figure 90).

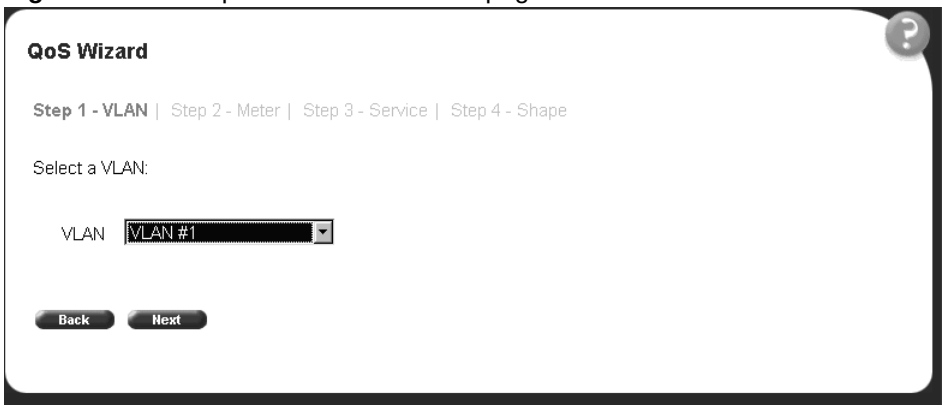
Prioritizing VLANs with the QoS Wizard

You can specify that different VLANs in your network configuration be marked with different priority levels.

1 In the packet prioritization window (Figure 91), click VLAN, and click Next.

A VLAN prioritization selection page opens (Figure 92).

Figure 92 VLAN prioritization selection page



2 Choose the VLAN and click Next.

A page opens (Figure 93) that asks if you want to set a Meter for the specified VLAN.

Figure 93 Meter for VLAN page

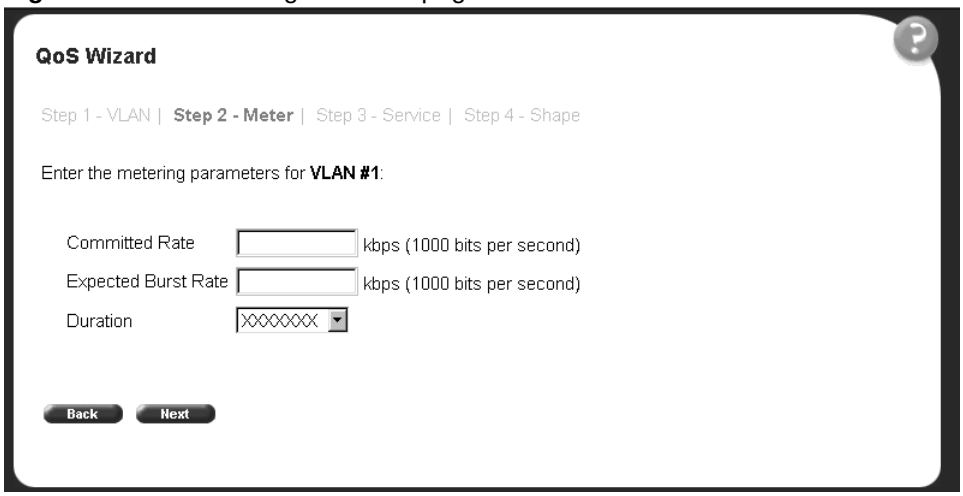
3 If you do not want to set a Meter, click No.

The system opens to the Service Class selection page (Figure 95), which appears with only one Service Class to set. You do not have In-Profile and Out-of-Profile without metering data.

4 If you want to set a Meter, click Yes.

A page opens (Figure 94) that allows you to set a Meter for the specified VLAN.

Figure 94 Meter setting for VLAN page



5 Enter the committed rate you want for this Meter.

6 Enter the expected burst rate you want for this Meter.

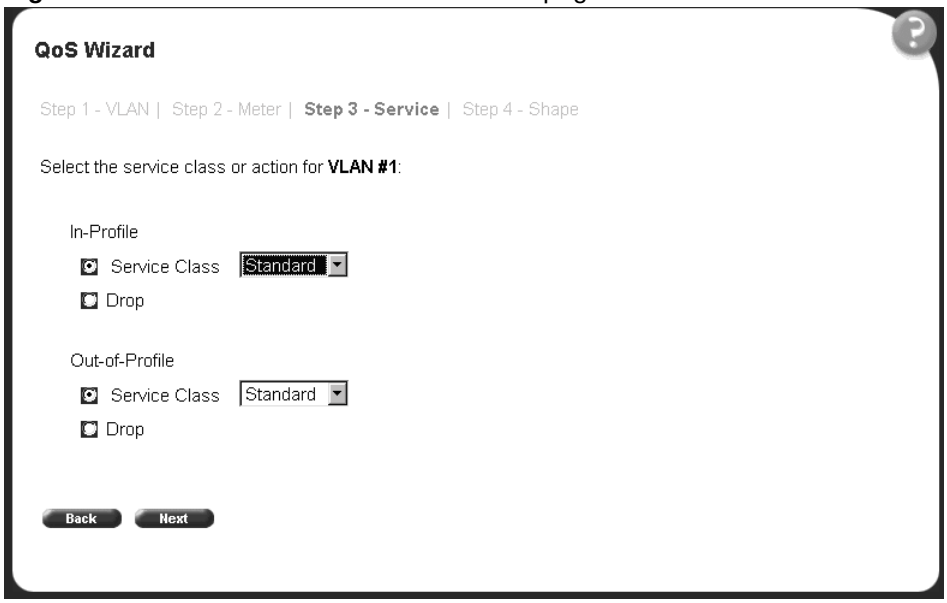
The system calculates a series of 7 or fewer possible durations for the committed and expected burst rates you set.

7 Choose the Duration you want.

8 Click Next.

A page opens (Figure 95) that allows you to select a Service Class separately for both the In-Profile and Out-of-Profile Action for the specified VLAN.

Figure 95 Service Class selection for VLAN page



9 Click either Service Class or Drop.

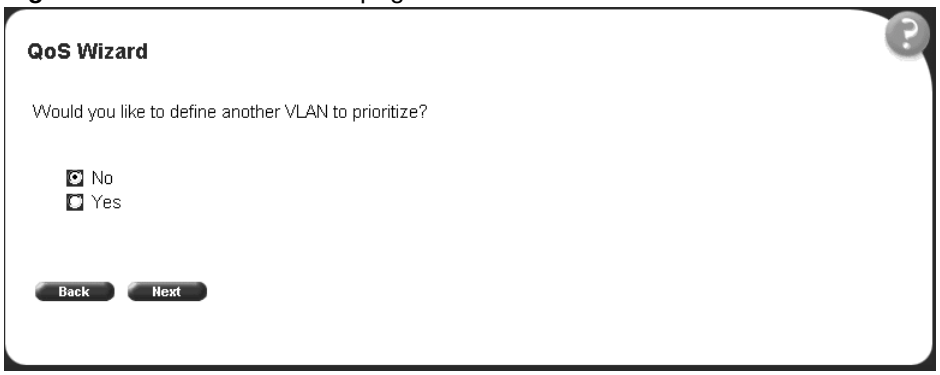
If you click Service Class, choose the Service Class you want from the pull-down menu.

If you click Drop, the traffic in the specified VLAN is dropped.

10 Click Next.

A page opens (Figure 96) that asks you if you want to prioritize traffic for another VLAN. If you fill the resources of the QoS Wizard, you will not be prompted for another VLAN.

Figure 96 Additional VLANs page



11 If you want to prioritize traffic for another VLAN, click Yes and Next.

The system returns you to the VLAN prioritization page (Figure 92), and you continue through steps 1 to 17 for the next VLAN.

12 If you do not want to prioritize traffic for another VLAN, click No and Next.

The system returns you to the packet prioritization page (Figure 97), with a check mark next to VLAN,. If you click Status, the QoS Policies to Configure table listing your new entry simultaneously appears in a pop-up window (Figure 98).

Figure 97 Packet prioritization page with prioritized VLAN(s)

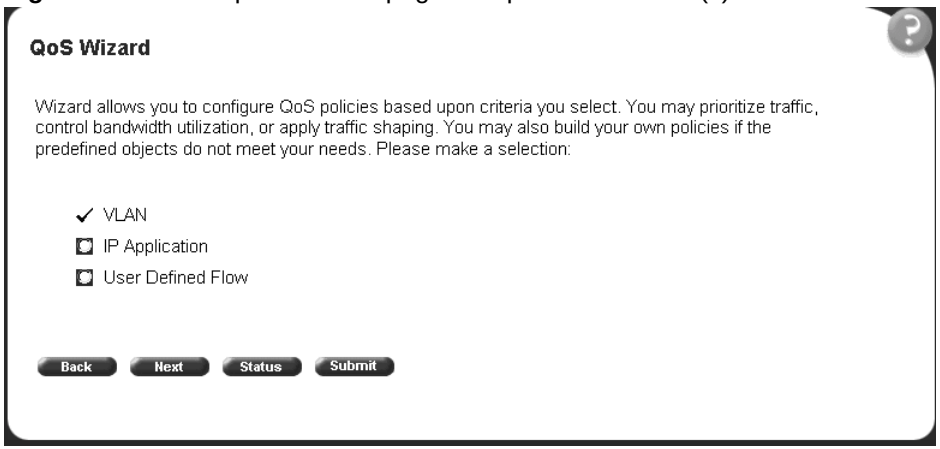
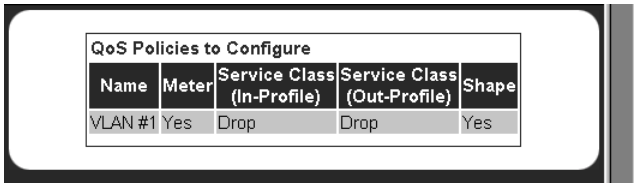


Figure 98 QoS Policies to Configure window with VLAN entry



QoS Policies to Configure

Name	Meter	Service Class (In-Profile)	Service Class (Out-Profile)	Shape
VLAN #1	Yes	Drop	Drop	Yes

13 When you are through with the table, click Back, then click Submit.

You will see a session confirmation page.

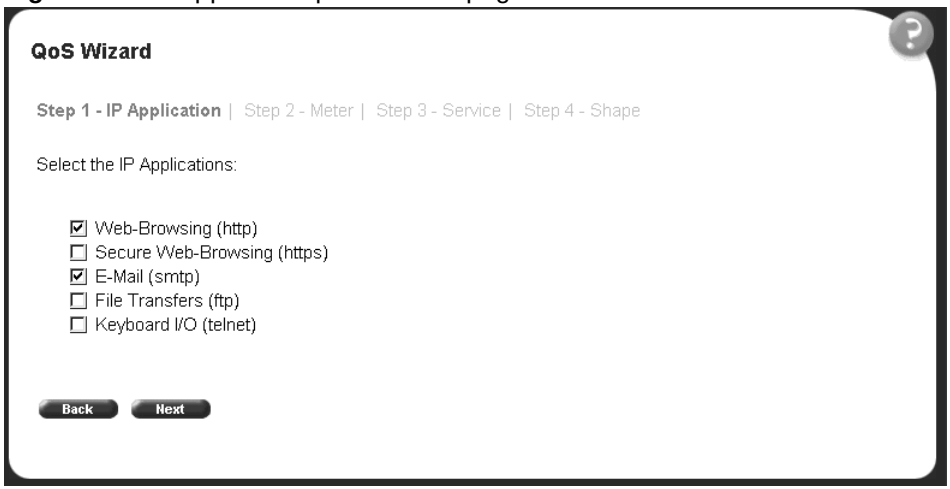
Prioritizing IP applications with the QoS Wizard

You can specify that different IP applications in your network configuration are marked with different priority levels.

1 In the packet prioritization window (Figure 91), click IP Application, and click Next.

An IP Application prioritization selection page opens (Figure 99).

Figure 99 IP Application prioritization page



2 Click the application(s) you want to prioritize and click Next.

A page opens (Figure 100) that asks if you want to set a Meter for the specified IP Application.

Figure 100 Meter for IP Application page

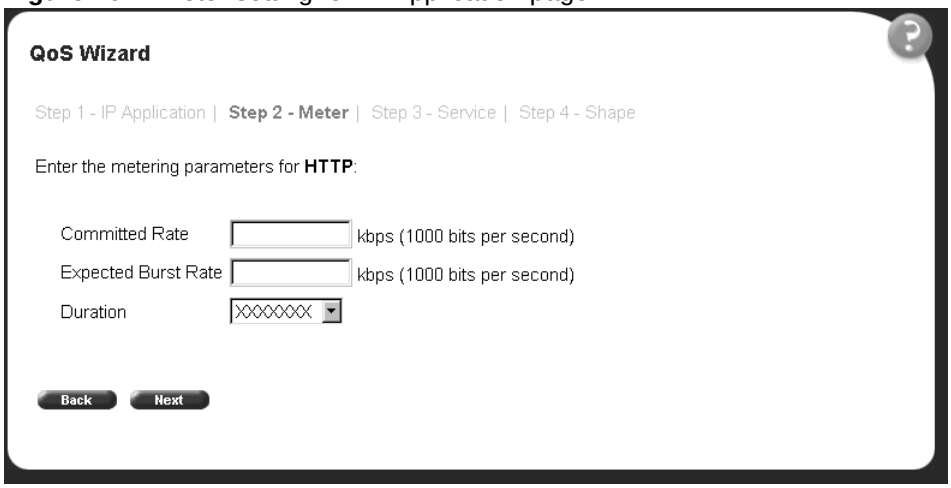
3 If you do not want to set a Meter, click No.

The system opens to the Service Class selection page (Figure 102), which appears with only one Service Class to set. You do not have In-Profile and Out-of-Profile without metering data.

4 If you want to set a Meter, click Yes.

A page opens (Figure 101) that allows you to set a Meter for the specified IP Application.

Figure 101 Meter setting for IP Application page



5 Enter the committed rate you want for this Meter.

6 Enter the expected burst rate you want for this Meter.

The system calculates a series of 7 or fewer possible durations for the committed and expected burst rates you set.

7 Choose the Duration you want.

8 Click Next.

A page opens (Figure 102) that allows you to select a Service Class separately for both the In-Profile and Out-of-Profile Action for the specified IP Application.

Figure 102 Service Class selection for IP Application page

9 Click either Service Class or Drop.

If you click Service Class, choose the Service Class you want from the pull-down menu.

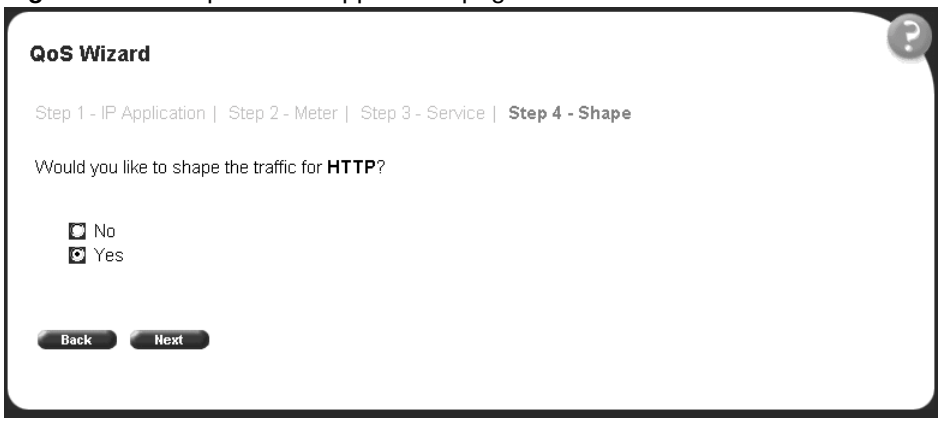
If you click Drop, the traffic in the specified IP Application is dropped.

10 Click Next.

A page opens (Figure 103) that allows you to set shaping criteria for the specified IP Application.

Note: You must be using either the BPS2000-1GT, BPS2000-2GT, or BPS2000-2GE MDA with the Business Policy Switch in order to implement the QoS shaping features.

Figure 103 Shaper for IP Application page



11 If you do not want to shape traffic for the specified IP Application, click No.

a If you chose more than one IP Application to prioritize, a page opens that asks if you want to set a Meter for the next specified IP Application (Figure 100). Repeat steps 3 through 17 for each IP Application you chose.

b If you chose just one IP Application, you have completed the QoS Wizard prioritization process for that flow. Go to The system returns you to the packet prioritization page (Figure 105), with a check mark next to IP Application,

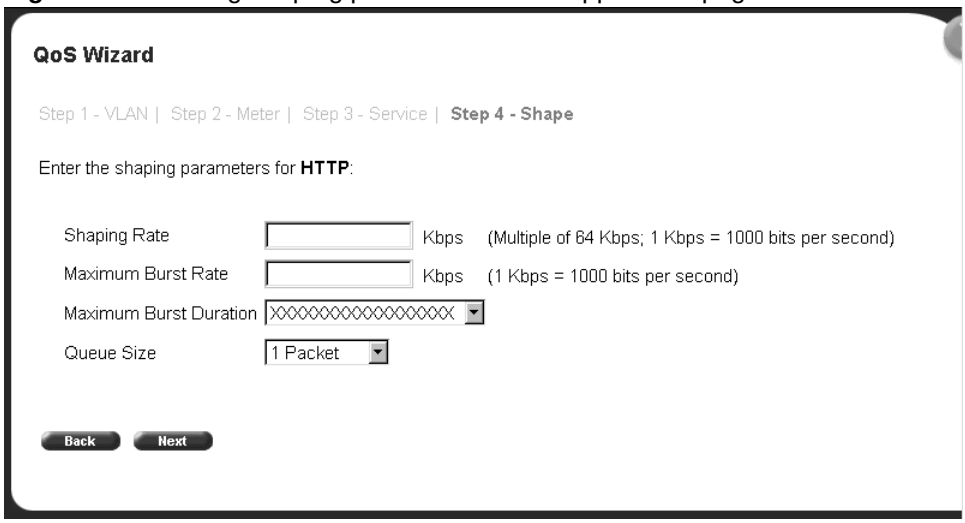
If you fill the resources of the QoS Wizard, you will not be prompted for another IP Application.

If you click Status, the QoS Policies to Configure table listing your new entry simultaneously appears in a pop-up window (Figure 106).

12 If you want to shape traffic for the specified IP Application, click Yes.

A page opens (Figure 104) that allows you to set shaping parameters for the specified IP Application.

Figure 104 Setting shaping parameters for IP Application page



13 Enter the shaping rate you want for this Shaper.

The system rounds up shaping rates you enter, including 0, to multiples of 64 Kbps.

14 Enter the maximum burst rate you want for this Shaper.

The system calculates a series of 6 or fewer possible durations for the shaping and maximum burst rates you set.

15 Choose the Maximum Burst Duration from the pull-down menu.

16 Choose the queue size you want for this Shaper.

17 Click Next.

a If you chose more than one IP Application to prioritize, a page opens that asks if you want to set a Meter for the next specified IP Application (Figure 100). Repeat steps 3 through 17 for each IP Application you chose.

b If you chose just one IP Application, you have completed the QoS Wizard prioritization process for that flow. The system returns you to the packet prioritization page (Figure 105), with a check mark next to IP Application. Press the Status button to view the QoS Policies to Configure table listing your new entry in a pop-up window (Figure 106).

If you fill the resources of the QoS Wizard, you will not be prompted for another IP Application.

Figure 105 Packet prioritization page with prioritized IP Application(s)

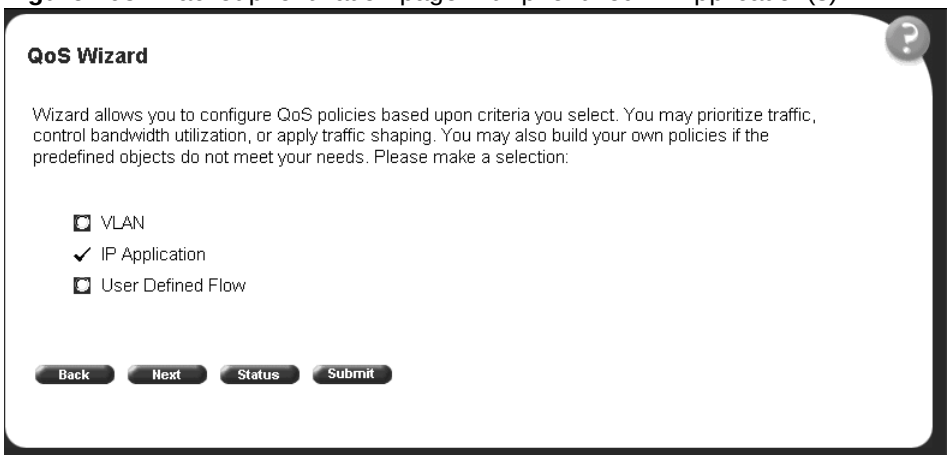
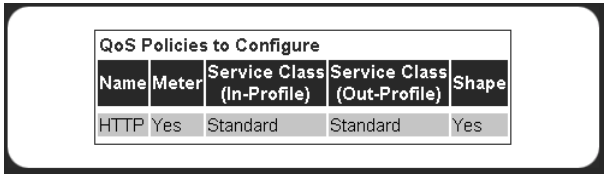


Figure 106 QoS Policies to Configure window with IP Application entry



QoS Policies to Configure

Name	Meter	Service Class (In-Profile)	Service Class (Out-Profile)	Shape
HTTP	Yes	Standard	Standard	Yes

18 When you are through viewing the table, click Back, then Submit.

You see a session confirmation page.

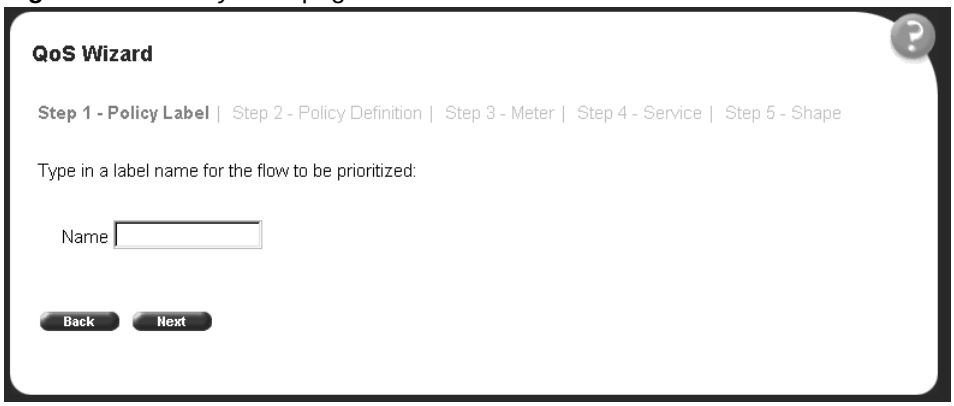
Prioritizing user defined flows with the QoS Wizard

You can specify that different user defined flows in your network configuration be marked with different priority levels.

1 In the packet prioritization window (Figure 91), click User Defined Flow, and click Next.

A page opens (Figure 107) that asks the user to assign a name to the flow.

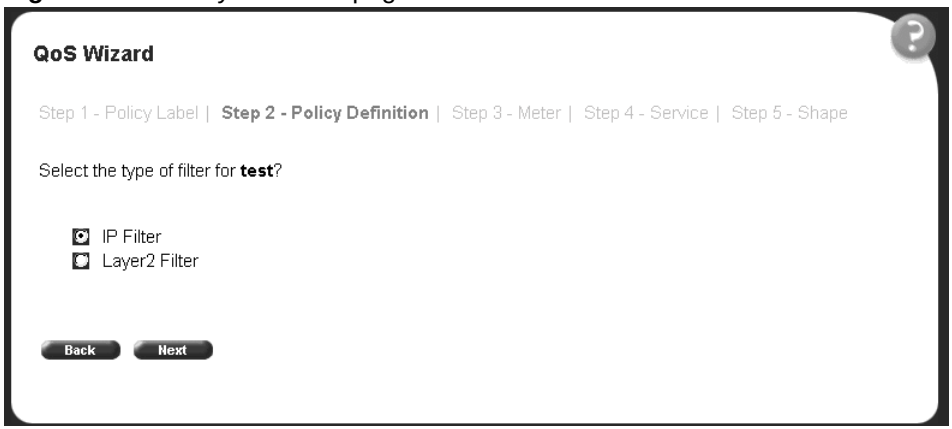
Figure 107 Policy label page



2 Enter the name of the flow and click Next.

A page opens (Figure 108) that asks if you want to set an IP filter or a layer 2 filter.

Figure 108 Policy definition page

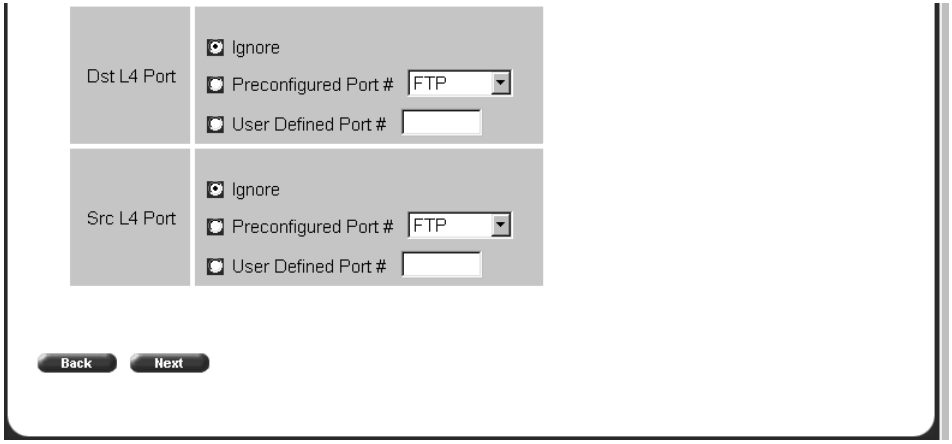


a If you want an IP filter, click IP Filter and click Next.

A page opens that requests the customer to choose the IP filter criteria for the specified flow (Figure 109 and Figure 110).

Figure 109 IP classification rules page (1 of 2)

Figure 110 IP classification rules page (2 of 2)



— Choose the IP filter parameters you want the flow to have. (Refer to Chapter 9 for a description of the parameters.)

— Click Next.

A page opens (Figure 113) that asks if you want to set a Meter for the specified flow.

b If you want a layer 2 filter, click Layer2 Filter and click Next.

A page opens that requests the customer to choose the layer 2 filter criteria for the specified flow (Figure 111 and Figure 112).

Figure 111 Layer 2 classification rules page (1 of 2)

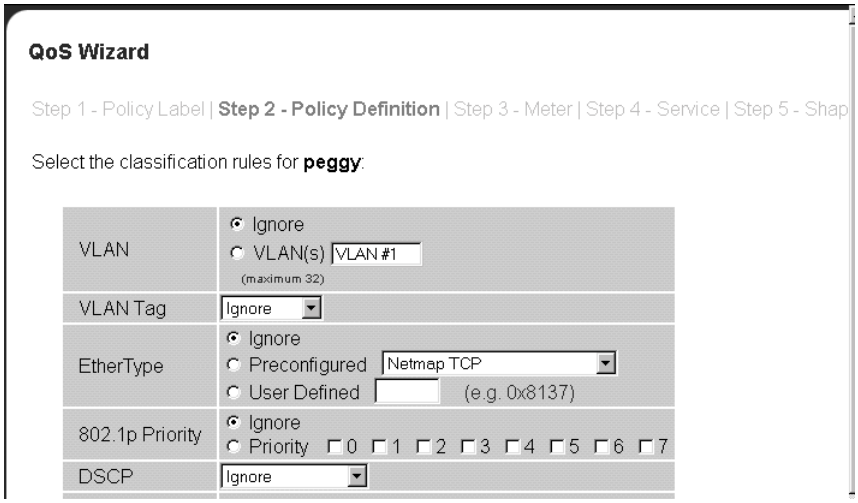
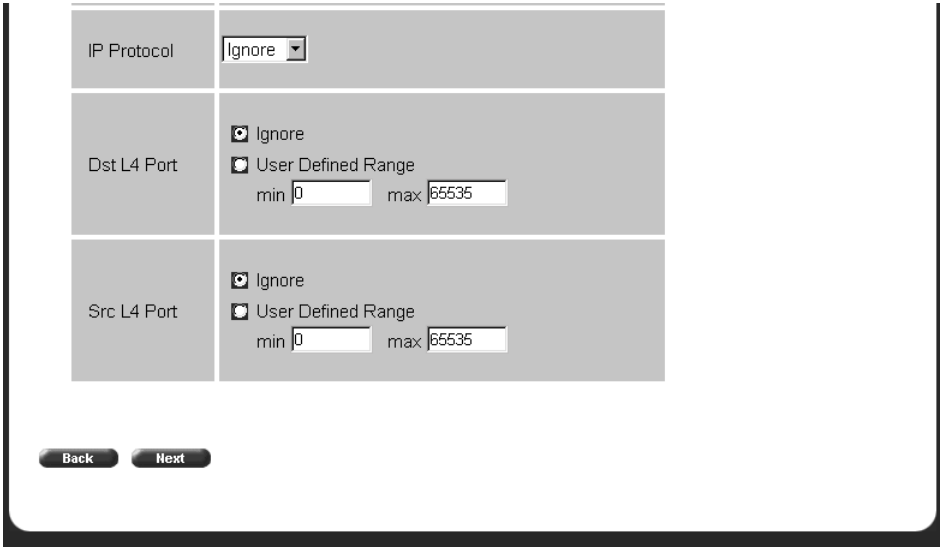


Figure 112 Layer 2 classification rules page (2 of 2)



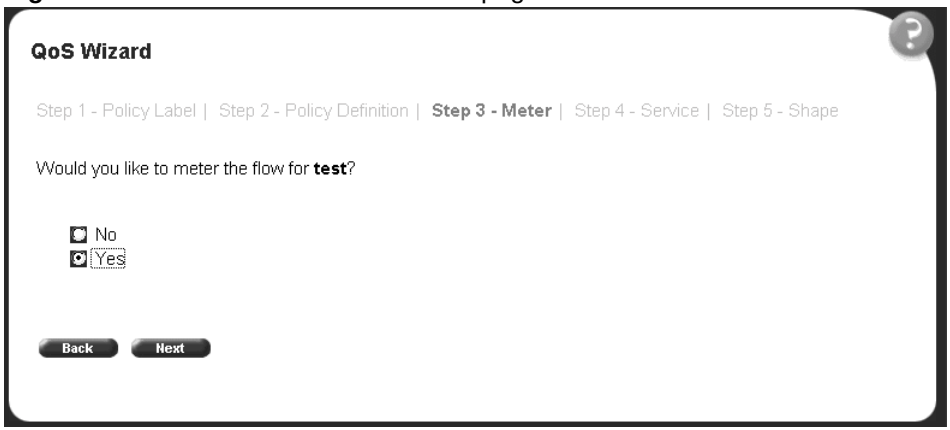
— Choose the layer 2 filter parameters you want the flow to have. (Refer to Chapter 9 for a description of the parameters.)

Beginning with software version 2.0, you can reference up to 32 VLANs with a single layer 2 filter.

— Click Next.

A page opens (Figure 113) that asks if you want to set a Meter for the specified flow.

Figure 113 Meter for user defined flow page



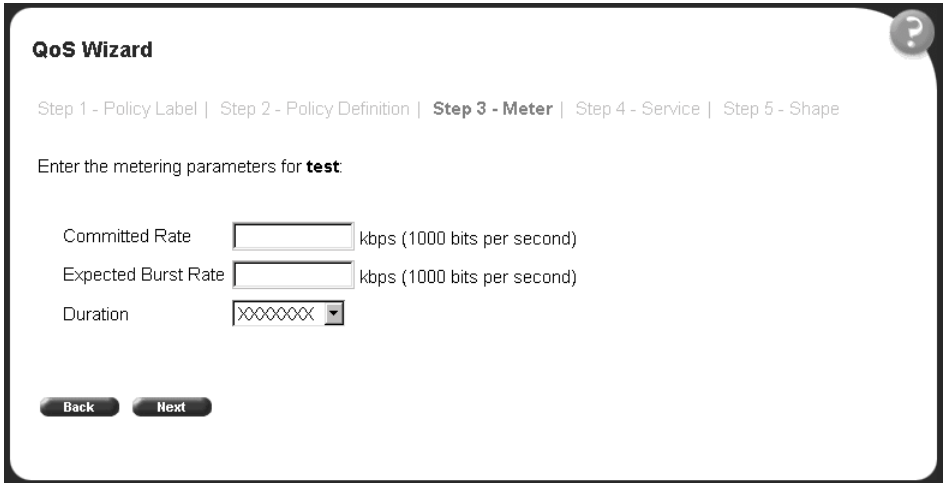
3 If you do not want to set a Meter, click No.

The system opens to the Service Class selection page (Figure 115), which appears with only one Service Class to set. You do not have In-Profile and Out-of-Profile without metering data.

4 If you want to set a Meter, click Yes.

A page opens (Figure 114) that allows you to set a Meter for the specified flow.

Figure 114 Meter setting for user defined flow page



5 Enter the committed rate you want for this Meter.

6 Enter the expected burst rate you want for this Meter.

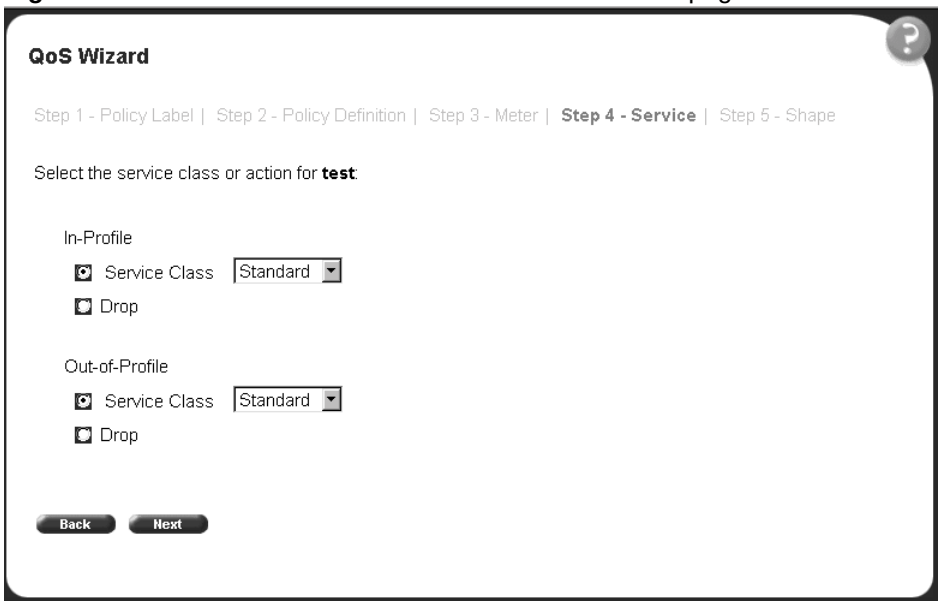
The system calculates a series of 7 or fewer possible durations for the committed and expected burst rates you set.

7 Choose the Duration you want.

8 Click Next.

A page opens (Figure 115) that allows you to select a Service Class separately for both the In-Profile and Out-of-Profile Action for the specified flow.

Figure 115 Service Class selection for user defined flow page



9 Click either Service Class or Drop.

If you click Service Class, choose the Service Class you want from the pull-down menu.

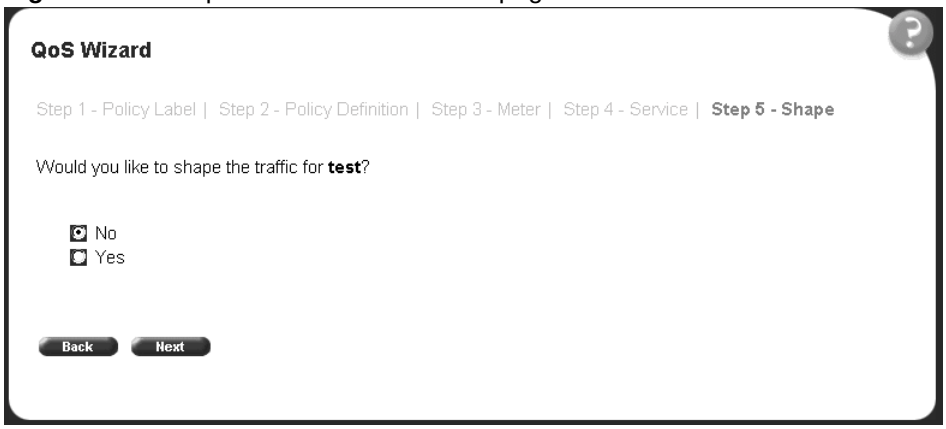
If you click Drop, the traffic in the specified flow is dropped.

10 Click Next.

A page opens (Figure 116) that allows you to set shaping criteria for the specified flow.

Note: You must be using either the BPS2000-1GT, BPS2000-2GT, or BPS2000-2GE MDA with the Business Policy Switch in order to implement the QoS shaping features.

Figure 116 Shaper for user defined flow page



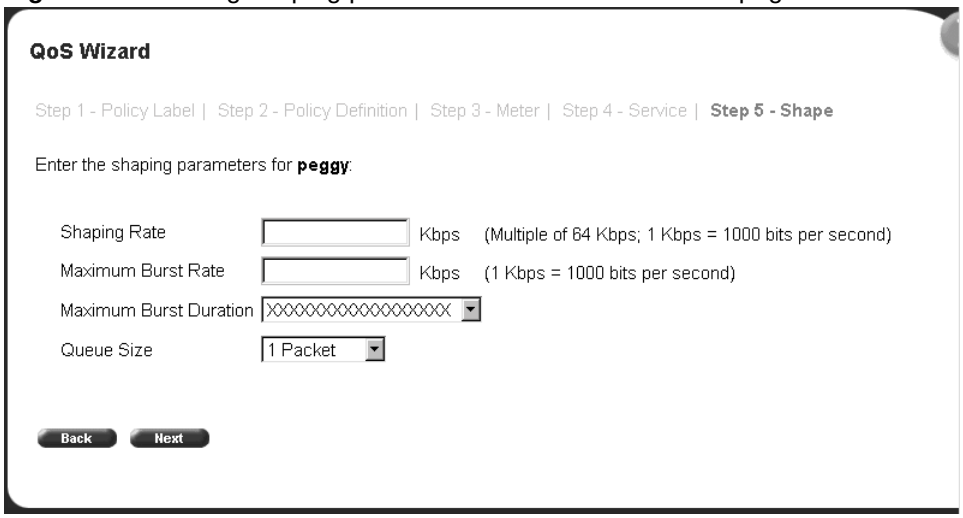
11 If you do not want to shape traffic for the specified flow, click No.

A page opens (Figure 118) that asks if you want to prioritize traffic for another user defined flow.

12 If you want to shape traffic for the specified flow, click Yes.

A page opens (Figure 117) that allows you to set shaping parameters for the specified flow.

Figure 117 Setting shaping parameters for user defined flow page



13 Enter the shaping rate you want for this Shaper.

The system rounds up shaping rates you enter, including 0, to multiples of 64 Kbps.

14 Enter the maximum burst rate you want for this Shaper.

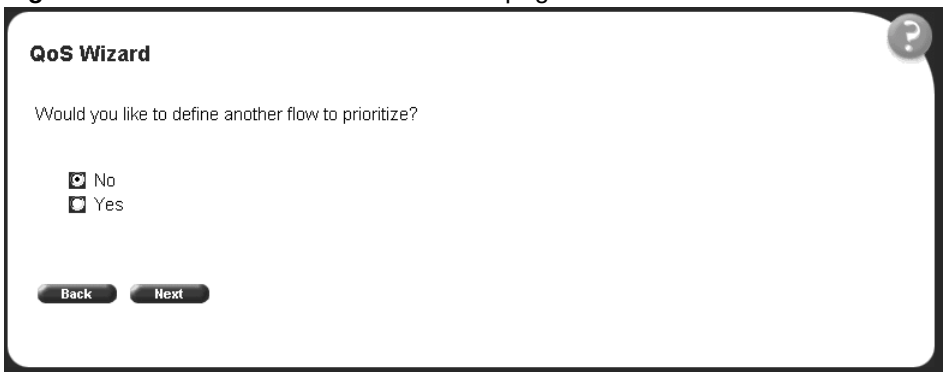
The system calculates a series of 6 or fewer possible durations for the shaping and maximum burst rates you set.

15 Choose the Maximum Burst Duration from the pull-down menu.

16 Choose the queue size you want for this Shaper.

A page opens (Figure 118) that asks you if you want to prioritize traffic for another user defined flow.

Figure 118 Additional user defined flows page



17 If you want to prioritize traffic for another user defined flow, click Yes and Next.

The system returns you to the policy label page (Figure 107), and you continue through steps 1 to 17 for the next user defined flow.

If you fill the resources of the QoS Wizard, you will not be prompted for another user defined flow.

18 If you do not want to prioritize traffic for another user defined flow, click No and Next.

The system returns you to the packet prioritization page (Figure 119), with a check mark next to User Defined Flow. Press the Status button to view the QoS Policies to Configure table listing your new entry in a pop-up window (Figure 120).

Figure 119 Packet prioritization page with prioritized User Defined Flow(s)

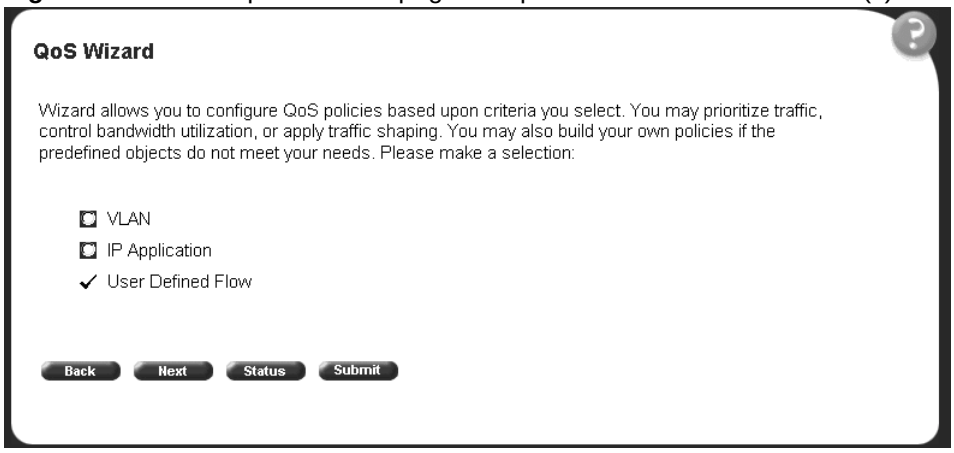
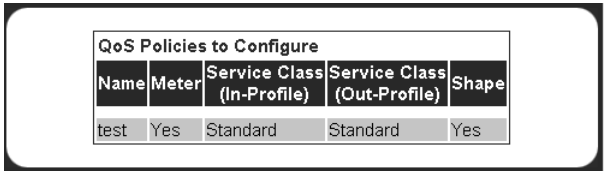


Figure 120 QoS Policies to Configure window with user defined flow entry



QoS Policies to Configure

Name	Meter	Service Class (In-Profile)	Service Class (Out-Profile)	Shape
test	Yes	Standard	Standard	Yes

19 When you are through viewing the table, click Back and then Submit.

You see a session confirmation page.

Using QoS Quick Config

This section describes how to use the QoS Quick Config option to configure QoS parameters for the BPS 2000. This section includes the following topics:

- "Using QoS Quick Config to configure interface groups" on page 225
- "Using QoS Quick Config to configure policies" on page 227

The QoS Quick Config option provides a set of Web pages for configuring QoS parameters. Using the QoS Quick Config does not reset the QoS parameters to default values as the QoS Wizard does. The QoS Quick Config condenses the QoS Advanced pages to just two pages and uses only default actions and mappings.

Using QoS Quick Config to configure interface groups

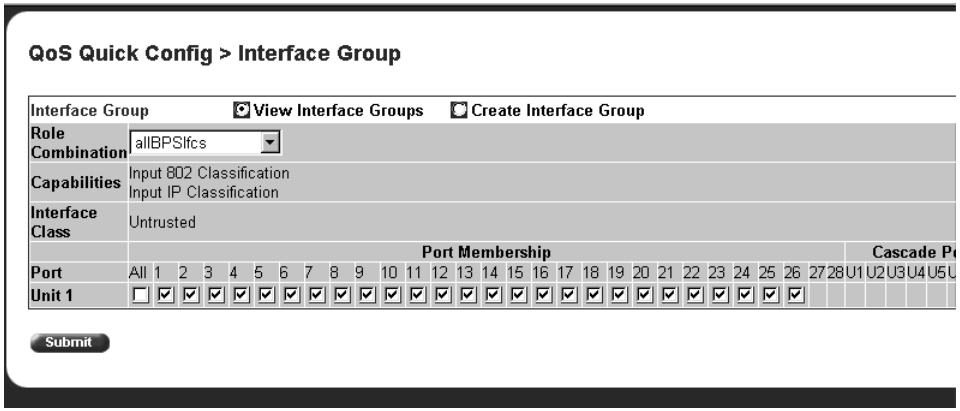
Note: If you do not need to define a new interface group (role combination), you can go directly to "Using QoS Quick Config to configure policies" on page 227.

To use the QoS Quick Config option:

1 From the main menu, choose Application > QoS > QoS Quick Config > Interface Group.

The QoS Quick Config Interface Group page opens (Figure 121) with the View Interface Groups option displaying.

Figure 121 QoS Quick Config Interface Group page—View Interface Group



2 To view the parameters of a specified Interface group, choose the Role Combination (Interface Group) you want to view and use the QoS Quick Config Interface Group page to view the following parameters:

— Capabilities

— Interface Class

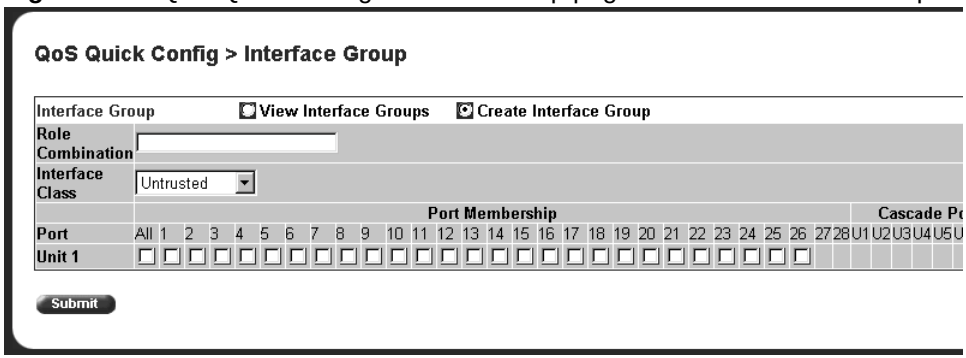
Refer to *Using the Business Policy Switch 2000 Software Version 2.5* for more information on interface classes.

— Port Membership

3 To create an Interface Group, click Create Interface Group.

The QoS Quick Config Interface Group page opens (Figure 122) with the Create Interface Groups option displaying.

Figure 122 QoS Quick Config Interface Group page—Create Interface Group



4 Enter the name you want for the new Role Combination (Interface Group).

5 Choose the Interface Class you want from Trusted, Untrusted, or Unrestricted.

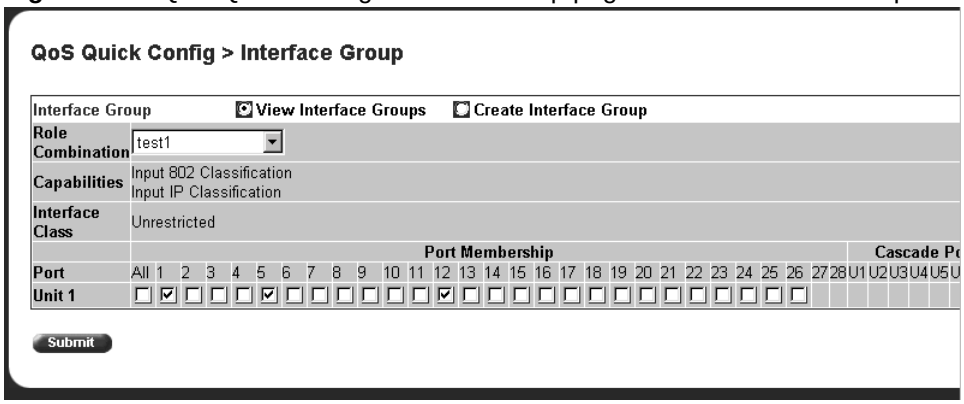
Refer to *Using the Business Policy Switch 2000 Software Version 2.5* for more information on interface classes.

6 Click the ports you want to belong to this Role Combination (Interface Group).

7 Click Submit.

The QoS Quick Config Interface Group page opens (Figure 121) with the View Interface Groups option displaying the new Role combination you just created.

Figure 123 QoS Quick Config Interface Group page—View Interface Group



8 Go to "Using QoS Quick Config to configure policies," next.

Using QoS Quick Config to configure policies

You use QoS Quick Config Web pages to configure the policies.

To configure QoS policies using QoS Quick Config:

➨ From the main menu, choose Application > QoS > QoS Quick Config > Policy.

The QoS Quick Config Policy page opens (Figure 124, Figure 125, and Figure 126).

Figure 124 QoS Quick Config Policy page (1 of 3)

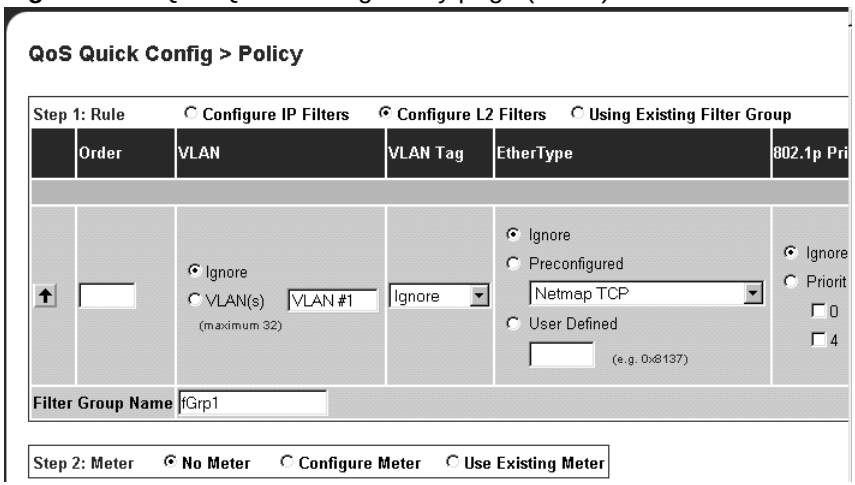


Figure 125 QoS Quick Config Policy page (2 of 3)

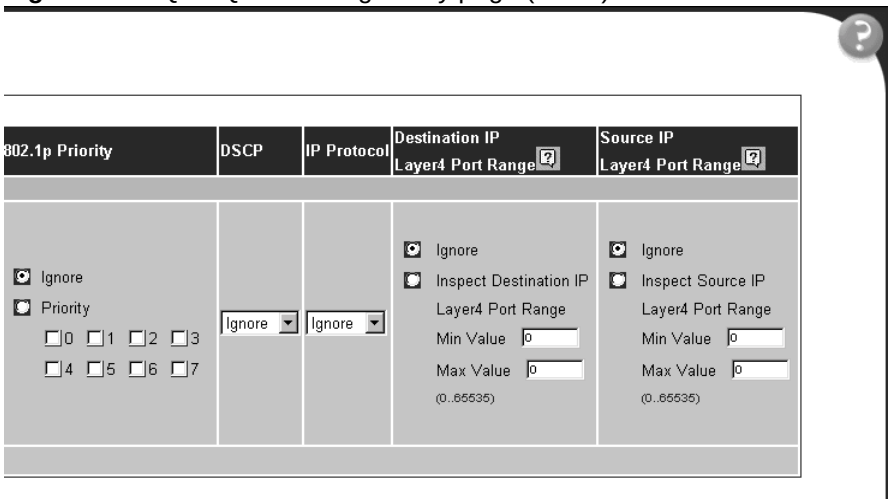


Figure 126 QoS Quick Config Policy page (3 of 3)

The QoS Quick Config Policy page contains the following four steps:

- Step 1: Rule
- Step 2: Meter
- Step 3: Shaper
- Step 4: Policy

This section discusses the following areas:

- "Configuring QoS Quick Config filters," next
- "Deleting Qos Quick Config filters from the filter group" on page 234
- "Configuring QoS Quick Config meters" on page 235
- "Configuring QoS Quick Config shapers" on page 236
- "Configuring QoS Quick Config policies" on page 238

Configuring QoS Quick Config filters

Using Step 1: Rule, you either configure a new filter group or use an existing group.

To configure a new IP filter group:

1 Click Configure IP Filters.

The QoS Quick Config Policy page for configuring IP filters opens (Figure 127 and Figure 128).

Figure 127 QoS Quick Config page for configuring IP filters page (1 of 2)

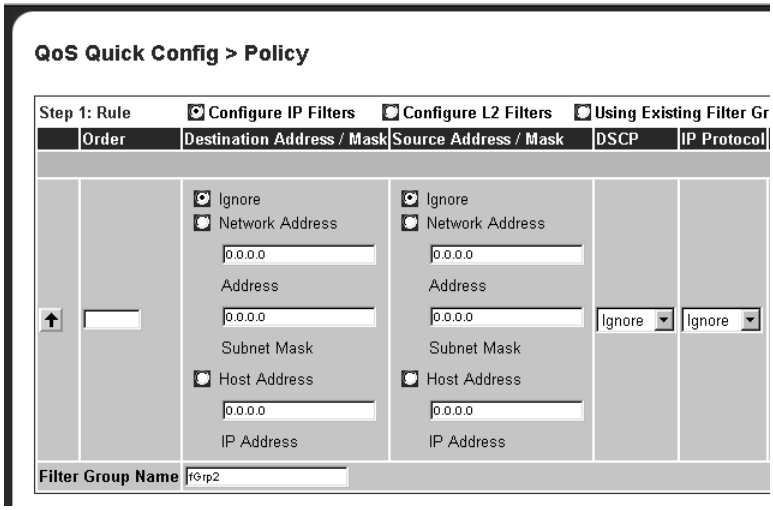
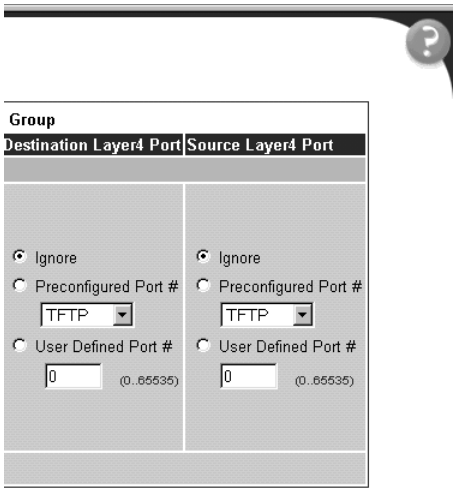


Figure 128 QoS Quick Config page for configuring IP filters page (2 of 2)



2 Enter the number you want for the order of the IP filter you are configuring.

3 Complete the Destination Address/Mask area by either:

— choosing Ignore

— entering the Network Address, Subnet Mask, and Host Address

4 Complete the Source Address/Mask area by either:

— choosing Ignore

— entering the Network Address, Subnet Mask, and Host Address

5 In the DSCP field, choose either Ignore or a value from the pull-down menu.

6 In the IP Protocol field, choose either Ignore or a protocol from the pull-down menu.

7 Complete the Destination Layer4 Port area by either:

— choosing Ignore

— choosing a preconfigured port number from the pull-down menu

— entering a value for the User Defined Port Number

8 Complete the Source Layer4 Port area by either:

— choosing Ignore

— choosing a preconfigured port number from the pull-down menu

— entering a value for the User Defined Port Number

9 Enter the name you want to assign to the newly created IP filter group.

10 Click the arrow on the far left to add the newly created filter into the filter group.

11 Repeat steps 2 to 8 to add additional filters into the filter group.

12 Go to "Configuring QoS Quick Config meters" on page 235.

To configure a new layer 2 filter group:

1 Click Configure L2 Filters.

The QoS Quick Config Policy page for configuring layer 2 filters opens (Figure 129 and Figure 130).

Figure 129 QoS Quick Config page for configuring layer 2 filters page (1 of 2)

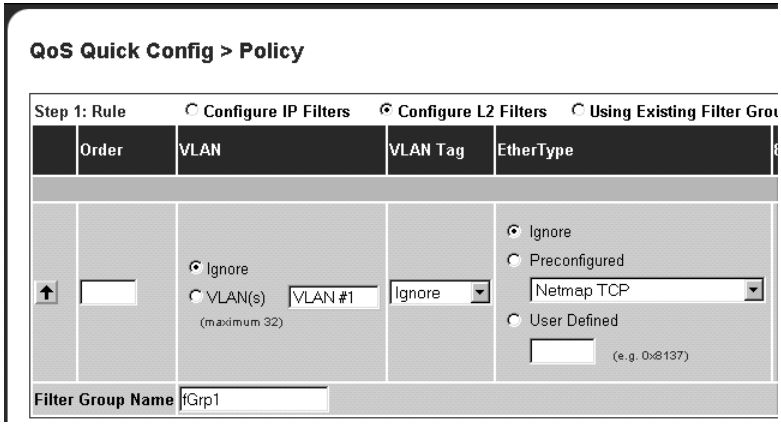
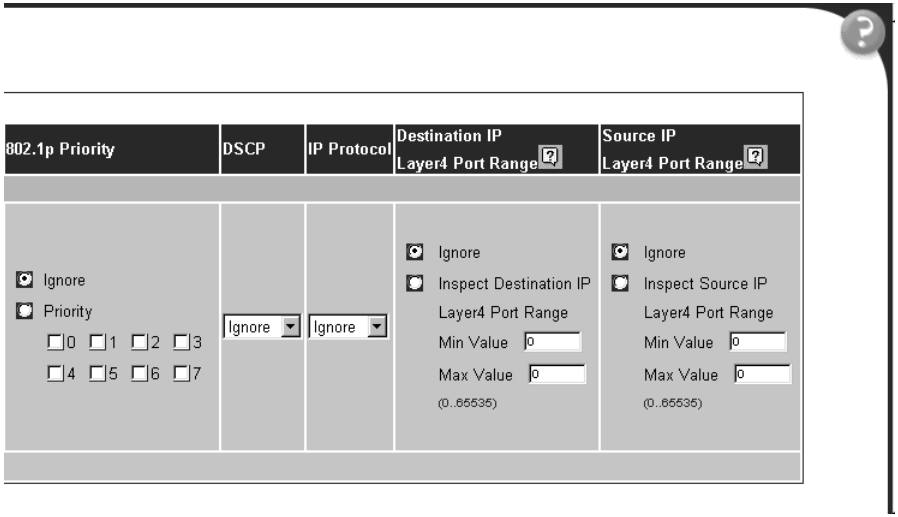


Figure 130 QoS Quick Config page for configuring layer 2 filters page (2 of 2)



2 Enter the number you want for the order of the layer 2 filter you are configuring.

3 In the VLAN area, choose the VLANs you want from the pull-down menu.

Note: Beginning with software version 2.0, you can reference up to 32 VLANs with a layer 2 filter.

4 In the VLAN Tag area, choose either Ignore, Tagged, or Untagged from the pull-down menu.

5 Complete the EtherType area by either:

— choosing Ignore

— choosing a preconfigured Ethernet type from the pull-down menu

— entering a hex value for the User Defined Ethernet type

6 Complete the 802.1p Priority area by either:

— choosing Ignore

— clicking Priority and choosing one of the 0-7 boxes for the priority value

7 In the DSCP field, choose either Ignore or a value from the pull-down menu.

8 In the IP Protocol field, choose either Ignore or a protocol from the pull-down menu.

9 Complete the Destination IP Layer4 Port Range area by either:

— choosing Ignore

— clicking Inspect Destination Layer4 Range and entering a value for both the maximum value and the minimum value

10 Complete the Source IP Layer4 Port Range area by either:

— choosing Ignore

— clicking Inspect Source Layer4 Range and entering a value for both the maximum value and the minimum value

11 Enter the name you want to assign to the newly created layer 2 filter group.

12 Click the arrow on the far left to add the newly created filter into the filter group.

13 Repeat steps 2 to 10 to add additional filters into the filter group.

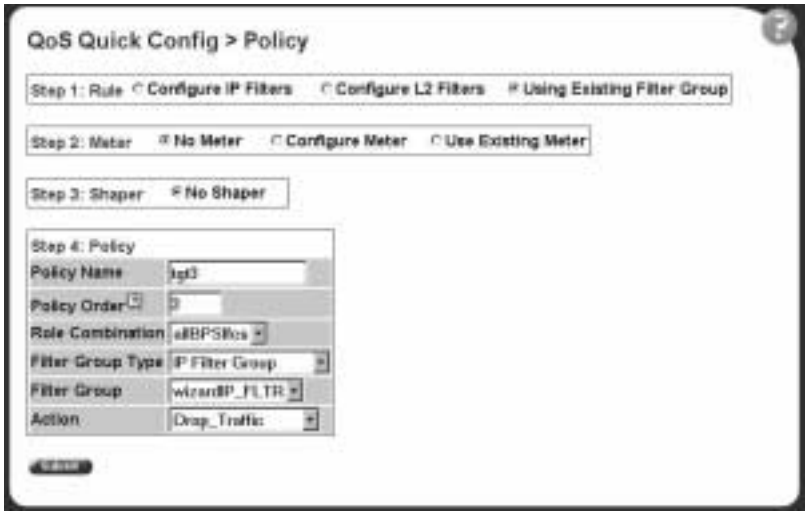
14 Go to"Configuring QoS Quick Config meters" on page 235.

To use an existing filter group:

1 Click Using Existing Filter Group.

A page opens that displays the Using Existing Filter Group option checked (Figure 131).

Figure 131 QoS Quick Config page with existing filter group choice



2 Go to "Configuring QoS Quick Config meters" on page 235.

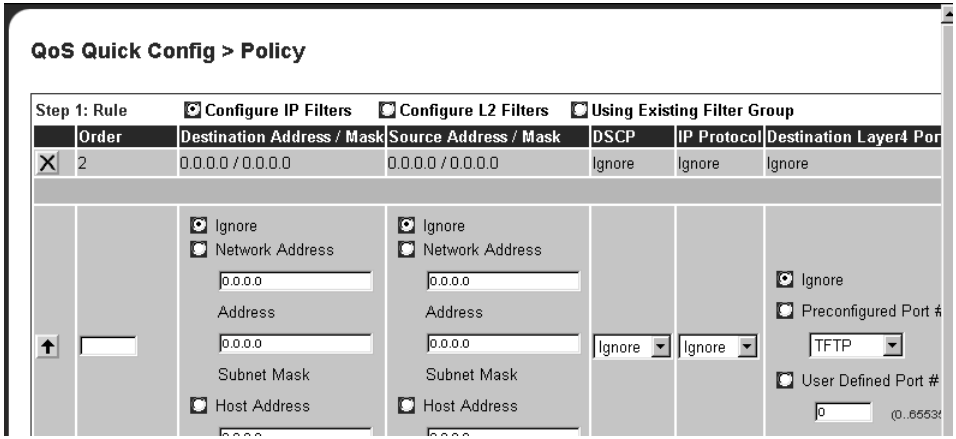
Deleting Qos Quick Config filters from the filter group

The filters of the filter group you created are displayed in a table at the top of the Step 1: Rule section of the QoS Quick Config Policy page. To delete a filter from the filter group:

1 Click QoS Quick Config > Policy.

The filter group you just configured displays in the table at the top of the Step 1: Rule section of the QoS Quick Config Policy page (Figure 132).

Figure 132 QoS Quick Config Policy page with displayed filter group



2 To delete the filter from the filter group, click the X icon at the far left of the table.

Configuring QoS Quick Config meters

Using Step 2: Meters, you choose to use nonmetered data for specified flow, to configure a new meter for the flow, or to use an existing meter for the flow.

To choose no metered data for the flow:

1 Click No Meter.

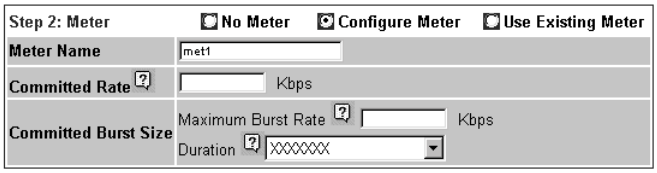
2 Go to "Configuring QoS Quick Config shapers" on page 236.

To create a new meter for the flow:

1 Click Configure Meter.

The system returns a page with the Step 2: Meter area expanded to allow you to configure QoS metering parameters (Figure 133).

Figure 133 QoS Quick Config Policy page with expanded meter area



2 Enter the name you want for the meter in the Meter Name field.

3 In the Committed Rate field, enter the rate you want for your meter.

4 In the Committed Burst Size field

— Enter the burst you want to allow

— Choose among the 6 or fewer durations the system calculates for the meter.

5 Go to "Configuring QoS Quick Config shapers" on page 236.

To use an existing meter for the flow:

1 Click Use Existing Meter.

2 Go to "Configuring QoS Quick Config shapers," next.

Configuring QoS Quick Config shapers

Note: You must be using either the BPS2000-1GT, BPS2000-2GT, or BPS2000-2GE MDA with the Business Policy Switch in order to implement the QoS shaping features.

Using Step 3: Shapers, you choose not to shape the data for specified flow, to configure a new shaper for the flow, or to use an existing shaper for the flow, or to reference an aggregate shaping group.

To choose not to shape the data for the flow:

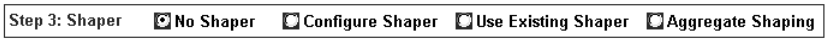
1 Click No Shaper.

2 Go to "Configuring QoS Quick Config policies" on page 238.

To configure a new shaper:

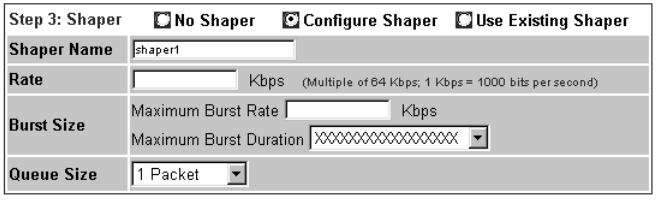
1 Click Configure Shaper, under Step 3: Shaper (Figure 134).

Figure 134 Step 3: Shaper



The Shaper box opens (Figure 135).

Figure 135 Shaper box



2 Enter the name for the shaper you are configuring in the Shaper Name field.

3 In the Rate field, enter the committed rate you want in Kbps.

The system rounds up the shaping rate you enter, including 0, to a multiple of 64 Kbps.

4 Enter the maximum rate in Kbps in the Maximum Burst Rate field.

5 Choose the duration from the pull-down menu in the Maximum Burst Duration field.

The system calculates the durations and presents you with 1 to 6 duration choices.

6 Choose the queue size from the pull-down menu in the Queue Size field.

The queue size is the amount to traffic that can exceed the maximum burst size and still be queued for transmission. This traffic is delayed for shaping purposes.

7 Go to "Configuring QoS Quick Config policies" on page 238.

To use an existing shaper for the flow:

1 Click Use Existing Shaper, under Step 3: Shaper (Figure 134).

2 Go to "Configuring QoS Quick Config policies" on page 238.

To use aggregate shaping for the flow:

1 Click Aggregate Shaping, under Step 3: Shaper (Figure 134).

2 Go to "Configuring QoS Quick Config policies," next.

Configuring QoS Quick Config policies

Using the Step 4: Policy area, you apply a policy to the specified flow (Figure 136).

Note: The Step:4 Policy area displays differently, depending on whether you are referencing meters and/or shapers:

- If you are not metering data, only an Action field appears.
- If you are metering data and have already assigned actions to the meter entry, no Action field appears.
- If you are metering data and have not assigned actions to the meter entry, the In-Profile and Out-of-Profile Action fields appear.
- If you are not referencing a shaper or creating a shaper, the Shaper field(s) do not appear.
- If you are referencing an existing shaper, the Shaper Name field appears.
- If you are referencing aggregate shaping, the Shaping Group field appear.

Figure 136 Policy area of QoS Quick Config Policy page

1. In the Policy Name field, enter a character string to assign a name for the policy you are configuring.
2. In the Policy Order field, enter the value you want for the evaluation order of the policy you are configuring.
3. In the Role Combination field, choose the Role Combination you want.
4. If you are referencing a meter with the policy:
   - Choose the In-Profile Action you want from the pull-down menu.
   - Choose the Out-of-Profile Action you want from the pull-down menu.
5. If you are referencing a existing shaper with the policy, choose the Shaper Name from the pull-down menu.
6. If you are referencing an existing aggregate shaper group with the policy, choose the Shaper Group group from the pull-down menu.
7. In the Track Statistics field, choose Yes or No from the pull-down menu.
8. Click Submit.

   The system returns you to the QoS Advanced Policies page, with your newly configured policy displayed in the Policy Table area (Figure 137 and Figure 138).

Figure 137 QoS Advanced Policies page with configured policies (1 of 2)

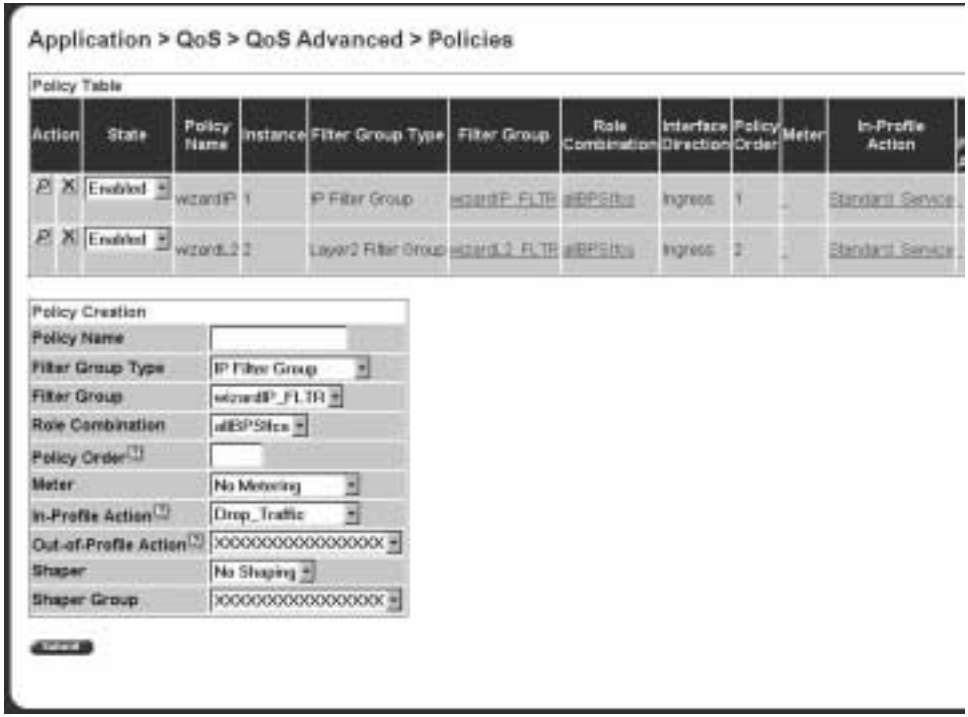
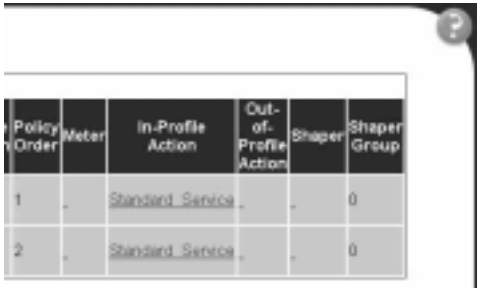


Figure 138 QoS Advanced Policies page with configured policies (2 of 2)



Chapter 9
Implementing QoS using QoS Advanced

The QoS application delivers a set of tools that, when optimally configured, combats escalating bandwidth costs and optimizes application performance in your network.

QoS tools allow you to prioritize your critical applications and sensitive traffic. You can tailor appropriate services to support this traffic over the wide area, thus maintaining the necessary performance levels on an end-to-end basis.

You can configure Quality of Service (QoS) features in your network by using the Web-based QoS Wizard, using the QoS Quick Config pages, or using the Advanced QoS configuration pages available in the Web-based management user interface. (Refer to Chapter 8 for descriptions of the QoS Wizard and QoS Quick Config options.)

Refer to *Using the Business Policy Switch 2000 Software Version 2.5*. for a sample QoS configuration using the advanced QoS Web pages.

This chapter explains configuring QoS using the Advanced QoS pages. The chapter covers the following topics:

- "Configuring QoS shapers" on page 282
- "Configuring QoS policies" on page 285
- "Configuring QoS Policy Agent (QPA) characteristics" on page 290

Note: To configure the features introduced with software version 1.2 and higher in a mixed stack, you must access a BPS 2000 unit.

Configuring an interface group

You view existing interface group configurations, or create or modify an interface group if you want a port (or ports) to assign the same QoS policy to all interfaces in the group.

Note: One default role combination covers all ports of the device.

Creating an interface group configuration

Note: For more information on QoS interface groups, or role combinations, refer to *Using the Business Policy Switch 2000 Software Version 2.5*.

To create an interface group configuration:

1. From the main menu, choose Application > QoS > QoS Advanced > Devices > Interface Configuration.

   The Interface Configuration page opens (Figure 139).

Figure 139 QoS Advanced Interface Configuration page

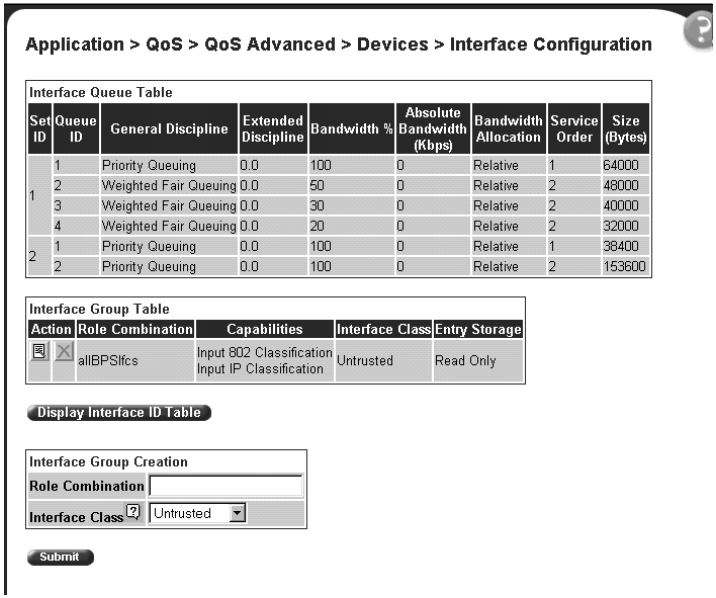


Table 75 describes the items on the Interface Queue Table section of the QoS Advanced Interface Configuration page.

Table 75 QoS Interface Queue Table section items

Item	Description
Set ID	The number that identifies a specific queue set.
Queue ID	The number that identifies the queue in the given set.
General Discipline	The queueing discipline that is associated with the specified queue. The options are: (1) Other - Use gosIfQueueExtDiscipline, (2) fifo - First In First Out Queuing, (3) pq -Priority Queuing, (4) fg - Fair Queuing, and (5) wfq - Weighted Fair Queuing
Extended Discipline	The queueing discipline that is associated with the specified queue. This attribute provides a means to add additional queueing mechanisms.
Bandwidth	The percentage of available bandwidth consumable to service the queue in one cycle.
Absolute Bandwidth	The absolute bandwidth consumable to service the queue in one cycle.
Bandwidth Allocation	Displays whether absolute or relative bandwidth is specified.
Service Order	The order in which a queue is serviced based on the defined discipline.
Size	The maximum size of the queue in bytes.

Table 76 describes the items on the Interface Group Table section of the QoS Advanced Interface Group page.

Table 76 Interface Group Table section items

Item	Description
	Opens a modification page.
	Deletes the row.
Role Combination	The tag used to identify interfaces with the characteristics specified by the attributes of this class instance (string 1..64). These identifiers are used within a number of classes to logically identify a physical set of interfaces to which policy rules and actions are applied.
Capabilities	A list of the interface capabilities used by the PDP or network manager to select which policies and configurations may be pushed to the Policy Enforcement Point (PEP). The options are: (0) Other, (1) InputIpClassification, (2) output Ip Classification, (3) input 802 Classification, (4) output 802 Classification, (5) single Queuing Discipline, and (6) hybrid Queuing Discipline.
Interface Class	The type of traffic received on interfaces associated with the specified role combination. The options are Trusted, Untrusted, and Unrestricted.
Entry Storage	Specifies whether or not the interface group can be deleted.

Note: For more information on QoS interface classes—or trusted, untrusted, and unrestricted ports—refer to *Using the Business Policy Switch 2000 Software Version 2.5*.

Table 77 describes the items on the Interface Group Creation section of the QoS Advanced Interface Group page.

Table 77 Interface Group Creation section page items

Item and MIB association	Range	Description
Role Combination (qosInterfaceTypeRoles)	1..64	Type a character string to identify the role combination.
Interface Class (qosInterfaceTypeExtIfClass)	(1) Trusted (2) Untrusted (3) Unrestricted	Choose an interface class: Selecting Trusted requests the incoming DSCP value to not be changed, and instead be used for 802.1p user priority and queue assignment based on values in the DSCP mapping table and DSCP mapping table. Selecting Untrusted forces the incoming DSCP value (and associated mappings) to modify to a standard value by default. Actions associated with untrusted interfaces must re-mark the DSCP. Selecting Unrestricted allows you to configure actions that: • re-mark the DSCP or leave the DSCP as is • re-mark the 802.1p priority value or leave as is

2 In the Interface Group Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new interface group configuration appears in the Interface Group Table (Figure 139)

Displaying Interface ID Table

To display the Interface ID Table:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Interface Configuration.

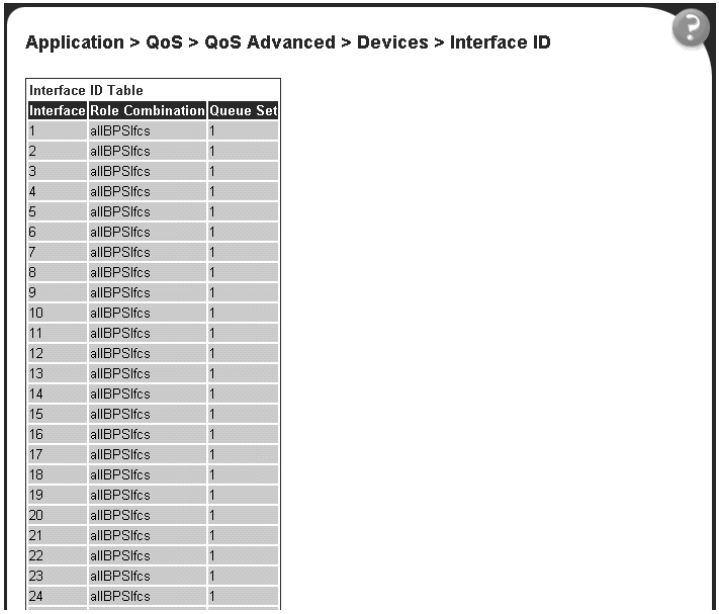
The QoS Advanced Interface Configuration page opens (Figure 139).

2 Click Display Interface ID Table.

The Interface ID page opens (Figure 140). The table displays all interfaces and the interface group (role combination) to which it belongs. If an interface does not belong to an interface group (role combination), it does not display in the table.

The table displays all created interface groups, whether created using the Qos Advanced pages, the QoS Wizard, or the QoS Quick config.

Figure 140 Interface ID page



Interface ID Table

Interface	Role Combination	Queue Set
1	allBPSIfcs	1
2	allBPSIfcs	1
3	allBPSIfcs	1
4	allBPSIfcs	1
5	allBPSIfcs	1
6	allBPSIfcs	1
7	allBPSIfcs	1
8	allBPSIfcs	1
9	allBPSIfcs	1
10	allBPSIfcs	1
11	allBPSIfcs	1
12	allBPSIfcs	1
13	allBPSIfcs	1
14	allBPSIfcs	1
15	allBPSIfcs	1
16	allBPSIfcs	1
17	allBPSIfcs	1
18	allBPSIfcs	1
19	allBPSIfcs	1
20	allBPSIfcs	1
21	allBPSIfcs	1
22	allBPSIfcs	1
23	allBPSIfcs	1
24	allBPSIfcs	1

Table 79 describes the items on the Interface ID page.

Table 78 Interface ID page items

Item	Description
Interface	Displays the unit and port number.
Role Combination	Displays the role combination associated with the interface.
Queue Sets	Displays the queue set associated with this interface.

Adding or removing interface group members

To select or deselect ports as members of an existing interface group:

1. From the main menu, choose Application > QoS > QoS Advanced > Devices > Interface Configuration.

   The QoS Advanced Interface Configuration page opens (Figure 139).

2 In the Interface Group Table section, in the row of your choice, click the Modify icon.

The Interface Group Assignment page opens (Figure 141).

Figure 141 Interface Group Assignment page

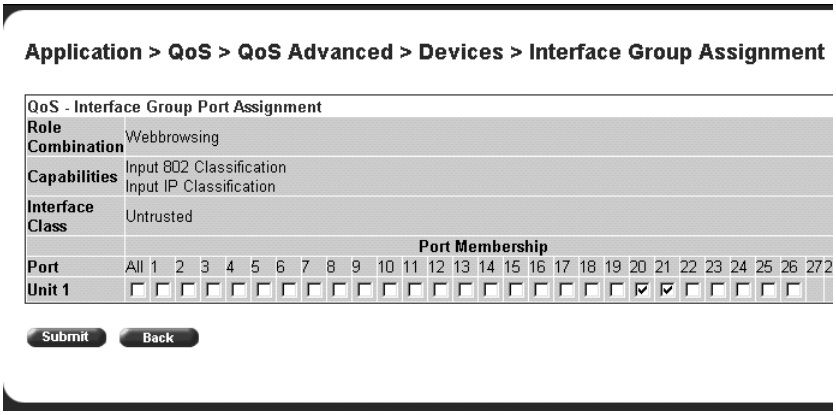


Table 79 describes the items on the Interface Group Assignment page.

Table 79 Interface Group Assignment page items

Item	Description
Role Combination	The tag used to identify interfaces with the characteristics specified by the attributes of this class instance (string 1..64). These identifiers are used within a number of classes to logically identify a physical set of interfaces to which policy rules and actions are applied. This is the group of interfaces (interface group) to which policy rules and actions are applied.
Capabilities	A list of the interface capabilities used by the PDP or network manager to select which policies and configurations may be pushed to the Policy Enforcement Point (PEP). The options are: (0) Other, (1) Input Ip Classification, (2) output Ip Classification, (3) input 802 Classification, (4) output 802 Classification, (5) single Queuing Discipline, and (6) hybrid Queuing Discipline
Interface Class	The type of traffic received on interfaces associated with the specified role combination. The options are Trusted, Untrusted, and Unrestricted.
Port Membership	Select the external ports to associate with the interface group, or select ALL to associate all ports on that unit.
Cascade Ports	The cascade (internal) ports to associate with the interface group.

3 In the Port Membership section, click the check boxes of the ports (or ALL to select all ports on the unit) to associate with the interface group.

Note: Beginning with software version 2.0, you can add all ports of one unit simultaneously, by clicking All. Also, if you are using stacked BPS 2000, you can modify, add, or delete the interfaces of only one unit at a time.

4 Do one of the following:

- Click Submit.
- Click Back to return to the Interface Configuration page without making changes.

Deleting an interface group configuration

To delete an Interface group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Interface Configuration.

The QoS Advanced Interface Configuration page opens (Figure 139).

2 In the Interface Group Table section, in the interface group configuration row of your choice, click the Modify icon.

The Interface Group Assignment page opens (Figure 141).

3 In the Port Membership section, click the check boxes to deselect all ports associated with the interface group.

Note: Beginning with software version 2.0, you can delete all ports of one unit simultaneously, by clicking All.

4 Click Submit.

The Interface Configuration page is displayed (Figure 139).

5 In the Interface Group Table section, in the configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

6 Do one of the following:

- Click Yes to delete the interface group configuration.
- Click Cancel to return to the Interface Configuration page without making changes.

Configuring 802.1p priority queue assignment

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

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

To configure 802.1p user priority:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Priority Q Assign.

The 802.1p Priority Queue Assignment page opens (Figure 142).

Figure 142 802.1p Priority Queue Assignment page

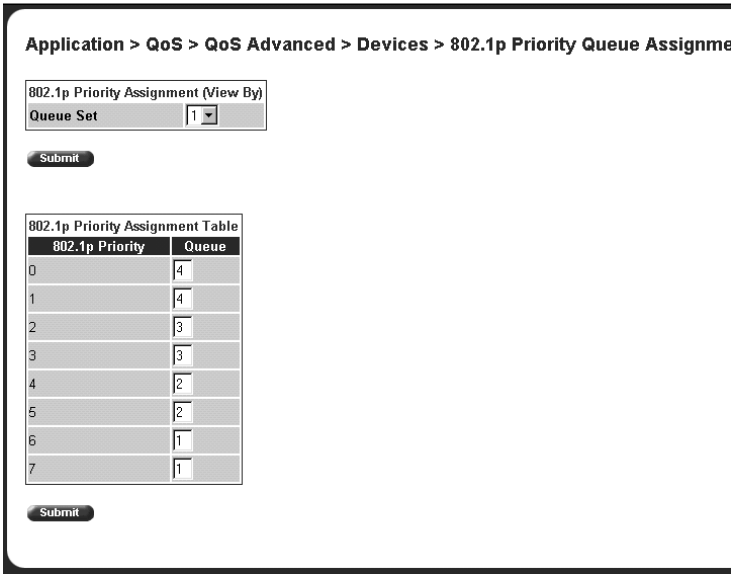


Table 80 describes the items on the 802.1p Priority Queue Assignment page.

Table 80 802.1p Priority Assignment Table section page items

Section	Item and MIB association	Description
802.1p Priority Assignment (View By)	Queue Set	Choose the queue set you want to modify.
802.1p Priority Assignment Table	802.1p Priority (ntnQosIfPriAssignmentPri)	The 802.1p user priority mapped to a queue.
	Queue (ntnQosIfPriAssignmentQueuet)	Type a number that signifies the desired queue in the specified queue set with which this priority is associated.

2 In the 802.1p Priority Assignment section, select the queue set to view in the 802.1p Priority Assignment Table.

3 Click Submit

The table is updated with the queue set you requested.

4 In the 802.1p Priority Assignment Table section, type the information in the text boxes.

5 Click Submit.

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

Configuring 802.1p priority mapping

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

To configure 802.1p priority to DSCP mapping:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Priority Mapping.

The 802.1p Priority Mapping page opens (Figure 143).

Figure 143 802.1p Priority Mapping page

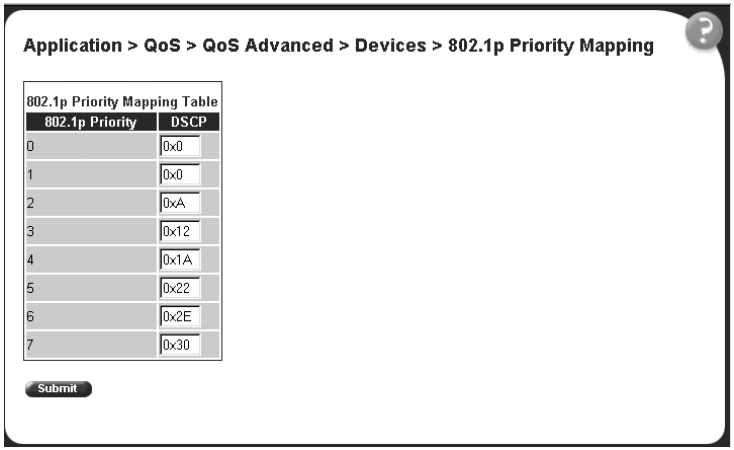


Table 81 describes the items on the 802.1p Priority Mapping page.

Table 81 802.1p Priority Mapping page items

Item	Description
802.1p Priority	The 802.1p user priority to map to a DSCP value at ingress.
DSCP	Type the DSCP value to associate with the specified 802.1p user priority value at ingress.

2 Type the information in the text boxes.

3 Click Submit.

Creating a DSCP queue assignment

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

To create a DSCP/queue set association:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > DSCP Q Assignment.

The DSCP Queue Assignment page opens (Figure 144).

Figure 144 DSCP Queue Assignment page

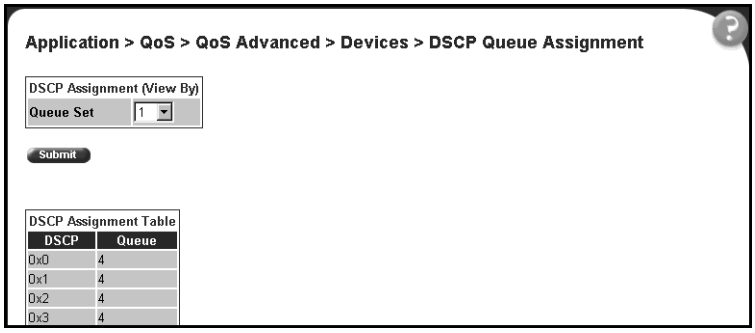


Table 82 describes the items on the DSCP Queue Assignment page.

Table 82 DSCP Queue Assignment page items

Section	Item	Format
DSCP Assignment (View By)	Queue Set	Choose the queue set to display in the DSCP Assignment Table.
DSCP Assignment Table	DSCP	The DSCP value to map to a queue.
	Queue	The queue set to which the traffic with the given DSCP value is associated.

2 In the DSCP Assignment (View By) section, choose the queue set to display in the DSCP Assignment Table.

   The table is updated with information for the selected queue.

3 In the DSCP Assignment Table section, type the information in the text boxes.

4 Click Submit.

Configuring DSCP mapping

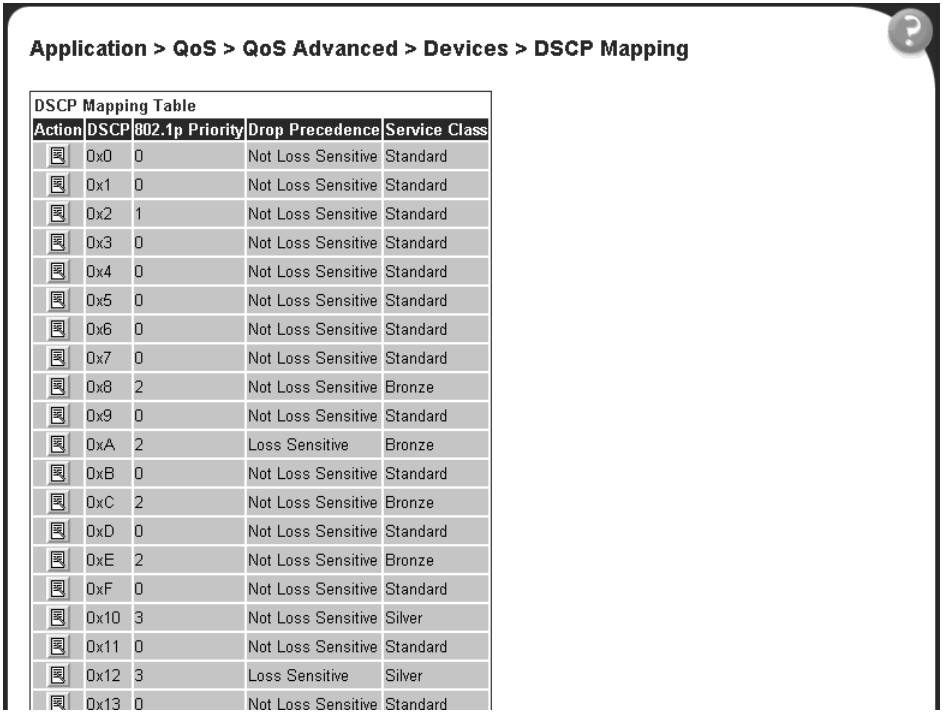
Note: Nortel Networks recommends using the default DSCP mappings to ensure end-to-end QoS connectivity.

To configure DSCP to 802.1p user priority/drop precedence mapping:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > DSCP Mapping.

   The DSCP Mapping page opens (Figure 145).

Figure 145 DSCP Mapping Table page



Application > QoS > QoS Advanced > Devices > DSCP Mapping

DSCP Mapping Table

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

Table 83 describes the items on the DSCP Mapping Table page.

Table 83 DSCP Mapping Table page items

Item	Format
	Opens a modification page.
DSCP	The attribute used internally to determine the appropriate Layer 2 cost of service (CoS) mappings.
802.1p Priority	The IEEE802 CoS value used when mapping the DSCP value specified by the qos802DscpMappingDscp attribute to an IEEE 802 CoS.
Drop Precedence	The drop value precedence used for traffic with the associated 802.1D user priority value with the identified queue. Note: Generally, low packet drop precedence receives preferential treatment.
Service Class	The current service class. The options are: Standard, Bronze, Silver, Gold, Platinum, Premium, and Network. Note: This field corresponds to the adjacent user priority levels.

2 In the row of your choice, click the Modification icon.

The DSCP Mapping Modification page opens (Figure 146).

Figure 146 DSCP Mapping Modification page

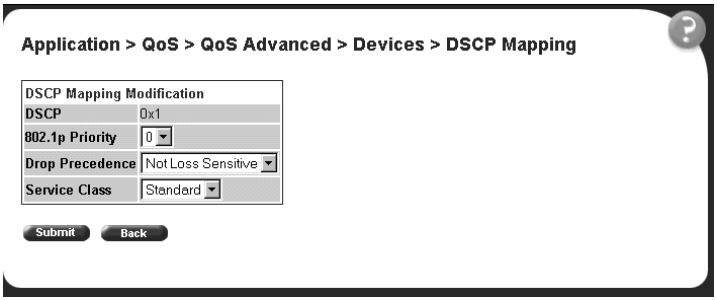


Table 84 describes the items on the DSCP Mapping Modification page.

Table 84 DSCP Mapping Modification page items

Item	Range	Format
DSCP	0..63	Type the attribute to use internally to determine the appropriate Layer 2 cost of service (CoS) mappings.
802.1p Priority	0..7	Choose the IEEE802 CoS value to use when mapping the DSCP value specified by the qos802DscpMappingDscp attribute to an IEEE 802 CoS.
Drop Precedence	Loss Sensitive Not Loss Sensitive	Choose the drop value precedence to use for traffic with the associated 802.1p user priority value with the identified queue. Selecting a Loss Sensitive value specifies a low packet drop precedence; selecting a Not Loss Sensitive value specifies a high packet drop precedence. Note: Generally, low packet drop precedence receives preferential treatment.
Service Class	Standard Bronze Silver Gold Platinum Premium Network	Choose the service class. Note: This field corresponds to the adjacent user priority levels.
	Note: Mappings created on the DSCP mapping modification page are used at egress for marking traffic: Trusted and unrestricted IP traffic—If you select the re-marking action of using the egress map, the mappings determine the 802.1p priority and drop precedence values associated with packets based on the DSCP of the received packet. Untrusted and untresticted traffic—If you select the re-marking action of using default, the mappings determine the 802.1p priority and drop precedence values associated with packets based on the DSCP value you specified in the Update DSCP action field.	

3 Select from a list.

4 Click Submit.

The modified configuration appears in the DSCP Mapping Table (Figure 145).

Note: For more information on QoS interface classes—or trusted, untrusted, and unrestricted ports—refer to *Using the Business Policy Switch 2000 Software Version 2.5*.

IP filter and IP filter group configurations

You can create an IP filter, which enables the switch to classify traffic. In turn, you can create an access control list from a series of defined filters to create an IP filter group. The filter group then determines access to and denial of network services.

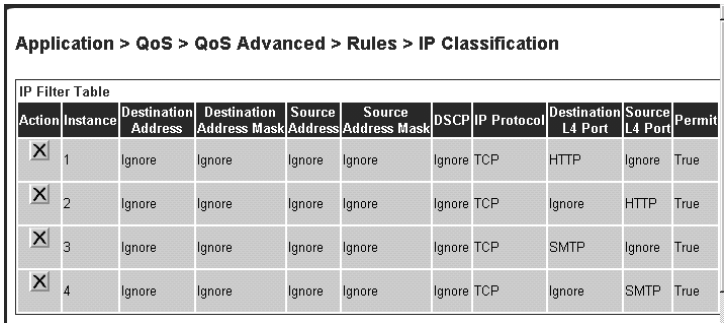
Creating an IP filter configuration

To create an IP filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 147, Figure 148, and Figure 149).

Figure 147 IP Classification page (1 of 3)



Application > QoS > QoS Advanced > Rules > IP Classification

IP Filter Table

Action	Instance	Destination Address	Destination Address Mask	Source Address	Source Address Mask	DSCP	IP Protocol	Destination L4 Port	Source L4 Port	Permit
X	1	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	HTTP	Ignore	True
X	2	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	Ignore	HTTP	True
X	3	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	SMTP	Ignore	True
X	4	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	Ignore	SMTP	True

Figure 148 IP Classification page (2 of 3)

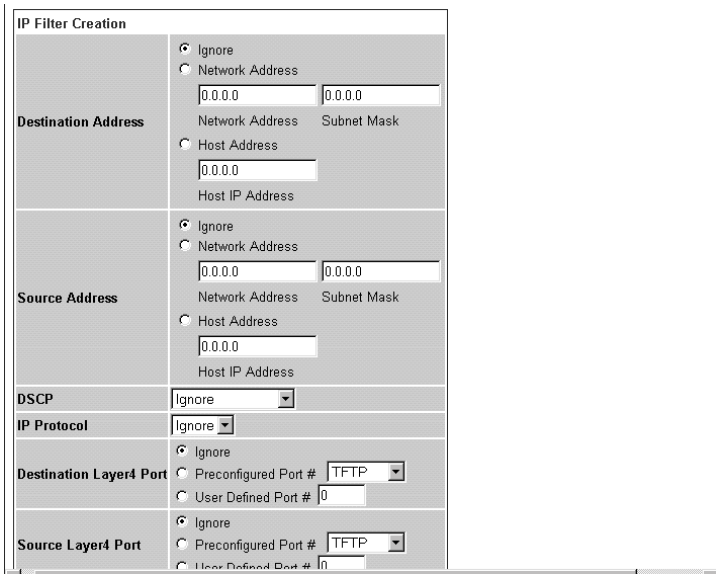
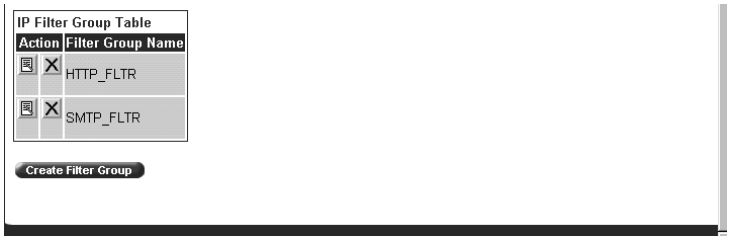


Figure 149 IP Classification page (3 of 3)



Note: When you choose the Ignore value, the filter matches all criteria for that parameter.

Table 85 describes the items on the IP Filter Table and IP Filter Creation sections of the IP Classification page.

Table 85 IP Filter Table and Filter Creation sections page items

Section	Item and MIB association	Range	Description
IP Filter Table	Action		Deletes the row. Note: You cannot delete a filter if it is referenced in a filter group.
	Instance		Displays unique identifier.
	Destination Address (qosIpAceDstAddr)	XXX.XXX.XXX.XXX	Displays the IP address to match against the packet's destination IP address.
	Destination Address Mask (qosIpAceDstAddrMask)	XXX.XXX.XXX.XXX	Displays the mask for the matching of the destination IP address. A zero bit in the mask means that the corresponding bit in the address always matches. One (1) bits must be left justified.
	Source Address (qosIpAceSrcAddr)	XXX.XXX.XXX.XXX	Displays the IP address to match against the packet's source IP address.
	Source Address Mask (qosIpAceSrcAddrMask)	XXX.XXX.XXX.XXX	Displays the mask for the matching of the source IP address. One (1) bits must be left justified.
	DSCP (qosIpAceDscp)	Ignore, Integer (0..63)	Displays the value that the DSCP in the packet must have and match this filter. This displays the DSCP value that this filter attempts to match.
	Protocol (qosIpAceProtocol)	TCP (6) UDP (17) ICMP (1) IGMP (2) RSVP (46) Ignore (0)	Displays the IP protocol to match against the packet's IP protocol field.
	Destination L4 Port (qosIpAceDstL4PortMin) (qosIpAceDstL4PortMax)	Integer (0.65535)	Displays the value that the packet's layer 4 destination port number must have and match this filter.
	Source L4 Port (qosIpAceSrcL4PortMin) (qosIpAceSrcL4PortMax)	Integer (0.65535)	Displays the value that the packet's layer 4 source port number must have and match this filter.
	Permit	(1) True (2) False	If the frame matches the filter when this is set to true, the matching process stops.
IP Filter Creation/ Destination Address	Ignore		Click if you want the filter to ignore the packet's destination IP address.
	Network Address	XXX.XXX.XXX.XXX	Click if you want the filter to match the packet's destination network address. Enter the IP address to match against the packet's destination IP address.
	Subnet Mask)	XXX.XXX.XXX.XXX	Enter the mask for the matching of the destination IP address. A zero bit in the mask means that the corresponding bit in the address always matches. One (1) bits must be left justified.

Table 85 IP Filter Table and Filter Creation sections page items (continued)

Section	Item and MIB association	Range	Description
	Host Address)	XXX.XXX.XXX.XXX	Click if you want the filter to match the packet's destination host IP address. Enter the IP address to match against the packet's destination IP address.
IP Filter Creation/ Source Address	Ignore		Click if you want the filter to ignore the packet's source IP address.
	Network Address	XXX.XXX.XXX.XXX	Click if you want the filter to match the packet's source network address. Enter the IP address to match against the packet's source IP address.
	Subnet Mask)	XXX.XXX.XXX.XXX	Enter the mask for the matching of the source IP address. One (1) bits must be left justified.
	Host Address)	XXX.XXX.XXX.XXX	Click if you want the filter to match the packet's source host IP address. Enter the IP address to match against the packet's source IP address.
IP Filter Creation/ DSCP	DSCP (qosIpAceDscp)	Ignore, Integer (0..63)	Choose the value that the DSCP in the packet must have and match this filter.
IP Filter Creation/ IP Protocol	Protocol (qosIpAceProtocol)	Ignore (0) TCP (6) UDP (17) ICMP (1) IGMP (2) RSVP (46)	Choose the IP protocol to match against the packet's IP protocol field.
IP Filter Creation/ Destination Layer4 Port	Ignore		Click if you want the filter to ignore the packet's layer 4 destination port.
	Preconfigured Port #	TFTP FTP TELNET SMTP HTTP HTTPS	Choose the value that the packet's layer 4 destination port number must have and match this filter.
	User Defined Port #	Integer	Enter the value that the packet's layer 4 destination port number must have and match this filter.
IP Filter Creation/ Source Layer4 Port	Ignore		Click if you want the filter to ignore the packet's layer 4 source port.
	Preconfigured Port #	TFTP FTP TELNET SMTP HTTP HTTPS	Choose the value that the packet's layer 4 source port number must have and match this filter.
	User Defined Port #	Integer	Enter the value that the packet's layer 4 source port number must have and match this filter.

2 In the IP Filter Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new IP filter configuration appears in the IP Filter Table (Figure 147). This table displays all IP filters you created, using QoS wizard, Qos Quick Config, or QoS Advanced pages.

Note: An IP filter configuration is not modifiable. The filter must be deleted and then re-created.

Deleting an IP filter configuration

To delete an IP filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 155).

2 In the IP Filter Table, in the IP filter configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the IP filter configuration.
- Click Cancel to return to the IP Classification page without making changes.

Note: You cannot delete a filter if it is referenced in a filter group.

Creating an IP filter group configuration

To create an IP filter group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 147).

Table 86 describes the items on the IP Filter Group section of the IP Classification page.

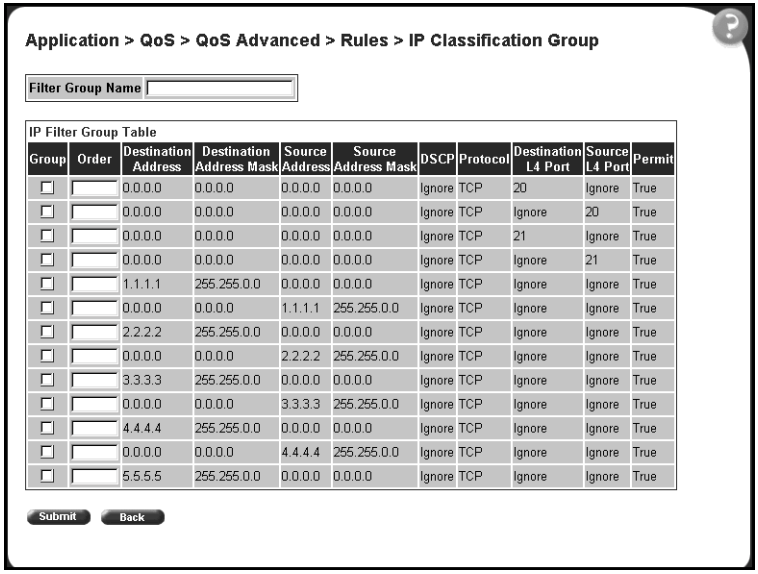
Table 86 IP Filter Group section page items

Item	Description
	Opens a modification page.
	Deletes the row.
Filter Group Name	A list of existing filter group configurations.
Create Filter Group	Opens a filter group creation page.

2 Click Create Filter Group.

The IP Classification Group page opens (Figure 150).This table displays all IP filters you created, using QoS wizard, Qos Quick Config, or QoS Advanced pages.

Figure 150 IP Classification Group page



Group	Order	Destination Address	Destination Address Mask	Source Address	Source Address Mask	DSCP	Protocol	Destination L4 Port	Source L4 Port	Permit
☐		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	20	Ignore	True
☐		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	20	True
☐		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	21	Ignore	True
☐		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	21	True
☐		1.1.1.1	255.255.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	Ignore	True
☐		0.0.0.0	0.0.0.0	1.1.1.1	255.255.0.0	Ignore	TCP	Ignore	Ignore	True
☐		2.2.2.2	255.255.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	Ignore	True
☐		0.0.0.0	0.0.0.0	2.2.2.2	255.255.0.0	Ignore	TCP	Ignore	Ignore	True
☐		3.3.3.3	255.255.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	Ignore	True
☐		0.0.0.0	0.0.0.0	3.3.3.3	255.255.0.0	Ignore	TCP	Ignore	Ignore	True
☐		4.4.4.4	255.255.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	Ignore	True
☐		0.0.0.0	0.0.0.0	4.4.4.4	255.255.0.0	Ignore	TCP	Ignore	Ignore	True
☐		5.5.5.5	255.255.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	Ignore	True

Table 87 describes the items on the IP Classification Group page.

Table 87 IP Classification Group page items

Item	Range	Description
Filter Group Name	1..16	Enter a character string to create an identity for the filter group configuration.
Group		Select (or deselect) the filter from membership in the filter group.
Order	Integer	Type a number to establish the evaluation order of filters in the group.
Destination Address		The IP address that is matched against the packet's destination IP address.
Destination Address Mask		The mask for the matching of the destination IP address. Note: A zero bit in the mask means that the corresponding bit in the address always matches.
Source Address		The IP address that is matched against the packet's source IP address.
Source Address Mask		The mask for the matching of the source IP address.
DSCP		The value that the DSCP in the packet must have and match this filter.
Protocol		The IP protocol that is matched against the packet's IP protocol field. The options are: Ignore, TCP, UDP, ICMP, IGMP, or RSVP
Destination L4 Port		The value that the packet's layer 4 destination port number can have and match the filter entry.

Table 87 IP Classification Group page items

Item	Range	Description
Source L4 Port		The value that the packet's layer 4 source port number can have and match the filter entry.
Permit	(1) True (2) False	If the frame matches the filter when this is set to true, the matching process stops.
	Note: To group multiple filters in a single group, assign Filter Index and Filter Order the same filter group name.	

3 Type information in the text boxes, or click the check box.

4 Click Submit.

The new configuration appears in the IP Filter Group Table (Figure 147).

Modifying an IP filter group configuration

To modify an IP filter group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 147).

2 In the IP Filter Group Table section, in the IP filter group configuration of your choice, click the Modify icon.

The IP Group Modification page opens (Figure). This table displays all IP filter you created, using QoS wizard, Qos Quick Config, or QoS Advanced pages. IP Group Modification page

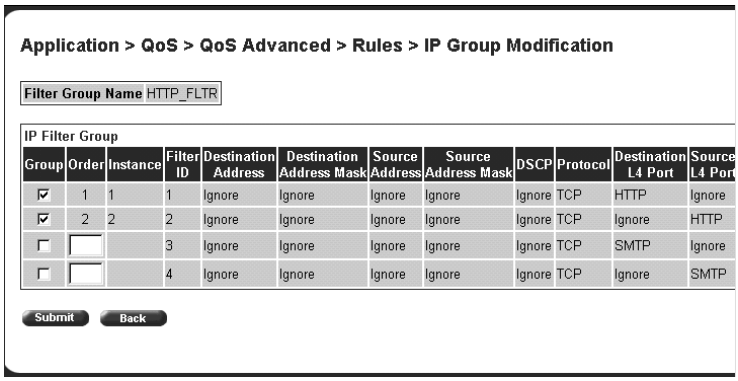


Table 88 describes the items on the IP Group Modification page.

Table 88 IP Modification Group page items

Item	Range	Description
Filter Group Name	1..16	Displays the name of the selected the filter group.
Group		Select (or deselect) the filter from membership in the filter group.
Order	Integer	Displays the order for existing groups. Enter the desired order for the entries you are adding to the group.
Instance		Displays unique identifier.
Filter ID		Displays the filter identifier.
Destination Address		The IP address that is matched against the packet's destination IP address.
Destination Address Mask		The mask for the matching of the destination IP address. Note: A zero bit in the mask means that the corresponding bit in the address always matches.
Source Address		The IP address that is matched against the packet's source IP address.
Source Address Mask		The mask for the matching of the source IP address.
DSCP		The value that the DSCP in the packet must have and match this filter.
Protocol		The IP protocol that is matched against the packet's IP protocol field. The options are: Ignore, TCP, UDP, ICMP, IGMP, or RSVP
Destination L4 Port		The value that the packet's layer 4 destination port number can have and match the filter entry.
Source L4 Port		The value that the packet's layer 4 source port number can have and match the filter entry.

Table 88 IP Modification Group page items

Item	Range	Description
Permit	(1) True (2) False	If the frame matches the filter when this is set to true, the matching process stops.
	Note: To group multiple filters in a single group, assign Filter Index and Filter Order the same filter group name.	

3 Select (or deselect) the filter as a member of the Filter Group.

4 Click Submit.

Deleting an IP filter group configuration

To delete an IP filter group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 147).

2 In the IP Filter Group Table section, in the IP filter group configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the IP filter group configuration.
- Click Cancel to return to the IP Classification page without making changes.

Note: You cannot delete a filter group that is referenced by a policy. You must first delete the policy.

Layer 2 filter and layer 2 filter group configurations

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

Beginning with software version 2.0, you can match up to 32 VLANs in one layer 2 filter.

Creating a layer 2 filter configuration

To create a layer2 filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

The Layer2 Classification page opens (Figure 151, and Figure 152).

Figure 151 Layer2 Classification page (1 of 2)

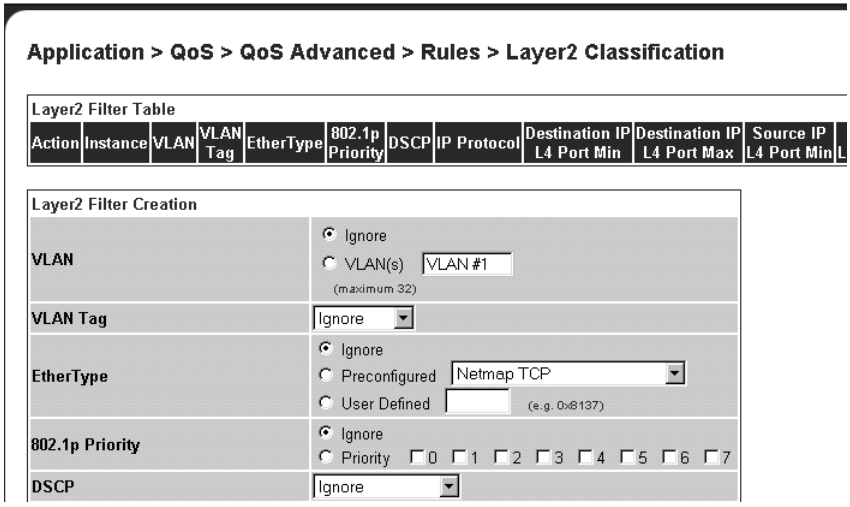


Figure 152 Layer2 Classification page (2 of 2)

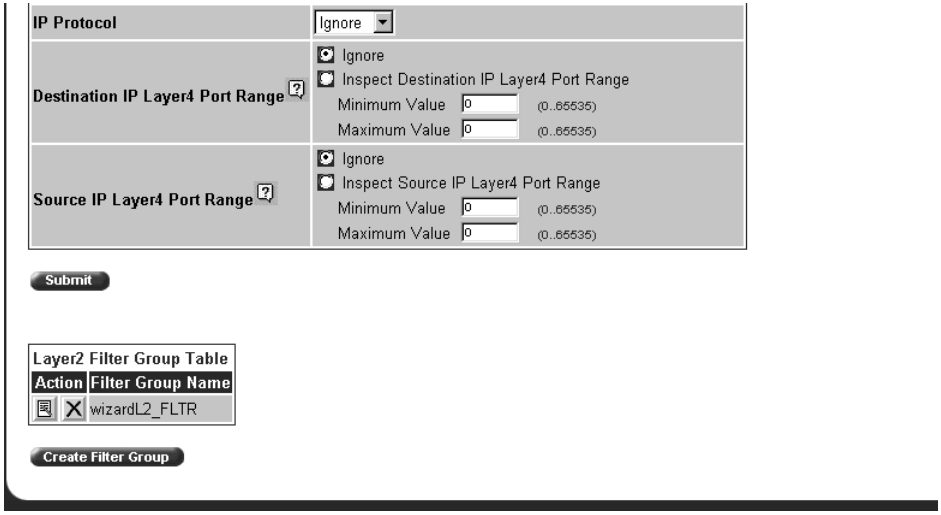


Table 89 describes the items on the Layer2 Filter Table and Layer2 Filter Creation sections of the Layer2 Classification page.

Table 89 Layer2 Filter Table and Layer2 Filter Creation section items

Section	Item	Range	Description
Layer 2 Filter Table	Action		Deletes the row.
	Instance		Displays unique identifier.
	VLAN	Ignore, 1-32	Click the VLANs you want to reference with this filer, up to 32 VLANs. Range is Ignore, 1 to 32.
	VLAN Tag	(1) Tagged (2) Untagged (3) Ignore	Displays whether or not to check VLAN tagging.

Table 89 Layer2 Filter Table and Layer2 Filter Creation section items (continued)

Section	Item	Range	Description
	EtherType	Ignore Netmap TCP Netmap XNS XTP LOOP Vines Vines IP Banyan Vines Echo Vines Banyan Echo ARP RARP IP IPv6 3Com NBP 3Com NBP Ack 3Com NBP ConnReq 3Com NBP ConnRsp 3Com NBP ConnComplt 3Com NBP CloseReq 3Com NBP CloseRsp 3Com NBP Datagram 3Com NBP Broadcast 3Com NBP NBP NameClaim 3Com NBP DelName LAP Atalk ARP Atalk IBM Net Mon IBMRT XNS Compatibility XNS IPX Netware SNMP User Defined	Displays the EtherType to match.
	802.1p Priority	Ignore, 0...7.	Displays the 802.1p priority level.
	DSCP	Ignore, Integer (0.63)	Displays the value that the DSCP in the packet must have and match this filter.

Table 89 Layer2 Filter Table and Layer2 Filter Creation section items (continued)

Section	Item	Range	Description
	IP Protocol	Ignore TCP UDP ICMP IGMP RSVP	Displays the IP protocol to match against the packet's IP protocol field.
	Destination IP L4 Port Min	Ignore, Integer (0.65535)	Displays the least value that the packet's layer 4 destination port number can have and match this filter.
	Destination IP L4 Port Max	Ignore, Integer (0.65535)	Displays the maximum value that the packet's layer 4 destination port number can have and match this filter.
	Source IP L4 Port Min	Ignore, Integer (0.65535)	Displays the least value that the packet's layer 4 source port number can have and match this filter.
	Source IP L4 Port Max	Ignore, Integer (0.65535)	Displays the maximum value that the packet's layer 4 source port number can have and match this filter.
Layer2 Filter Creation	VLAN	Ignore, 1-32	Choose up to 32 VLAN names or ID numbers.
	VLAN Tag	(1) Tagged (2) Untagged (3) Ignore	Choose whether or not to check VLAN tagging.

Table 89 Layer2 Filter Table and Layer2 Filter Creation section items (continued)

Section	Item	Range	Description
	EtherType	Ignore Netmap TCP Netmap XNS XTP LOOP Vines Vines IP Banyan Vines Echo Vines Banyon Echo ARP RARP IP IPv6 3Com NBP 3Com NBP Ack 3Com NBP ConnReq 3Com NBP ConnRsp 3Com NBP ConnComplt 3Com NBP CloseReq 3Com NBP CloseRsp 3Com NBP Datagram 3Com NBP Broadcast 3Com NBP NBP NameClaim 3Com NBP DelName LAP Atalk ARP Atalk IBM Net Mon IBMRT XNS Compatibility XNS IPX Netware SNMP User Defined	Choose the EtherType to match. Note: If you choose User Defined, enter the value.
	802.1p Priority	Ignore, 0...7.	Click the 802.1p priority level.
	DSCP	Ignore, Integer (0..63)	Choose the value that the DSCP in the packet must have and match this filter.

Table 89 Layer2 Filter Table and Layer2 Filter Creation section items (continued)

Section	Item	Range	Description
	IP Protocol	Ignore TCP UDP ICMP IGMP RSVP	Select the IP protocol to match against the packet's IP protocol field.
	Destination IP L4 Port Range	Ignore, Min, Max	Choose Ignore or type the minimum value and the maximum value that the packet's layer 4 destination port number can have and match this filter.
	Source IP L4 Port Range	Ignore, Min, Max	Choose Ignore or type the minimum value and the maximum value that the packet's layer 4 source port number can have and match this filter.

2 Type the information in the text boxes, or select from a list.

3 Click Submit.

The new Layer2 filter configuration appears in the Layer2 Filter Table (Figure 151).

Note: You cannot delete a filter if it is referenced in a filter group.

Deleting a layer 2 filter configuration

To delete a layer 2 filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

The Layer2 Classification page opens (Figure 151). This table displays all layer 2 filters you created, using QoS wizard, Qos Quick Config, or QoS Advanced pages.

2 In the Layer2 Filter Table, in the layer 2 filter configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the filter configuration.
- Click Cancel to return to the Layer2 Classification page without making changes.

Note: A Layer 2 filter configuration cannot be modified. The configuration must be deleted and then recreated.

Creating a layer 2 filter group configuration

To create a Layer 2 filter group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

The Layer2 Classification page opens (Figure 151).This table displays all layer 2 filters you created, using QoS wizard, Qos Quick Config, or QoS Advanced pages.

Table 90 describes the items on the Layer2 Filter Group Table section of the Layer2 Classification page.

Table 90 IP Filter Group Table section items

Item	Description
	Opens a modification page.
	Deletes the row.
Filter Group Name	Lists existing filter group configurations.
Create Filter Group	Opens a filter group creation page.

2 Click Create Filter Group.

The Layer2 Group page opens (Figure 153).

Figure 153 Layer2 Group page

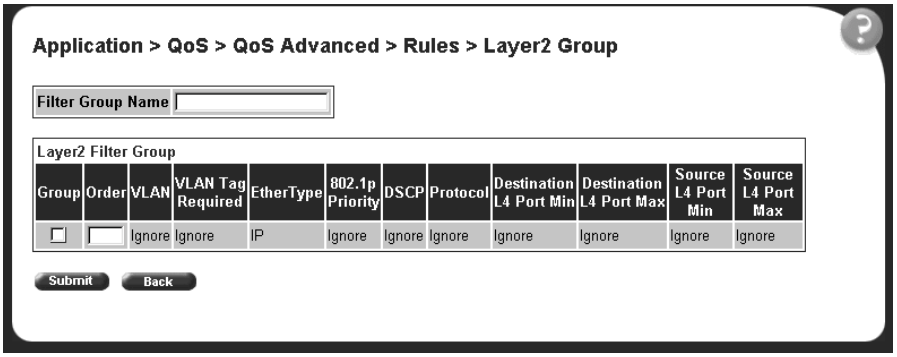


Table 91 describes the items on the Layer2 Group page.

Table 91 Layer2 Group page items

Item	Range	Description
Filter Group Name	1..16	Enter a character string to create an identity for the filter group configuration.
Group		Select (or deselect) the filter from membership in the filter group.
Order	Integer	Enter a number to establish the evaluation order of filters in the group.
VLAN		The VLAN ID(s) specified when the layer 2 filter was created.
VLAN Tag Required		The VLAN tag requirement option selected when the filter was created.
EtherType		The EtherType selected when the filter was created.
802.1p Priority		The 802.1p priority selected when the filter was created.
DSCP		The value that the DSCP in the packet can have and match this filter.
Protocol		The IP protocol that is matched against the packet's IP protocol field. The options are: Ignore, TCP, UDP, ICMP, IGMP, or RSVP.
Destination L4 Port Min		The least value that the packet's layer 4 destination port number can have and match this filter.
Destination L4 Port Max		The maximum value that the packet's layer 4 destination port number can have and match this filter.
Source L4 Port Min		The least value that the packet's layer 4 source port number can have and match this filter.

Table 91 Layer2 Group page items

Item	Range	Description
Source L4 Port Max		The maximum value that the packet's layer 4 source port number can have and match this filter.
	Note: To group multiple filters in a single group, assign Filter Index and Filter Order the same filter group name.	

3 Type information in the text boxes, or click the check box.

4 Click Submit.

The new layer 2 filter group configuration appears in the Layer 2 Filter Group Table (Figure 151). This table displays all Layer 2 filters you created with QoS Wizard, QoS Quick Config, and QoS Advanced.

Modifying a layer 2 filter group configuration

To modify a layer 2 filter group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

The Layer2 Classification page opens (Figure 151).

2 In the Layer2 Filter Group Table section, in the layer 2 filter group configuration of your choice, click the Modify icon.

The Layer2 Group modification page opens (Figure 154).This table displays all Layer 2 Filter Groups you created with QoS Wizard, QoS Quick Config, and QoS Advanced.

Figure 154 Layer2 Group modification page

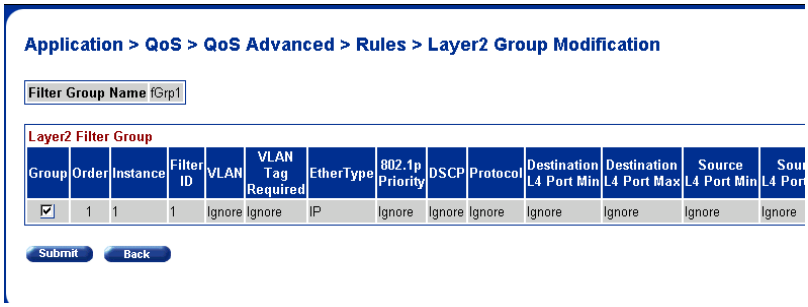


Table 92 describes the items on the Layer2 Group modification page.

Table 92 Layer2 Group modification page items

Item	Range	Description
Filter Group Name	1..16	Displays the filter group name.
Group		Select (or deselect) the filter from membership in the filter group.
Order	Integer	Enter a number to establish the evaluation order of filters in the group.
Instance		Displays a unique identifier.
Filter ID		Displays the filter identifier.
VLAN		The VLAN ID(s) specified when the layer 2 filter was created.
VLAN Tag Required		The VLAN tag requirement option selected when the filter was created.
EtherType		The EtherType selected when the filter was created.
802.1p Priority		The 802.1p priority selected when the filter was created.
DSCP		The value that the DSCP in the packet can have and match this filter.
Protocol		The IP protocol that is matched against the packet's IP protocol field. The options are: Ignore, TCP, UDP, ICMP, IGMP, or RSVP.
Destination L4 Port Min		The least value that the packet's layer 4 destination port number can have and match this filter.
Destination L4 Port Max		The maximum value that the packet's layer 4 destination port number can have and match this filter.
Source L4 Port Min		The least value that the packet's layer 4 source port number can have and match this filter.
Source L4 Port Max		The maximum value that the packet's layer 4 source port number can have and match this filter.

3 Type information in the text boxes, or click the check box.

4 Click Submit.

Deleting a layer 2 filter group configuration

To delete a layer 2 filter group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

The Layer2 Classification page opens (Figure 151).

2 In the Layer2 Filter Group Table section, in the layer 2 filter group configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the filter group configuration.
- Click Cancel to return to the Layer2 Classification page without making changes.

Note: You cannot delete a filter group that is referenced by a policy. You must first delete the policy.

Configuring QoS actions

When you create a filter action, you specify the actions to be associated with specific IP and IEEE 802 filter groups. An action specifies the type of behavior you want a policy to apply to a flow of packets. When the filters match the incoming packets, the created actions are performed on those packets.

Creating a filter action configuration

To create a filter action configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Actions.

The Action page opens (Figure 155).

Note: Beginning with software version 2.0, there are default actions for each service class.

Figure 155 Action page

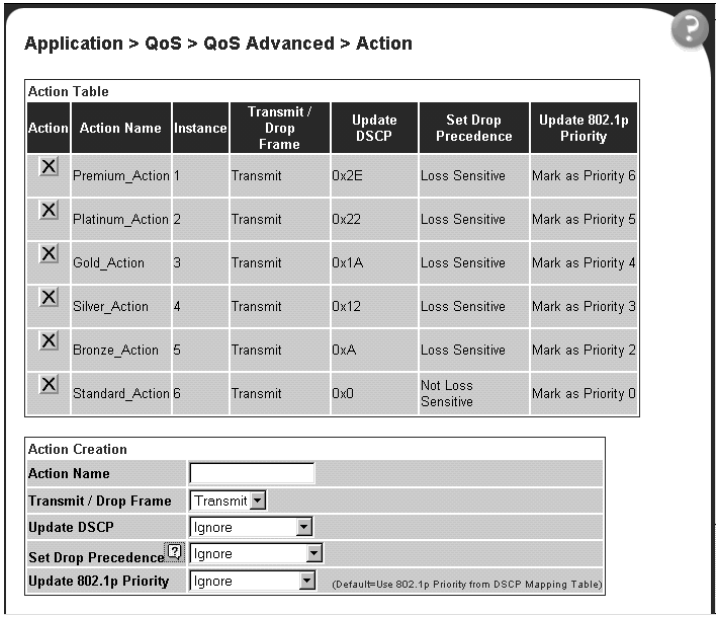


Table 93 describes the items on the Action page.

Table 93 Action page items

Item and MIB association	Range	Description
		Deletes the row.
Action Name	1..16	Type a character string to uniquely identify the action configuration.
Instance		Displays the unique identifier.
Transmit/Drop Frame (qosActionDrop)	(1) Transmit (2) Drop	Choose whether the frame being evaluated should be dropped or transmitted by this attribute. The default setting is Transmit.
Update DSCP (qosActionUpdateDSCP)	Ignore or integer	Type a value. When this field is defined, it causes the value contained in the Differentiated Services (DS) field of an associated IP datagram to be updated with the value of this object. The default setting is Ignore.

Table 93 Action page items (continued)

Item and MIB association	Range	Description
Set Drop Precedence (ntnQosActionExtSetDropPrec)	(1) Ignore (2) Loss Sensitive (3) Not loss Sensitive (4) Use Defaults (5) Use Egress Map	Choose a packet drop precedence value. Note: Generally, low packet drop precedence receives preferential treatment The default setting is Use Defaults
Update 802.1p Priority (ntnQosActionExtUpdatePri)	(1) Ignore (2) Priority 0 (3) Priority 1 (4) Priority 2 (5) Priority 3 (6) Priority 4 (7) Priority 5 (8) Priority 6 (9) Priority 7 (10) Use Defaults (11) Use Egress Map	Choose the action attribute that causes the value contained in the 802.1p priority field to be updated based on the value of this object. The update priority range values are 0 (lowest priority) to 7 (highest priority). Note: Use Defaults=Use 802.1p priority from DSCP mapping table. The default setting is Use Defaults.

2 In the Action Creation section, type information in the text boxes, or select from a list

3 Click Submit.

The new filter action configuration appears in the Action Table (Figure 155).

Note: Actions are not modifiable. They must be deleted and re-created.

Deleting an action configuration

To delete an action configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Actions.

The Action page opens (Figure 155).

2 In the Action Table section, in the filter action configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the filter configuration.
- Click Cancel to return to the Action page without making changes.

Note: You cannot delete an action that is referenced by a meter. you must first delete the meter.

Configuring QoS meters

Using the QoS Advanced pages, you can create, view, or delete meters. If you do not want to meter the data in your flow, go to "Configuring QoS shapers" on page 282.

Creating a meter

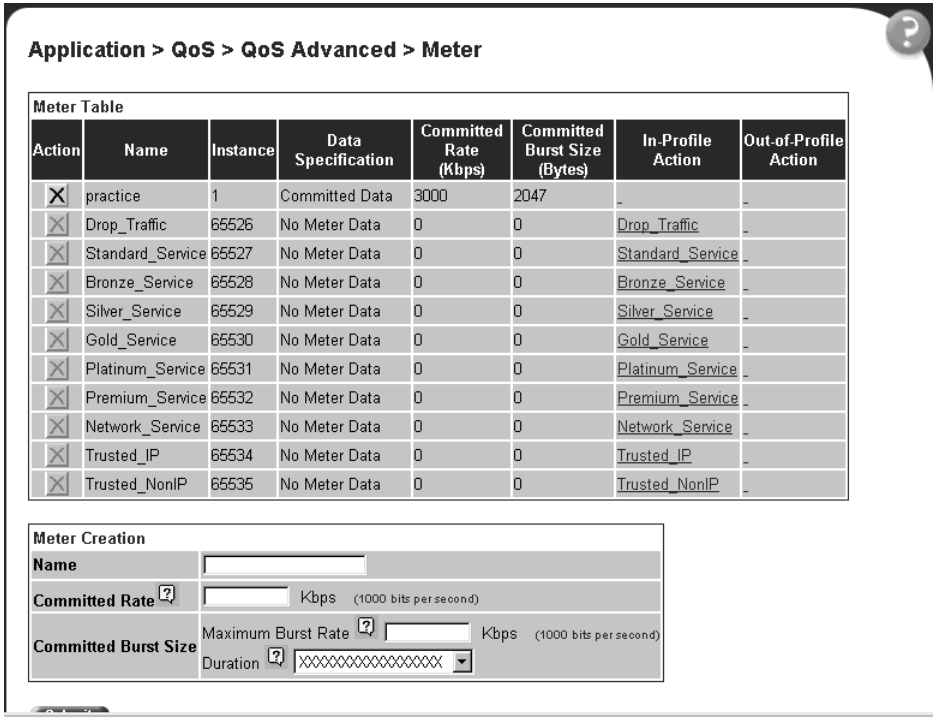
To create a meter:

1. From the main menu, choose Application > QoS > QoS Advanced > Meters.

   The Qos Advanced Meter page opens (Figure 156). This table displays all meters you created with QoS Wizard, QoS Quick Config, and QoS Advanced.

Note: Beginning with software version 2.0, there are default meters for each service class.

Figure 156 QoS Advanced Meter page



2 In the Meter Creation area, create the meter.

Table 94 describes the fields in the Meter Creation area, which you use to set new meters.

Table 94 Meter Creation fields

Item	Range	Description
Name	1 to 16 alphanumeric characters with no spaces	Enter the name for the meter you are creating.
Committed Rate	13 - 1,700,000 Kbps	Enter the Committed Rate in Kbps here.
Committed Burst Size	2,047 to 131,071 bytes Up to 7 durations	Maximum Burst Rate—Enter the Maximum Burst Rate in bytes. Duration—From the pull-down menu, choose 1 of up to 7 durations for the period that the Maximum Burst Rate is allowed.

3 Click Submit.

4 If you have not already specified the interface assignments, choose Applications > QoS > QoS Advanced > Devices > Interface Configuration page to connect the desired ports to the desired filters.

Note: Meter configurations are not modifiable. They must be deleted and the information re-entered.

Viewing meters

To view a meter:

1 From the main menu, choose Application > QoS > QoS Advanced > Meters.

The QoS Advanced Meters page opens (Figure 156).

2 View created meters in the Meter Table.

Table 95 describes the fields in the Meter Table area.

Table 95 Meter Table fields

Item	Range	Description
Action		Deletes the meter.
Name		Displays the name of the meter.
Instance		Displays the unique identifier.
Data Specification	(1) No Meter Data (2) Metered Data	Displays whether the meter has metered data or not. (All meters created with software version 2.0 or higher have only metered data.)
Committed Rate	13 - 1,700,000 Kbps	Displays the Committed Rate in kbps.
Committed Burst Size	2,047 to 131,071 bytes	Displays the Committed Burst Size in bytes.
In-Profile Action	Configured, user-defined action	Displays the In-Profile Action for this meter.
Out-Profile Action	Configured, user-defined action	With a meter using metered data, this field displays the action specified for traffic that is out-of-profile. With a meter using no metered data, this field displays N/A. (All meters created with software version 2.0 or higher have only metered data.)

Deleting a meter

To delete a meter:

1. From the main menu, choose Application > QoS > QoS Advanced > Meters.

   The Meter page opens (Figure 156).

2. In the Meter Table section, click the Delete icon to delete the meter.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the meter configuration.
   - Click Cancel to return to the Meter page without making changes.

Note: You cannot delete a meter that is referenced by a policy. You must delete the policy first.

Configuring QoS shapers

Note: You must be using either the BPS2000-1GT, BPS2000-2GT, or BPS2000-2GE MDA with the Business Policy Switch in order to implement the QoS shaping features.

Using the QoS Advanced pages, you can create, view, or delete shapers. If you do not want to shape the data in your flow, go to "Configuring QoS policies" on page 285.

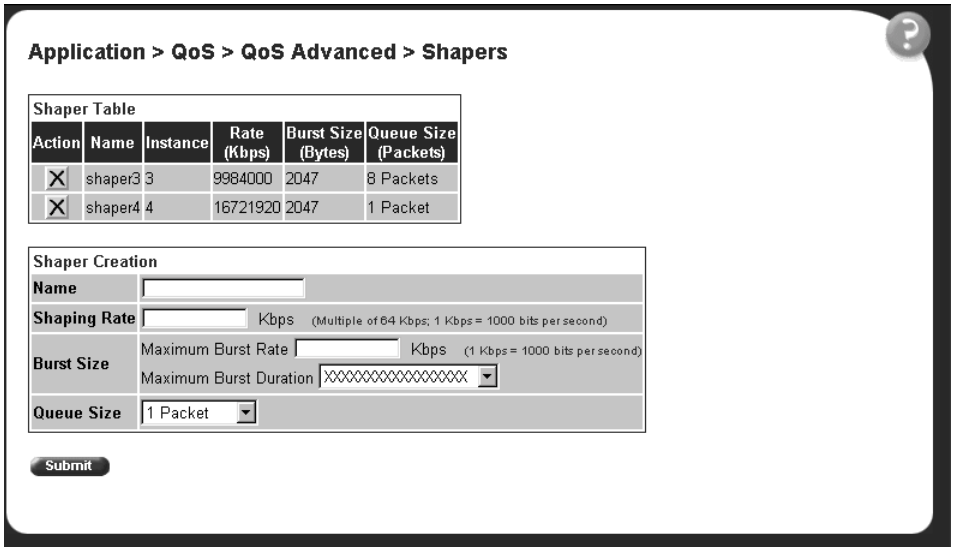
Creating a shaper

To create a shaper:

1 From the main menu, choose Application > QoS > QoS Advanced > Shapers.

The Qos Advanced Shapers page opens (Figure 157). All Shapers, including those created using the QoS Wizard and Qos Quick Config pages, display on this page.

Figure 157 QoS Advanced Shapers page



2 In the Shaper Creation area, create the shape.

Table 94 describes the fields in the Shaper Creation area, which you use to set new shapers.

Table 96 Shaper Creation fields

Item	Range	Description
Name	1 to 16 alphanumeric characters with no spaces	Enter the name for the shaper you are creating.
Shaping Rate	1 - 4294967296	Enter the Shaping Rate in Kbps here. This is the maximum rate at which traffic shaped using this shaper will be transmitted over a given duration. Note: The system rounds up the shaping rate you enter to a multiple of 64 Kbps.

Table 96 Shaper Creation fields (continued)

Item	Range	Description
Burst Size	6 durations	Maximum Burst Rate—Enter the Maximum Burst Rate in Kbps. This determines the maximum traffic burst size that can be transmitted without a shaping delay. Duration—From the pull-down menu, choose 1 of the 6 durations for the period that the Maximum Burst Rate is allowed.
Queue Size	1, 2, 4, 8, or 16 packets	Choose the queue depth from the pull-down menu. This is the number of packets that can exceed the traffic burst size and still be queued for transmission.

3 Click Submit.

Note: Shaper configurations are not modifiable. They must be deleted and the information re-entered.

Viewing shapers

To view a shaper:

1 From the main menu, choose Application > QoS > QoS Advanced > Shapers.

The QoS Advanced Shapers page opens (Figure 156).

2 View created shapers in the Shaper Table. This table displays all the shapers you configured, including those with QoS Wizard and QoS Quick Config.

Table 97 describes the fields in the Shaper Table area.

Table 97 Shaper Table fields

Item	Range	Description
Action		Deletes the shaper.
Name		Displays the name of the shaper.
Instance		Displays the unique identifier.
Rate	1 - 4294967296	Displays the maximum rate at which traffic shaped using this shaper will be transmitted over a given duration. Displays the rate rounded up to multiples of 64 Kbps.

Table 97 Shaper Table fields (continued)

Item	Range	Description
Burst Size		Displays the maximum traffic burst size that can be transmitted without a shaping delay. Calculated internally using the configured Maximum Burst Rate and Maximum Burst Duration.
Queue Size	1, 2, 4, 8, or 16 packets	Displays the number of packets that can exceed the traffic burst size and still be queued for transmission.

Deleting a shaper

To delete a shaper:

1. From the main menu, choose Application > QoS > QoS Advanced > Shapers.

   The Qos Advanced Shaper page opens (Figure 157).

2. In the Shaper Table section, click the Delete icon to delete the shaper.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the shaper configuration.
   - Click Cancel to return to the Shaper page without making changes.

Note: You cannot delete a shaper that is referenced by a policy. You must delete the policy first.

Configuring QoS policies

You can configure QoS policies by creating filters in the hardware that apply a set of packet filtering criteria and actions to individual interfaces.

If you want to meter your data, you must reference both an In-Profile action and an Out-Profile action. The In-Profile action directs the switch how to handle the data flow that is within the meter you set (refer to "Configuring QoS meters"), and the Out-Profile directs the switch how to handle all other data.

Installing defined filters

To create a hardware policy filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Policies.

The QoS Advanced Policies page opens (Figure 158). This table displays all configured policies, including ones created with QoS Wizard and QoS Quick Config.

Figure 158 QoS Advanced Policies page

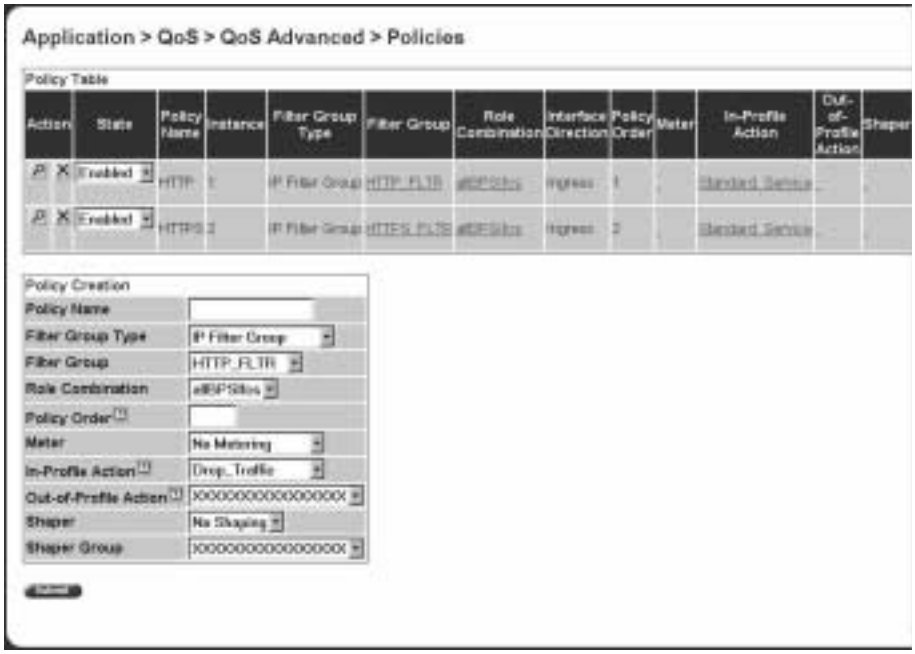


Table 98 describes the items on the QoS Advanced Policy page.

Table 98 Policy page items

Section	Item and MIB association	Range	Description
Policy Table	Action		Opens a view only statistics table. The table displays current filter statistics in bytes and packets.
			Deletes the row.
	State	(1) Enabled (2) Disabled	Enables or disables the policy.
	Policy Name	1..16	A list of the names of existing target configurations.
	Instance		Displays the unique identifier.
	Filter Group Type		The type of filter group that is referenced by this instance of the Target class. The options are: IP Filter Group or Layer2 Filter Group.
	Filter Group		The filter group that is associated with this target.
	Role Combination		The interfaces to which this target specification applies, specified in terms of a role combination tag.
	Interface Direction		The direction of packet flow at the interface to which this target specification applies.
	Policy Order		The number used to determine the order of precedence for this target specification.
	Meter		The meter associated with this entry, if there is one.
	In-Profile Action		Displays the name of the In-Profile action for this policy.
	Out-of-Profile Action		Displays the name of the Out-of-Profile action for this policy. This field applies only to metered data.
	Shaper		Displays the name of the shaper for this policy, if there is one
	Shaper Group	2 - 63	Displays the shaper group ID for this policy.
Policy Creation	Policy Name	1..64	Type a character string to create a unique name to identify this policy.
	Filter Group Type (qosTargetAclType)	(1) IP Filter Group (2) Layer2 Filter Group	Choose the type of filter group to associate with this policy.
	Filter Group		Choose the filter group to associate with this policy.

Table 98 Policy page items

Section	Item and MIB association	Range	Description
	Role Combination (qosTargetInterfaceRoles)		Choose the type of interface to which this policy applies, specified in terms of a role combination.
	Policy Order (qosTargetOrder)	Integer	Enter a number to use as a determinate of the order of precedence for this filter.
	Meter (qosTargetMeter)		Choose the meter associated with this entry.
	In-Profile Action (qosTargetInProfilelAction)		Choose the action you want to take for the data associated with this policy.
	Out-of-Profile Action (qosTargetOutOfProfilelAction)		Choose the action you want to take associated with this policy for metered data that is not within the configured profile.
	Shaper (qosTargetShaping Params)		Choose the shaper, if any, to apply to this policy
	Shaper Group (qosTargetShapingGroup)	2- 63	Choose the shaper group, if any, to apply to this policy.

2 Complete the fields as described.

3 Click Submit.

Note: Beginning with software version 2.0, you can enable or disable a policy. The default setting is Enabled.

Viewing hardware policy statistics

To view statistics for a selected hardware policy configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Policies.

The QoS Advanced Policies page opens (Figure 158).

2 In the Policy Table section, in the filter group configuration of your choice, click the View icon.

The Policy Statistics page opens (Figure 159).

Figure 159 Policy Statistics page

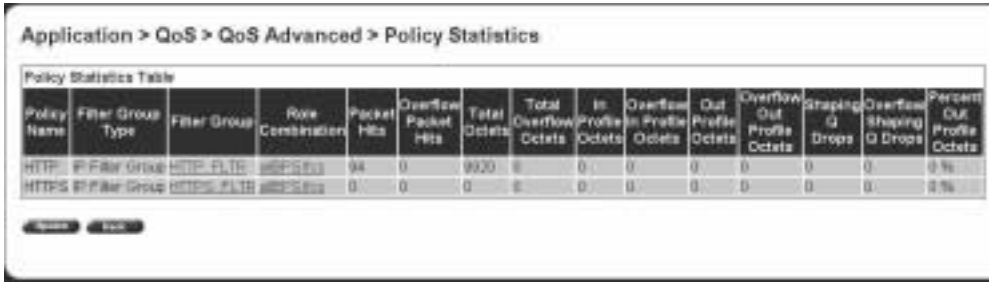


Table 99 describes the items on the Policy Statistics page.

Table 99 Policy Statistics page items

Item and MIB association	Description
Policy Name	The name of the selected policy.
Filter Group Type	The type of group that is referenced by this instance of the filter policy class. The options are: IP Filter Group or Layer2 Filter Group.
Filter Group	The filter group associated with the selected policy.
Role Combination	The interfaces to which this policy applies, specified in terms of a role combination.
Packet Hits (ntnQosTargetStatsPkHits)	The packets selected for additional processing. The action taken is based on a match with specified filter and/or threshold information.
Overflow Packet Hits (ntnQosTargetStatsOverflowPkHits)	The number of times the associated ntnQosTargetStatsPktHits counter overflowed.
Total Octets (ntnQosTargetStatsTotalOctets)	The total number of octets associated with packet hits for this policy.
Total Overflow Octets (ntnQosTargetStatsTotalOverflowOctets)	The total number of times the associated ntnQosTargetStatsTotalOctets counter overflowed.
In Profile Octets (ntnQosTargetStatsTotalInProfOctets)	The total number of in-profile octets associated with packet hits for this policy.
Overflow In Profile Octets (ntnQosTargetStatsTotalInProfOverflowOctets)	The number of times the associated ntnQosTargetStatsTotalInProfOctets counter overflowed.
Out Profile Octets (ntnQosTargetStatsTotalOutProfOctets)	The total number of out-of-profile octets associated with packet hits for this policy.

Table 99 Policy Statistics page items (continued)

Item and MIB association	Description
Overflow Out Profile Octets (ntnQosTargetStatsTotalOutProfOverflowOctets)	The number of times the associated ntnQosTargetStatsTotalOutProfOctets counter overflowed.
Shaping Q Drops (ntnQosTargetStatsShapingQDrops)	The total number of octets dropped from the shaping queues for this policy.
Overflow Shaping Q Drops (ntnQosTargetStatsOverflowShapingQDrops)	The number of times the associated ntnQosTargetStatsShapingQDrops counter overflowed.
Percent Out Profile Octets	The percentage of out-of-profile octets associated with packet hits for this policy.

3 To refresh the hardware policy statistics, click Update.

Deleting a hardware policy configuration

To delete a hardware policy configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Policies.

The QoS Advanced Policies page opens (Figure 158).

2 In the Policy Table section, in the hardware policy configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the hardware policy configuration.
- Click Cancel to return to the Policy page without making changes.

Configuring QoS Policy Agent (QPA) characteristics

You can configure QPA operational parameters.

To open the Agent page:

1 From the main menu, choose Application > QoS > QoS Advanced > Agent.

The Agent page opens (Figure 160 and Figure 161).

Figure 160 Agent page (1 of 2)

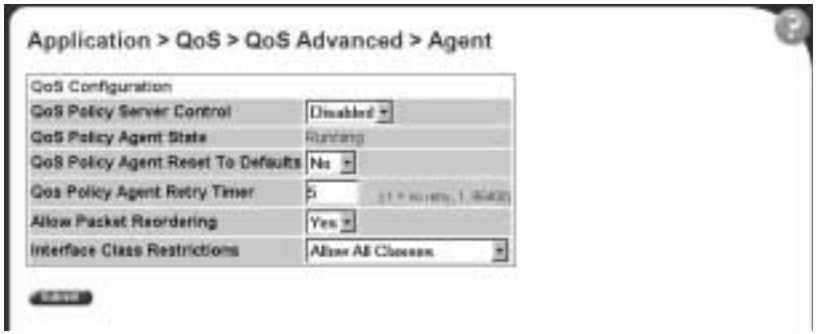
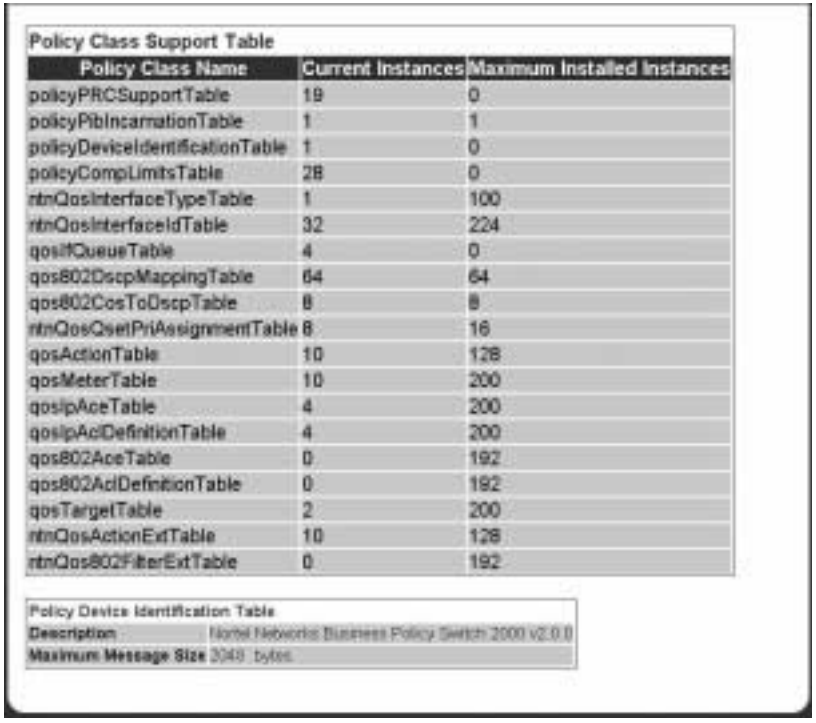


Figure 161 Agent page (2 of 2)



Policy Class Support Table

Policy Class Name	Current Instances	Maximum Installed Instances
policyPRCSupportTable	19	0
policyPibIncarnationTable	1	1
policyDeviceIdentificationTable	1	0
policyCompLimitsTable	28	0
ntnQosInterfaceTypeTable	1	100
ntnQosInterfaceIdTable	32	224
qosIfQueueTable	4	0
qos802DscpMappingTable	64	64
qos802CosToDscpTable	8	8
ntnQosQsetPriAssignmentTable	8	16
qosActionTable	10	128
qosMeterTable	10	200
qosIpAceTable	4	200
qosIpAclDefinitionTable	4	200
qos802AceTable	0	192
qos802AclDefinitionTable	0	192
qosTargetTable	2	200
ntnQosActionExtTable	10	128
ntnQos802FilterExtTable	0	192

Policy Device Identification Table

Description	Nortel Networks Business Policy Switch 2000 v2.0.0
Maximum Message Size	2048 bytes

Table 100 describes the items on the Agent page.

Table 100 Agent page items

Section	Item and MIB association	Range	Description
QoS Configuration	QoS Policy Server Control	Enabled Disabled	Choose to enable or disable the QoS Policy server control. Note: Choosing to enable COPS disables local policy control.
	QoS Policy Agent State (ntnQosConfigQpaState)	Running Initialized Disabled	The current status of the policy agent.
	QoS Policy Agent Reset to Defaults (ntnQosConfigQpaState)	(1) Yes (2) No	Choose whether or not to reset the policy agent to the default settings.
	QoS Policy Agent Retry Timer (ntnQosConfigQpaRetryTimer)	-1 = no retry, 1..86400	Type the time, in seconds, between the receipt of a connection termination/rejection indication and the start of a new connection request. Note: A value of -1 indicates that a connection retry should not be attempted after a failed attempt.
	Allow Packet Reordering (ntnQosConfigAllowPacket Reordering)	(1) Yes (2) No	Support for certain PHBs requires that packets within a flow not be reordered when transmitted. Choose: • Yes—Allows full flexibility of assigning packet to egress queue. • No—Agent verifies that in-profile and out-of-profile actions associated with the flow do not cause packets from same flow to be assigned to different egress queues.
	Interface Class Restrictions (ntnQosConfigIfcClassRestrictions)	Allow All Classes Trusted and Unrestricted Unrestricted Only	Specify which interface class types can be defined by the user. Default filters are installed to support the different interface classes. Limiting the classes that can be used reduces, or eliminates entirely, the default filter resources that must be consumed, making these resources available for administrator use. Note: Modifications to this attribute will not take effect until the system is initialized.
Policy Class Support Table	Policy Class Names		The name of the policy.

Table 100 Agent page items (continued)

Section	Item and MIB association	Range	Description
	Current Instances		The current class entries.
	Maximum Installed Instances		The maximum number of allowed class entries.
Policy Device Identification Table	Description		The system description.
	Maximum Message Size		The maximum target message size supported by the device.

2 In the QoS Configuration section, type information in the text boxes, or select from a list.

3 Click Submit.

Chapter 10
Implementing Common Open Policy Services (COPS)

Enabling COPS in your networks allows the policy server to:

- Gather all relevant information.
- Make a decision based on your (as network administrator) set policies and network resources,
- Communicate that decision in the form of proper service to the appropriate group or client (bandwidth, ACLs, QoS).

A solid COPS strategy is closely tied to Internet Protocol (IP) address management and network management.

This chapter discusses the COPS options available to you in the Web-based management interface.

The COPS options are:

- Viewing COPS statistics and capabilities (next)
- Creating COPS client configurations (page 300)

Viewing COPS statistics and capabilities

You can view a list of the capabilities of the COPS client to connect to a COPS server and view a table displaying the current status of all COPS server connections.

To view COPS capabilities and statistics:

1 From the main menu, choose Application > COPS > Status.

The Status page opens (Figure 162).

Figure 162 Status page

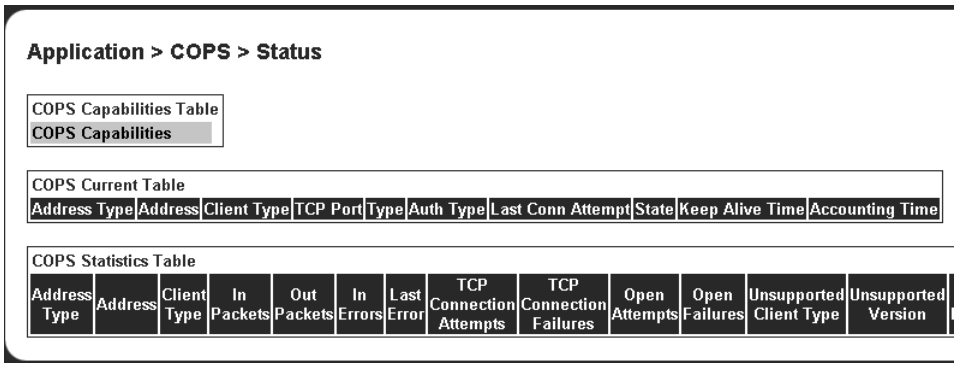


Table 101 describes the items on the Status page.

Table 101 Status page items

Section	Item	Descriptions
COPS Capabilities Table	COPS Capabilities	A list of COPS protocols supported by the Business Policy Switch 2000. The current supported version is COPSv1 protocol.
COPS Current Table	Address Type	The type of address in copsClientServerAddress.
	Address	The IPv4, IPv6, or DNS address of a COPS server.
	Client Type	The protocol client type for this entry. Note: Multiple client types can be served by a single COPS server. Note: The value 0 (zero) indicates that this entry contains information about the underlying connection.
	TCP Port	The TCP port number on the COPS server to which the client is connected.

Table 101 Status page items (continued)

Section	Item	Descriptions
COPS Current Table, cont.	Type	The indicator of the source of the COPS server information. Note: COPS servers can be configured by network management into copsClientServerConfigTable and appear in this entry with type copsServerStatic(1). Alternatively, the type, or entry, can be a notification from another COPS server by way of the COPS PDP-Redirect mechanism and appear as copsServerRedirect(2).
	Authorization Type	The indicator of the current security mode in use between the client and the COPS server.
	Last Conn Attempt	The timestamp of the last time the client attempted to connect to this COPS server.
	State	The operational state of the connection and COPS protocol with respect to this COPS server.
	Keep Alive Time	The value of the Keepalive timeout, in centiseconds, currently in use by the client, as specified by the COPS server in the Client-Accept operation. Note: A value of 0 (zero) indicates no keepalive activity is expected.
	Accounting Time	The value of the COPS protocol Accounting timeout, in centiseconds, currently in use by the client, as specified by the COPS server in the Client-Accept operation. Note: A value of 0 (zero) indicates that the client should not send any unsolicited accounting reports.
COPS Statistics Table	Address Type	The type of address in copsClientServerAddress.
	Address	The IPv4, IPv6, or DNS address of a COPS server.
	Client Type	The protocol client type for this entry. Note: Multiple client types can be served by a single COPS server. Note: The value 0 (zero) indicates that this entry contains information about the underlying connection.
	In Packets	The total number of COPS packets that the client has received from this COPS server marked for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
	Out Packets	The total number of COPS packets that the client has sent to this COPS server marked for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
	In Errors	The total number of COPS packets that the client has received from this COPS server marked for the selected client type that contained errors in syntax. Note: This is a cumulative value and *is not* zeroed on new connections.
	Last Error	The code contained in the last COPS protocol Error Object received by the client from this COPS server marked for the selected client type. Note: This value *is not* zeroed on COPS Client-Open operations.

Table 101 Status page items (continued)

Section	Item	Descriptions
COPS Statistics Table, cont.	TCP Connection Attempts	The number of times that the COPS client attempted to open a TCP connection to the COPS server. Note: This value is valid only for client type 0. Note: This is a cumulative value and *is not* zeroed on new connections.
	TCP Connection Failures	The number of times that the COPS client failed to open a TCP connection to the COPS server. Note: This value is valid only for client type 0. Note: This is a cumulative value and *is not* zeroed on new connections.
	Open Attempts	The number of times that the COPS client attempted to perform a COPS Client-Open to a COPS server for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
	Open Failures	The number of times that the COPS client failed to perform a COPS Client-Open to a COPS server for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
	Unsupported Client Type	The total number of COPS packets that this client has received from COPS servers that referred to client types that are unsupported by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Unsupported Version	The total number of COPS packets that this client has received from COPS servers marked for the selected client type that had a COPS protocol version number that is unsupported by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Length Mismatch	The total number of COPS packets that the client received from COPS servers marked for the selected client type that had a COPS protocol message length that did not match the actual received packet. Note: This is a cumulative value and *is not* zeroed on new connections.
	Unknown Opcode	The total number of COPS packets that the client received from COPS servers marked for the selected client type having a COPS protocol Op Code not recognized by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Unknown Cnum	The total number of COPS packets that the client received from COPS servers marked for the selected client type containing a COPS protocol object C-Num not recognized by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Bad Ctype	The total number of COPS packets that the client received from COPS servers marked for the selected client type containing a COPS protocol object C-Type not defined for the C-Nums known by the client. Note: This is a cumulative value and *is not* zeroed on new connections.

Table 101 Status page items (continued)

Section	Item	Descriptions
COPS Statistics Table, cont.	Bad Sends	The total number of COPS packets that the client attempted to send to COPS servers marked for the selected client type that resulted in a transmit error. Note: This is a cumulative value and *is not* zeroed on new connections.
	Wrong Objects	The total number of COPS packets that the client received from COPS servers marked for the selected client type not containing a permitted set of COPS protocol objects. Note: This is a cumulative value and *is not* zeroed on new connections.
	Wrong OpCode	The total number of COPS packets that the client received from COPS servers marked for the selected client type having a COPS protocol Op Code that should not have been sent to a COPS client, for example, Open-Requests. Note: This is a cumulative value and *is not* zeroed on new connections.
	Timedout Clients	The total number of times that the client has been shut down for the selected client type by COPS servers that detected a COPS protocolKeepalive timeout. Note: This is a cumulative value and *is not* zeroed on new connections.
	Auth Failures	The total number of times that the client received a COPS packet marked for the selected client type that could not be authenticated using the authentication mechanism used by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Auth Missing	The total number of times that the client received a COPS packet marked for this client type not containing authentication information.

Creating a COPS configuration

You can select the COPS server(s) to use to obtain policy information by creating COPS configurations.

To create a COPS configuration:

1 From the main menu, choose Application > COPS > Configuration.

The Configuration page opens (Figure 163).

Figure 163 Configuration page

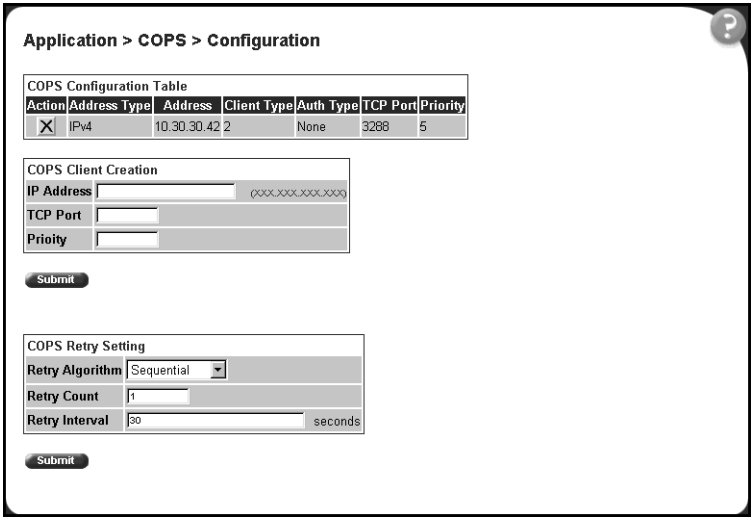


Table 102 describes the items on the COPS Configuration Table section of the Configuration page.

Table 102 COPS Configuration Table section items

Section	Item	Range	Description
COPS Configuration Table			Deletes the row.
	Address Type		The type of address in copsClientServerConfigAddress.
	Address		The IPv4, IPv6, or DNS address of the COPS server.
	Client Type		The COPS protocol client type this COPS server is capable of serving. Note: A single COPS server can serve multiple client types.

Table 102 COPS Configuration Table section items (continued)

Section	Item	Range	Description
COPS Configuration Table, cont.	Auth Type		The authentication mechanism for this COPS client to request when negotiating security at the start of a connection to a COPS server.
	TCP Port		The TCP port number on the COPS server.
	Priority		The level of priority assigned to the client. Note: When a COPS client attempts to contact COPS servers for the appropriate client type, it contacts higher numbers (priority) first. The order used for server entries with the same priority is undefined. COPS servers notified to the client using the COPS protocol PDP-Redirect mechanism are always processed with higher priority than any entries in this table.
COPS Client Creation	IP Address	XXX.XXX.XXX.XXX	The IP address of the COPS client.
	TCP Port	Integer	Type the TCP port number on the COPS server.
	Priority		Type a number that represents the level of priority. Note: When a COPS client attempts to contact COPS servers for the appropriate client type, it contacts higher numbers (priority) first. The order used for server entries with the same priority is undefined. COPS servers notified to the client using the COPS protocol PDP-Redirect mechanism are always processed with higher priority than any entries in this table.
COPS Retry Setting	Retry Algorithm	(1) Sequential (2) Round Robin	Choose the type of algorithm to use.
	Retry Count	Integer	Type the number of retry attempts.
	Retry Interval	Integer	Type, in seconds, the retry interval.

2 Type information in the text boxes, or select from a list.

Click Submit.

Note: COPS configurations are not modifiable. They must be deleted and the information recreated.

Deleting a COPS client configuration

To delete a COPS client configuration:

1 From the main menu, choose Application > COPS > Configuration.

The Configuration page opens (Figure 163).

2 In the COPS Configuration Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the configuration.
- Click Cancel to return to the Configuration page without making changes.

Chapter 11
Support menu

The customer support options available to you are:

- Help
- Release Notes
- Manuals
- Upgrade

Using the online help option

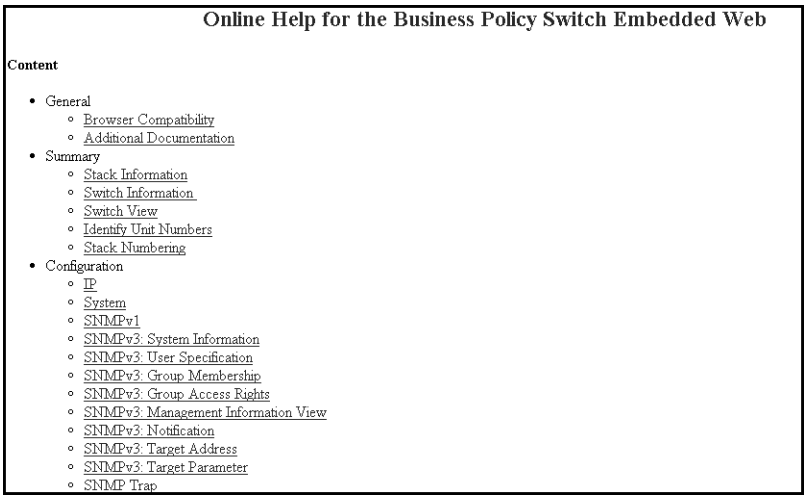
You can read information about management page functions in the online help menu embedded in the Web-based management interface.

To open online help:

1 From the main menu, choose Support > Help or click the Help icon located in the upper right corner of any management page.

The Online Help menu opens in a separate Web browser (Figure 164).

Figure 164 Online help window



2 Click on any content item to read information about the topic (if you clicked the Help icon on a management page, information about that page is immediately displayed).

3 Click Return to Top to return to the Content index.

4 Close the Web browser

Downloading technical publications

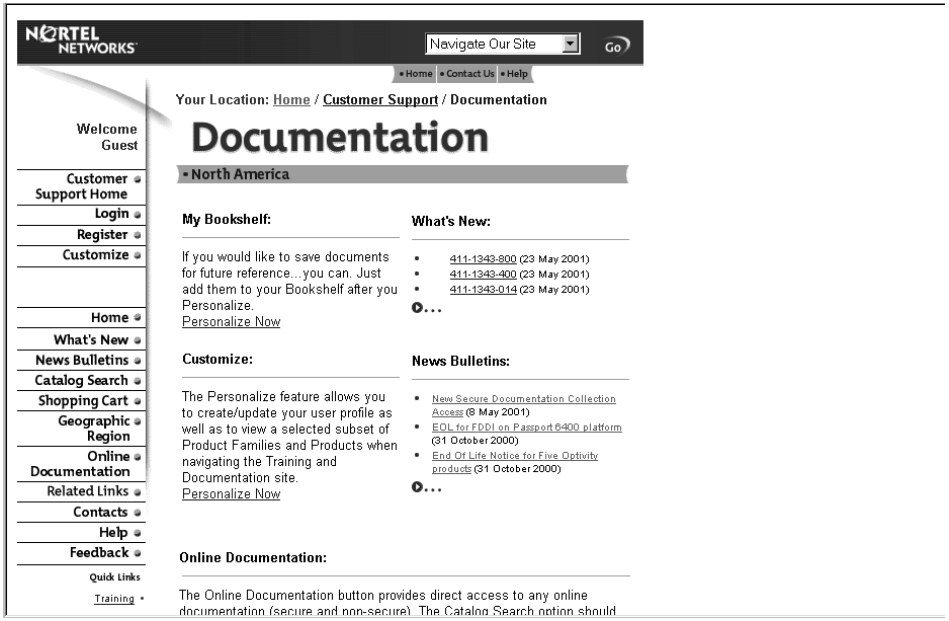
You can download current documentation about the Web-based management user interface from Nortel Networks Technical Documentation Web site.

To download current documentation:

1 From the main menu, choose Support > Release Notes.

Nortel Networks Technical Documentation Web site opens in a separate Web browser (Figure 165).

Figure 165 Nortel Networks Technical Documentation Web site



2 Locate your product, and click the document you want to download.

The BPS 2000 documentation is in the Data and Internet Product Family.

3 Click on the PDF icon to start the download process (you need Adobe Acrobat 3.0 or later to view or print documents from this site).

4 Follow the prompts to download the documentation.

5 Close the Web browser.

Upgrade option

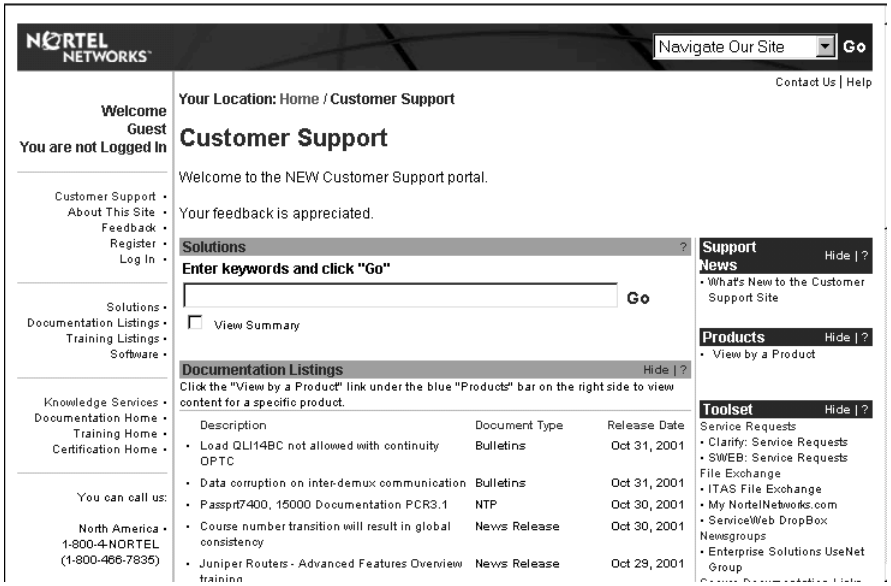
You can upgrade your Web-based management user interface to the most recent software release.

To upgrade to the most recent software release:

1 From the main menu, choose Support > Upgrade.

Nortel Networks Customer Support opens in a separate Web browser (Figure 166).

Figure 166 Nortel Networks Customer Support Web site



2 Follow the prompts to download the software release.

3 Close the Web browser.

Refer to Chapter 4 for complete instructions on downloading software to a standalone BPS 2000, to a stack of pure BPS 2000, and to a mixed (Hybrid) stack.

Index

Numbers

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W