Part No. 209570-A
August 2000

4401 Great America Parkway
Santa Clara, CA 95054

Using Web-Based Management for the Business Policy Switch 2000

NORTEL NETWORKS™

Nortel Networks NA Inc. software license agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License grant. Nortel Networks NA Inc. ("Nortel Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks NA Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED,

INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks, 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS

AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Figures

Tables

Preface

Welcome to *Using Web-Based Management for the Nortel Networks Business Policy Switch 2000*.

Default values are defined for all Business Policy Switch™ features that allow the switch to begin forwarding packets as soon as it is powered up and connected to compatible devices.

The Web-based management interface is one of many tools specifically designed to assist the network manager in creating complex standalone or network configurations. For information on the default values defined within the Business Policy Switch, or for information on additional products available to configure your switch, refer to *Using the Business Policy Switch 2000* (part number 208700-A).

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

Before you begin

This guide is intended for network managers who are responsible for configuring Business Policy Switches. 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 Business Policy Switch, refer to the following publications:

- *Using the Business Policy Switch 2000* (part number 208700-A)

  Describes how to use the Business Policy Switch 2000.

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

  Describes how to install the Business Policy Switch 2000.

- *Release Notes for the Business Policy Switch 2000* (part number 209320-A)

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

You can print selected technical manuals and release notes free, directly from the Internet. Go to the *http://www12.nortelnetworks.com/library* Web address. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe Acrobat Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to the Adobe Systems Web address at *www.adobe.com* to download a free copy of Acrobat Reader.

You can purchase selected documentation sets, CDs, and technical publications though the Internet at the *www1.fatbrain.com/documentation/nortel/* Web address.

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
EMEA	(33) (4) 92-966-968
North America	(800) 2LANWAN or (800) 252-6926
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

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 *www12.nortelnetworks.com/* URL and click ERC at the bottom of the page.

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 Business Policy Switch.

Requirements

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

- A computer connected to any of the network ports
- One of the following Web browsers installed on the computer:
  - 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 policy switch

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

Note: In order to use all the Business Policy Switch management features (for example, downloading software), you must connect your console terminal into a Business Policy Switch port within your mixed stack.

Logging in to the Web-based management interface

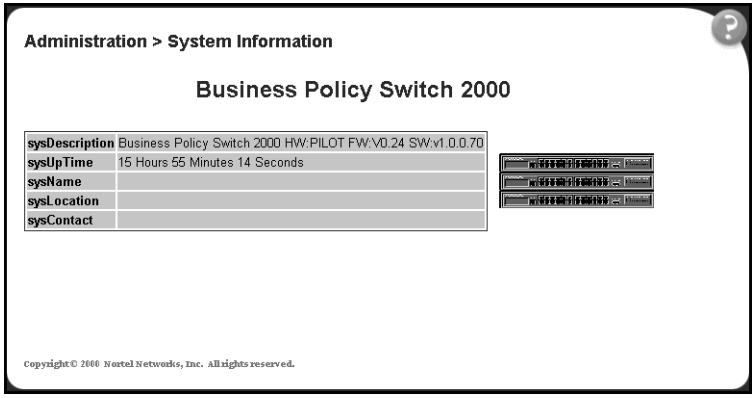
Before you log in to the Web-based management interface, use the console interface to verify the VLAN port assignments and to ensure that your switch CPU and your computer are assigned to the same VLAN. If the devices are not connected to the same VLAN, the IP address of the switch will not open the home page.

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, for example, http://10.30.31.105, and press [Enter].

   The home page opens (Figure 1).

Figure 1 Web-based management interface home page

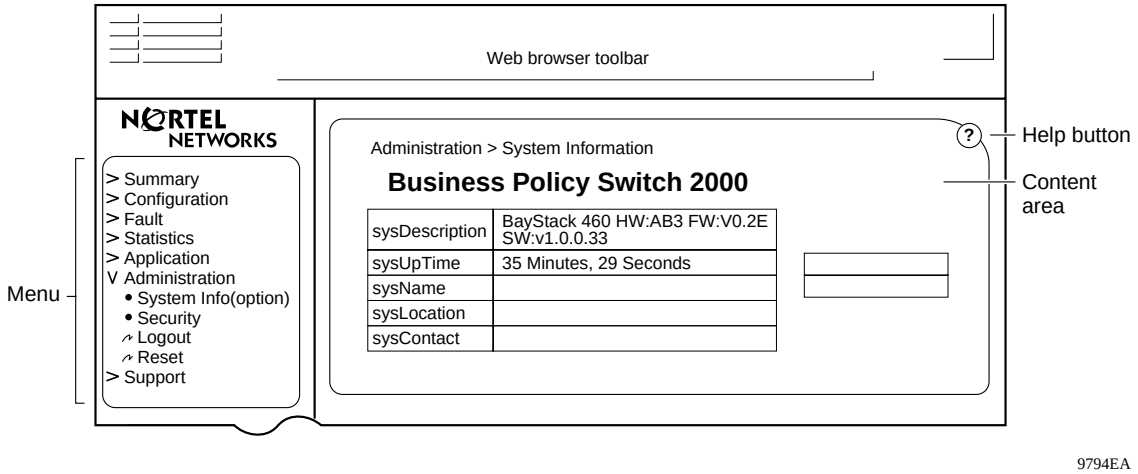


Network security does not yet exist the first time you access the Web-based management user interface. As the system administrator, you must create access parameters and passwords to protect the integrity of your network configuration(s). For more information on setting access parameters and system passwords, see “Configuring system security” on page 35.

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 Switch View Identify Unit Numbers (stack mode only) Stack Numbering (stack mode only)
Configuration	IP System 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
Statistic	Port Interface Ethernet Errors Transparent Bridging RMON Ethernet RMON History
Application	Port Mirroring Rate Limiting IGMP VLAN Spanning Tree Multilink Trunk QoS COPS
Administration	System Information Security Logout Reset Reset to Defaults
Support	Help Release Notes Manuals Upgrades

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.

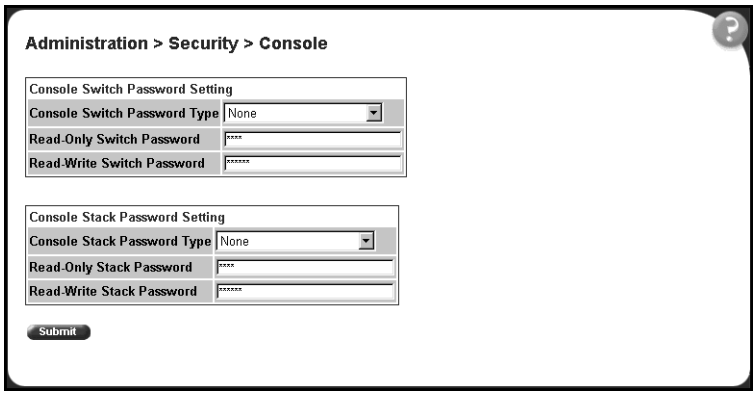
Table 2 Menu icons

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.
	Pie Chart	Displays statistics information in a pie chart format.
	Bar Graph	Displays statistics information in a bar graph format.
	Line Graph	Displays statistics information in a line graph format.
	Help	Accesses the 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:

- Viewing system information (next)
- Setting system passwords and remote access parameters (page 35)
- Logging in to the management interface (page 38)
- Logging out of the management interface (page 39)
- Resetting the management interface (page 39)

Viewing system information

You can view an image of the Business Policy Switch 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, see "Modifying system settings" on page 56.

Figure 4 System Information home page

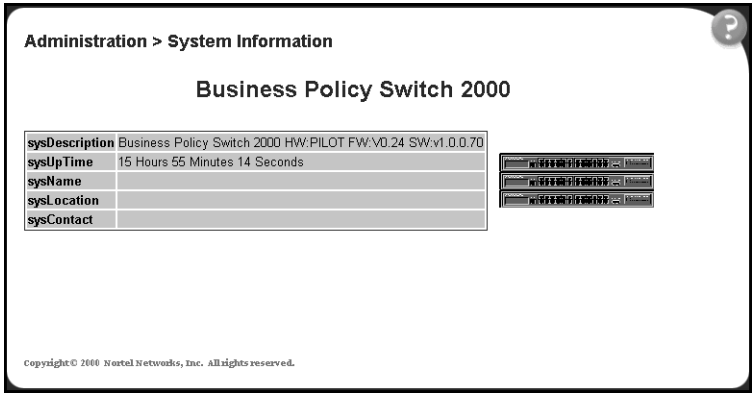


Table 4 describes the items on the System Information page.

Table 4 System Information page items

Item	Description
sysDescription	The default description of the Business Policy Switch 2000.
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.

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

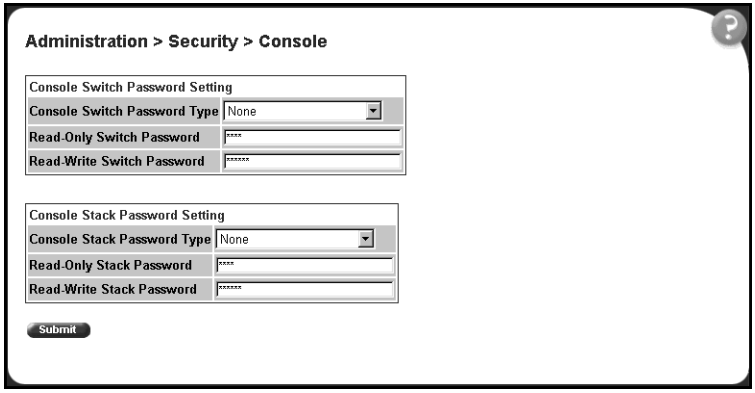


Table 5 describes the items on the Console page.

Table 5 Console page items

Section	Item	Setting	Description
Note: Console, Telnet, and Web settings share the same switch and stack password type and password.			
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	Type the read-only password setting for the read-only access user.
	Read-Write Switch Password	1..15	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 switch password types. Note: The default is None.
	Read-Only Stack Password	1..15	Type the read-only password setting for the read-only access user.
	Read-Write Stack Password	1..15	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 remote dial-in access security

To configure remote dial-in access security parameters:

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

The RADIUS page opens.

Figure 6 RADIUS page

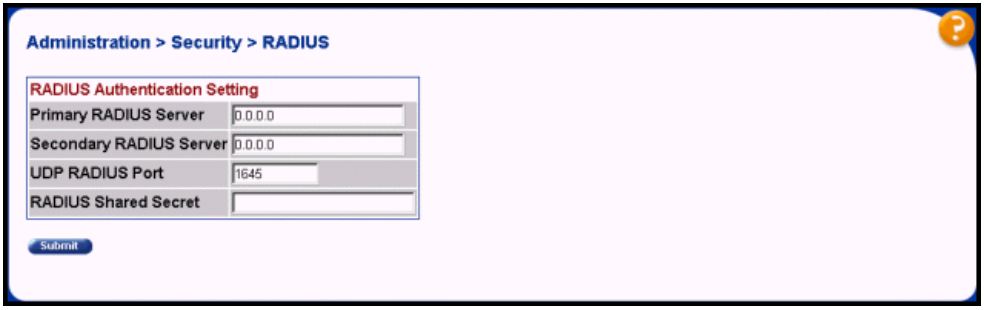


Table 6 describes the items on the RADIUS page.

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.

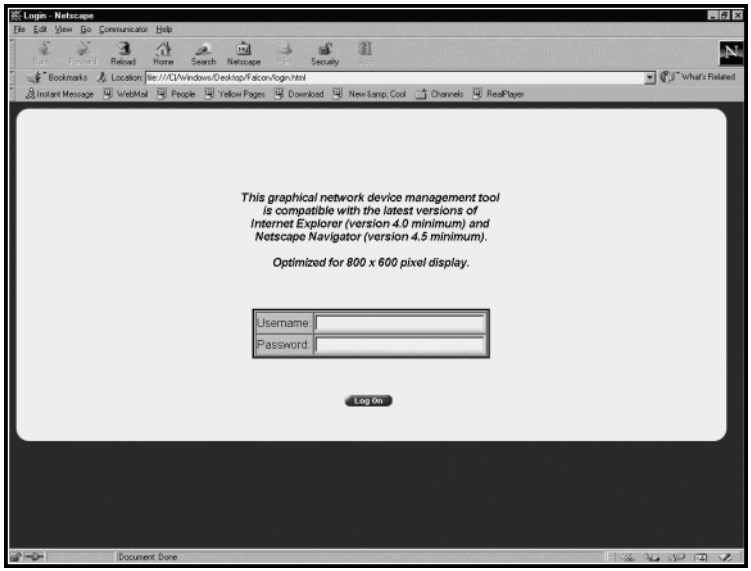
2 Type the information.

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

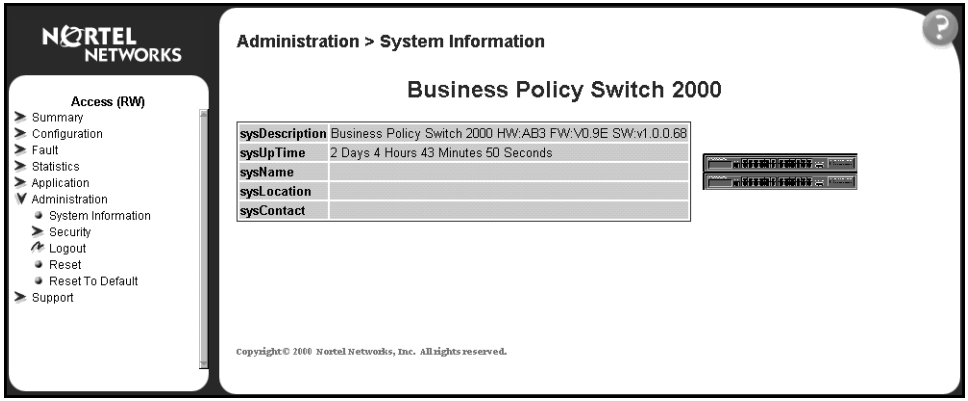


To log on to the Web-based management interface:

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 pre-defined user levels are available and each user level has a corresponding username and password.

Table 7 shows an example of the two pre-defined 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 Business Policy Switch

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.

To reset the Business Policy Switch without making changes (since your last Submit request):

1 From the main menu, choose Administration > Reset.

The Reset page opens (Figure 9).

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 26. If you have configured system password security, a reset returns you to a log on page, as shown in Figure 7 on page 38.

Resetting the Business Policy Switch 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. For more information on factory default settings, see *Using the Business Policy Switch 2000* (208700-A).

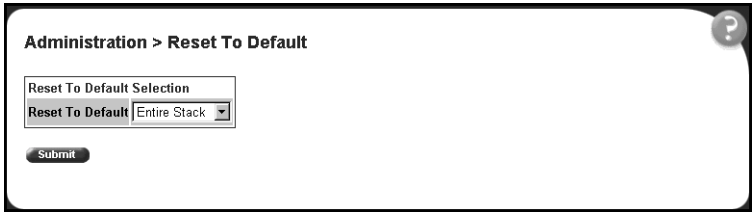
During the reset process, the switch initiates a self-test that comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

To reset the Business Policy Switch to system defaults:

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

The Reset to Default page opens (Figure 10).

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 26. If you have configured system password security, a reset returns you to a log on page, as shown in Figure 7 on page 38.

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:

- Viewing stack information (next)
- Viewing switch information (page 45)
- Viewing switch information in real time (page 47)
- Viewing and configuring stack numbering (page 49)
- Identifying unit numbers (page 51)

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.

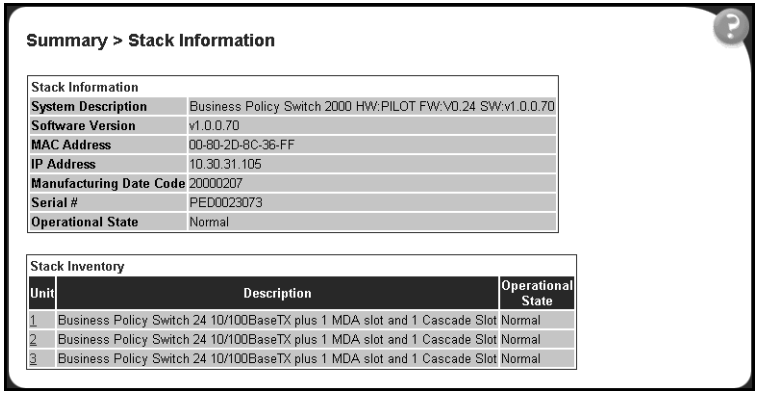
Note: The Web-based management user interface automatically detects the operational mode of your system. If the system is in standalone mode, the Stack Information page is not an option listed in the menu. For information on how to set system operational modes, see "Setting system operational modes" on page 93.

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



Summary > Stack Information

Stack Information

System Description	Business Policy Switch 2000 HW:PILOT FW:V0.24 SW:v1.0.0.70
Software Version	v1.0.0.70
MAC Address	00-80-2D-8C-36-FF
IP Address	10.30.31.105
Manufacturing Date Code	20000207
Serial #	PED0023073
Operational State	Normal

Stack Inventory

Unit	Description	Operational State
1	Business Policy Switch 24 10/100BaseTX plus 1 MDA slot and 1 Cascade Slot	Normal
2	Business Policy Switch 24 10/100BaseTX plus 1 MDA slot and 1 Cascade Slot	Normal
3	Business Policy Switch 24 10/100BaseTX plus 1 MDA slot and 1 Cascade Slot	Normal

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 49.
	Description	The description of the device or its subcomponent.
	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

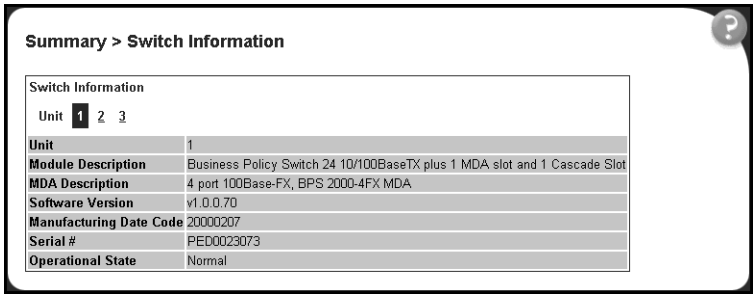


Table 9 describes the fields on the Switch Information page.

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 49.
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 Data 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.

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.

Viewing switch information in real time

You can display the port and LED status information of a selected policy switch in real time.

To display a physical view of the policy switch:

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

The Switch View page opens in a separate Web browser (Figure 13).

Figure 13 Switch View page

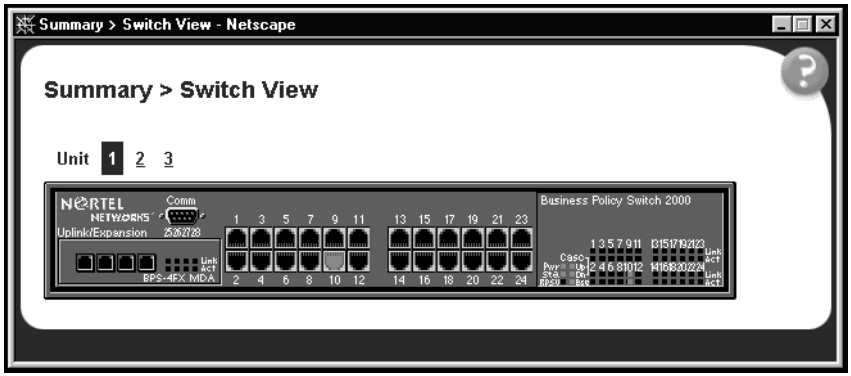


Table 10 describes the fields on the Switch View page.

Table 10 Business Policy Switch switch LED descriptions

Label	Type	Color	State	Meaning
Pwr	Power status	Green	On	DC power is available to the switch's internal circuitry.
			Off	No AC power to switch or power supply failed.
Status	System status	Green	On	Self-test passed successfully and switch is operational.
			Blinking	A nonfatal error occurred during the self-test.
			Off	The switch failed the self-test.
RPSU	RPSU status	Green	On	The switch is connected to the RPSU and can receive power if needed.
			Off	The switch is not connected to the RPSU or RPSU is not supplying power.
CAS Up Stack mode			Off	The switch is in standalone mode.
		Green	On	The switch is connected to the *upstream* unit's Cascade A In connector.
		Amber	On	The Cascade A Out connector (CAS Up) for this switch is looped internally (wrapped to the secondary ring).
CAS Dwn Stack mode			Off	The switch is in standalone mode.
		Green	On	The switch is connected to the *downstream* unit's Cascade A Out connector.
		Amber	On	The Cascade A In connector (CAS Dwn) for this switch is looped internally (wrapped to the secondary ring).
Base	Base mode	Green	On	The switch is configured as the stack base unit.
			Off	The switch is *not* configured as the stack base unit (or is in standalone mode).
		Amber	On	This unit is operating as the stack configuration's *temporary base unit*. This condition occurs automatically if the base unit (directly downstream from this unit) fails. If this happens, the following events take place: The two units directly upstream and directly downstream from the failed unit automatically wrap their cascade connectors and indicate this condition by lighting their Cas Up and Cas Dwn LEDs (see Cas Up and Cas Dwn description in this table). If the temporary base unit fails, the next unit directly downstream from this unit becomes the new temporary base unit. This process can continue until there are only two units left in the stack configuration. This automatic failover is a temporary safeguard only. If the stack configuration loses power, the temporary base unit will not power up as the base unit when power is restored. For this reason, you should always assign the temporary base unit as the base unit (set the Unit Select switch to Base) until the failed unit is repaired or replaced.

Table 10 Business Policy Switch switch LED descriptions (continued)

Label	Type	Color	State	Meaning
10/100	10/100 Mb/s port speed indicator	Green	On	The corresponding port is set to operate at 100 Mb/s and the link is good.
		Amber	On	The corresponding port is set to operate at 10 Mb/s and the link is good.
			Off	The link connection is bad or there is no connection to this port.
Link	Link status	Green	On	Valid communications link established.
			Off	The communications link connection is bad or there is no connection to this port.
Activity	Port activity	Green or Amber	Blinking	Indicates network activity for the corresponding port. A high level of network activity can cause the LEDs to appear to be on continuously.

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

The Switch View page is updated with a view of 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 93.

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 14).

Figure 14 Stack Numbering Setting page

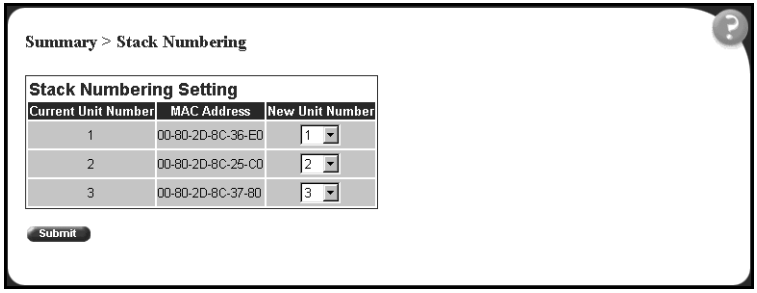


Table 11 describes the fields on the Stack Numbering Setting page.

Table 11 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

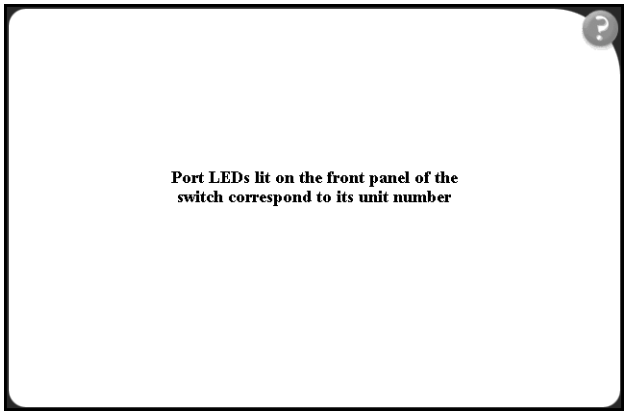
You can identify the unit numbers of the switches participating in a stack configuration by viewing the LEDs on the front panel of each switch.

To identify unit numbers in your configuration:

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

The Identify Unit Numbers page opens (Figure 15).

Figure 15 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:

- Configuring BootP, IP and gateway settings (next)
- Configuring system parameters (page 56)
- Configuring SNMPv1 (page 57)
- Configuring SNMPv3 (page 59)
- Configuring SNMP traps (page 78)
- Viewing learned MAC addresses (page 80)
- Finding MAC addresses (page 81)
- Port management (page 83)
- Managing high speed flow control (page 85)
- Downloading switch images (page 86)
- Downloading and uploading configuration files (page 86)
- Setting port baud rates (page 92)
- Setting system operational modes (page 93)

Note: In order to use all the Business Policy Switch management features (for example, downloading software), you must connect your console terminal into a Business Policy Switch port within your 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.

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 16).

Figure 16 IP page

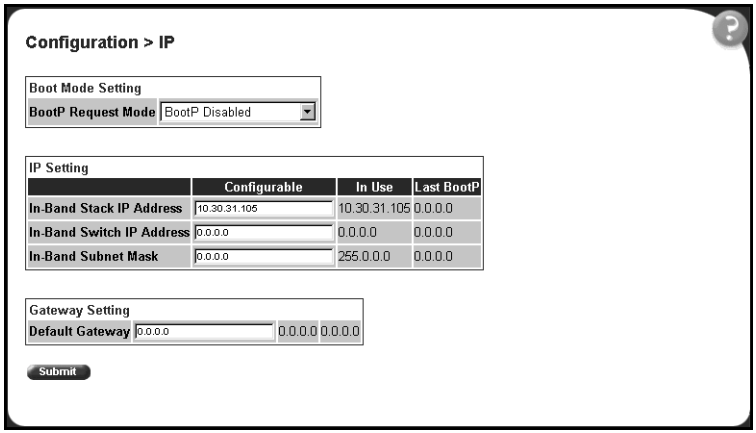


Table 12 describes the items on the IP page.

Table 12 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.
		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 26).

To configure system settings:

1 From the main menu, choose Configuration > System.

The System page opens (Figure 17).

Figure 17 System page

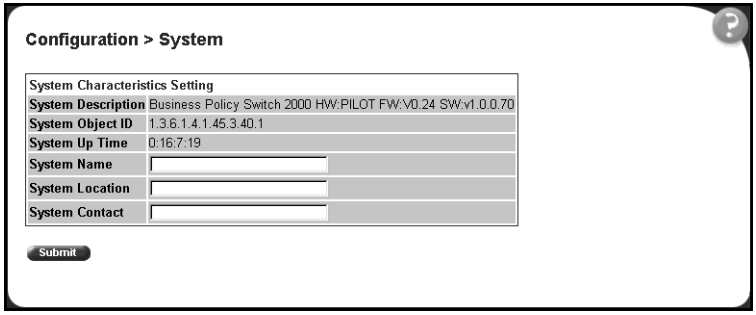


Table 13 describes the items on the System page.

Table 13 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

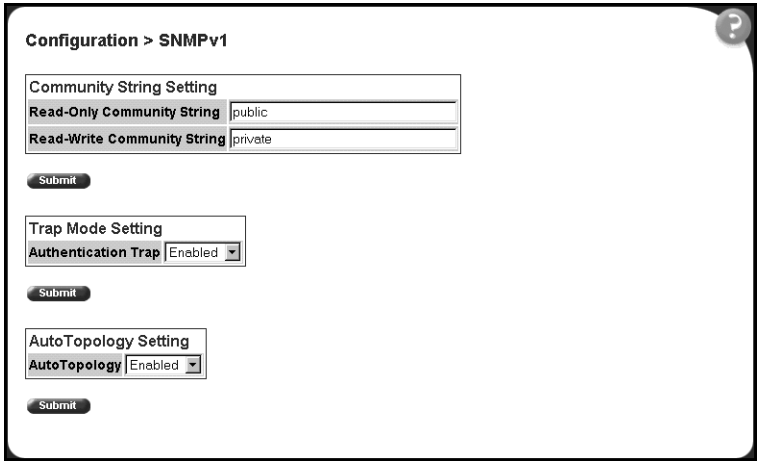


Table 14 describes the items on the SNMPv1 page.

Table 14 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

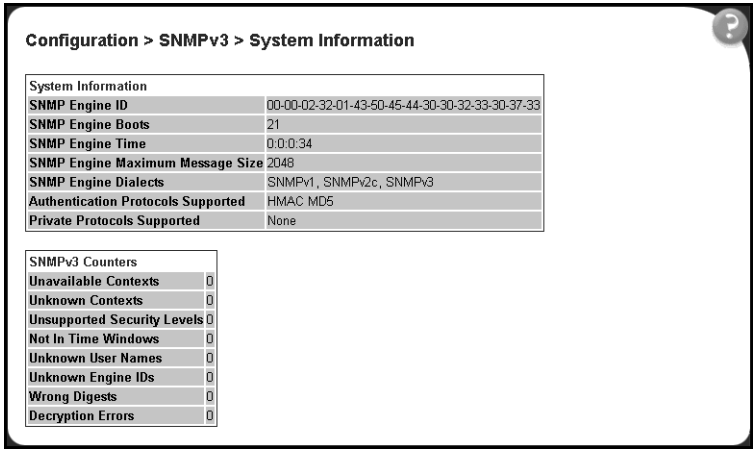


Table 15 describes the fields on the System Information section of the SNMPv3 System Information page.

Table 15 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, HMAC SHA, 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 16 describes the fields on the SNMPv3 Counters section of the SNMPv3 System Information page.

Table 16 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

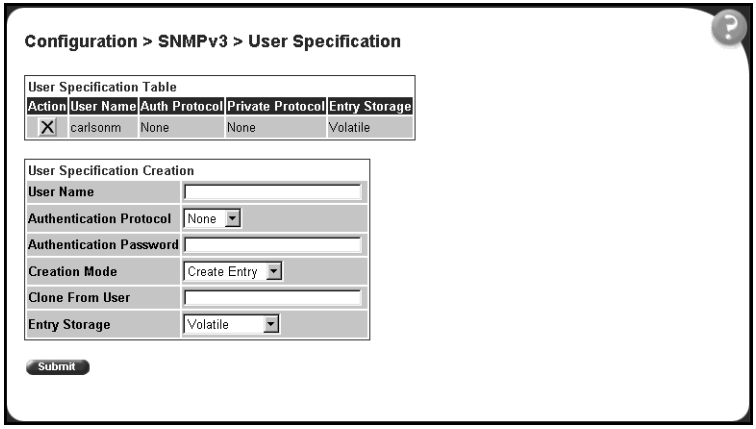


Table 17 describes the items on the User Specification Table section of the User Specification page.

Table 17 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 18 describes the items on the User Specification Creation section of the User Specification page.

Table 18 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.
Creation Mode	Create Entry	Choose to create a new, unique user specification entry.
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

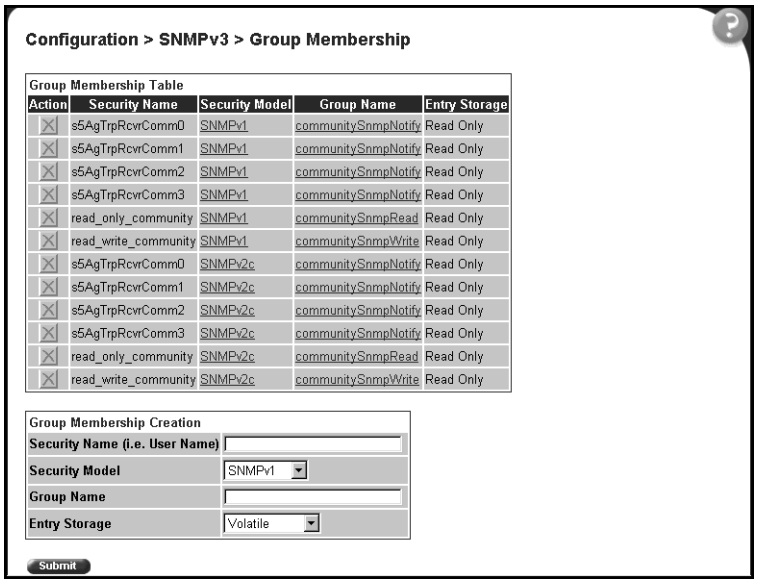


Table 19 describes the items on the Group Membership page.

Table 19 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 61 and "Configuring SNMPv3 group access rights" on page 67.

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

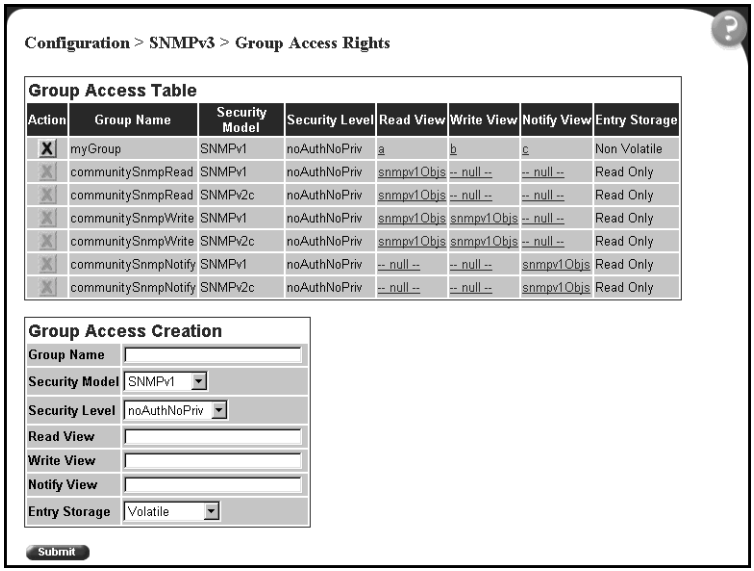


Table 20 describes the items on the Group Access Rights page.

Table 20 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 69.

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

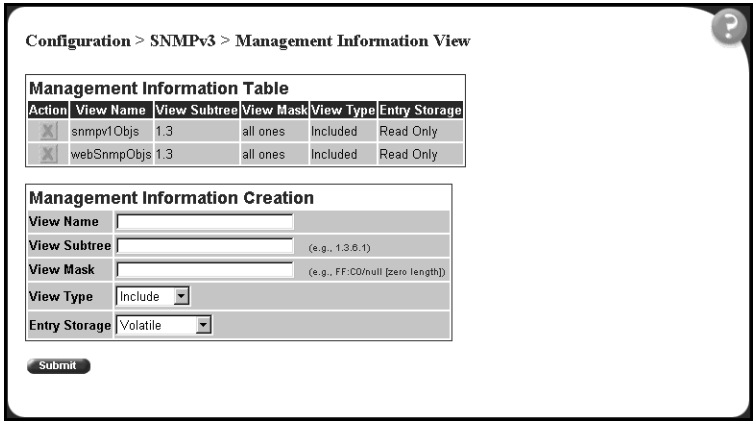


Table 21 describes the items on the Management Information View page.

Table 21 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

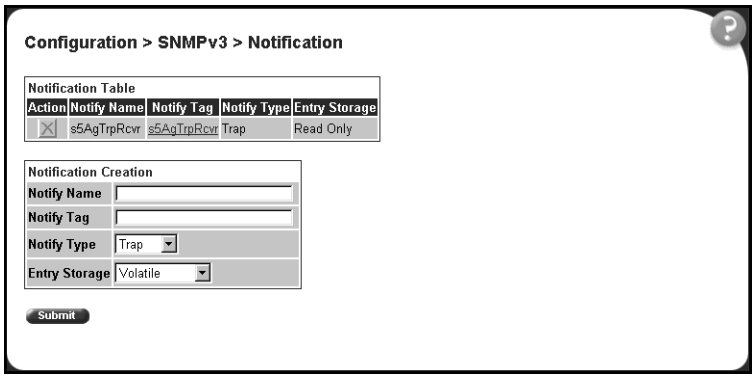


Table 22 describes the items on the Notification page.

Table 22 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 76.

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

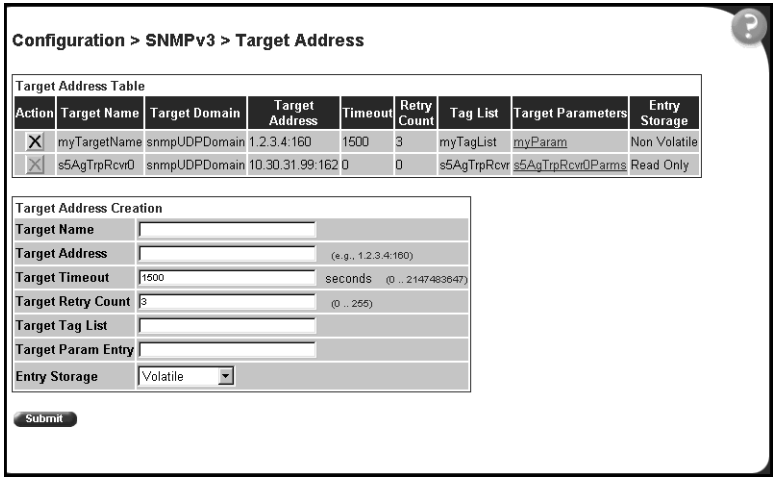


Table 23 describes the items on the Target Address page.

Table 23 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 74).
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 76.

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

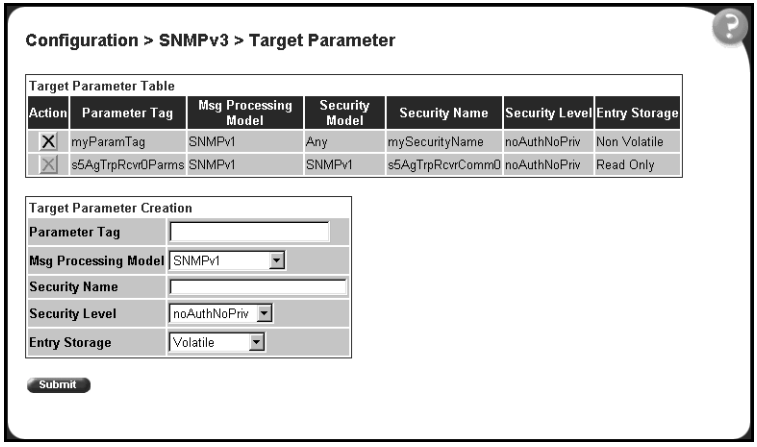


Table 24 describes the items on the Target Parameter page.

Table 24 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 an SNMP trap receiver

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 Receiver.

   The SNMP Trap Receiver page opens (Figure 27).

Figure 27 SNMP Trap Receiver page

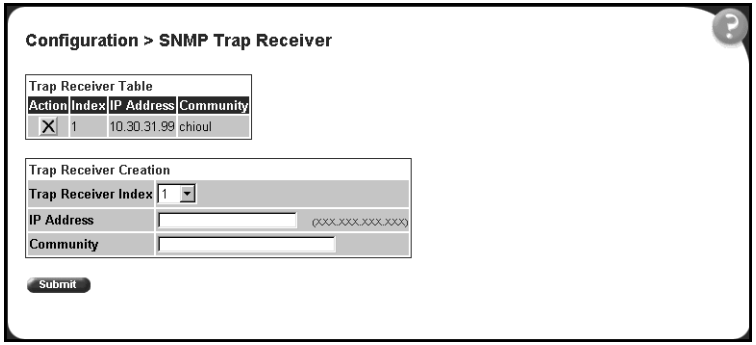


Table 25 describes the items on the Trap Receiver Table and Trap Receiver Creation sections of the SNMP Trap Receiver page.

Table 25 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 Receiver.

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.

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 28).

Figure 28 MAC Address Table page

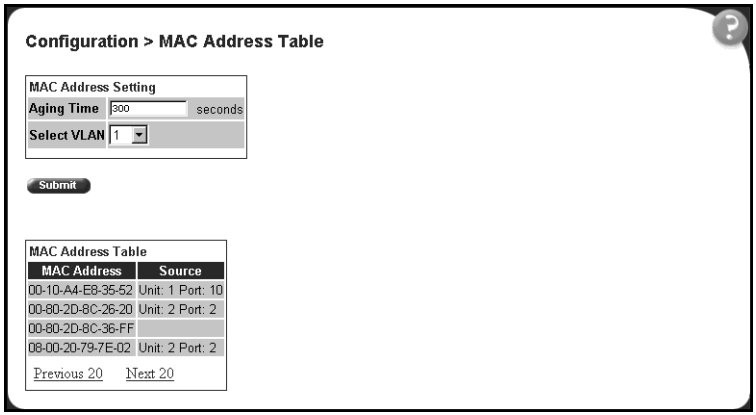


Table 26 describes the items on the MAC Address Table page.

Table 26 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..64	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 28).

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 29).

Figure 29 Find MAC Address Table page

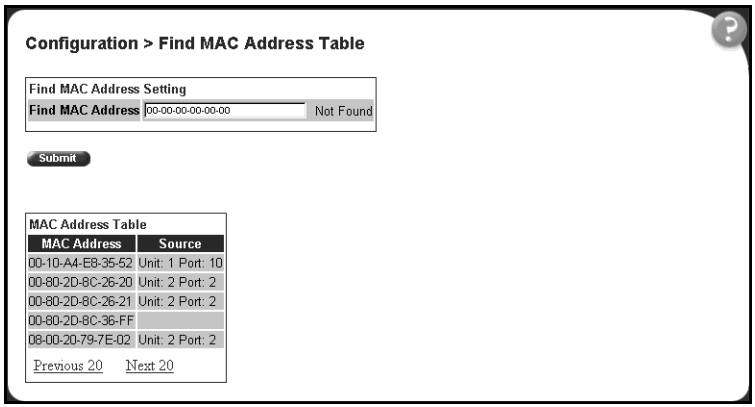


Table 26 on page 81 describes the items on the Find MAC Address Table page.

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 switch port autonegotiation speed

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 100 Mbps fiber optic ports).

To configure a switch port's autonegotiation speed:

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

The Port Management page opens (Figure 30).

Figure 30 Port Management page

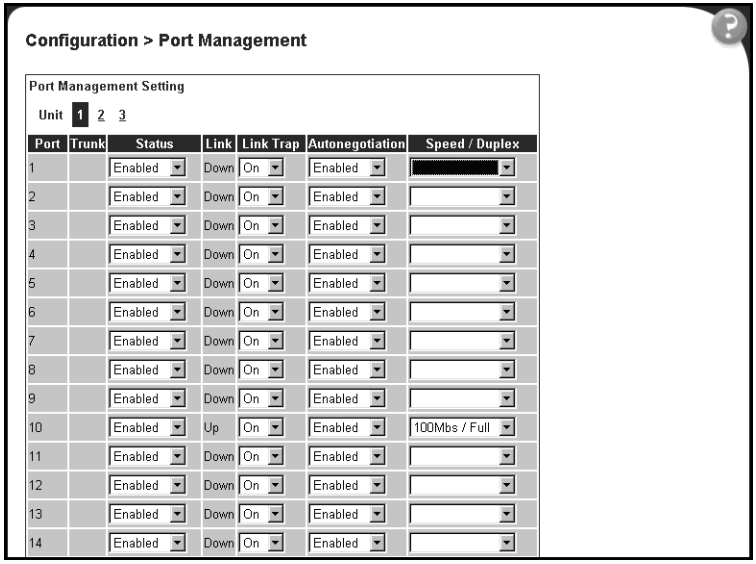


Table 27 describes the items on the Port Management page.

Table 27 Port Management page items

Item	Range	Description
Port		The switch port number of the corresponding row. 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 85.
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 161.
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 other than gigabit fiber optic ports. The default setting is Enabled.
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: Fiber optic ports can only be set to 100 Mb/s/Half or 100 Mb/s/Full. 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 media dependent adapters (MDAs) when the switch is participating in a stack configuration.

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 31).

Figure 31 High Speed Flow Control page

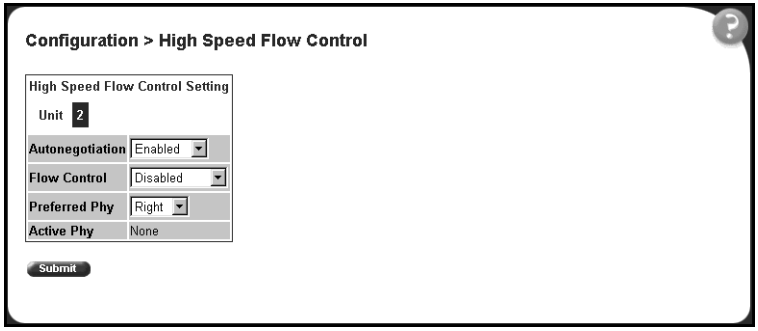


Table 28 describes the items on the High Speed Flow Control page.

Table 28 High Speed Flow Control page items

Item	Range	Description
Autonegotiation	(1) Enabled (2) Disabled	Choose to enable or disable the autonegotiation feature. When enabled, the port advertises support only for 1000Mb/s operation in full-duplex mode.
Flow Control	(1) Enabled (2) Symmetric (3) Asymmetric	Choose your flow control preference to control traffic and avoid congestion on the gigabit MDA port.
Preferred Phy	(1) Left (2) Right	Choose the preferred physical port. The port not selected automatically reverts to a backup physical port.
Active Phy		The current operating physical port. The physical port options are left or right.

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 Business Policy Switch software image that is located in non-volatile flash memory. To download the Business Policy Switch 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 54.

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

To download a switch image:

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

The Software Download page opens (Figure 32).

Figure 32 Software Download page

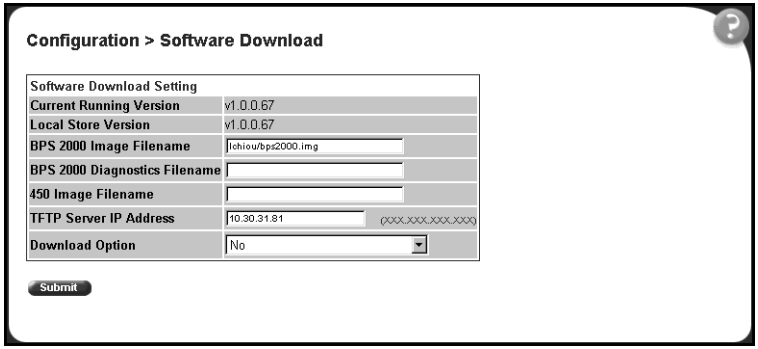


Table 29 describes the items on the Software Download page.

Table 29 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.
Download Option	(1) No (2) BPS 2000 Image (3) BPS 200 Diagnostics (4) 450/410 Image (5) BPS 2000 and 450/410 Images	Choose the software image to load.

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

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.

Table 30 describes the LED indications during the software download process.

Note: The LED indications described in Table 30 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 30 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 30 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.

Storing and retrieving a switch configuration file from a TFTP server

You can store switch and stack configuration parameters on a 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 Business Policy Switch configuration file, 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 54.

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 33).

Figure 33 Configuration File Download/Upload page

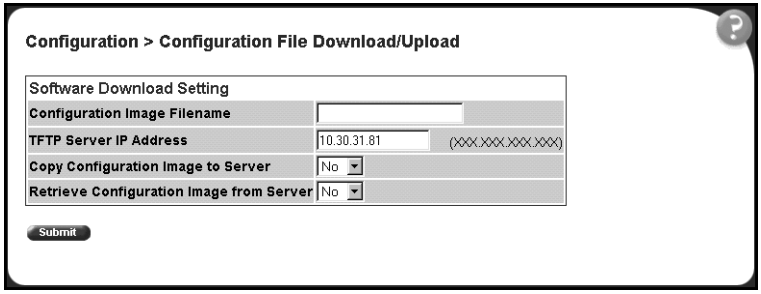


Table 31 describes the items on the Configuration File page.

Table 31 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 32 describes the requirements for storing or retrieving configuration parameters on a TFTP server.

Table 32 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 33 describes the parameters that are not saved to the configuration file.

Table 33 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	54
In-Band Switch IP Address		
In-Band Subnet Mask		
Default Gateway		
Configuration Image Filename	Configuration File Download/Upload	89
TFTP Server IP Address		
Console Read-Only Switch Password	Console/Comm Port Configuration	92
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 34).

Figure 34 Console/Communication Port page

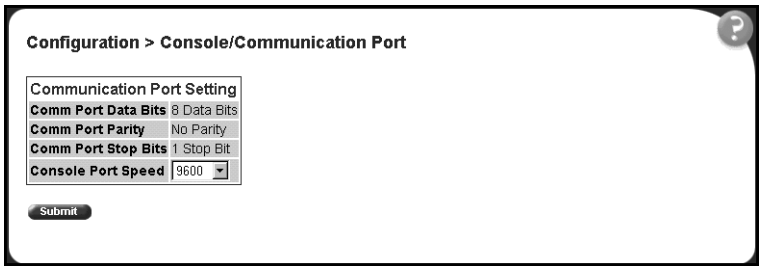


Table 34 describes the items on the Console/Communication Port page.

Table 34 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 Business Policy Switches only, or a mixed stack of Business Policy Switches and BayStack 450 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 35).

Figure 35 Stack Operational Mode page

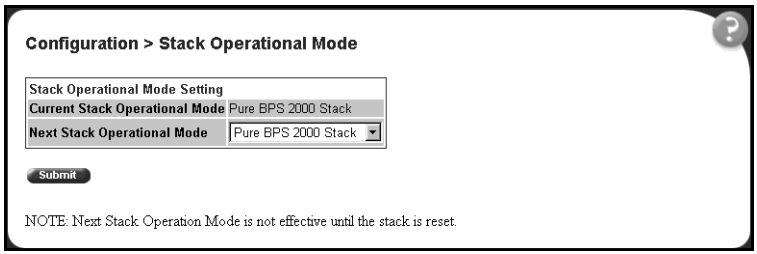


Table 35 describes the items on the Stack Operational Mode Setting page.

Table 35 Stack Operational Mode page items

Item	Range	Description
Current Stack Operational Mode		Current stack operational mode. The options are Business Policy Switch Only or Hybrid.
Next Stack operational Mode	(1) Business Policy Switch Only (2) Hybrid	Choose whether your stack is Business Policy Switches only, or a mixed stack of BayStack 450 and Business Policy Switches (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:

- Creating and displaying alarms for user-defined events (next)
- Viewing RMON Ethernet statistics (page 102)
- Viewing RMON history (page 106)
- Viewing the System Log (page 100)

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 36).

Figure 36 RMON Threshold page

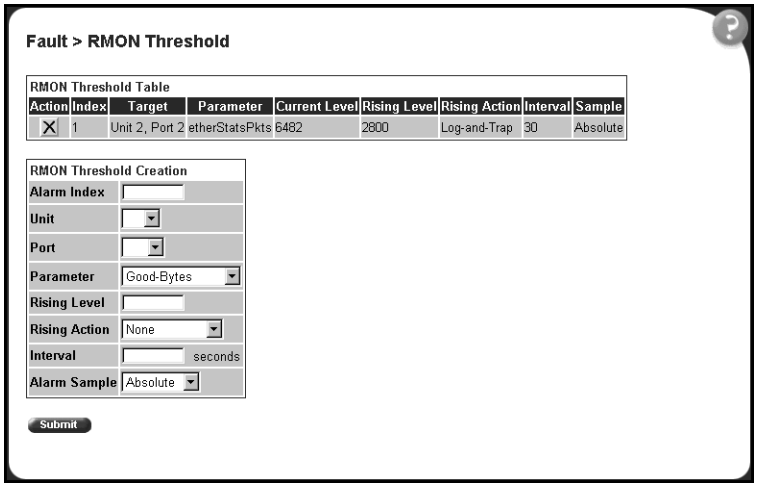


Table 36 describes the items on the RMON Threshold page.

Table 36 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.

Table 36 RMON Threshold page items (continued)

Item	Range	Description
Parameter	(1) Good-Bytes (2) Good-Packets (3) Multicast (4) Broadcast (5) CRC-Errors (6) Misaligned (7) Runts (8) Fragments (9) Frame-Too-Long (10) Collisions (11) Late 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.
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 36).

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 36).

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 37).

Figure 37 RMON Event Log page

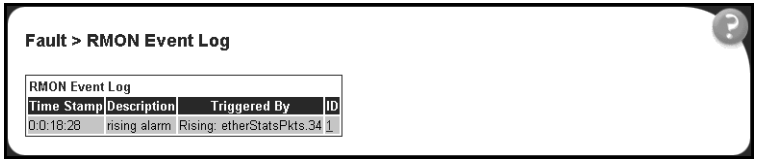


Table 37 describes the fields on the RMON Event Log page.

Table 37 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 38).

Figure 38 System Log page

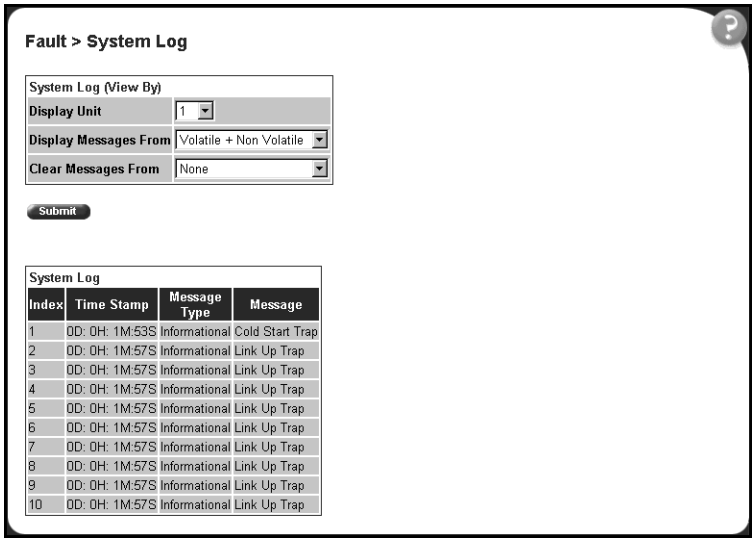


Table 38 describes the fields on the System Log page.

Table 38 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 38).

Viewing RMON Ethernet statistics

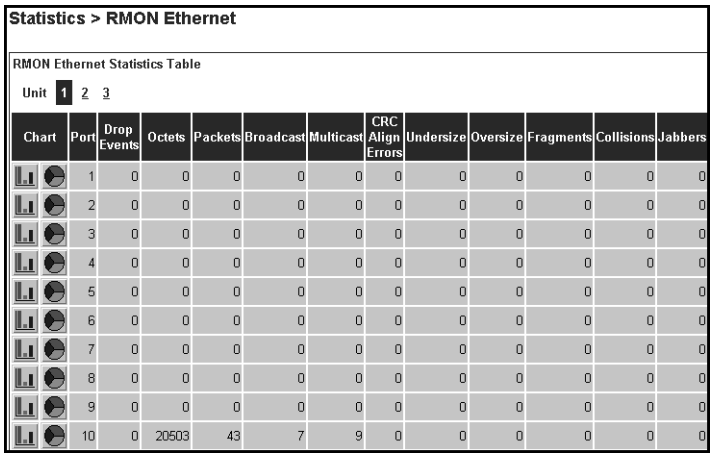
You can gather and graph RMON Ethernet statistics in a variety of formats.

To gather and graph RMON Ethernet statistics:

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

The RMON Ethernet page opens (Figure 39).

Figure 39 RMON Ethernet page



Statistics > RMON Ethernet

RMON Ethernet Statistics Table

Unit 1 2 3

Chart	Port	Drop Events	Octets	Packets	Broadcast	Multicast	CRC Align Errors	Undersize	Oversize	Fragments	Collisions	Jabbers
	1	0	0	0	0	0	0	0	0	0	0	0
	2	0	0	0	0	0	0	0	0	0	0	0
	3	0	0	0	0	0	0	0	0	0	0	0
	4	0	0	0	0	0	0	0	0	0	0	0
	5	0	0	0	0	0	0	0	0	0	0	0
	6	0	0	0	0	0	0	0	0	0	0	0
	7	0	0	0	0	0	0	0	0	0	0	0
	8	0	0	0	0	0	0	0	0	0	0	0
	9	0	0	0	0	0	0	0	0	0	0	0
	10	0	20503	43	7	9	0	0	0	0	0	0

Table 39 describes the items on the RMON Ethernet page.

Table 39 RMON Ethernet page items

Item	Description
	Displays statistics as a bar graph.
	Displays statistics as a pie chart.
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).

Table 39 RMON Ethernet page items (continued)

Item	Description
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.
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 39).

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 39).

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 40).

Figure 40 RMON Ethernet: Chart in a bar graph format

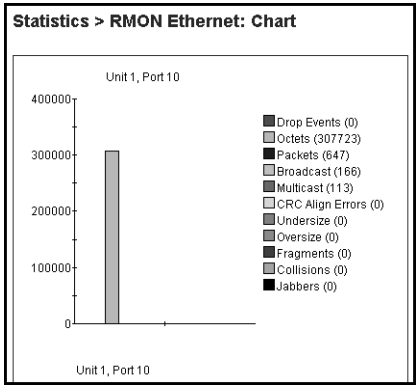


Table 39 describes the items on the RMON Ethernet: Chart page.

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

Viewing RMON Ethernet statistics in a pie chart format

To view RMON Ethernet statistics in a pie chart format:

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

The RMON Ethernet page opens (Figure 39).

2 In the port row of your choice, click the pie chart icon.

The RMON Ethernet: Chart page appears in a pie chart format (Figure 41).

Figure 41 RMON Ethernet: Chart in a pie chart format

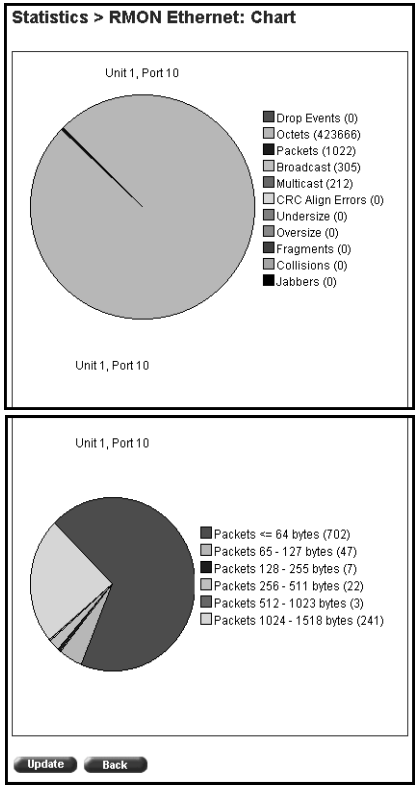


Table 39 describes the items on the RMON Ethernet: Chart page.

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

Viewing RMON history

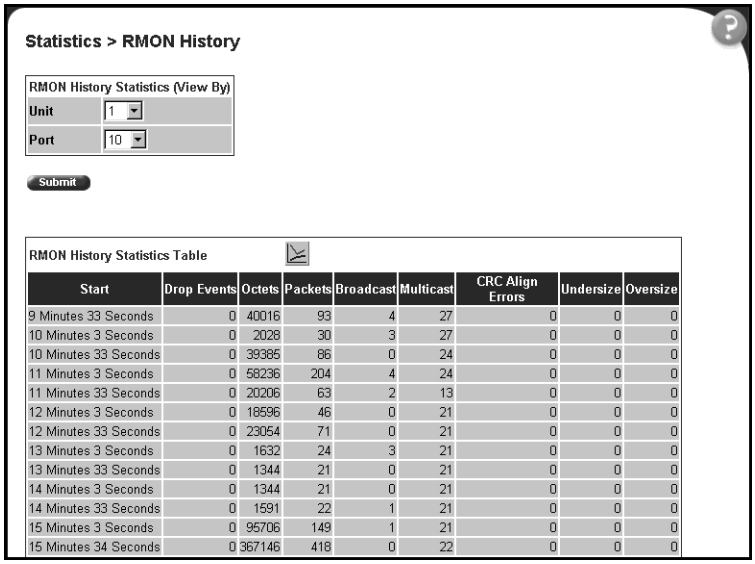
You can view a periodic statistical sampling of data from various types of networks.

To view periodic statistical data:

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

The RMON History page opens (Figure 42).

Figure 42 RMON History page



Start	Drop Events	Octets	Packets	Broadcast	Multicast	CRC Align Errors	Undersize	Oversize
9 Minutes 33 Seconds	0	40016	93	4	27	0	0	0
10 Minutes 3 Seconds	0	2028	30	3	27	0	0	0
10 Minutes 33 Seconds	0	39385	86	0	24	0	0	0
11 Minutes 3 Seconds	0	58236	204	4	24	0	0	0
11 Minutes 33 Seconds	0	20206	63	2	13	0	0	0
12 Minutes 3 Seconds	0	18596	46	0	21	0	0	0
12 Minutes 33 Seconds	0	23054	71	0	21	0	0	0
13 Minutes 3 Seconds	0	1632	24	3	21	0	0	0
13 Minutes 33 Seconds	0	1344	21	0	21	0	0	0
14 Minutes 3 Seconds	0	1344	21	0	21	0	0	0
14 Minutes 33 Seconds	0	1591	22	1	21	0	0	0
15 Minutes 3 Seconds	0	95706	149	1	21	0	0	0
15 Minutes 34 Seconds	0	367146	418	0	22	0	0	0

Table 40 describes the items on the RMON History page.

Table 40 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.
		Displays statistics as a line graph.
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 Port Statistics section, choose the unit and port number to be monitored.

3 Click Submit.

The Port Statistics Table is updated with information about the selected device and port (Figure 42).

Viewing RMON statistics in a line graph format

You can view RMON statistical data in a line graph format.

To view statistics in a line graph format:

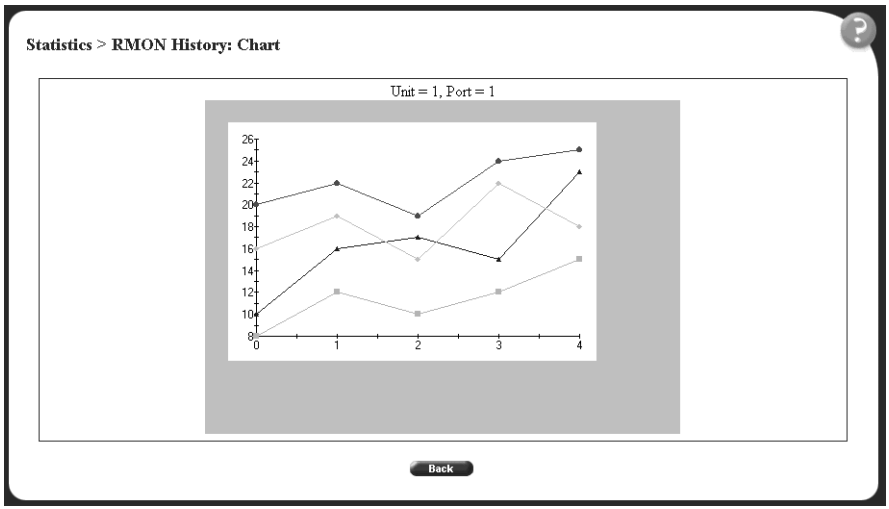
1 From the main menu, choose Statistics > RMON History.

The RMON History page opens (Figure 42).

2 In the RMON History Statistics Table, click the line graph icon.

The RMON History: Chart page opens in a line graph format (Figure 43).

Figure 43 RMON History page: Chart in line graph format



3 Click Back to return to the RMON History page.

Chapter 6
Viewing system statistics

The options available to monitor system statistical data are:

- Viewing port statistics (next)
- Viewing interface statistics (page 114)
- Viewing Ethernet Error statistics (page 118)
- Viewing Transparent Bridging statistics (page 122)

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 44).

Figure 44 Port page

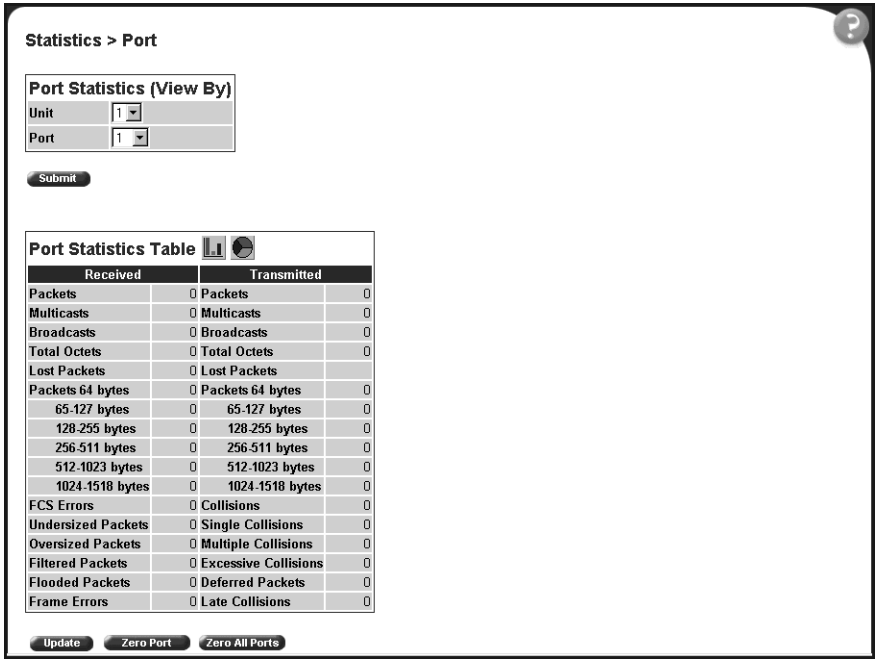


Table 41 describes the items on the Port page.

Table 41 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.
		Displays statistics in a pie chart format.

Table 41 Port page items (continued)

Section	Item	Description
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.
	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.

Table 41 Port page items (continued)

Section	Item	Description
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 44).

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 pie chart format

You can view port statistics in a pie chart format.

To view the displayed statistical information in a pie chart format:

1 In the Port Statistics Table, click the pie chart icon.

The Port: Chart page opens in a pie chart format (Figure 45).

Figure 45 Port: Chart page in a pie chart format

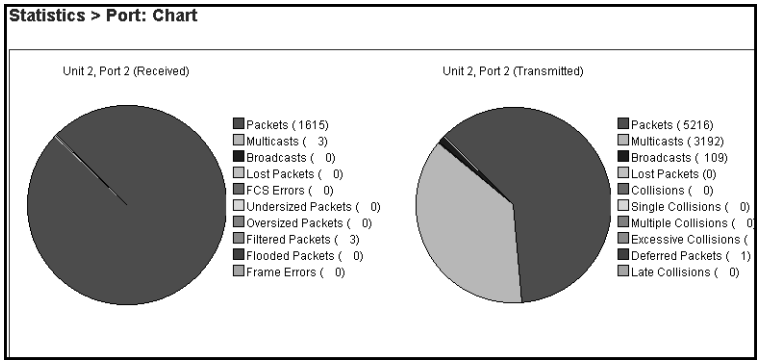


Table 41 describes the items on the Port: Chart page.

2 Click Back to return to the Port page.

Viewing port statistics in a bar graph format

You can view port statistics in a bar graph format.

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 46).

Figure 46 Port: Chart page in a bar graph format

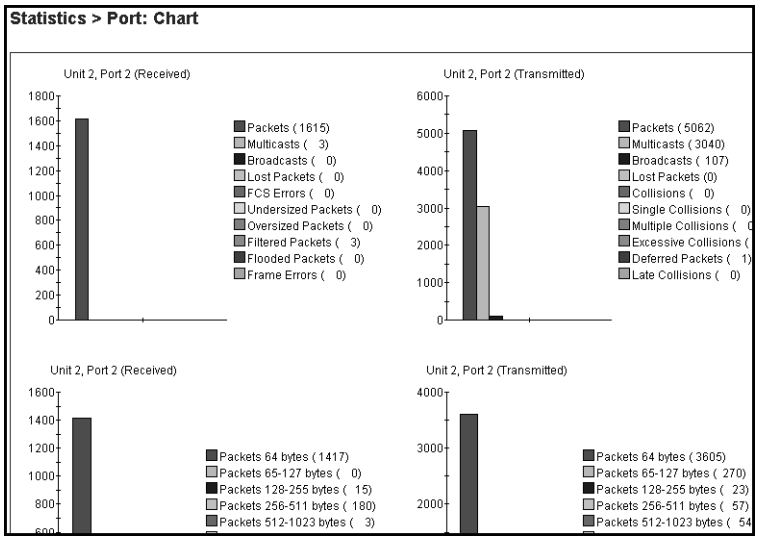


Table 41 describes the items on the Port: Chart page.

2 Click Back to return to the Port page.

Viewing interface statistics

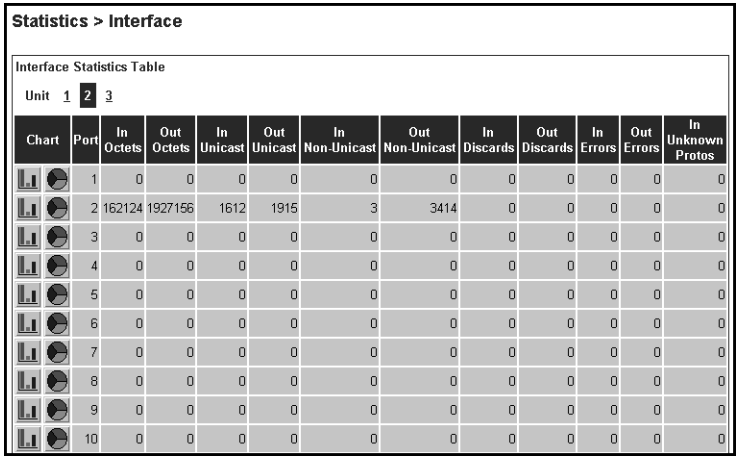
You can view selected switch interface statistics.

To view an interface's statistical information:

1 From the main menu, choose Statistics > Interface.

The Interface page opens (Figure 47).

Figure 47 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
	1	0	0	0	0	0	0	0	0	0	0	0
	2	162124	1927156	1612	1915	3	3414	0	0	0	0	0
	3	0	0	0	0	0	0	0	0	0	0	0
	4	0	0	0	0	0	0	0	0	0	0	0
	5	0	0	0	0	0	0	0	0	0	0	0
	6	0	0	0	0	0	0	0	0	0	0	0
	7	0	0	0	0	0	0	0	0	0	0	0
	8	0	0	0	0	0	0	0	0	0	0	0
	9	0	0	0	0	0	0	0	0	0	0	0
	10	0	0	0	0	0	0	0	0	0	0	0

Table 42 describes the items on the Interface page.

Table 42 Interface page items

Item	Description
	Displays statistics in a bar graph format.
	Displays statistics in a pie chart 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.

Table 42 Interface page items (continued)

Item	Description
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 Protocols	The number of packets received through the interface which were discards due to 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 47).

3 To update the statistical information, click Update.

Viewing interface statistics in a pie chart format

You can view interface statistics in a pie chart format.

To view interface statistics in a pie chart format:

1 From the main menu, choose Statistics > Interface.

The Interface page opens (Figure 47).

2 In the port row of your choice, click the pie chart icon.

The Interface: Chart page opens in a pie chart format (Figure 48).

Figure 48 Interface: Chart in a pie chart format

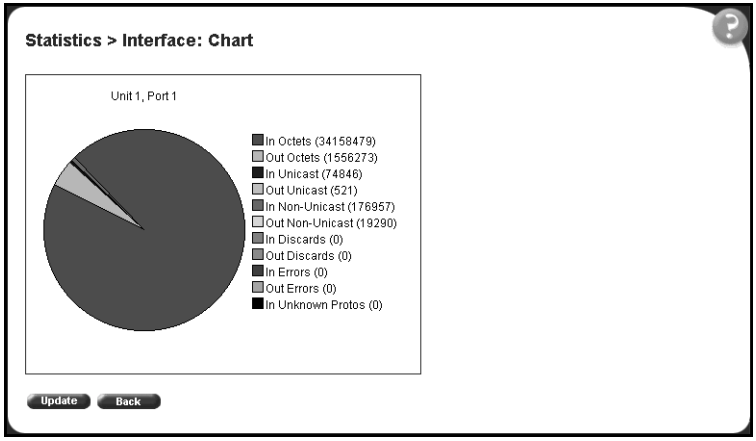


Table 42 describes the items on the Interface: Chart page.

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

Viewing interface statistics in a bar graph format

You can view interface statistics in a bar graph format.

To view interface statistics in a bar graph format:

1 From the main menu, choose Statistics > Interface.

The Interface page opens (Figure 47).

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

The Interface: Chart page opens in a bar graph format (Figure 48).

Figure 49 Interface: Chart in a bar graph format

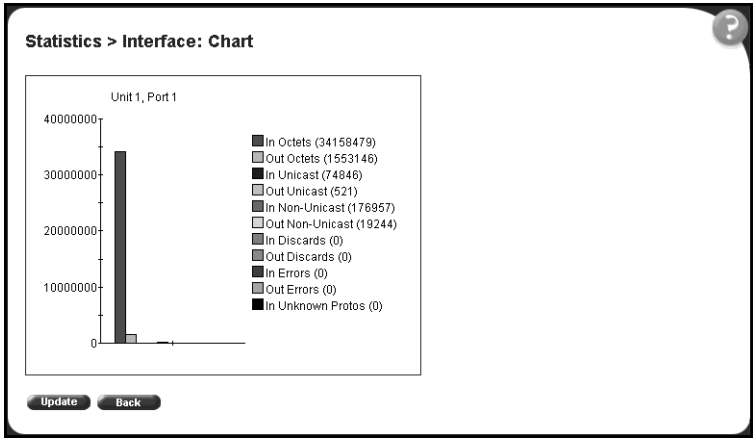


Table 42 describes the items on the Interface: Chart page.

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

Viewing Ethernet error statistics

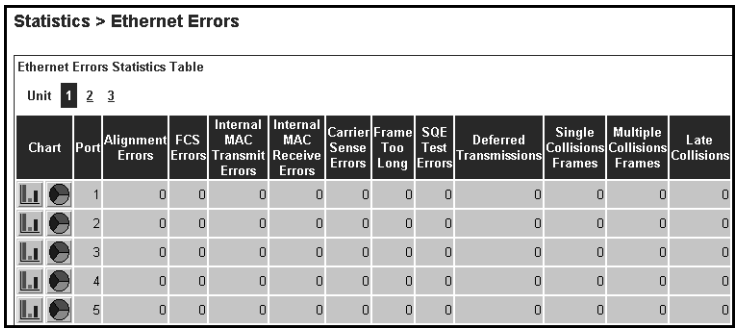
You can view Ethernet error statistics for each monitored interface linked to the Business Policy Switch 2000.

To view Ethernet error statistics:

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

The Ethernet Errors page opens (Figure 50).

Figure 50 Ethernet Errors page



Statistics > Ethernet Errors

Ethernet Errors Statistics Table

Unit 1 2 3

Chart	Port	Alignment Errors	FCS Errors	Internal MAC Transmit Errors	Internal MAC Receive Errors	Carrier Sense Errors	Frame Too Long	SQE Test Errors	Deferred Transmissions	Single Collisions Frames	Multiple Collisions Frames	Late Collisions
	1	0	0	0	0	0	0	0	0	0	0	0
	2	0	0	0	0	0	0	0	0	0	0	0
	3	0	0	0	0	0	0	0	0	0	0	0
	4	0	0	0	0	0	0	0	0	0	0	0
	5	0	0	0	0	0	0	0	0	0	0	0

Table 43 describes the items on the Ethernet Errors page.

Table 43 Ethernet Errors page items

Item	Description
	Displays statistics in a bar graph format.
	Displays statistics in a pie chart 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.
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.

Table 43 Ethernet Errors page items (continued)

Item	Description
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 pie chart format

You can view Ethernet Errors statistics in a pie chart format.

To view Ethernet Errors statistics in a pie chart format:

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

The Ethernet Errors page opens (Figure 47).

2 In the port row of your choice, click the pie chart icon.

The Ethernet Errors: Chart page opens in a pie chart format (Figure 51).

Figure 51 Ethernet Error: Chart in a pie chart format

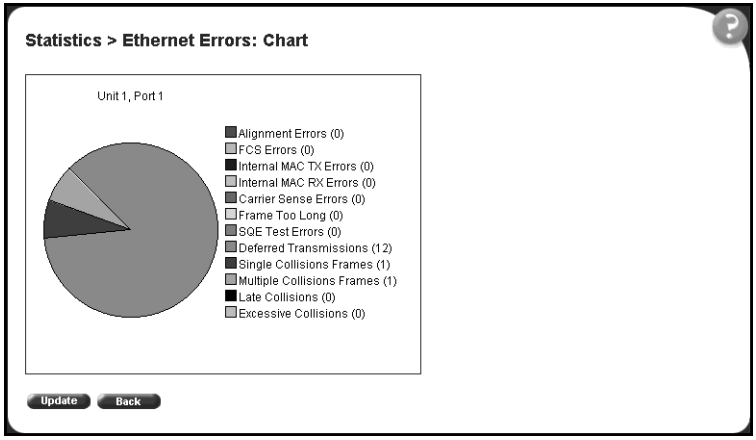


Table 44 describes the items on the Ethernet Errors: Chart page.

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

Viewing Ethernet error statistics in a bar graph format

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

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 47).

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 52).

Figure 52 Ethernet Error: Chart in a bar graph format

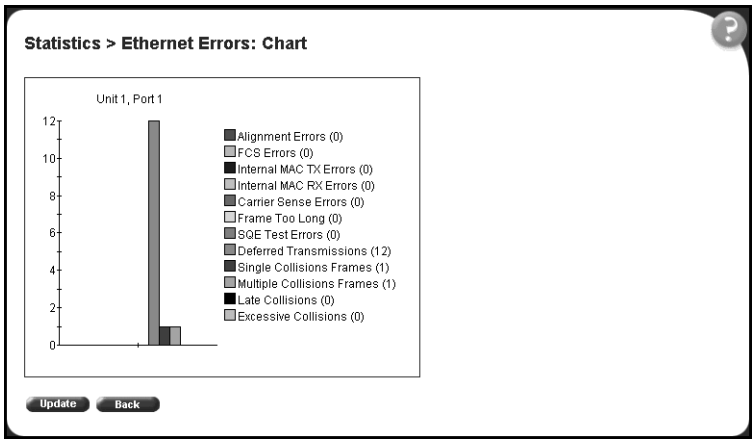


Table 43 describes the items on the Ethernet Errors: Chart page.

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

Viewing transparent bridging statistics

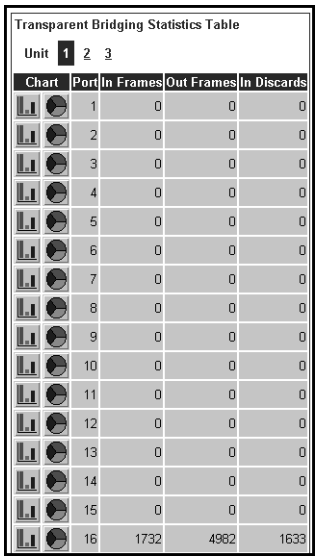
You can view the transparent bridging statistics measured for each monitored interface on the device.

To view transparent bridging statistics:

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

The Transparent Bridging page opens (Figure 53).

Figure 53 Transparent Bridging page



Transparent Bridging Statistics Table

Unit 1 2 3

Chart	Port	In Frames	Out Frames	In Discards
	1	0	0	0
	2	0	0	0
	3	0	0	0
	4	0	0	0
	5	0	0	0
	6	0	0	0
	7	0	0	0
	8	0	0	0
	9	0	0	0
	10	0	0	0
	11	0	0	0
	12	0	0	0
	13	0	0	0
	14	0	0	0
	15	0	0	0
	16	1732	4982	1633

Table 44 describes the items on the Transparent Bridging page.

Table 44 Transparent Bridging page items

Item	Description
	Displays statistics in a bar graph format.
	Displays statistics in a pie chart format.
Port	The port number that corresponds to the selected switch.
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.
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.
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 pie chart format

You can view measured transparent bridging statistics in a pie chart format.

To view transparent bridging statistics in a pie chart format:

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

The Transparent Bridging page opens (Figure 47).

2 In the port row of your choice, click the pie chart icon.

The Transparent Bridging: Chart page opens in a pie chart format (Figure 54).

Figure 54 Transparent Bridging: Chart in a pie chart format

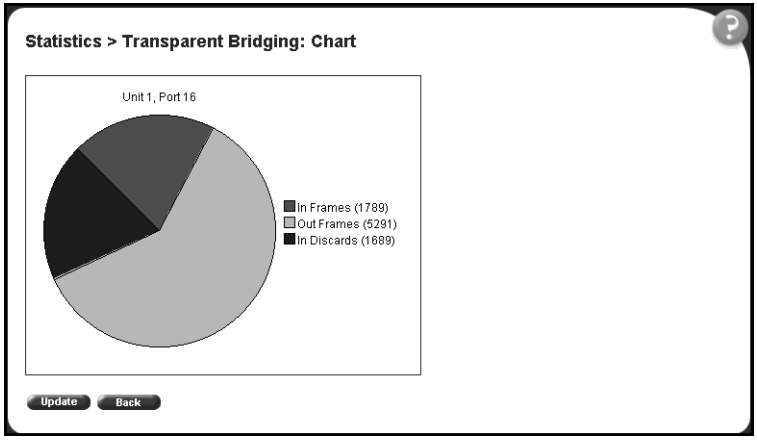


Table 44 describes the items on the Transparent Bridging: Chart page.

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

Viewing transparent bridging statistics in a bar graph format

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

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 47).

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 55).

Figure 55 Transparent Bridging: Chart in a bar graph format

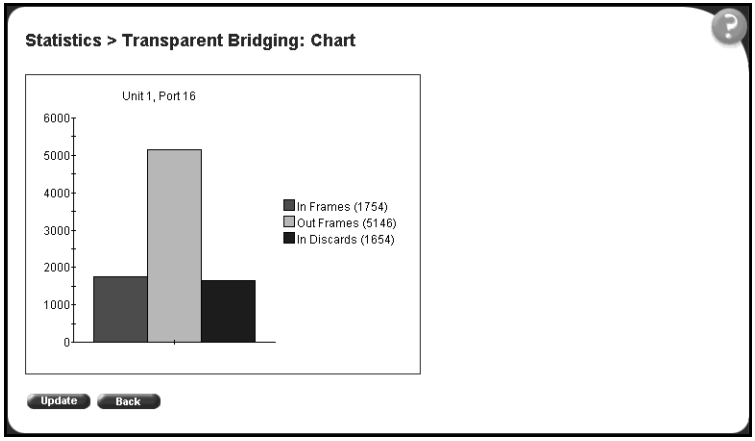


Table 44 describes the items on the Transparent Bridging: Chart page.

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:

- Configuring port mirroring (next)
- Configuring rate limiting (page 130)
- Configuring IGMP (page 132)
- Configuring VLANs (page 138)
- Configuring Spanning Tree Protocol (page 157)
- Configuring MultiLink Trunking (page 161)

Configuring port mirroring

The Business Policy Switch 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.

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* (208700-A).

To configure port mirroring:

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

The Port Mirroring page opens (Figure 56).

Figure 56 Port Mirroring page

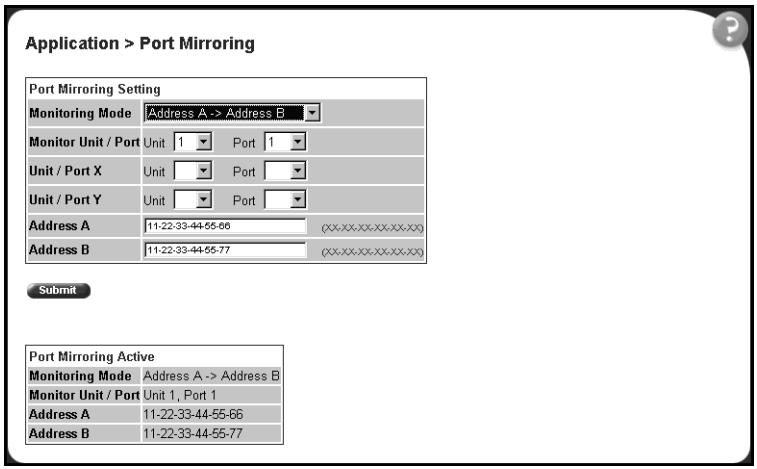


Table 45 describes the items on the Port Mirroring page.

Table 45 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 46 on page 129. 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 47 on page 130. 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.

Table 45 Port Mirroring page items (continued)

Item	Range	Description
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 46 describes the port-based monitoring modes.

Table 46 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.
--> 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).
<-- --> 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).

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 47 describes the address-based monitoring modes.

Table 47 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 Business Policy Switch 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.

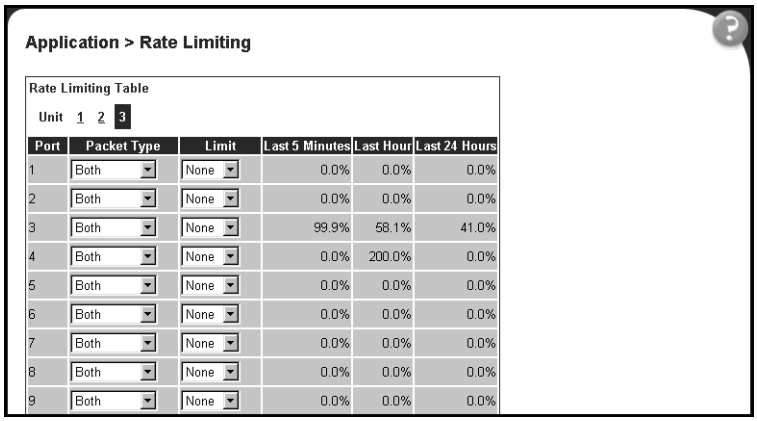
Note: If a port is configured for rate limiting, and it is a MultiLink trunk member, all trunk member ports implement rate limiting. If the port becomes disabled, all trunk members become disabled.

To configure rate limiting:

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

The Rate Limiting page opens (Figure 57).

Figure 57 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 48 describes the items on the Rate Limiting page.

Table 48 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.

Table 48 Rate Limiting page items (continued)

Item	Range	Description
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* (208700-A).

To configure IGMP:

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

The IGMP page opens (Figure 58).

Figure 58 IGMP page

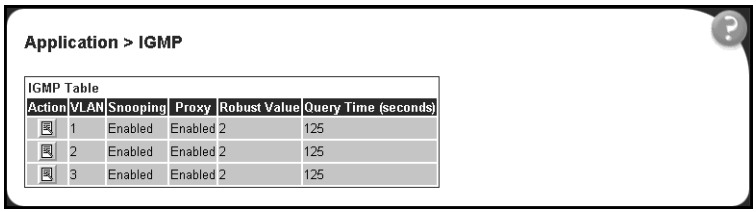


Table 49 describes the items on the IGMP page.

Table 49 IGMP 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 136.
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.
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 59).

Figure 59 IGMP: VLAN Configuration page

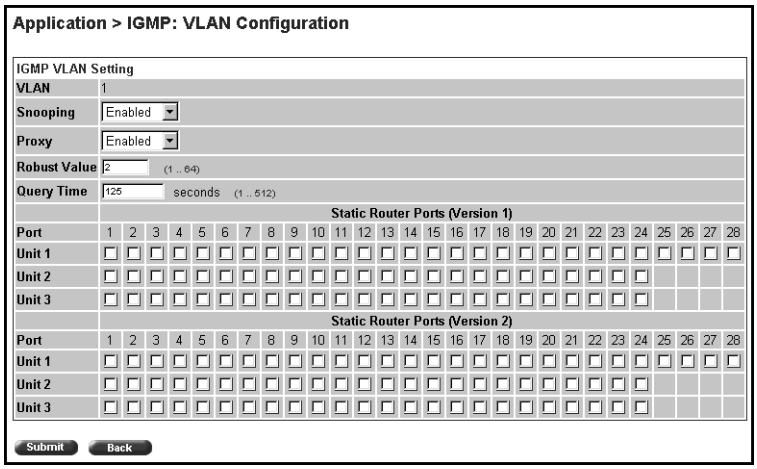


Table 50 describes the items on the IGMP: VLAN Configuration page.

Table 50 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 136.
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.
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.

Table 50 IGMP: VLAN Configuration page items (continued)

Item	Range	Description
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 58).

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 Multicast Group.

The IGMP Multicast Group Membership page opens (Figure 60).

Figure 60 IGMP Multicast Group Membership page

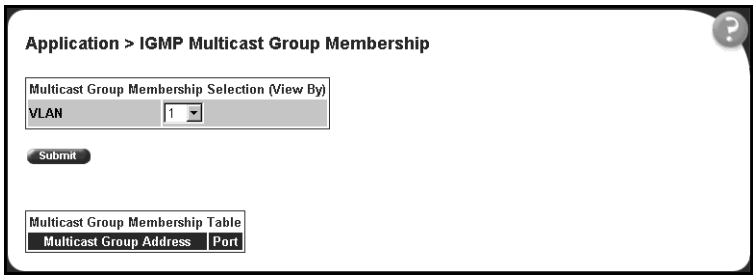


Table 51 describes the items on the IGMP Multicast Group Membership page.

Table 51 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 60).

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.

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

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

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.

Protocol-based VLANs

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 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.

To open the VLAN Configuration page:

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

The VLAN Configuration page opens (Figure 61).

Figure 61 VLAN Configuration page

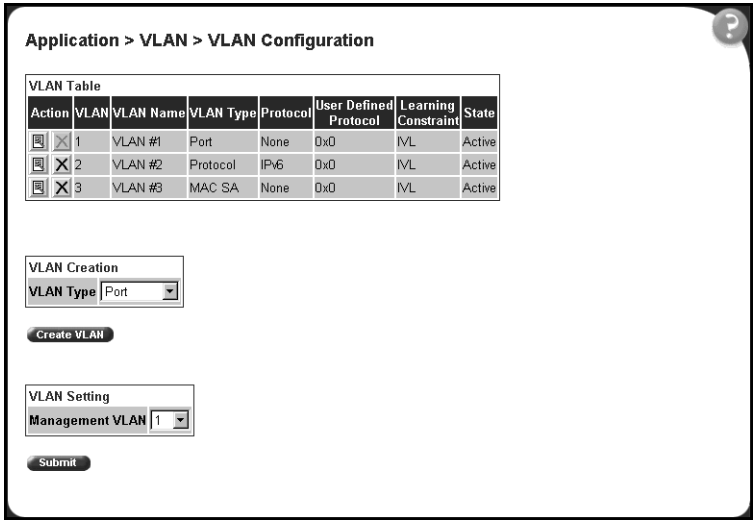


Table 52 describes the items on the VLAN Configuration page.

Table 52 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 56 on page 145.
	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,” the default setting is IVL. 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 140), protocol-based (page 143), and MAC SA-based (page 148).
VLAN Setting	Management VLAN	Choose the VLAN to designate as the management VLAN.

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 61).

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

   The VLAN Configuration: Port Based Setting page opens (Figure 62).

Figure 62 VLAN Configuration: Port Based Setting page

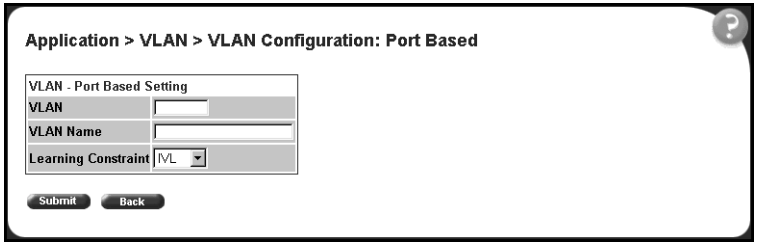


Table 53 describes the items on the VLAN Configuration: Port Based Setting page.

Table 53 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. 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 93.

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 61).

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 61).

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 63).

Figure 63 VLAN Configuration: Port Based modification page

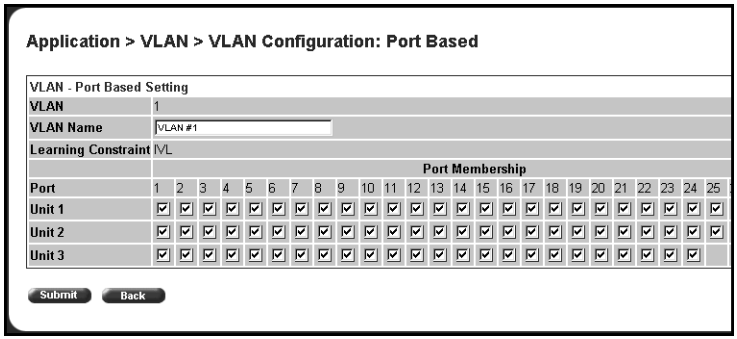


Table 54 describes the items on the VLAN Configuration: Port Based modification page.

Table 54 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. 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 (see the Tagging field descriptions in "Port Configuration page items" on page 158). 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 61).

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 61).

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

   The VLAN Configuration: Protocol Based Setting page opens (Figure 64).

Figure 64 VLAN Configuration: Protocol Based Setting page

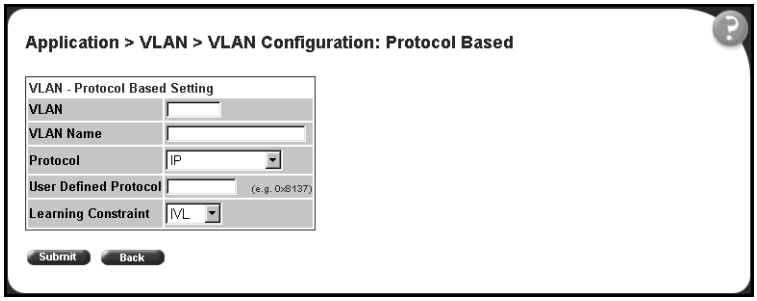


Table 55 describes the items on the VLAN Configuration: Protocol Based Setting page.

Table 55 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 56 on page 145.
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 57 on page 146.
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. 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 93.

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 61).

Caution: Gigabit 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 154).

Table 56 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 57 for a list of rereserved PIDS that are not available for user-defined PIDs.

Table 56 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 56 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 56 on page 145

Table 57, describes the PIDS that are reserved and not available for user-defined PIDs.

Table 57 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 57 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 57 on page 146.

Modifying a protocol-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 61).

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 65).

Figure 65 VLAN Configuration: Protocol Based modification page

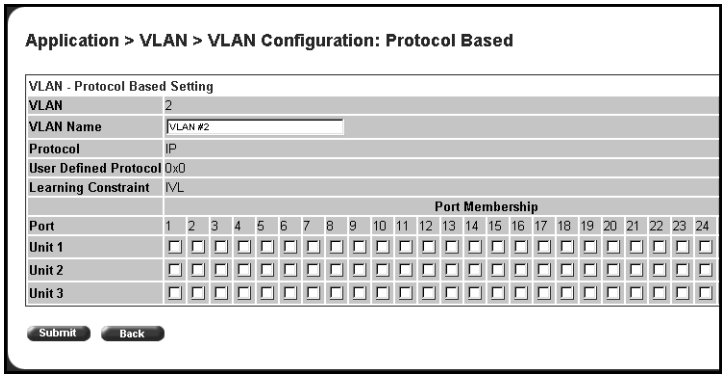


Table 58 describes the items on the VLAN Configuration: Protocol Based modification page.

Table 58 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. 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 61).

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 61).

2 In the VLAN Creation section, choose MAC SA.

3 Click Create VLAN.

The VLAN Configuration: MAC SA Based Setting page opens (Figure 66).

Figure 66 VLAN Configuration: MAC SA Based Setting page

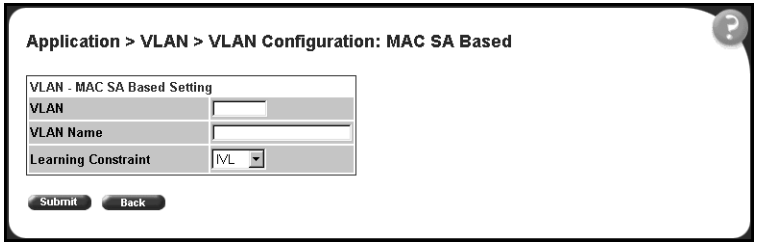


Table 59 describes the items on the VLAN Configuration: MAC SA Based Setting page.

Table 59 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. 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 93.

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 61).

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 61).

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 67).

Figure 67 VLAN Configuration: MAC SA Based modification page

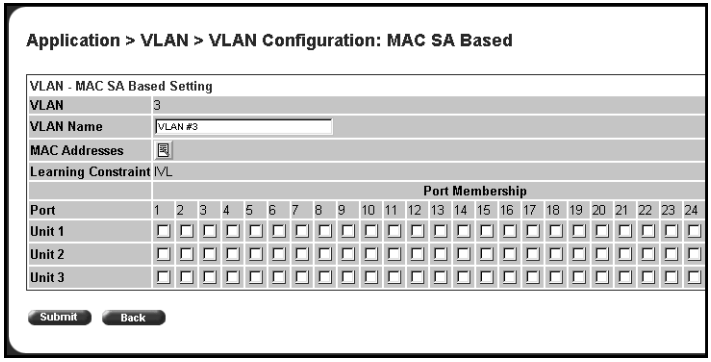


Table 60 describes the items on the VLAN Configuration: MAC SA Based modification page.

Table 60 VLAN Configuration: MAC SA Based modification page items

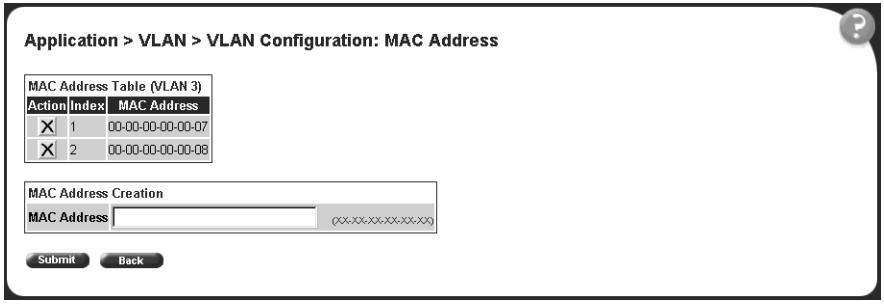
Item	Description
VLAN	The number assigned to the VLAN when the VLAN was created.
VLAN Name	(Re)name the VLAN.
	Opens the VLAN Configuration: MAC Address page (Figure 68).
Learning Constraint	The type of learning constraint selected when the VLAN was created. The learning constraint choices are IVL and SVL. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. 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 68).

Figure 68 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 68).

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 61).

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 61).

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 61).

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.

Configuring broadcast domains

You can configure specified VLAN switch ports with the appropriate PVID/VLAN association that enables the creation of broadcast domains. 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 69).

Figure 69 Port Configuration page

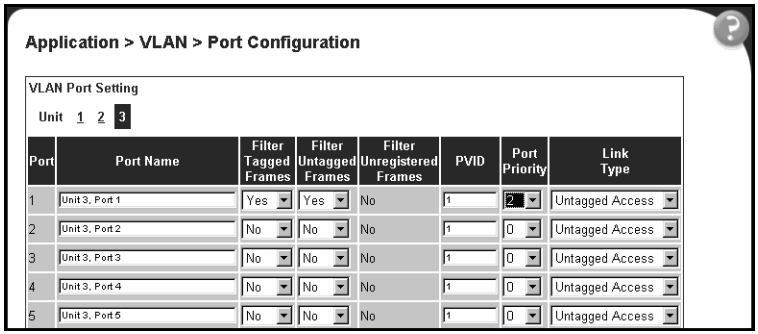


Table 61 describes the items on the Port Configuration page.

Table 61 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.
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.
Port Priority	0-7	Choose the level of priority for each port.
Link Type	(1) Untagged Access (2) Tagged Trunk	Choose the link type 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 70).

Figure 70 Port Information page

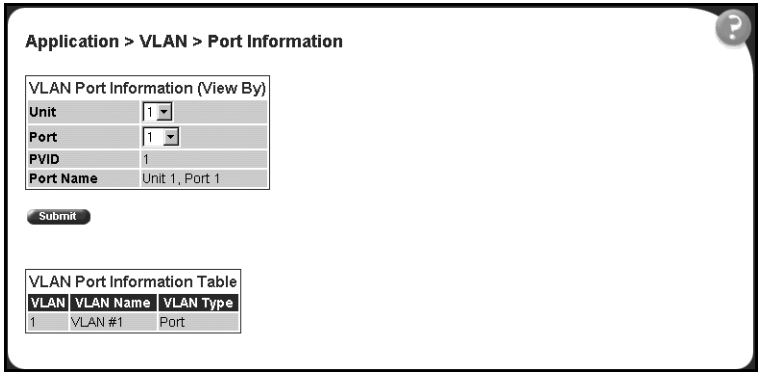


Table 62 describes the items on the Port Information page.

Table 62 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 70).

Managing Spanning Tree Protocol (STP)

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.

To configure switch ports for Spanning Tree participation:

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

The Port Configuration page opens (Figure 71).

Figure 71 Port Configuration page

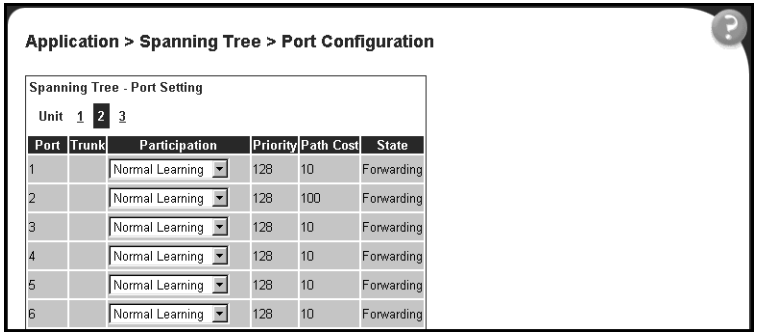


Table 63 describes the items on the Port Configuration page.

Table 63 Port Configuration page items

Item	Description/Command
Port	The port number of the currently displayed unit.
Trunk	The trunk that corresponds to the switch ports specified as MLT members. For more information on MLT, see "Type information in the text boxes, or select from a list." on page 161.
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.
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 In the port row(s) of your choice, choose to enable STP (normal learning or fast learning) or disable STP.

3 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 Bridge Information page opens (Figure 72).

Figure 72 Bridge Information page

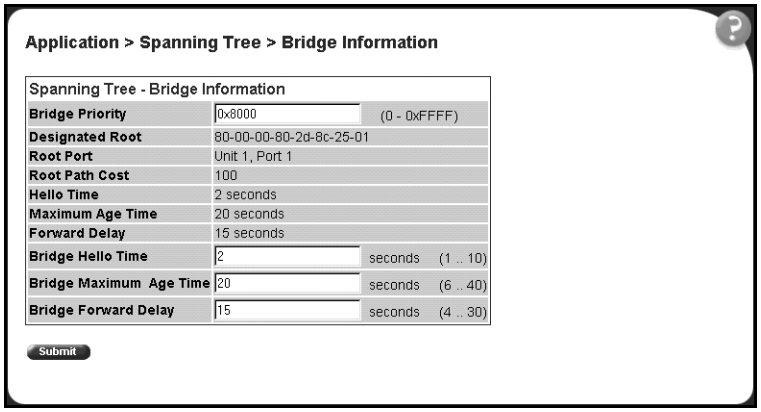


Table 64 describes the items on the Bridge Information page.

Table 64 Bridge Information page items

Item	Range	Description
Bridge Priority	0..65535	Type the priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. The STA 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	XXXXXXXXXXXXXX	The bridge ID of the root bridge, as determined by the STA.
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 64 Bridge Information page items (continued)

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.

Table 64 Bridge Information page items (continued)

Item	Range	Description
Bridge Maximum Age Time	6..40 seconds	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: 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. See also Maximum Age Time. The default setting is 20 seconds.
Bridge Forward Delay	4..30 seconds	The amount of time that the bridge ports remains in the Listening and Learning states before entering the Forwarding state. Note: All bridges participating in the spanning tree network use the root bridge's Forward Delay parameter value. See also Forward Delay. The default setting is 15 seconds.

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 Business Policy Switch 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.

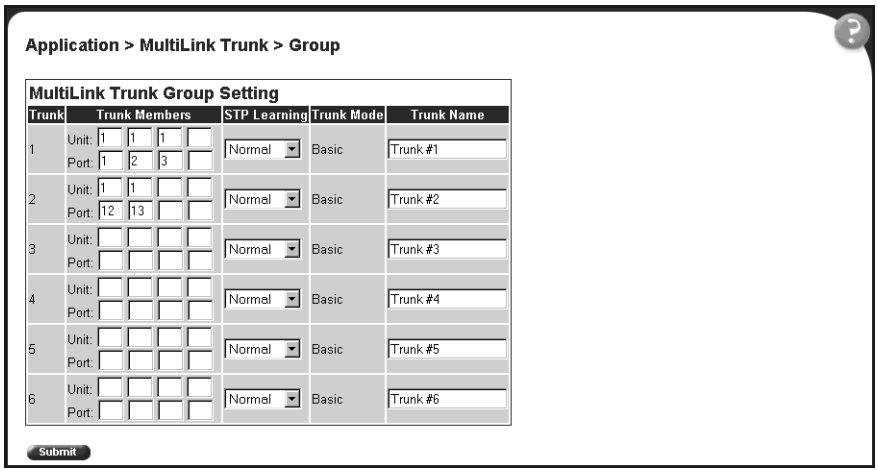
You can configure two to four switch ports together as members of a trunk to a maximum of six trunks.

To configure MultiLink Trunk members:

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

The Group page opens (Figure 73).

Figure 73 Group page



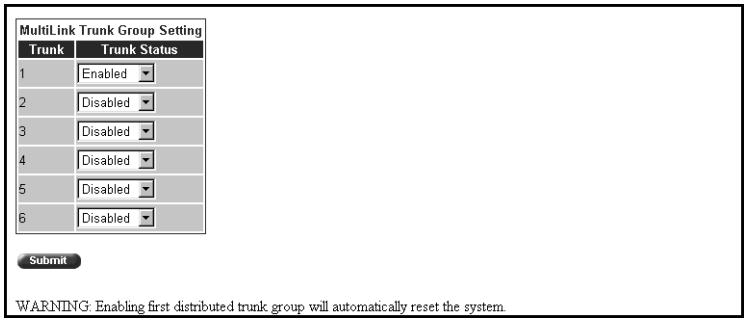


Table 65 describes the items on the Group page.

Table 65 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 30 on page 83) and Spanning Tree Configuration (see Figure 69 on page 154). 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 74).

Figure 74 Utilization page

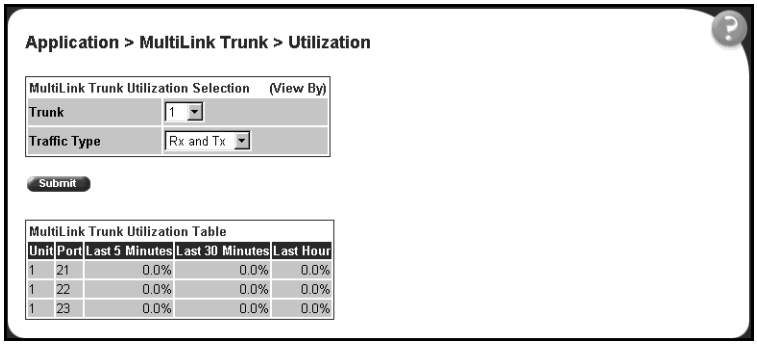


Table 66 describes the items on the Utilization page.

Table 66 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 66 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 74).

Chapter 8
Implementing Quality of Service (QoS)

You can configure QoS features in your network using the Web-based QoS Wizard or by using the advanced QoS configuration pages available in the Web-based management user interface.

The QoS options available to you are:

- Starting the QoS Wizard (page 168)
- Configuring QoS devices:
  - Interface groups (page 169)
  - Priority queue assignment (page 174)
  - DSCP queue assignment (page 177)
  - DSCP mapping (page 178)
- Configuring QoS rules:
  - IP filters or IP filter groups (page 180)
  - Layer 2 filters or layer2 filter groups (page 186)
- Configuring QoS filter actions (page 193)
- Configuring QoS policies (page 196)
- Configuring QoS Policy Agent high level operation (page 199)

About QoS

The QoS application delivers a set of tools that, when optimally configured, combat escalating bandwidth costs and optimize 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 QoS in your network with the Web-based management user interface using the “wizard” option or the detailed QoS pages.

Note: For sample configurations using the Web-based QoS Wizard and Web-based management user interface, see *Using the Business Policy Switch 2000* (part number 208700-A).

Starting the Web-based QoS Wizard

The QoS Wizard automates the definition of common QoS settings for the Business Policy Switch. It features:

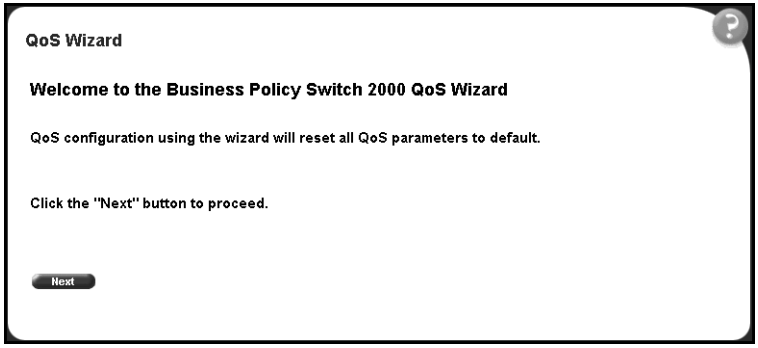
- Automatic generation of common QoS filters
- Optimizes configuration of real time applications, for example, VoIP and streaming video

To start the QoS Wizard:

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

The Business Policy Switch QoS Wizard page opens (Figure 75).

Figure 75 Business Policy Switch QoS Wizard opening page



For information on how to configure your network with the Business Policy Switch QoS Wizard (including a sample configuration), see *Using the Business Policy Switch 2000* (part number 208700-A).

Configuring an interface group

You view existing interface group configurations, or create or modify an interface group if you want a port (or ports) associated with a role combination for the purpose of assigning the same QoS policy to all interfaces in the group.

Note: Three default role combinations are always present, covering all ports of the device.

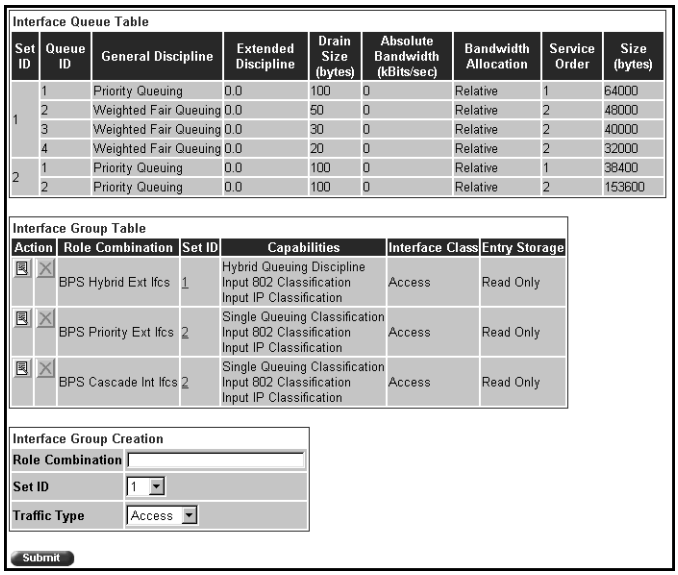
Creating an interface group configuration

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 76).

Figure 76 Interface Configuration page



Interface Queue Table

Set ID	Queue ID	General Discipline	Extended Discipline	Drain Size (bytes)	Absolute Bandwidth (kBits/sec)	Bandwidth Allocation	Service Order	Size (bytes)
1	1	Priority Queuing	0.0	100	0	Relative	1	64000
	2	Weighted Fair Queuing	0.0	50	0	Relative	2	48000
	3	Weighted Fair Queuing	0.0	30	0	Relative	2	40000
	4	Weighted Fair Queuing	0.0	20	0	Relative	2	32000
2	1	Priority Queuing	0.0	100	0	Relative	1	38400
	2	Priority Queuing	0.0	100	0	Relative	2	153600

Interface Group Table

Action	Role Combination	Set ID	Capabilities	Interface Class	Entry Storage
	BPS Hybrid Ext Ifcs	1	Hybrid Queuing Discipline Input 802 Classification Input IP Classification	Access	Read Only
	BPS Priority Ext Ifcs	2	Single Queuing Classification Input 802 Classification Input IP Classification	Access	Read Only
	BPS Cascade Int Ifcs	2	Single Queuing Classification Input 802 Classification Input IP Classification	Access	Read Only

Interface Group Creation

Role Combination

Set ID 1

Traffic Type Access

Submit

Table 67 describes the items on the Interface Queue Table section of the Interface Configuration page.

Table 67 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.
Drain Size	The percentage of available bandwidth consumable to service the queue in one cycle.
Absolute Bandwidth	The absolute (number of bytes) 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 68 describes the items on the Interface Group Table section of the Interface Group page.

Table 68 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.
Set ID	The number that identifies the associated queue set.
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) outputIpClassification, (3) input802Classification, (4) output802Classification, (5) singleQueuingDiscipline, and (6) hybridQueuingDiscipline
Interface Class	The type of traffic received on interfaces associated with the specified role combination. The options are Trusted and Untrusted. See also “Traffic Type” in Table 69.
Entry Storage	Specifies whether or not the interface group can be deleted.

Table 69 describes the items on the Interface Group Creation section of the Interface Group page.

Table 69 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.
Set ID (qosInterfaceTypeId)	1 = 4-queue port 2 = 2-queue port	Choose a Set ID. Note: Certain ports are assigned to a role combination based only on their queueing capabilities.
Traffic Type (qosInterfaceTypeExt1fClass)	(1) Trusted (2) Untrusted	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 remark the DSCP.

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 76)

Adding or removing interface group members

To select or deselect ports as members of an existing interface group:

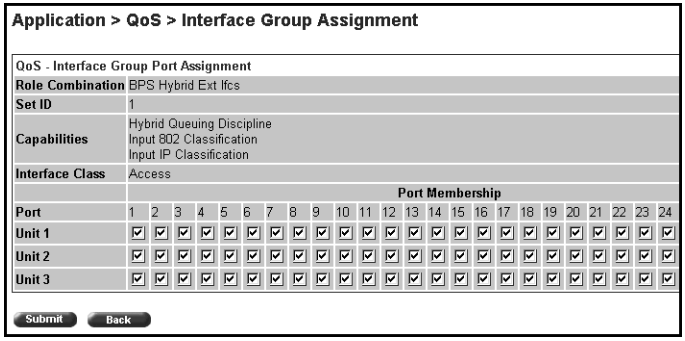
1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Interface Configuration.

The Interface Configuration page opens (Figure 76).

2 In the Interface Group Table section, in the Role Combination configuration row of your choice, click the Modify icon.

The Interface Group Assignment page opens (Figure 77).

Figure 77 Interface Group Assignment page



Application > QoS > Interface Group Assignment

QoS - Interface Group Port Assignment																								
Role Combination	BPS Hybrid Ext Ifcs																							
Set ID	1																							
Capabilities	Hybrid Queuing Discipline Input 802 Classification Input IP Classification																							
Interface Class	Access																							
	Port Membership																							
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Unit 1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Unit 2	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Unit 3	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Submit Back

Table 70 describes the items on the Interface Group Assignment page.

Table 70 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.
Set ID	The number that identifies the associated queue set.
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) outputIpClassification, (3) input802Classification, (4) output802Classification, (5) singleQueuingDiscipline, and (6) hybridQueuingDiscipline
Interface Class	The type of traffic received on interfaces associated with the specified role combination. The options are Trusted and Untrusted. See also “Traffic Type” in Table 69.
Port Membership	Select the external ports to associate with the interface group.
Cascade Ports	The cascade (internal) ports to associate with the interface group.
	Note: Port queueing capabilities determine if a port can be added to an existing role combination.

3 In the Port Membership section, click the check boxes of the ports to associate with the interface group.

4 Do one of the following:

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

Deleting an interface group configuration

To delete an Interface group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Interface Configuration.

The Interface Configuration page opens (Figure 76).

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 77).

3 In the Port Membership section, click the check boxes to deselect all ports associated with the interface group.

4 Click Submit.

The Interface Configuration page is displayed (Figure 76).

5 In the Interface Group Table section, in the role combination 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 a user priority queue assignment

You can assign 802.1D 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 user priority:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Priority Q Assign.

The User Priority Assignment page opens (Figure 78).

Figure 78 User Priority Assignment page

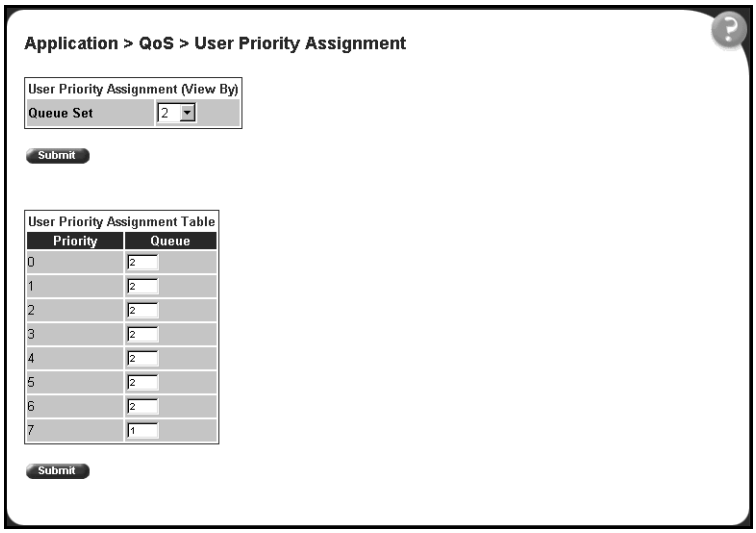


Table 71 describes the items on the User Priority Assignment page.

Table 71 Priority Assignment Table section page items

Section	Item and MIB association	Description
User Priority Assignment (View By)	Queue Set	Choose the queue set you want to modify.
User Priority Assignment Table	Priority (ntnQosIfPriAssignmentPri)	The 802.1D 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 User Priority Assignment section, select the queue set to view in the User Priority Assignment Table.

3 Click Submit

The table is updated with the queue set you requested.

4 In the User Priority Assignment Table section, type the information in the text boxes.

5 Click Submit.

Note: Clicking Submit in the User Priority Assignment Table section results in a system reset.

Configuring user priority mapping

To configure 802.1p user priority to DSCP mapping:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Priority Mapping.

The User Priority Mapping page opens (Figure 79).

Figure 79 User Priority Mapping page

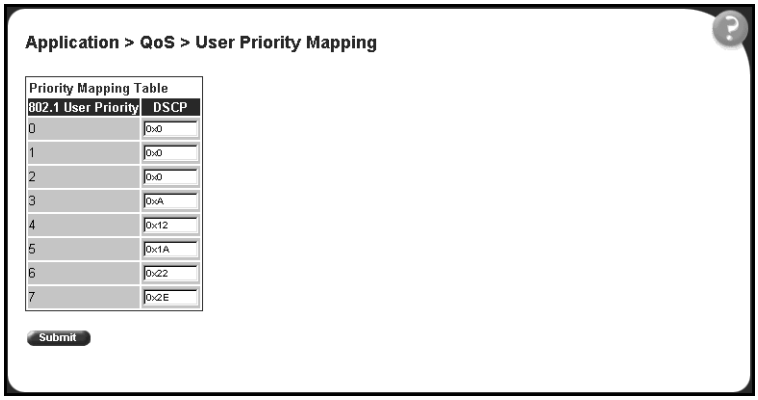


Table 72 describes the items on the User Priority Mapping page.

Table 72 User Priority Mapping page items

Item	Description
802.1 User 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

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 80).

Figure 80 DSCP Queue Assignment page

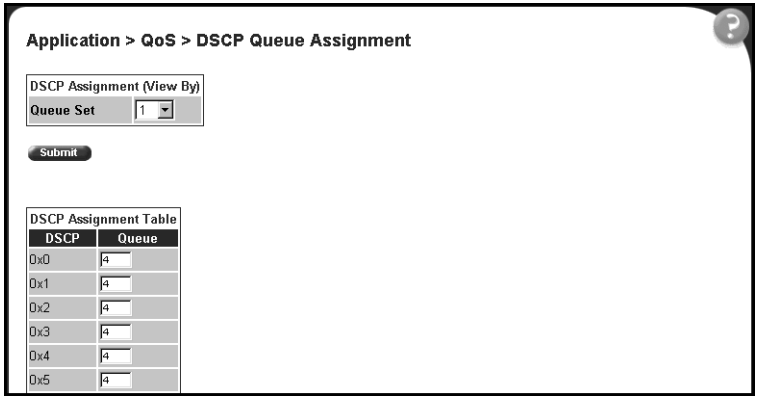


Table 73 describes the items on the DSCP Queue Assignment page.

Table 73 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.

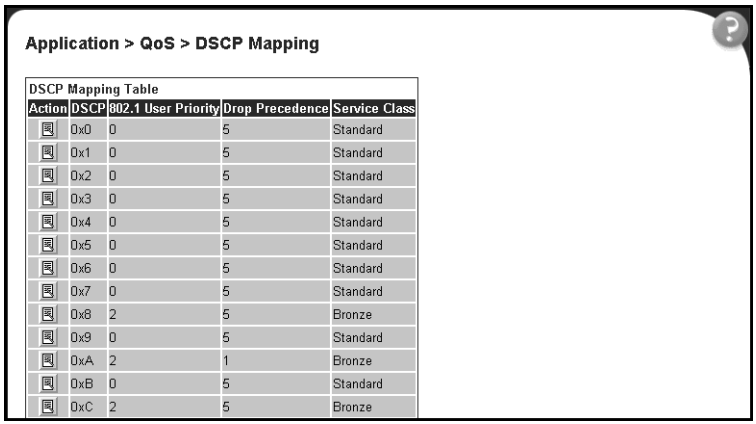
Configuring DSCP mapping

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 Table page opens (Figure 81).

Figure 81 DSCP Mapping Table page



Application > QoS > DSCP Mapping

DSCP Mapping Table

Action	DSCP	802.1 User Priority	Drop Precedence	Service Class
	0x0	0	5	Standard
	0x1	0	5	Standard
	0x2	0	5	Standard
	0x3	0	5	Standard
	0x4	0	5	Standard
	0x5	0	5	Standard
	0x6	0	5	Standard
	0x7	0	5	Standard
	0x8	2	5	Bronze
	0x9	0	5	Standard
	0xA	2	1	Bronze
	0xB	0	5	Standard
	0xC	2	5	Bronze

Table 74 describes the items on the DSCP Mapping Table page.

Table 74 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.
802.1 User 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: 1) Premium, (2) Platinum, (3) Gold, (4) Silver, (5) Bronze, and (6) Standard. 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 82).

Figure 82 DSCP Mapping Modification page

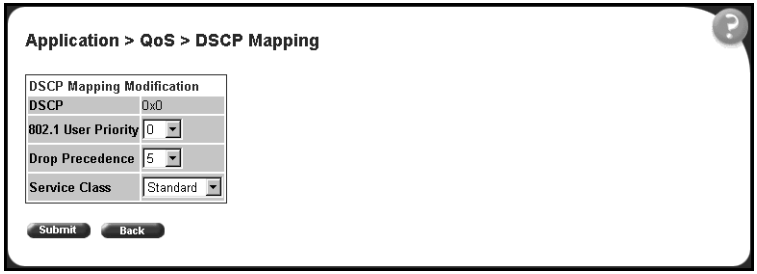


Table 75 describes the items on the DSCP Mapping Modification page.

Table 75 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.
802.1 User 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	1..8	Choose the drop value precedence to use for traffic with the associated 802.1D user priority value with the identified queue. Selecting a value between 1-4 specifies a low packet drop precedence; selecting a value between 5-8 specifies a high packet drop presentness. Note: Generally, low packet drop precedence receives preferential treatment.
Service Class	(1) Premium (2) Platinum (3) Gold (4) Silver (5) Bronze (6) Standard	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 trusted traffic.	

3 Select from a list.

4 Click Submit.

The modified configuration appears in the DSCP Mapping Table (Figure 81).

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 83).

Figure 83 IP Classification page

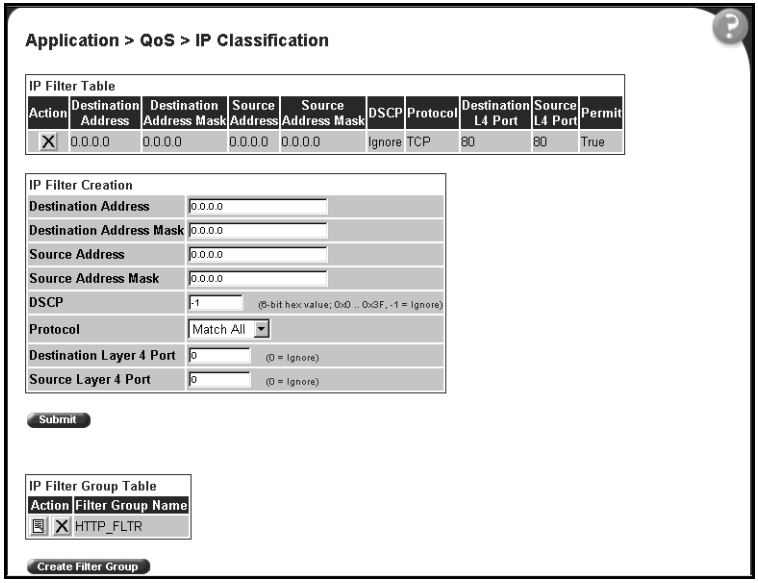


Table 76 describes the items on the IP Filter Table and IP Filter Creation sections of the IP Classification page.

Table 76 IP Filter Table and IP Filter Creation section items

Item and MIB association	Range	Description
✕		Deletes the row. Note: You cannot delete a filter if it is referenced in a filter group.
Destination Address (qosIpAceDstAddr)	XXX.XXX.XXX.XXX	Type the IP address to match against the packet's destination IP address.

Table 76 IP Filter Table and IP Filter Creation section items (continued)

Item and MIB association	Range	Description
Destination Address Mask (qosIpAceDstAddrMask)	XXX.XXX.XXX.XXX	Type 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	Type the IP address to match against the packet's source IP address.
Source Address Mask (qosIpAceSrcAddrMask)	XXX.XXX.XXX.XXX	Type the mask for the matching of the source IP address. One (1) bits must be left justified.
DSCP (qosIpAceDscp)	Integer (-1, 0..63)	Type the value that the DSCP in the packet must have and match this filter.
Protocol (qosIpAceProtocol)	TCP (6) UDP (17) ICMP (1) IGMP (2) RSVP (46) Match All (0)	Choose the IP protocol to match against the packet's IP protocol field.
Destination L4 Port (qosIpAceDstL4PortMin) (qosIpAceDstL4PortMax)	Integer (0.65535)	Type 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)	Type 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 83).

Note: An IP filter configuration is not modifiable. The filter must be deleted and then reconfigured.

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 89).

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.

Note: An IP filter configuration cannot be modified. The configuration must be deleted and then recreated.

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 83).

Table 77 describes the items on the IP Filter Group section of the IP Classification page.

Table 77 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 84).

Figure 84 IP Classification Group page

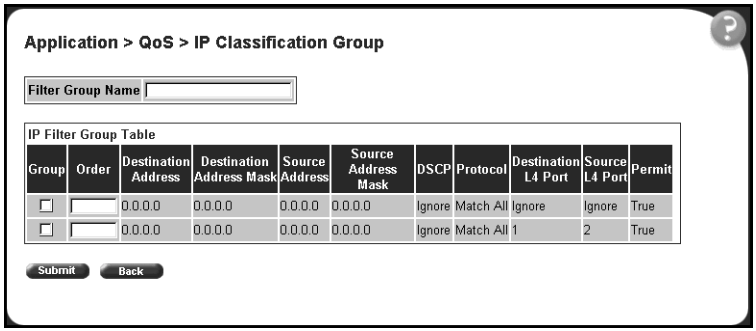


Table 78 describes the items on the IP Classification Group page.

Table 78 IP Classification Group page items

Item	Range	Description
Filter Group Name	1..64	Type 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: TCP, UDP, ICMP, IGMP, RSVP, or Match All
Destination L4 Port		The value that the packet's layer 4 destination port number can have and match the ACE.
Source L4 Port		The value that the packet's layer 4 source port number can have and match the ACE.
	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 83).

Modifying an IP filter group configuration

To modify an IP filter group configuration:

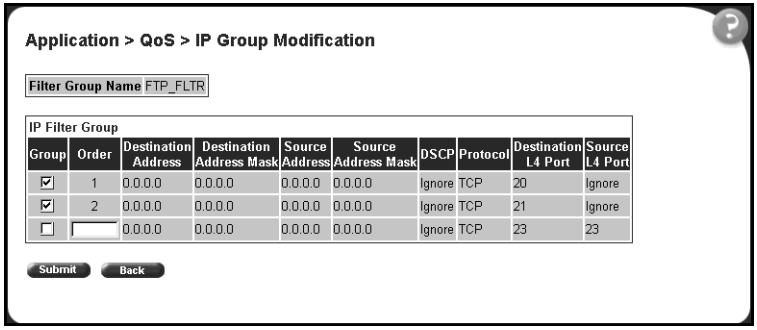
1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 89).

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 85).

Figure 85 IP Group Modification page



Group	Order	Destination Address	Destination Address Mask	Source Address	Source Address Mask	DSCP	Protocol	Destination L4 Port	Source L4 Port
☑	1	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	20	Ignore
☑	2	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	21	Ignore
☐		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	23	23

Table 78 describes the items on the IP Group Modification page.

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 89).

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.

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.

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 86).

Figure 86 Layer2 Classification page

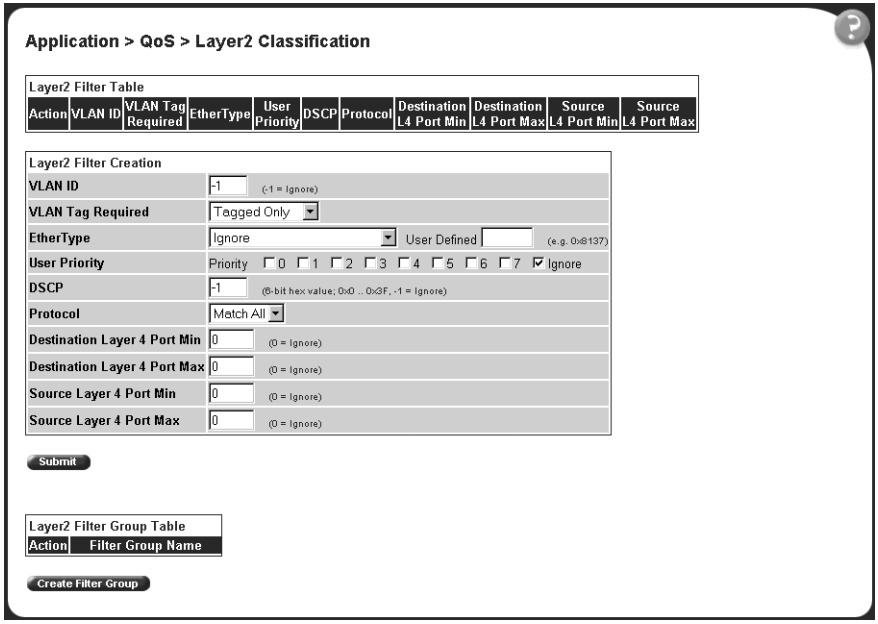


Table 79 describes the items on the Layer2 Filter Table and Layer2 Filter Creation sections of the Layer2 Classification page.

Table 79 Layer2 Filter Table and Layer2 Filter Creation section items

Item	Range	Description
		Deletes the row.
VLAN ID	-1 = ignore, 1-4094	Type the VLAN number.
VLAN Tag Required	(1) Tagged Only (2) Untagged Only (3) Ignore	Specify whether or not to check VLAN tagging.

Table 79 Layer2 Filter Table and Layer2 Filter Creation section items (continued)

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.
User Defined		If you chose User Defined as the EtherType, type the user defined Ether type.
User Priority		Select the user priority level.
DSCP	Integer (-1, 0..63)	Type the value that the DSCP in the packet must have and match this filter. Note: -1 = Ignore

Table 79 Layer2 Filter Table and Layer2 Filter Creation section items (continued)

Item	Range	Description
Protocol	TCP UDP ICMP IGMP RSVP Match All	Select the IP protocol to match against the packet's IP protocol field.
Destination L4 Port Min	Integer (0.65535)	Type the least value that the packet's layer 4 destination port number can have and match this filter.
Destination L4 Port Max	Integer (0.65535)	Type the maximum value that the packet's layer 4 destination port number can have and match this filter.
Source L4 Port Min	Integer (0.65535)	Type the least value that the packet's layer 4 source port number can have and match this filter.
Source L4 Port Max	Integer (0.65535)	Type 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 86).

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 86).

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: You cannot delete a layer 2 filter if it is referenced in a layer 2 filter group.

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 86).

Table 80 describes the items on the Layer2 Filter Group Table section of the Layer2 Classification page.

Table 80 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 87).

Figure 87 Layer2 Group page

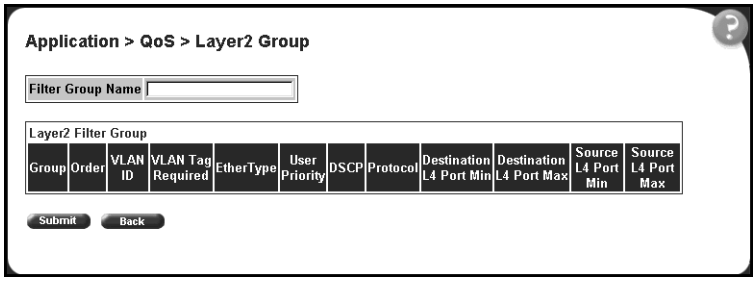


Table 81 describes the items on the Layer2 Group page.

Table 81 Layer2 Group page items

Item	Range	Description
Filter Group Name	1..64	Type 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.
VLAN ID		The VLAN ID 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.
User Priority		The user 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: TCP, UDP, ICMP, IGMP, RSVP, or Match All
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.
	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 Filter Group Table (Figure 86).

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 86).

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 88).

Figure 88 Layer2 Group modification page

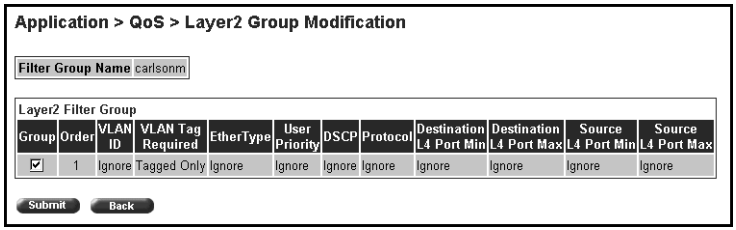


Table 81 describes the items on the Layer2 Group modification page.

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 86).

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.

Configuring a filter action

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 > Action.

   The Action page opens (Figure 89).

Figure 89 Action page

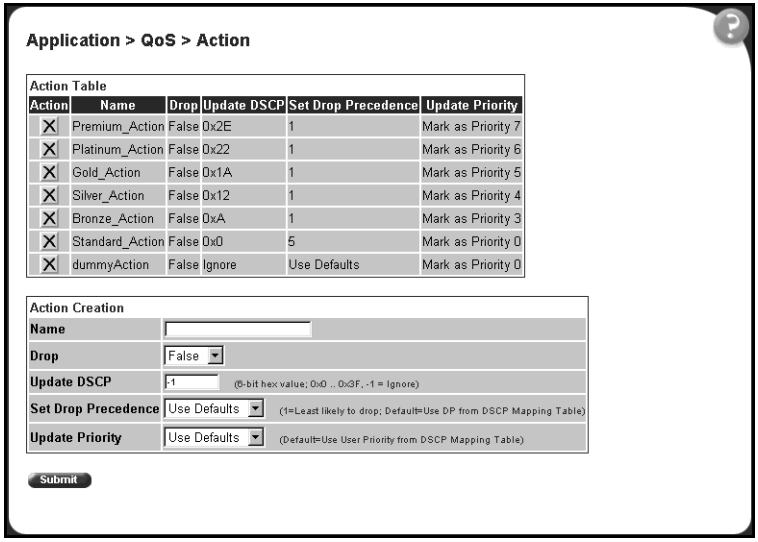


Table 82 describes the items on the Action page.

Table 82 Action page items

Item and MIB association	Range	Description
✕		Deletes the row.
Name	1..64	Type a character string to uniquely identify the action configuration.
Drop (qosActionDrop)	(1) True (2) False	Choose whether the frame being evaluated should be dropped (true) or not dropped (false) by this attribute. The default setting is False.
Update DSCP (qosActionUpdateDSCP)	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 -1 (ignore).

Table 82 Action page items (continued)

Item and MIB association	Range	Description
Set Drop Precedence (ntnQosActionExtSetDropPrec)	1-8, Use Defaults	Choose a packet drop precedence value. Selecting a value between 1-4 specifies a low packet drop precedence; selecting a value between 5-8 specifies a high packet drop precedence. Note: Generally, low packet drop precedence receives preferential treatment. The default setting is Use Defaults.
Update Priority (ntnQosActionExtUpdatePri)	0-7, Use Defaults	Choose the action attribute that causes the value contained in the user priority field in the 802.1Q frame to be updated based on the value of this object. The update priority range values are 0 (lowest priority) to 7 (highest priority). Note: If you select Use Defaults, a definition value is chosen based on the DSCP mapping tables. 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 89).

Note: Action filter configurations are not modifiable. They must be deleted and the information recreated.

Deleting a filter action configuration

To delete a filter action configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Action.

The Action page opens (Figure 89).

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.

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.

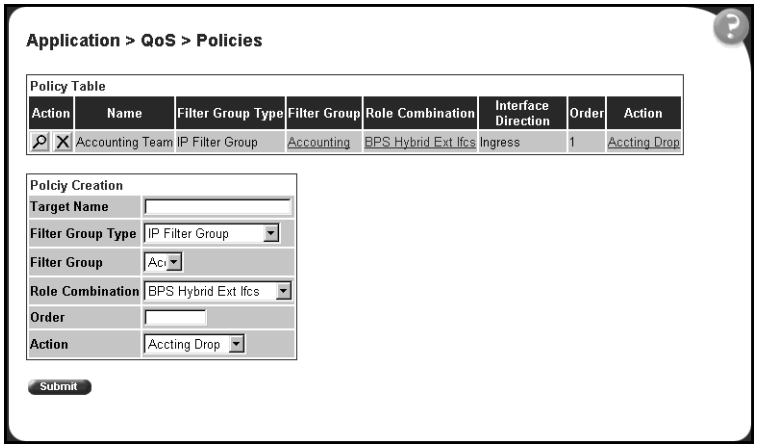
Installing defined filters

To create a hardware filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Policies.

The Policies page opens (Figure 90).

Figure 90 Policies page



Note: Policy configurations are not modifiable. They must be deleted and the information re-entered.

Table 83 describes the items on the Policy page.

Table 83 Policy page items

Section	Item and MIB association	Range	Description
Policy Table			Opens a view only statistics table. The table displays current filter statistics in bytes and packets.
			Deletes the row.
	Name		A list of the names of existing target configurations.
	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.
	Order		The number used to determine the order of precedence for this target specification.
	Action		The filter action associated with this entry. Note: Filter actions are created on the Action management page (see "Configuring a filter action" on page 193).
Policy Creation	Target Name	1..64	Type a character string to create a unique name to identify this target.
	Filter Group Type (qosTargetAc1Type)	(1) IP Filter Group (2) Layer2 Filter Group	Choose the type of filter group to associate with this target.
	Filter Group		Choose the filter group to associate with this target.
	Role Combination (qosTargetInterfaceRoles)		Choose the type of interface to which this target specification applies, specified in terms of a role combination.
	Order	Integer	Type a number to use as a determinate of the order of precedence for this filter.
	Action	Acting Drop	Choose the filter action associated with this entry. Note: Filter actions are created on the Action management page (see "Configuring a filter action" on page 193).

Viewing a hardware policy configuration

To view statistics for a selected hardware policy configuration:

1. From the main menu, choose Application > QoS > QoS Advanced > Policies.

   The Policies page opens (Figure 90).

2. In the Policy Table section, in the filter group configuration of your choice, click the View icon.

   The Target Statistics page opens (Figure 91).

Figure 91 Target Statistics page

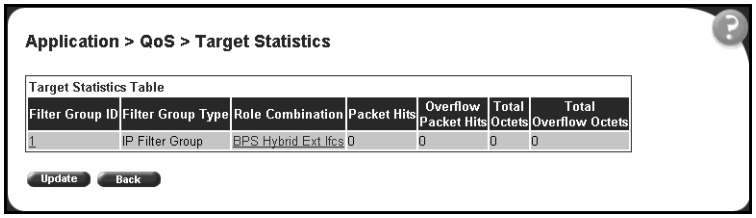


Table 84 describes the items on the Target Statistics page.

Table 84 Target Statistics page items

Item and MIB association	Description
Filter Group ID	The filter group associated with the selected target.
Filter Group Type	The type of group that is referenced by this instance of the filter Target class. The options are: IP Filter Group or Layer2 Filter Group.
Role Combination	The interfaces to which this target specification applies, specified in terms of a role combination.
Packet Hits	The packets selected for additional processing. The action taken is based on a match with specified filter and/or threshold information.
Overflow Packet Hits	The number of times the associated ntnQosTargetPktHits counter overflowed.
Total Octets	The total number of octets associated with packet hits for this target.
Total Overflow Octets	The total number of times the associated ntnQosTargetTotalOctets counter overflowed.

3 To refresh the hardware policy statistics, click Update.

Deleting a hardware policy configuration

To delete a hardware filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Policies.

The Policies page opens (Figure 90).

2 In the Policy Table section, in the hardware 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 hardware filter 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 Configuration page:

1 From the main menu, choose Application > QoS > QoS Advanced > Agent.

The Configuration page opens (Figure 92).

Figure 92 Configuration page

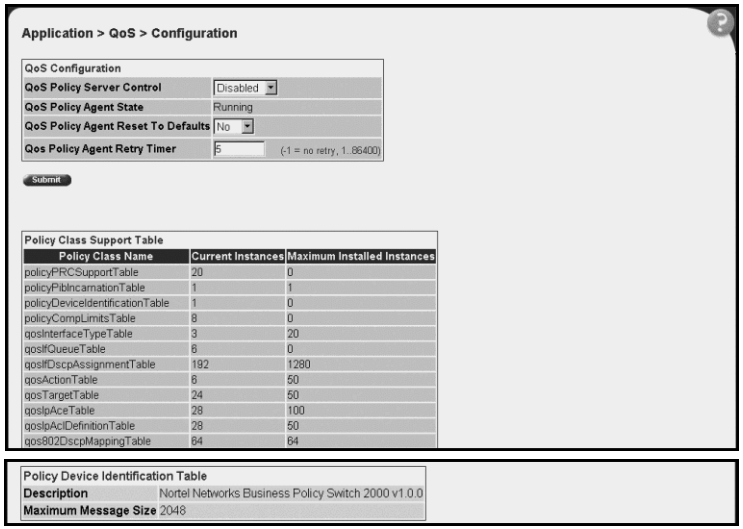


Table 85 describes the items on the Configuration page.

Table 85 Configuration 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)		The current status of the policy agent. The status options are: Running, Initializing, or Disabled.
	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.
Policy Class Support Table	Current Instances		The current class entries.
	Maximum Installed Instances		The maximum number of allowed class entries.

Table 85 Configuration page items (continued)

Section	Item and MIB association	Range	Description
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 9
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 208)

Viewing COPS statistics and capabilities

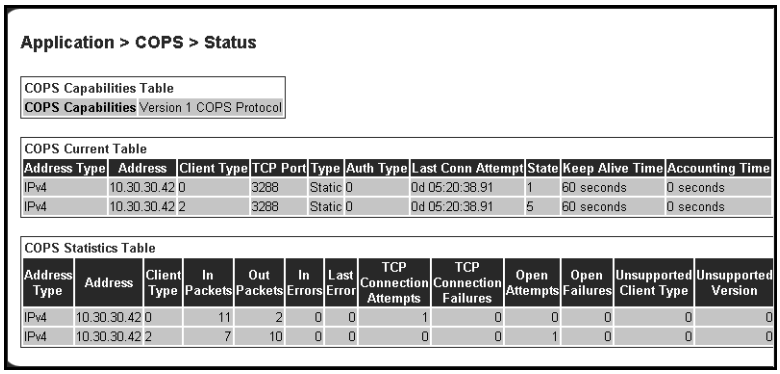
You can view a list of the capabilities of the COPS client to connect to a COPS server and view a table displaying the current status of all COPS server connections.

To view COPS capabilities and statistics:

1 From the main menu, choose Application > COPS > Status.

The Status page opens (Figure 93).

Figure 93 Status page



Application > COPS > Status

COPS Capabilities Table

COPS Capabilities	Version 1 COPS Protocol

COPS Current Table

Address Type	Address	Client Type	TCP Port	Type	Auth Type	Last Conn Attempt	State	Keep Alive Time	Accounting Time
IPv4	10.30.30.42	0	3288	Static	0	0d 05:20:38.91	1	60 seconds	0 seconds
IPv4	10.30.30.42	2	3288	Static	0	0d 05:20:38.91	5	60 seconds	0 seconds

COPS Statistics Table

Address Type	Address	Client Type	In Packets	Out Packets	In Errors	Last Error	TCP Connection Attempts	TCP Connection Failures	Open Attempts	Open Failures	Unsupported Client Type	Unsupported Version
IPv4	10.30.30.42	0	11	2	0	0	1	0	0	0	0	0
IPv4	10.30.30.42	2	7	10	0	0	0	0	1	0	0	0

Table 86 describes the items on the Status page.

Table 86 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 86 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 86 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 86 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 94).

Figure 94 Configuration page

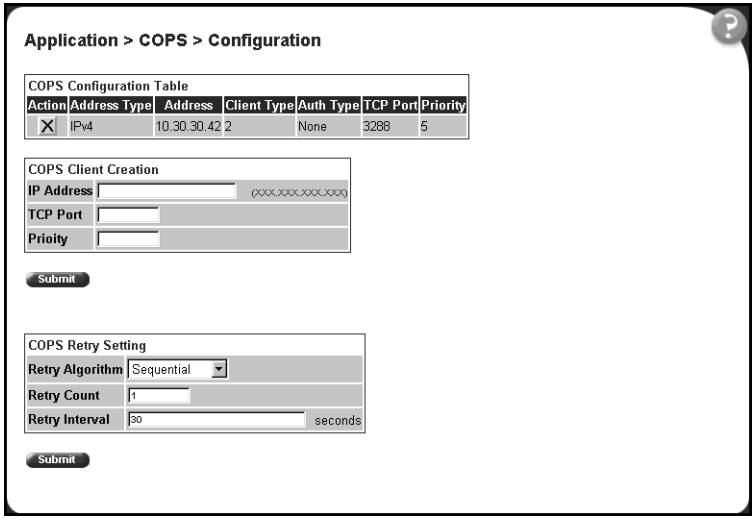


Table 87 describes the items on the COPS Configuration Table section of the Configuration page.

Table 87 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 87 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 94).

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 10
Support menu

The customer support options available to you are:

- Help
- Release Notes
- Manuals
- Upgrades

Using the online help option

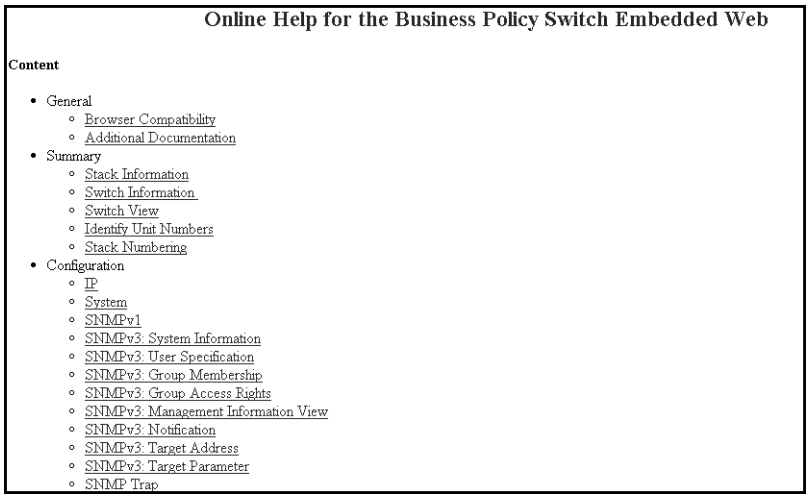
You can read information about management page functions in the online help menu embedded in the Web-based management interface.

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 95).

Figure 95 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

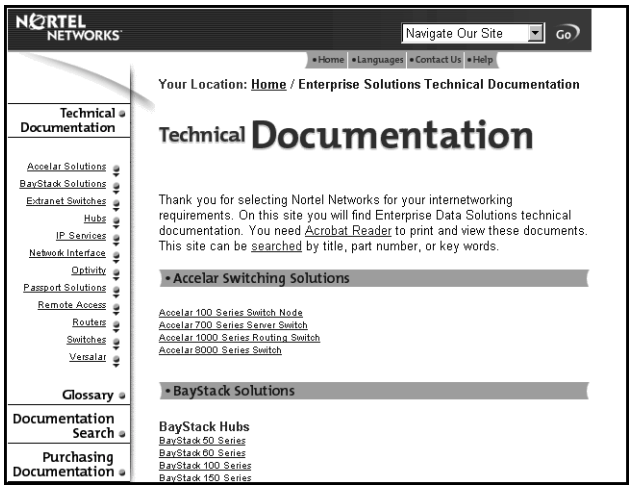
You can download current documentation about the Web-based management user interface from Nortel Networks Technical Documentation Web site.

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 96).

Figure 96 Nortel Networks Technical Documentation Web site



2 Locate your product, and click the document you want to download.

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 Technical Documentation Web site opens in a separate Web browser (Figure 96).

2 Follow the prompts to download the software release.

3 Close the Web browser.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S