Part No. 208700-D
November 2002

4655 Great America Parkway
Santa Clara, CA 95054

Using the Business Policy Switch 2000 Version 2.5

NORTEL NETWORKS™

Copyright © 2002 Nortel Networks

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

Trademarks

Nortel Networks is a trademark of Nortel Networks.

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

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

Acrobat Reader and Adobe are registered trademarks of Adobe Systems Incorporated.

Java is a registered trademark of Sun Microsystems, Inc.

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

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

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

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

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

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

USA requirements only

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

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

European requirements only

EN 55 022 statement

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

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

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

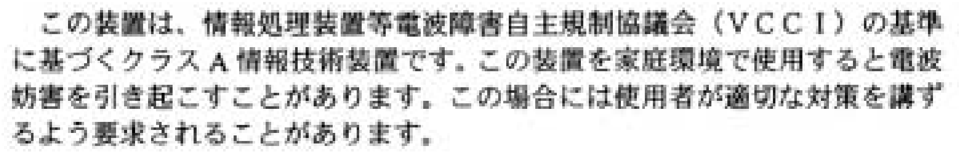
Attention: Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l’utilisateur de prendre les mesures spécifiques appropriées.

AEC Declaration of Conformity

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

Japan/Nippon requirements only

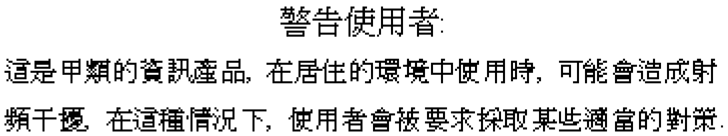
Voluntary Control Council for Interference (VCCI) statement



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

Taiwan requirements

Bureau of Standards, Metrology and Inspection (BSMI) Statement



警告使用者:

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

Canada requirements only

Canadian Department of Communications Radio Interference Regulations

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

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (<product or system name>) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

Nortel Networks Inc. software license agreement

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

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

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

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

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

4. General

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

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

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

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

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

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

Contents

Chapter 3

Figures

Tables

Preface

This guide describes the Nortel Networks* Business Policy Switch 2000* features and uses. The terms "Business Policy Switch 2000," "Business Policy Switch," and "BPS 2000" are used synonymously in this document. The Business Policy Switch introduces policy-enabled networking features to optimize consistent performance and behavior for your network traffic. The Differentiated Services (DiffServ) network architecture offers varied levels of service for different types of data traffic. DiffServ lets you designate a specific level of performance on a per-packet basis. For more information about configuring policy-enabled networking, see Chapter 4, "Policy-enabled networks."

The Business Policy Switch includes a dedicated Uplink Module slot for attaching optional media dependent adapters (MDAs) that support a range of media types, including Gigabit Ethernet. Installation instructions are included with each MDA (see your Nortel Networks sales representative for ordering information). For more information about the MDAs, refer to *Installing Media Dependent Adapters (MDAs)* and *Installing Gigabit Interface Converters and Small Form Factor Interface Converters*.

You can use the Business Policy Switch in:

- A standalone switch configuration.
- A Business Policy Switch 2000-only stack configuration.
- A mixed stack configuration consisting of BayStack* 450, BayStack 410, *and* Business Policy Switch 2000 switches.

The Business Policy Switch 2000 provides fail-safe stackability when you install the optional BayStack 400-ST1 Cascade Module.

This chapter covers the following topics:

- "Before you begin," next
- "Related publications" on page 28

- "How to get help" on page 31

Before you begin

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

- Basic knowledge of networks, Ethernet bridging, and IP and IPX routing
- Familiarity with networking concepts and terminology
- Specific knowledge about the networking devices, protocols, topologies, and interfaces that comprise your network
- Experience with windowing systems, graphical user interfaces (GUIs), or Web browsers

Related publications

For more information about using the Business Policy Switch 2000, refer to the following publications:

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

  Documents important changes about the software and hardware that are not covered in other related publications.
- *Installing the Business Policy Switch 2000* (part number 209319-A)

  Describes how to install the Business Policy Switch 2000.
- *Getting Started with the Business Policy Switch 2000 Management Software Operations* (part number 209321-A)

  Describes how to install the Java*-based device level software management application.
- *Reference for the Business Policy Switch 2000 Management Software Version 2.5* (part number 209322-D)

  Describes how to use the Java-based device-level software management application.

- *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5* (part number 209570-D)

  Describes how to use the Web-based management tool to configure switch features.

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

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

- *Configuring the BayStack and Business Policy Switches with the Preside Network Configuration System* (part number 312061-B Rev 00)

  Describes how to use the Network Configuration System (NCS) to configure and manage the BPS 2000.

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

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

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

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

- *Installing the BayStack 400-ST1 Cascade Module (*part number 304433-B)

  Describes how to connect up to eight switches into a stack configuration by installing optional BayStack 400-ST1 Cascade Modules.

- *BayStack 10 Power Supply Unit Installation Instructions* (part number 208558-B)

  Describes installation, power-up, power-down and fan replacement procedures.

- *Release Notes for the BayStack 10 Power Supply Unit* (part number 208560-B)

  Documents important changes about the RPSU/UPS that are not covered in other related publications.

- *Installation and Reference for the BayStack RPSU/UPS* (part number 208296-C)

  Describes how to install the optional RPSU/UPS to your Business Policy Switch 2000.

- *100 Watt DC-DC Converter Installation and Reference Guide* (part number 209132-B)

  Describes installation and removal procedures for the 100-watt DC-to-DC converter for your Business Policy Switch 2000.

- *Reference Note: Gigabit Ethernet Physical Layer Considerations* (part number 201540-B)

  Provides information about gigabit transmission over fiber optic cable and mode conditioning.

- *Release Notes for Optivity Quick2Config for the Business Policy Switch 2000 2.2.1* (part number 310621-A)

  Documents important Quick2Config changes that are not covered in other related publications.

- *Configuring Business Policy Switches with Optivity Quick2Config 2.2* (part number 311208A)

  Describes how to configure the BPS 2000 using Quick2Config.

- *Installing and Administering Optivity Quick2Config 2.2* (part number 207809-B)

  Describes how to install Quick2Config.

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

  Describes how to install Optivity Policy Services*.

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

  Describes how to configure and manage Optivity Policy Services.

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

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

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

  Provides a quick map to installing Optivity Policy Services.

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

  Describes known anomalies with Optivity Policy Services.

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

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

How to get help

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

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

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

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

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

Chapter 1
The Business Policy Switch 2000

This chapter introduces the Business Policy Switch 2000 and covers the following topics:

- "General description," next
- "Stacking compatibility" on page 33
- "Upgrading software" on page 35
- "Software version 2.5 compatibility with BayStack 450 switches" on page 38
- "Physical description" on page 39
- "Features" on page 50
- "Configuration and switch management" on page 96
- "Supported standards and RFCs" on page 99

General description

The Business Policy Switch introduces policy-enabled networking features to optimize consistent performance and behavior for your network traffic. The Differentiated Services (DiffServ) network architecture offers varied levels of service for different types of data traffic. DiffServ lets you designate a specific level of performance on a per-packet basis.

Stacking compatibility

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

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

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

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

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

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

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

Refer to Appendix B for complete information on interoperability and compatibility between the BPS 2000 and BayStack switches.

Upgrading software

Note: Use the Command Line Interface (CLI), console interface (CI) menus, or the Web-based management system to upgrade to software version 2.5. For detailed instructions, refer to Chapter 3, *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5*, and *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*.

You use one of the management systems to upgrade or downgrade software. You follow a different procedure depending on whether you are using a Pure BPS 2000 stack or a Hybrid stack.

The stacking software compatibility requirements are as follows:

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

This section discusses the following topics:

- "Upgrading software in a Pure BPS 2000 stack," next
- "Upgrading software in a Hybrid stack" on page 36

Upgrading software in a Pure BPS 2000 stack

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

1. Download the operational software, or agent, image.
2. Download the diagnostics image.

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

➡ **Note:** Once you begin the upgrading process, do not interrupt the process at all. Interrupting the downloading (or upgrading) process may cause loss of connectivity.

Upgrading software in a Hybrid stack

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

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

- ISVN 1
  - — BayStack 410 or Bay Stack 450—version 3.1
  - — BPS 2000—versions 1.0 and 1.0.1

- ISVN 2
  - — BayStack 410 or BayStack 450—versions 4.0, 4.1 and 4.2
  - — BPS 2000—versions 1.1, 1.1.1, 1.2, 2.0, 2.0.5, and 2.5

This section describe the steps for the following software upgrades:

- "Upgrading software when ISVN is 2," next
- "Upgrading software when ISVN is 1" on page 37

Upgrading software when ISVN is 2

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

1. Download the BPS 2000 image file.

   The system resets.

2. Download the BPS 2000 diags file.

   The system resets.

Note: Once you begin the upgrading process, do not interrupt the process at all. Interrupting the downloading (or upgrading) process may cause loss of connectivity.

Upgrading software when ISVN is 1

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

1. Download the BPS 2000 image file and the BayStack 450/410 file *simultaneously.*

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

The system resets.

2 Download the other BayStack 450 image file.

The system resets.

3 Download the BPS 2000 diags file.

The system resets.

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

➡ **Note:** Once you begin the upgrading process, do not interrupt the process at all. Interrupting the downloading (or upgrading) process may cause loss of connectivity.

Software version 2.5 compatibility with BayStack 450 switches

The BPS 2000 software version 2.5 is compatible with BayStack 450 software version 4.0, 4.1 and 4.2.

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

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

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

You can use 256 port-, protocol-, and MAC SA-based VLANs for the stack with a Pure BPS 2000 stack running software version 2.5 (The maximum number of MAC SA-based VLANs available is 48). If you are working with a mixed, or hybrid, stack, you can use 64 VLANs for the entire stack. When you change from a Pure BPS 2000 Stack mode to a Hybrid Stack mode:

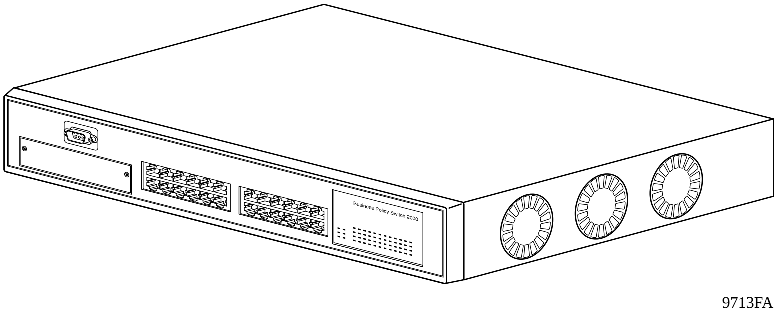
- If you have up to 64 VLANs on the Pure BPS 2000 Stack, they will be retained when you change to a Hybrid Stack.
- If you have more than 64 VLANs on the Pure BPS 2000 Stack, you will lose them all. The Hybrid Stack will return to the default VLAN configuration.

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

Physical description

Figure 1 depicts the front and side views of the Business Policy Switch.

Figure 1 Business Policy Switch 2000



Front panel

Figure 2 shows the front-panel configuration for the Business Policy Switch 2000. Descriptions of the front-panel components follow the figure.

For descriptions of the back-panel Business Policy Switch components, see “Back panel” on page 46.

Figure 2 Business Policy Switch 2000 front panel

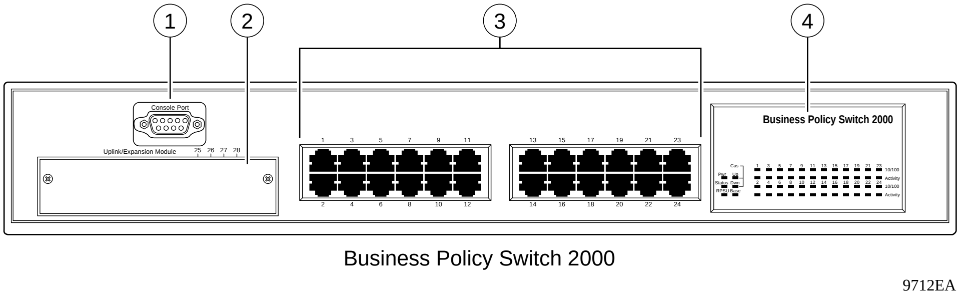


Table 1 Business Policy Switch 2000 front-panel description

1	Console port
2	Uplink/expansion slot

Table 1 Business Policy Switch 2000 front-panel description (continued)

3	Port connectors
4	LED display panel

Console port

The console port allows you to access the console interface (CI) screens and customize your network using the supplied menus and screens (see Chapter 3).

The console port is a DB-9, RS-232-D male serial port connector. You can use this connector to connect a management station or console/terminal to the Business Policy Switch by using a straight-through DB-9 to DB-9 standard serial port cable. You must use a VT100/ANSI-compatible terminal (for cursor control and to enable cursor and functions keys) to use the console port. See *Installing the Business Policy Switch 2000* for more information.

➡ **Note:** The console port is configured as a data communications equipment (DCE) connector. Ensure that your RS-232 cable pinouts are configured for DCE connections (see Appendixes).

The console port default settings are: 9600 baud with 8 data bits, 1 stop bit, and no parity as the communications format, with flow control set to enabled.

Uplink/Expansion slot

The Uplink/Expansion slot allows you to attach optional media dependent adapters (MDAs) that support a range of media types (see Appendixes for more information about MDA types available from Nortel Networks).

Port connectors

The Business Policy Switch uses 10BASE-T/100BASE-TX RJ-45 (8-pin modular) port connectors.

The 10BASE-T/100BASE-TX port connectors are configured as MDI-X (media-dependent interface-crossover). These ports connect over straight cables to the network interface card (NIC) in a node or server, similar to a conventional Ethernet repeater hub. If you are connecting to an Ethernet hub or Ethernet switch, use a crossover cable unless an MDI connection exists on the associated port of the attached device (see “Appendixes).

The Business Policy Switch uses autosensing ports designed to operate at 10 Mb/s (megabits per second) or at 100 Mb/s, depending on the connecting device. These ports support the IEEE 802.3u autonegotiation standard, which means that when a port is connected to another device that also supports the IEEE 802.3u standard, the two devices negotiate the best speed and duplex mode.

The 10BASE-T/100BASE-TX switch ports also support half- and full-duplex mode operation (refer to *Installing the Business Policy Switch 2000*).

The 10BASE-T/100BASE-TX RJ-45 ports can connect to 10 Mb/s or 100 Mb/s Ethernet segments or nodes.

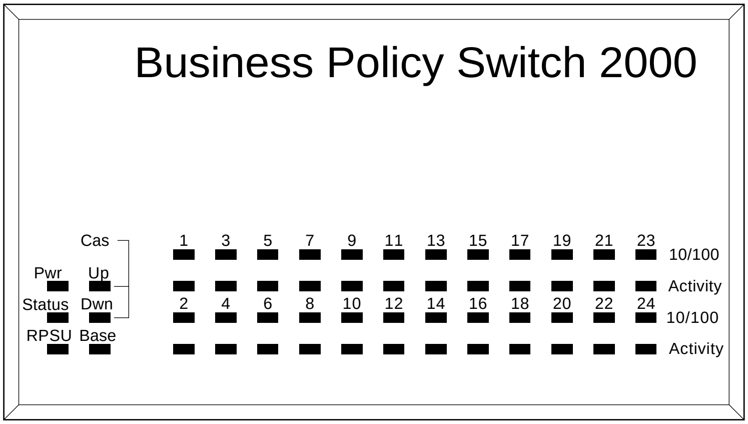
Note: Use only Category 5 copper unshielded twisted pair (UTP) cable connections when connecting 10BASE-T/100BASE-TX ports.

See Appendixes for more information about the RJ-45 port connectors.

LED display panel

Figure 3 shows the Business Policy Switch LED display panel. See Table 2 for a description of the LEDs.

Figure 3 Business Policy Switch 2000 LED display panel



9714EA

Table 2 Business Policy Switch 2000 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. (This includes nonworking fans.)
			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.

Table 2 Business Policy Switch 2000 LED descriptions (continued)

Label	**Type**	**Color**	**State**	**Meaning**
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	This unit has detected a problem with the switch connected to the cascade up connector. In order to maintain the integrity of the stack, this unit has bypassed its upstream neighbor and has wrapped the stack backplane onto an alternate path.
		Amber or Green	Blinking	Incompatible software revision or unable to obtain a unit ID (Renumber Stack Unit table full). The unit is on the ring but cannot participate in the stack configuration.
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	This unit has detected a problem with the switch connected to the cascade down connector. In order to maintain the integrity of the stack, this unit has bypassed its downstream neighbor and has wrapped the stack backplane onto an alternate path.
		Amber or Green	Blinking	Incompatible software revision or unable to obtain a unit ID (Renumber Stack Unit table full). The unit is on the ring but cannot participate in the stack configuration.

Table 2 Business Policy Switch 2000 LED descriptions (continued)

Label	Type	Color	State	Meaning
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).
			Blinking	Stack configuration error: indicates that *multiple* base units or *no* base units are configured in the stack.
		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.
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.
			Blinking	The corresponding port has been disabled by software.
		Amber	On	The corresponding port is set to operate at 10 Mb/s, and the link is good.
			Blinking	The corresponding port has been disabled by software.
			Off	The link connection is bad, or there is no connection to this port.

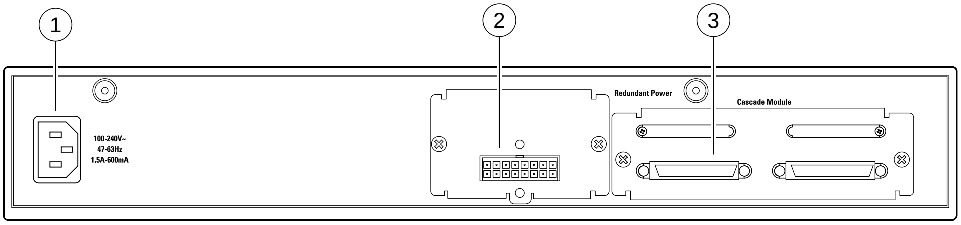
Table 2 Business Policy Switch 2000 LED descriptions (continued)

Label	Type	Color	State	Meaning
Link	Link status	Green	On	Valid communications link established.
			Off	The communications link connection is bad or there is no connection to this port.
			Blinking	The corresponding port is management disabled.
Activity	Port activity	Green	Blinking	Indicates network activity for the corresponding port. A high level of network activity can cause the LEDs to appear to be on continuously.

Back panel

The switch back panel is shown in Figure 4.

Figure 4 Business Policy Switch 2000 back panel



9719EA

Table 3 Business Policy Switch 2000 back-panel descriptions

1	AC power receptacle
2	RPSU connector
3	Cascade Module slot

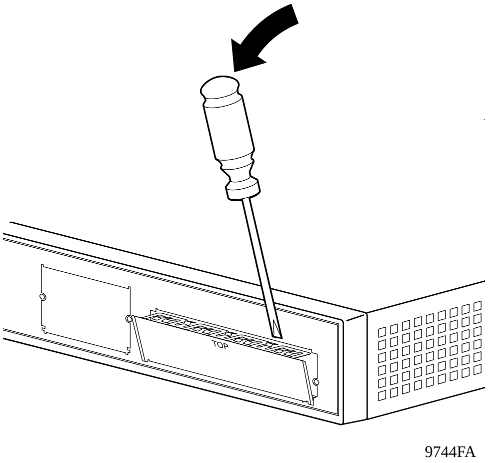
Cascade Module slot

The Cascade Module slot allows you to attach an optional BayStack 400-ST1 Cascade Module to the switch (see “Stack configurations” on page 112).

You can connect up to eight switches into a redundant stack configuration. Installation instructions are provided with each BayStack 400-ST1 Cascade Module (see *Installing the BayStack 400-ST1 Cascade Module*). Use a flathead screwdriver to remove the filler panel that covers the Cascade Module slot (Figure 5).

For more information about cascade modules, see *Installing the Cascade 400-ST1 Cascade Module*. See your Nortel Networks sales representative for cascade module ordering information.

Figure 5 Removing the cascade module filler panel



Cooling fans

Three cooling fans are located on one side of the Business Policy Switch to provide cooling for the internal components. (See Figure 1 on page 40.) When you install the switch, be sure to allow enough space on *both sides* of the switch for adequate air flow. See *Installing the Business Policy Switch 2000* for detailed information.

AC power receptacle

The AC power receptacle accepts the AC power cord (supplied). For installation outside of North America, make sure that you have the proper power cord for your region. Any cord used must have a CEE-22 standard V female connector on one end and must meet the IEC 320-030 specifications. Table 4 lists specifications for international power cords.

Table 4 International power cord specifications

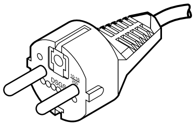
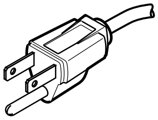
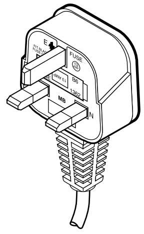
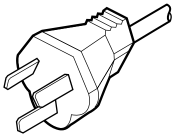
Country/Plug description	Specifications	Typical plug
Continental Europe: • CEE7 standard VII male plug • Harmonized cord (HAR marking on the outside of the cord jacket to comply with the CENELEC Harmonized Document HD-21)	220 or 230 VAC 50 Hz Single phase	
U.S./Canada/Japan: • NEMA5-15P male plug • UL recognized (UL stamped on cord jacket) • CSA certified (CSA label secured to the cord)	100 or 120 VAC 50–60 Hz Single phase	

Table 4 International power cord specifications (continued)

Country/Plug description	Specifications	Typical plug
United Kingdom: • BS1363 male plug with fuse • Harmonized cord	240 VAC 50 Hz Single phase	 229FA
Australia: • AS3112-1981 Male plug	240 VAC 50 Hz Single phase	 230FA

Redundant power supply unit (RPSU) and uninterruptible power supply (UPS)

The redundant power supply connector allows you to connect a backup power supply unit to the Business Policy Switch. Nortel Networks provides an optional redundant power supply unit (RPSU) for this purpose. The BayStack 10 Power Supply Unit is a hot-swappable power supply unit that provides uninterrupted operation to as many as four Business Policy Switches in the event that any of the switch power supplies fail.

The BayStack 10 Power Supply Unit has a powerful, modular redundant and uninterruptible power supply (UPS) functionality in a single chassis. It provides scalable power redundancy and protection to your networking equipment. The modules fit into the right-hand side of the rear of the chassis. The UPS and associated battery pack module fit into the front of the chassis.

For further information, refer to *Installation and Reference for the BayStack 10 Power Supply Unit* (part number 208296-C). Contact your Nortel Networks sales representative for more information.

100 Watt DC-DC Converter

The 100 Watt DC-DC Converter operates in conjunction with the Nortel Networks BayStack 10 Power Supply Unit and 200 Watt AC/DC Power Supply Module. The 100 Watt DC-DC Converter provides a plug-and-play redundant power supply unit for the Business Policy Switch 2000, as well as other products available from Nortel Networks. Contact your Nortel Networks sales representative for information about the Nortel Networks products that use the 100 Watt DC-DC Converter.

For further information about the 100 Watt DC-DC Converter, refer to *Installation and Reference for the 100 Watt DC-DC Converter Module* (part number 209132-B).

Features

The Business Policy Switch 2000 provides wire-speed switching that allows high-performance, low-cost connections to full-duplex and half-duplex 10/100/1000 Mb/s Ethernet local area networks (LANs). The Business Policy Switch provides the features detailed in the following sections:

- Introduced with software version 2.5
  - “Secure Shell” on page 52
  - “Per VLAN egress tagging” on page 53
  - “QoS enhancements” on page 53
- Introduced with software version 2.0.5
  - “Support for Far End Fault Indication (FEFI)” on page 54
  - Increased support from 40 to 150 RMON alarms
  - CLI support for RMON

- SNMP support for downloading ASCII configuration files
- Settable Multicast MAC address for Spanning Tree Groups (STG)
- SNMP support for downloading diagnostics
- Support for IGMP FAST LEAVE in Hybrid mode
- “Unknown multicast frame handling enhancement” on page 54
- BPS 2000-2GE MDA laser turned off when port disabled
- CLI enhancement for clearing Common Open Policy Services (COPS) server table
- CLI enhancement for saving configuration to NVRAM
- CLI enhancement for removing all VLANs
- “BPS 2000 Image If Newer option added to the software download menu” on page 53

- Introduced with software version 2.0
  - “Enhancement to BootP mode” on page 55
  - “Support for BPS 2000-1GT, BPS 2000-2GT, and BPS 2000-2GE MDAs” on page 55
  - “Policy-enabled networks with QoS shaping” on page 56
  - “Enhancements for QoS configuration using the Web” on page 57
  - “Port Naming” on page 57
  - “DA filtering using MAC address-based security” on page 58
  - “IP address for each unit in a stack” on page 58
  - “View CPU/memory utilization” on page 58
  - “Increased RMON alarms” on page 59
  - “QoS filtering of multiple VLANs” on page 56
- Introduced with software version 1.2
  - “CLI management system” on page 59
  - “Increased VLANs” on page 59
  - “Multiple Spanning Tree Protocol groups” on page 60
  - “ASCII configuration file” on page 65
  - “IP manager list” on page 68

- Introduced with software version 1.1
  - "Policy-enabled networks with QoS metering" on page 69
  - "Support for the BayStack 450-1GBIC MDA (GBIC MDA)" on page 69
  - "EAPOL-based security" on page 70
  - "Automatic PVID" on page 70
  - "Tabular port statistics" on page 72
  - "Ability to ping" on page 72
  - "Improved STP Fast Learning Mode" on page 73
  - "BootP menu item for a stack of only BPS 2000 switches" on page 73
- Introduced with software version 1.0
  - "Policy-enabled networking" on page 73
  - "Virtual Local Area Networks (VLANs)" on page 74
  - "Security" on page 78
  - "Flash memory storage" on page 92
  - "MultiLink Trunking" on page 93
  - "Port mirroring (conversation steering)" on page 94
  - "Autosensing and autonegotiation" on page 94
  - "BootP automatic IP configuration/MAC address" on page 95
  - "SNMP MIB support" on page 97
  - "SNMP trap support" on page 98

Secure Shell

With software version 2.5, you may establish a secure shell (SSH) connection to the BPS 2000. Using a combination of host, server, and session keys, the SSH protocol can provide strong authentication and secure communication over an unsecure network, offering protection from the following security risks:

- IP Spoofing
- IP source routing
- DNS spoofing

- Man-in-the-middle/TCP hijacking attacks
- Eavesdropping/Password sniffing.

Even if network security is compromised, traffic cannot be played back or decrypted, and the connection cannot be hijacked.

SSH can only be configured via the command line interface (NNCLI) or Device Manager. Refer to "Secure Shell" on page 87 for more information about the Secure Shell feature.

Per VLAN egress tagging

With software version 2.5, BPS 2000 ports can be configured to transmit frames tagged on some VLANs, and untagged on other VLANs.

Refer to "IEEE 802.1Q tagging" on page 119 for more information about the VLAN tagging feature.

QoS enhancements

Beginning with software version 2.5, there are up to 24 layer 2 filters available per unit. The number of available layer 2 filters varies according to the category of interface class you have configured.

Refer to "Layer 2 filters" on page 302 for more information about layer 2 filters and configuring interface classes.

BPS 2000 Image If Newer option added to the software download menu

If a newer image file is found, it will be downloaded and the switch will reset when the download process finishes successfully. Support for this feature has been added to the CLI, console, SNMP and Web-management.

Unknown multicast frame handling enhancement

By default, unknown multicast traffic is flooded to all ports in a VLAN. In situations where there is a multicast transmitter that is not doing IGMP and there are no multicast receivers, the traffic transmitted by the transmitter is flooded.

The new IGMP unknown mcast no flood CLI commands included in software version 2.0.5 allow you to send all unknown multicast traffic to IGMP static router ports only. This traffic will not be forwarded to dynamically discovered mrouter ports. If you want to forward unknown unicast traffic to certain ports only, you can set those ports as static mrouter ports.

- When disabled, BPS 2000 will treat unknown multicast traffic like broadcast traffic (flood). This is the default behavior.
- User setting for the unknown mcast no flood feature will be stored in NVRAM. In a stack, if settings on different units differ, Base Unit setting will take precedence. This feature can be enabled or disabled at any time.
- In a mixed BPS 2000/BayStack 450 stack, the unknown mcast no flood feature, if enabled, will take effect only on BPS 2000s. BayStack 450s will still flood unknown multicast traffic. Enabling this feature is not recommended in a mixed BPS 2000/BayStack 450 stack.
- It is suggested that this feature be used when IGMP snooping is enabled.

Support for Far End Fault Indication (FEFI)

When a fiber optic transmission link to a remote device fails, the remote device indicates the failure and the port is disabled. To use FEFI, you must enable autonegotiation on the port.

Note: FEFI will not work with the BPS 2000-2GE MDA because the BPS 2000-2GE MDA does not support autonegotiation.

Enhancement to BootP mode

Beginning with software version 2.0, the BootP or Last Address mode of BootP will always BootP for its IP configuration, regardless of whether a configured IP address is present, when the Stack BootP Mac Address Type is set to Base Unit Mac Address. If BootP is successful, the retrieved IP parameters are used by the switch or stack. The retrieved IP parameters are copied to the Last BootP IP parameters and overwrite any user-configured IP parameters. This feature applies only to a standalone BPS 2000 unit or to a stack consisting only of BPS 2000 units with the Stack Operational Mode set to Pure BPS 2000 Stack.

Support for BPS 2000-1GT, BPS 2000-2GT, and BPS 2000-2GE MDAs

Support for the BPS 2000-1GT, BPS 2000-2GT, and BPS 2000-2GE MDAs is provided with software version 2.5. The BPS 200-1GT, BPS 2000-2GT, and BPS 2000-2GE MDAs provide support for 8 priority queues for egress traffic and Weighted Round Robin (WRR) queuing.

The BPS 200-1GT MDA is a 1-port 1000BASE-T MDA; the BPS 2000-2GT MDA is a 2-port 1000BASE-T MDA; and the BPS 2000-2GE MDA accepts 2 small form factor pluggable (SFP) Gigabit Interface Connectors (GBICs).

The BPS 2000-2GE MDA supports the following SFP GBICs:

- 1000BASE-SX—This SFP GBIC uses shortwave 850 nm fiber optic connectors to connect devices over multimode (550 m or 1,805 ft) fiber optic cable.
- 1000BASE-LX—This SFP GBIC uses longwave 1,300 nm fiber optic connectors to connect devices over single mode (5 km or 3.1 mi) or multimode (550 m or 1,805 ft) fiber optic cable.

Refer to *Installing Media Dependent Adapters (MDA)s* and *Installing Gigabit Interface Converters and Small Form Factor Pluggable Interface Converters* for more information on installation, technical specifications, connectors, and cabling for the BPS 200-1GT, BPS 2000-2GT, and BPS 2000-2GE MDA.

Policy-enabled networks with QoS shaping

With version 2.0, the BPS 2000 supports the shaping, or traffic shaping, feature of IETF Differentiated Services (DiffServ) Quality of Service (QoS) architecture on a standalone BPS 2000 set to Pure BPS 2000 Stack operational mode.

➡ **Note:** You must use the BPS 2000-1GT, BPS 2000-2GT, or BPS 2000-2GE MDA with the Business Policy Switch in order to be able to configure the shaping features of QoS.

Refer to "Policy-enabled networking" on page 73, for a more complete description of policy-enabled networks, and refer to Chapter 4 for a complete discussion of policy-enabled networks, Differentiated Services (DiffServ), and Quality of Service (QoS). For information on configuring policy-enabled networks, DiffServ, and QoS, refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*, *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5*, and *Reference for the Business Policy Switch 2000 Management Software Version 2.5*.

QoS filtering of multiple VLANs

Beginning with BPS 2000 software version 2.0, you can filter multiple VLANs with a single layer 2 filter. You can filter up to 32 VLANs with a single layer 2 filter.

Enhancements for QoS configuration using the Web

With software version 2.0, the Web-based management system has an additional feature for configuring QoS. The QoS Quick Config pages provide a two-step process for configuring QoS policies.

The improved QoS Wizard is easier to use.

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

Finally, several of the Advanced QoS Web pages have been changed to make QoS configuration easier.

Refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*, for complete information about the Web-based management interface for configuring QoS parameters.

Port Naming

You can name, or specify a text string for, each port starting with software version 2.0. This feature provides easy identification of the connected users.

For information on naming ports, refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*, and *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5*.

Note: You must use either the CLI, DM, or the Web-based management system to name ports.

DA filtering using MAC address-based security

With software version 2.0, you can use the MAC address-based security feature (BaySecure*) to configure the BPS 2000 to drop all packets with specified MAC destination addresses (DAs). You can enter up to 10 specific MAC DAs you want filtered. This is an enhancement to the current MAC address-based security system that allows you to filter MAC source addresses (SAs).

Note: You must use either the Web-based management system or the CLI to configure MAC DA filtering.

Refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*, and *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5* and for information on configuring MAC address-based DA filtering.

IP address for each unit in a stack

You can assign an IP address to each unit in a stack from a single console port with BPS 2000 software version 2.0.

You must use either the console interface (CI) menus or the CLI to configure the IP addresses for each unit within a stack.

Refer to Chapter 3 and *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5* for information on configuring IP addresses for each unit in the stack from a single connection.

View CPU/memory utilization

You can view the amount of CPU and memory utilization with BPS 2000 software version 2.0. You can view this information using either the Web-based management system or SNMP.

Refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*, *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5,* and *Reference for the Business Policy Switch 2000 Management Software Version 2.5* for information on viewing the CPU and memory utilization.

Increased RMON alarms

Beginning with BPS 2000 software version 2.0, the RMON alarms are increased from 10 to 40 alarms.

CLI management system

With software version 1.2, the BPS 2000 offers a Command Line Interface (CLI) management system. You can issue CLI commands through the serial port of the switch or through a Telnet session. (The SNMPv3 and RMON features are not supported.)

You can work with the CLI interactively, when you use the CLI command to configure the switch command-by-command. You can also work with the CLI all at once, when you use the CLI command to configure the network.

Refer to *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5* for complete information on accessing the CLI and all commands.

Increased VLANs

The BPS 2000 software version 1.2 provides support for 256 virtual local area networks (VLANs). These 256 VLANs can be spread among port-based, protocol-based, and MAC source address-based VLANs (maximum of 48 MAC source address-based VLANs). Finally, the 256 VLANs can be on a standalone BPS 2000 with software version 1.2 or across a Pure BPS 2000 Stack with software version 1.2.

If you are working with more than 64 VLANs in a Pure BPS 2000 Stack and you change to a Hybrid Stack, you lose *all* VLANs. However, if you have up to 64 VLANs in the Pure BPS 2000 Stack and you change to a Hybrid Stack, you will retain all the VLANs.

Refer to "Virtual Local Area Networks (VLANs)" on page 74 for a more complete description of VLANs. For information on configuring VLANs, refer to Chapters 2 and 3, *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*, *Reference for the Business Policy Switch 2000 Management Software Version 2.5*, and *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5*.

Multiple Spanning Tree Protocol groups

BPS 2000 switches support the Spanning Tree Protocol (STP) as defined in IEEE 802.1D. As defined in the IEEE 802.1D standard, the Spanning Tree Protocol detects and eliminates logical loops in a bridged or switched network. When multiple paths exist, the spanning tree algorithm configures the network so that a bridge or switch uses only the most efficient path. If that path fails, the protocol automatically reconfigures the network to make another path become active, thus sustaining network operations.

Starting with software version 1.2**,** the BPS 2000 supports multiple spanning tree groups (STGs). The BPS 2000 supports a maximum of 8 STGs, either all in one standalone switch or across a stack consisting of **only** BPS 2000 switches (Pure BPS 2000 Stack mode). Multiple STGs provide multiple data paths, which can be used for load-balancing and redundancy. You enable load balancing between two BPS 2000 switches using multiple STGs by configuring each path with a different VLAN and then assigning each VLAN to a separate STG**.** Each STG is independent. Each STG sends its own Bridge Protocol Data Units (BPDUs), and each STG must be independently configured.

To use more that one STG, ensure that the Stack Operational Mode is set to Pure BPS 2000 Stack mode. To view and set the Stack Operational Mode, refer to Chapter 3, *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*, or *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5.*You have only the single default STG available if you are in Hybrid Stack mode, which is for running mixed stacks.

The STG, or bridge group, forms a loop-free topology that includes one or more virtual LANs (VLANs). With software version 1.2, the BPS 2000 supports multiple instances (8) of STGs running simultaneously.

As noted in "Increased VLANs," the BPS 2000 with software version 1.2 supports a maximum of 256 VLANs. With a maximum of 8 STGs, on average, each STG will have 32 VLANs.

In the default configuration of the BPS 2000, a single STG with the ID of 1 includes all ports on the switch. It is called the default STG. Although ports can be added to or deleted from the default STG, the default STG (STG1) itself **cannot** be deleted from the system. Also you cannot delete the default VLAN (VLAN1) from STG1.

The tagging for the BPDUs from STG1, or the default STG, is user-configurable (as are tagging settings for all STGs). However, by default STG1 sends out only untagged BPDUs in order to operate with all devices that support only one instance of STP. (The default tagging of STG2 through STG8 is tagged.)

Note: When you change the Stack Operational Mode from Pure BPS 2000 Stack mode to Hybrid Stack mode, you lose all STGs above 1 (the default STG).

All other STGs, except the Default STG, must be created by the user. To become active, each STG must be enabled by the user after creation. Each STG will be assigned an ID number from 2 to 8 (the Default STG is assigned the ID number 1). You assign ports or VLANs to an active STG. However, a port that is not a member of a VLAN will not be allowed to join an STG.

When you not longer need a particular STG, disable and delete that particular one. The procedure is to disable the STG, delete all VLAN and port memberships, and then delete the STG.

STG configuration guidelines

This section provides important information on configuring STGs:

- An STG must be created in the following order:
  - Create the STG
  - Add the existing VLAN and port memberships
  - Enable the STG
- When you create a VLAN, that VLAN automatically belongs to STG 1, the default STG. If you want the VLAN in another STG, you must move the VLAN by assigning it to another STG.
- You move a newly created VLAN to an existing STG by following this order:
  - Create the VLAN
  - Add the VLAN to an existing STG

> **Note:** Beginning with software version 2.0, you can move VLANs directly into STGs; you no longer need to delete them from the previous, or default, STG first.

- You cannot delete or move VLAN1 from STG1.

- VLANs must be contained **within** a single STG; a VLAN cannot span multiple STGs. By confining VLANs within a single STG, you avoid problems with spanning tree blocking ports and causing a loss of connectivity within the VLAN. When a VLAN spans multiple switches, the VLAN must be within the same spanning tree group (have the same STG ID) across all the switches.
- All VLANs in the same shared database (SVL) must be assigned to the same STG.
- All members of a particular MultiLink Trunking (MLT) group must be assigned to the same STG; that is, they can belong to one and only one STG.
- A port that is not a member of any VLAN cannot be added to any STG. The port must be added to a VLAN, and that VLAN added to the desired STG.
- Tagged ports can belong to more than one STG, but untagged ports can belong to **only one** STG.
- When a tagged port belongs to more than one STG, the egress BPDUs are tagged to distinguish the BPDUs of one STG from those of another STG.
- Because some STP-compliant devices do not support tagging, you can configure whether to send tagged or untagged BPDUs, even from tagged ports, with the BPS 2000 with software version 1.2. The VLAN ID for the tagged BPDUs will be 4000+STG ID.

Note: Beginning with software version 2.0, you can select a VLAN ID for tagged BPDUs for each STG. Valid VLAN IDs are 1 to 4094.

- An untagged port cannot span multiple STGs.
- When you add a port to a VLAN that belongs to an STG, the port is also added to the STG. However, if the port you are adding is an untagged port *and* is already a member of an STG, that port will *not* be added to an additional STG because an untagged port cannot belong to more that one STG. As an example, assume that VLAN1 belongs to STG1. You add an untagged port, port 1, that does not belong to any STG to VLAN1, and port 1 will become part of STG1.

However, if in the example explained above, the untagged port 1 already belongs to STG2, then port will not become a member of STG1.

- When you remove a port from VLAN that belongs to an STG, that port will also be removed from the STG. However, if that port belongs to another VLAN in the same STG, the port remains in the STG.

  As an example, assume that port 1 belongs to VLAN1, and VLAN1 belongs to STG1. When you remove port 1 from VLAN1, port 1 is also removed from STG1.

  However, if port 1 belongs to both VLAN1 and VLAN2 and both VLANs belong to STG1, removing port 1 from VLAN1 does *not* remove port 1 from STG1 because VLAN2 is still a member of STG1.

- An STG cannot be deleted until you disable it. Additionally, you cannot delete an STG while it contains VLAN members, so you must first delete the VLANs from the STG.

Spanning Tree Fast Learning

Spanning Tree Fast Learning is an enhanced port mode supported by the BPS 2000. If you enable Spanning Tree Fast Learning on a port with no other bridges, the port is brought up more quickly following the switch initialization or a spanning tree change. The port goes through the normal blocking and learning states before the forwarding state, but the hold times for these states is the bridge hello timer (2 seconds by default) instead of the bridge forward delay timer (15 seconds by default). If the port sees a BPDU it will revert to regular behavior.

With BPS 2000 software version 1.1 and higher, the port set with Fast Learning can forward data immediately, as soon as the switch learns that the port is enabled.

Fast Learning is intended for access ports where only one device is connected to the switch (as in workstations with no other spanning tree devices). It may not be desirable to wait the usual 30 to 35 seconds for spanning tree initialization and bridge learning.

Note: Use Spanning Tree Fast Learning with caution. This procedure is contrary to that specified in the IEEE 802.1D standard for Spanning Tree Protocol (STP), in which a port enters the blocking state following the initialization of the bridging device or from the disabled state when the port is enabled through configuration.

ASCII configuration file

Beginning with software version 1.2, the BPS 2000 can download a user-editable ASCII configuration file from a TFTP server. You can load the ASCII configuration file automatically at boot time or on demand using the management systems (console menus or CLI). Once downloaded, the configuration file automatically configures the switch or stack according to the Command Line Interface (CLI) commands in the file. This feature allows the flexibility of generating command configuration files that can be use on several switches or stacks with minor modifications. (The maximum size for an ASCII configuration file is 100 KBs; larger configuration files must be split into multiple files.)

Use a text editor to edit the ASCII configuration; the command format is the same as that of the CLI.

You can initiate the ASCII configuration file download using CLI commands only while connected to the base unit, and the ASCII configuration script will execute to completion. When you initiate downloading the ASCII configuration file from the console interface, the console does not display output. For this reason, it is important that you review the commands in the file to ensure accuracy and completeness.

For information on setting the parameters for the ASCII configuration file feature, refer to Chapter 3.

Sample ASCII configuration file

This section shows a sample ASCII configuration file. This file is an example only and shows a basic configuration for a standalone BPS 2000 that includes Multi-Link Trunking, VLANs, port speed and duplex, and SNMP configurations.

```
! ---------------------------------------------------------
! example script to configure different features from CLI
! ---------------------------------------------------------
!
enable
configure terminal
!
!
! ---------------------------------------------------------
! add several MLTs and enable
! ---------------------------------------------------------
mlt 3 name lag3 enable member 13-14
mlt 4 name lag4 enable member 15-16
mlt 5 name lag5 enable member 17-18
!
!
! ---------------------------------------------------------
! add vlans and ports
! ---------------------------------------------------------
!
! create vlan portbased
vlan create 100 name vlan100 type port
!
! add Mlts created above to this VLAN
vlan members add 100 17
!
! create vlan ip protocol based
vlan create 150 name vlan150 type protocol-ipEther2
!
! add ports to this VLAN
! in this case all ports
```

```
vlan members add 150 ALL
vlan ports ALL priority 3
!
! create vlan MACSA based
vlan create 90 name MAC90 type macsa
! add ports to this VLAN
! in this case all ports
vlan members add 90 ALL
!
! igmp
! you could disable proxy on vlan 100
vlan igmp 100 proxy disable
!
! -------------------------------------------------------
! Examples of changing interface parameters
! -------------------------------------------------------
! change speed of port 3
interface Fastethernet 3
speed 10
duplex half
exit
!
! change speed of port 4
interface Fastethernet 4
speed auto
duplex auto
!
!
! -------------------------------------------------------
! SNMP configuration
! -------------------------------------------------------
snmp host 192.168.100.125 private
snmp community private
!
!
exit
end
```

```
! -------------------------------------------------------
! Finished
! -------------------------------------------------------
```

Note: To add comments to the ASCII configuration file, add an exclamation point (!) to the beginning of the line.

Refer to *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5* for complete information on using the CLI commands.

IP manager list

With software version 1.2, you can limit access to the management features of the BPS 2000 by defining the IP addresses allowed access to the switch. The features provided by the IP manager list are:

- Definitions of up to 10 allowed IP addresses and masks
- Options to enable or disable access for Telnet, SNMP, and the Web-based management system

You must change the Telnet access field through direct access to the interface; you cannot change the Telnet access field through Telnet. You must set the Telnet feature after the first power-up.

Note: To avoid locking a user out of the switch, Nortel Networks recommends that you configure *ranges* of IP addresses that you allow access.

When you configure the access, you are setting access for the *next* session. The current session any user has open is unaffected.

For information on configuring the IP manager list, refer to Chapter 3, *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*, and *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5***.**

Policy-enabled networks with QoS metering

With version 1.1, the BPS 2000 supports the traffic policing, or metering, feature of IETF Differentiated Services (DiffServ) Quality of Service (QoS) architecture.

Refer to "Policy-enabled networking" on page 73, for a more complete description of policy-enabled networks, and refer to Chapter 4 for a complete discussion of policy-enabled networks, Differentiated Services (DiffServ), and Quality of Service (QoS). For information on configuring policy-enabled networks, DiffServ, and QoS, refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*, *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5*, and *Reference for the Business Policy Switch 2000 Management Software Version 2.5*.

Support for the BayStack 450-1GBIC MDA (GBIC MDA)

The BPS 2000 software version 1.1 provides support for the Gigabit Interface Connector (GBIC) MDA, named the BayStack 450-1GBIC MDA. The BayStack 450-1GBIC MDA provides only two priority queues.

The BayStack 450-1GBIC MDA supports the following GBICs:

- 1000BASE-SX—This GBIC uses shortwave 850 nm fiber optic connectors to connect devices over multimode (550 m or 1,805 ft) fiber optic cable.
- 1000BASE-LX—This GBIC uses longwave 1,300 nm fiber optic connectors to connect devices over single mode (5 km or 3.1 mi) or multimode (550 m or 1,805 ft) fiber optic cable.
- 1000BASE-XD—This GBIC uses single mode fiber to connect devices over distances up to 50 km (or 31 mi), depending on the quality of the cable.

- 1000BASE-ZX—This GBIC uses single mode fiber to connect devices over distances up to 70 km (or 43 mi), depending on the quality of the cable. The ports on this GBIC operate only in full-duplex mode.

Refer to *Installing Media Dependent Adapters (MDA)s* and *Installing Gigabit Interface Converters and Small Form Factor Interface Converters* for more information on installation, technical specifications, connectors, and cabling for the BayStack 450-1GBIC MDA.

EAPOL-based security

BPS 2000 software version 1.1 provides support for security based on the Extensible Authentication Protocol over LAN (EAPOL), which uses the EAP as described in the IEEE Draft P802.1X to allow you to set up network access control on internal LANs.

Refer to "Security" on page 78 for complete information on EAPOL-based security. For information on configuring EAPOL-based security using the Console Interface (CI) menus, refer to Chapter 3. To configure this feature using the Web-based management system, refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*. To use Device Manager (DM) to configure EAPOL-based security, refer to *Reference for the Business Policy Switch 2000 Management Software Version 2.5***.** And, to configure this feature using CLI commands, refer to *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5*.

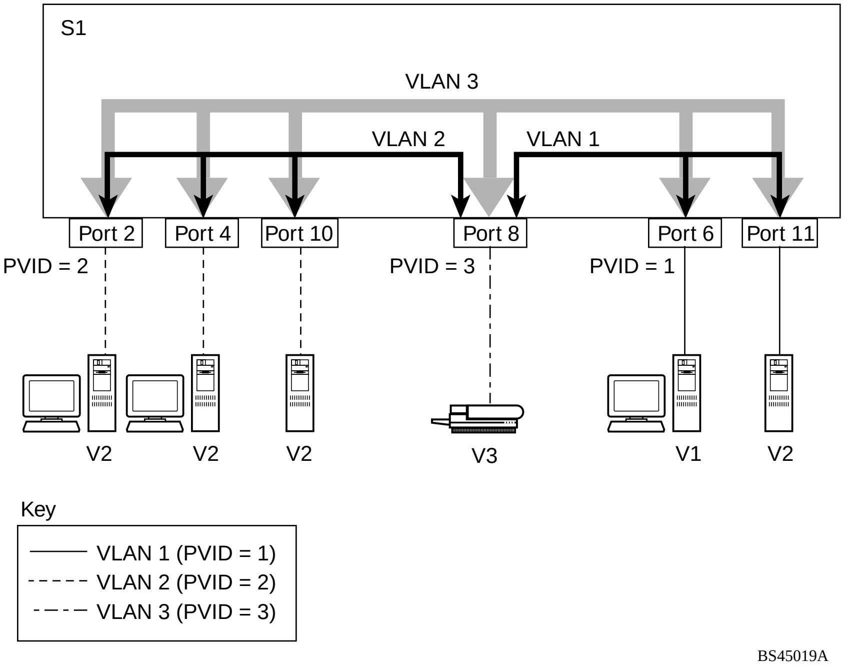
Automatic PVID

With software version 1.1, the BPS 2000 provides the Automatic PVID feature for configuring virtual local area networks (VLANs).

Refer to "Virtual Local Area Networks (VLANs)" on page 74 for more complete information on VLANs. Refer to Chapter 3 for information on configuring Automatic PVID using the Console Interface (CI) menus. Refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5* for information on configuring this feature using the Web-based management system. And, refer to *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5* for information on configuring Automatic PVID with CLI commands. Finally refer to *Reference for the Business Policy Switch 2000 Management Software Version 2.5* for information on configuring this feature using DM.

For example, to create a broadcast domain for each VLAN shown in Figure 6, configure each VLAN with a port membership and each port with the appropriate PVID/VLAN association:

Figure 6 VLAN broadcast domains within the switch



In Figure 6 the ports have the following PVID/VLAN associations:

- Ports 8, 6, and 11 are untagged members of VLAN 1.

The PVID/VLAN association for ports 6 and 11 is: PVID = 1.

- Ports 2, 4, 10, and 8 are untagged members of VLAN 2.

  The PVID/VLAN association for ports 2, 4, and 10 is: PVID = 2.

- Ports 2, 4, 10, 8, 6, and 11 are untagged members of VLAN 3.

  The PVID/VLAN association for port 8 is: PVID = 3.

Refer to Chapter 3 for information on configuring Automatic PVID using the Console Interface (CI) menus. Refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5* for information on configuring this feature using the Web-based management system. And, refer to *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5* for information on configuring Automatic PVID with CLI commands. Refer to *Reference for the Business Policy Switch 2000 Management Software Version 2.5* for information on configuring this feature with DM.

Tabular port statistics

With BPS 2000 software version 1.1, you can view all ports in an entire stack that have an error. If a particular port has no errors, it will not be displayed.

Refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5* to display tabular port statistics.

Ability to ping

With software version 1.1, you can ping from a BPS 2000. This ability greatly enhances the ease of network management.

Refer to Chapter 3 for information on using the Console Interface (CI) menus to ping and to *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5* for information on pinging with CLI commands.

Improved STP Fast Learning Mode

A front BPS 2000 port set for Fast Learning Mode for the Spanning Tree Protocol (STP) is improved in version 1.1 of BPS 2000 software. The port can forward data immediately, as soon as it detects that the link is on.

BootP menu item for a stack of only BPS 2000 switches

In a stack consisting only of BPS 2000 switches, you can perform BootP using the MAC address of the base unit.

Refer to "BootP automatic IP configuration/MAC address" on page 95 for more information on BootP and MAC addresses. You must use the console interface (CI) menus to choose this option. Refer to Chapter 3 for information on using the base unit MAC address for BootP.

Policy-enabled networking

The BPS 2000 enables system administrators to implement classes of service and assign priority levels to different types of traffic. You can configure policies that monitor the characteristics of traffic (for example, its source, destination, and protocol) and perform a controlling action on the traffic when certain user-defined characteristics are matched.

Differentiated Services (DiffServ) is a network architecture that lets service providers and enterprise network environments offer varied levels of service for different types of data traffic. Instead of using the "best-effort" service model to ensure data delivery, DiffServ's Quality of Service (QoS) lets you designate a specific level of performance on a packet-by-packet basis. If you have applications that require high performance and reliable service, such as voice and video over IP, you can use DiffServ to give preferential treatment to this data over other traffic. With BPS 2000 software version 1.1, you can use metering with QoS. BPS 2000 software version 2.0 introduces support for QoS shaping, or traffic shaping, on a standalone BPS 2000 set to the Pure BPS 2000 Stack operational mode.

➡ **Note:** You must use the BPS 2000-1GT, BPS 2000-2GT, or BPS 2000-2GE MDA in a Business Policy Switch in order to be able to configure the shaping features of QoS.

The Business Policy Switch 2000 uses DiffServ to manage network traffic and resources. The information that is required to support DiffServ and multi-field classification is transferred using the Common Open Policy Services (COPS) protocol. COPS is a query and response protocol that exchanges policy information messages using the Transmission Control Protocol (TCP). All configuration can be performed using SNMP, the CLI, and the Web-based interface. The BPS2000 switch can interoperate with the Nortel Networks Optivity* Policy Server using Common Open Policy Services (COPS).

Refer to Chapter 4, “Chapter 4, “Policy-enabled networks.”

To configure this feature using the Web-based management system, refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*. To use Device Manager (DM) to configure QoS, refer to *Reference for the Business Policy Switch 2000 Management Software Version 2.5*. And, to configure this feature using CLI commands, refer to *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5*.

For information on using COPS with the BPS 2000, go to the www.nortelnetworks.com/documentation URL. Then choose the specific software product (in this case, Optivity Policy Services).

Virtual Local Area Networks (VLANs)

➡ **Note:** For information on configuring VLANs, STGs, and MLTs, refer to “STG configuration guidelines” on page 62.

In a traditional shared-media network, traffic generated by a station is transmitted to all other stations on the local segment. Therefore, for any given station on the shared Ethernet, the local segment is the *collision domain* because traffic on the segment has the potential to cause an Ethernet collision. The local segment is also the *broadcast domain* because any broadcast is sent to all stations on the local segment. Although Ethernet switches and bridges divide a network into smaller collision domains, they do not affect the broadcast domain. In simple terms, a virtual local area network (VLAN) provides a mechanism to fine-tune broadcast domains.

Your Business Policy Switch allows you to create three types of VLANs:

- IEEE 802.1Q 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, you assign a Port VLAN Identifier (PVID) and specify which ports belong to the VLAN. The PVID is used to coordinate VLANs across multiple switches.

  In software version 1.1, automatic PVID automatically sets the PVID when you configure a port-based VLAN. The PVID value will be the same value as VLAN. The user can also manually change the PVID value.

  The default setting for AutoPVID is Off; you must enable this feature.

- Protocol-based VLANs

  A protocol-based VLAN is a VLAN in which you assign your switch ports as members of a broadcast domain, based on the protocol information within the packet. Protocol-based VLANs can localize broadcast traffic and assure that only the protocol-based VLAN ports are flooded with the specified protocol type packets. The maximum number of available protocols is 14.

- MAC source address (SA)-based VLANs

  A MAC SA-based VLAN is a VLAN in which you assign switch ports as members of a broadcast domain, based on the source MAC address information within the packet. MAC SA-based VLANs can be used to provide a MAC-level security scheme to organize and group different users. The maximum number of available MAC SA-based VLANs is 48.

Policy-based VLANs are determined by the information within the packet. A port can be a member of multiple policy-based VLANs. The order in which the rules for VLAN classification are applied are:

1. Is the packet tagged?
2. Does the packet belong in a MAC SA-based VLAN?
3. Does the packet belong in a protocol-based VLAN?

If none of the criteria applies, the packet belongs in the VLAN identified by the PVID of the ingress port. See Chapter 2, “Network configuration,” for more information.

In addition, you configure VLANs as:

- Shared VLAN Learning (SVL) mode—Multiple VLANs use a single forwarding database.

  OR

- Independent VLAN Learning (IVL) mode—Each VLAN uses a unique forwarding database.

The IVL mode is only an option when using the Business Policy Switch 2000; you must use the SVL mode when operating a hybrid stack. Business Policy Switches support up to 64 VLANs (port-, protocol-, or MAC SA-based), including VLAN #1 which is always port-based. With software version 1.2, the switch supports up to 256 VLANs. (The maximum number of available MAC SA-based VLANs is always 48.)

Note: The maximum 256 VLANs is supported only if the Stack Operational Mode is in Pure BPS 2000 Stack mode. A standalone BPS 2000 also supports a maximum 256 VLANs. (The maximum number of MAC SA-based VLANs is always 48.)

A mixed stack that consists of BPS 2000 and BayStack 450 switches has only 64 VLANs.

If you change from a Pure BPS 2000 Stack to a Hybrid Stack, you lose *all* VLANs.

When a switch port is configured to be a member of a VLAN, it is added to a group of ports (workgroup) that belong to one broadcast domain. You can assign different ports (and therefore the devices attached to these ports) to different broadcast domains. This feature allows network flexibility because you can reassign VLANs to accommodate network moves, additions, and changes, eliminating the need to change physical cabling.

Using 256 VLANs

The BPS 2000 software version 1.2 provides support for 256 VLANs. These 256 can be spread among port-based, protocol-based, and MAC SA-based VLANs (maximum of 48 MAC source address-based VLANs).

If you are working with more than 64 VLANs in a Pure BPS 2000 Stack and you change to a Hybrid Stack, you lose *all* VLANs. However, if you have up to 64 VLANs in the Pure BPS 2000 Stack and you change to a Hybrid Stack, you will retain all the VLANs.

To have more than 64 VLANs available, you must be operating in Pure BPS 200 Stack mode; you cannot be in Hybrid mode. The 256 VLANs are supported on either a standalone BPS 2000 with software version 1.2 or across a Pure BPS2000 Stack with software version 1.2.

Before you begin configuring more than 64 VLANs, you must ensure that you are operating in Pure BPS 2000 Stack mode, and not in Hybrid Stack mode. For information on viewing and setting the stack operational mode, refer to Chapter 3, *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*, or *Reference for the Business Policy Switch 2000 Management Software Version 2.5.*

Refer to Chapter 2, "Network configuration," for more information on VLANs. For information on configuring VLANs using the CI menus, refer to Chapter 3. To configure this feature using the Web-based management system, refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*. To use Device Manager (DM) to configure VLANs, refer to *Reference for the Business Policy Switch 2000 Management Software Version 2.5***.** And, to configure this feature using CLI commands, refer to *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5*.

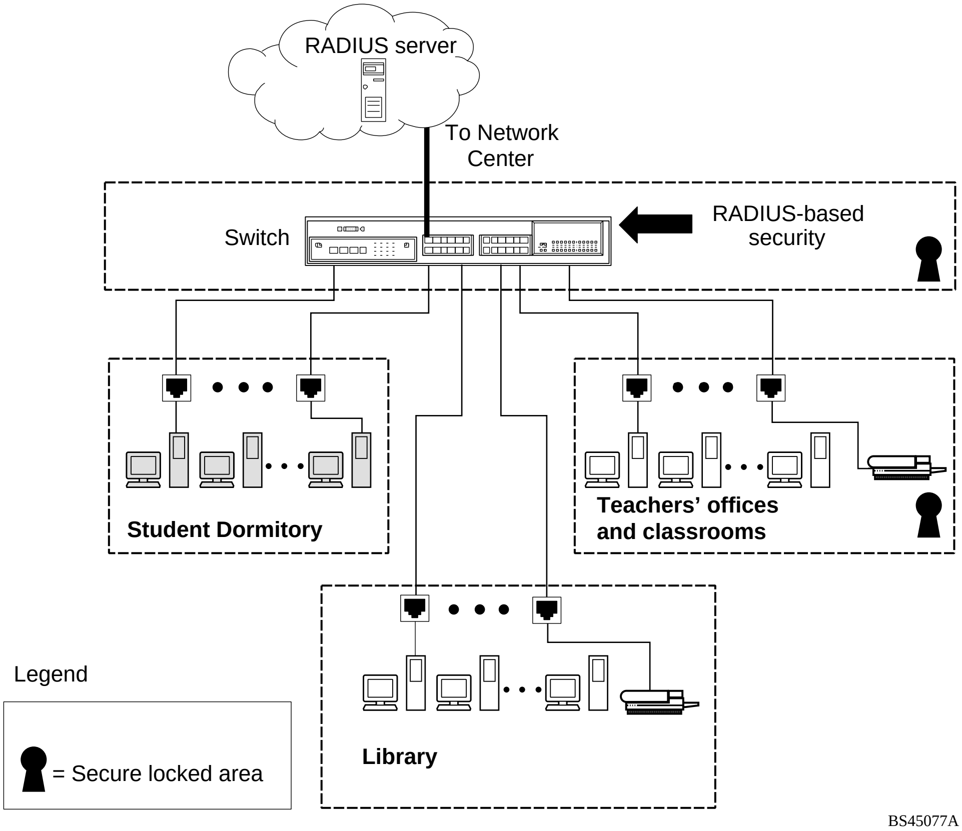
Security

The Business Policy Switch security features provide three levels of security for your local area network (LAN):

- RADIUS-based security—limits administrative access to the switch through user authentication
- MAC address-based security— limits access to the switch based on allowed source MAC addresses (and allowed destination MAC addresses, beginning with software version 2.0)
- EAPOL-based security—allows the exchange of authentication information between any end station or server connected to the switch and authentication server (such as a RADIUS server)

Figure 7 shows a typical campus configuration using the RADIUS-based and MAC address-based security features for the Business Policy Switch. This example assumes that the switch, the teachers' offices and classrooms, and the library are physically secured. The student dormitory may (or may not be) physically secure.

Figure 7 Business Policy Switch 2000 security feature



In this configuration example, the following security measures are implemented:

- The switch
  - — RADIUS-based security is used to limit administrative access to the switch through user authentication (see "RADIUS-based network security" on page 80).

  - MAC address-based security is used to allow up to 448 authorized stations (MAC addresses) access to one or more switch ports (see "MAC address-based security" on page 81).
  - The switch is located in a locked closet, accessible only by authorized Technical Services personnel.

- Student dormitory

  Dormitory rooms are typically occupied by two students and have been prewired with two RJ-45 jacks. Only students who are authorized (as specified by the MAC address-based security feature) can access the switch on the secured ports.

- Teachers' offices and classrooms

  The PCs that are located in the teachers' offices and in the classrooms are assigned MAC address-based security that is specific for each classroom and office location. The security feature logically locks each wall jack to the specified station and prevents unauthorized access to the switch should someone attempt to connect a personal laptop PC into the wall jack. The printer is assigned as a single station and is allowed full bandwidth on that switch port.

  It is assumed that all PCs are password protected and that the classrooms and offices are physically secured.

- Library

  The wall jacks in the library are set up so that the PCs can be connected to any wall jack in the room. This arrangement allows the PCs to be moved anywhere in the room. The exception is the printer, which is assigned as a single station with full bandwidth to that port.

  It is assumed that all PCs are password protected and that access to the library is physically secured.

RADIUS-based network security

The RADIUS-based security feature allows you to set up network access control, using the Remote Authentication Dial-In User Services (RADIUS) security protocol. The RADIUS-based security feature uses the RADIUS protocol to authenticate local console and Telnet logins.

You will need to set up specific user accounts (user names and passwords, and Service-Type attributes) on your RADIUS server before the authentication process can be initiated. To provide each user with appropriate levels of access to the switch, set the following username attributes on your RADIUS server:

- Read-write access—Set the Service-Type field value to Administrative.
- Read-only access—Set the Service-Type field value to NAS-Prompt.

For detailed instructions to set up your RADIUS server, refer to your RADIUS server documentation.

MAC address-based security

The MAC address-based security feature allows you to set up network access control, based on source MAC addresses of authorized stations.

You can:

- Create a list of up to 10 MAC destination addresses (DAs) that you want to filter. All packets with the specified DAs are dropped. The packet with the specified MAC DA will be dropped regardless of the ingress port, source address (SA) intrusion, or VLAN membership.

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

Note: Ensure that you do not enter the MAC address for the stack or any of the units you are using.

- Create a list of up to 448 MAC source addresses (SAs) and specify which SAs are authorized to connect to your switch or stack configuration. The 448 MAC SAs can be configured within a single standalone switch, or they can be distributed in any order among the units in a single stack configuration.
  - Specify which of your switch ports each MAC SA is allowed to access.

    The options for allowed port access include: NONE, ALL, and single or multiple ports that are specified in a list, for example, 1/1-4,1/6,2/9.

— Specify optional actions to be exercised by your switch if the software detects an SA security violation.

  The response can be to send a trap, turn on destination address (DA) filtering for the specified SAs, disable the specific port, or any combination of these three options.

The MAC address-based security feature is based on Nortel Networks BaySecure LAN Access for Ethernet, a real-time security system that safeguards Ethernet networks from unauthorized surveillance and intrusion.

With software version 2.0, you can configure the BPS 2000 to drop all packets with specified MAC destination addresses (DA). You can enter up to 10 specific MAC DAs you want filtered.

For instructions on configuring the MAC address-based security feature, refer to Chapter 3, *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*, *Reference for the Business Policy Switch 2000 Management Software Version 2.5*, and *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5*.

➡ **Note:** You must use either the CLI or the Web-based management system to configure MAC DA filtering.

EAPOL-based security

BPS 2000 software version 1.1 provides support for security based on the Extensible Authentication Protocol over LAN (EAPOL), which uses the EAP as described in the IEEE Draft P802.1X to allow you to set up network access control on internal LANs.

For information on configuring EAPOL-based security using the Console Interface (CI) menus, refer to Chapter 3. To configure this feature using the Web-based management system, refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*. To use Device Manager (DM) to configure EAPOL-based security, refer to *Reference for the Business Policy Switch 2000 Management Software Version 2.5***.** And, to configure this feature using CLI commands, refer to *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5*. book.

EAP allows the exchange of authentication information between any end station or server connected to the switch and an authentication server (such as a RADIUS server). The EAPOL-based security feature operates in conjunction with a RADIUS-based server to extend the benefits of remote authentication to internal LAN clients.

The following example illustrates how the BPS 2000, configured with the EAPOL-based security feature, reacts to a new network connection:

- The switch detects a new connection on one of its ports.
  - — The switch requests a user ID from the new client.
  - — EAPOL encapsulates the user ID and forwards it to the RADIUS server.
  - — The RADIUS server responds with a request for the user’s password.
- The new client forwards an encrypted password to the switch, within the EAPOL packet.
  - — The switch relays the EAPOL packet to the RADIUS server.
  - — If the RADIUS server validates the password, the new client is allowed access to the switch and the network.

Some components and terms used with EAPOL-based security are:

- Supplicant—the device applying for access to the network.
- Authenticator—software with the sole purpose of authorizing a supplicant that is attached to the other end of a LAN segment.
- Authentication Server—a RADIUS server that provides authorization services to the Authenticator.
- Port Access Entity (PAE)—a software entity associated with each port that supports the Authenticator or Supplicant functionality. In the preceding example, the Authenticator PAE resides on the switch.
- Controlled Port—any switch port with EAPOL-based security enabled.

The Authenticator communicates with the Supplicant using an encapsulation mechanism known as EAP over LANs (EAPOL).

The Authenticator PAE encapsulates the EAP message into a RADIUS packet before sending the packet to the Authentication Server. The Authenticator facilitates the authentication exchanges that occur between the Supplicant and the Authentication Server by encapsulating the EAP message to make it suitable for the packet's destination.

The Authenticator determines the controlled port's operational state. After the RADIUS server notifies the Authenticator PAE about the success or failure of the authentication, it changes the controlled port's operational state accordingly.

The Authenticator PAE functionality is implemented for each controlled port on the switch. At system initialization, or when a supplicant is initially connected to the switch's controlled port, the controlled port's state is set to Blocking. During that time, EAP packets are processed by the authenticator.

When the Authentication server returns a "success" or "failure" message, the controlled port's state is changed accordingly. If the authorization is successful, the controlled port's operational state is set to Forwarding. Otherwise, the controlled port's state depends on the Operational Traffic Control field value in the EAPOL Security Configuration screen.

The Operational Traffic Control field can have one of the following two values:

- Incoming and Outgoing—If the controlled port is unauthorized, frames are not transmitted through the port; all frames received on the controlled port are discarded. The controlled port's state is set to Blocking.
- Incoming—If the controlled port is unauthorized, frames received on the port are discarded, but the transmit frames are forwarded through the port.

EAPOL dynamic VLAN assignment

If EAPOL-based security is enabled on a port, and then the port is authorized, the EAPOL feature dynamically changes the port's VLAN configuration according to preconfigured values, and assigns a new VLAN. The new VLAN configuration values are applied according to previously stored parameters (based on the user_id) in the Authentication server.

The following VLAN configuration values are affected:

- Port membership

- PVID
- Port priority

When the EAPOL-based security is disabled on a port that was previously authorized, the port's VLAN configuration values are restored directly from the switch's non-volatile random access memory (NVRAM).

The following exceptions apply to dynamic VLAN assignments:

- The dynamic VLAN configuration values assigned by EAPOL are **not** stored in the switch's NVRAM.
- You can override the dynamic VLAN configuration values assigned by EAPOL; however, be aware that the values you configure are not stored in NVRAM.
- When EAPOL is enabled on a port, and you configure values other than VLAN configuration values, those values are applied and stored in NVRAM.

You set up your Authentication server (RADIUS server) for EAPOL dynamic VLAN assignments. The Authentication server allows you to configure user-specific settings for VLAN memberships and port priority.

When you log on to a system that has been configured for EAPOL authentication, the Authentication server recognizes your user ID and notifies the switch to assign preconfigured (user-specific) VLAN membership and port priorities to the switch. The configuration settings are based on configuration parameters that were customized for your user ID and previously stored on the Authentication server.

To set up the Authentication server, set the following "Return List" attributes for all user configurations (refer to your Authentication server documentation):

- VLAN membership attributes
  - — Tunnel-Type: value 13, Tunnel-Type-VLAN
  - — Tunnel-Medium-Type: value 6, Tunnel-Medium-Type-802
  - — Tunnel-Private-Group-Id: ASCII value 1 to 4094 (this value is used to identify the specified VLAN)
- Port priority (vendor-specific) attributes
  - — Vendor Id: value 562, Nortel Networks vendor Id
  - — Attribute Number: value 1, Port Priority

  - Attribute Value: value 0 (zero) to 7 (this value is used to indicate the port priority value assigned to the specified user)

System requirements

The following are minimum system requirements for the EAPOL-based security feature:

- At least one of the following supported switches:
  - BayStack 350/410-24T/450 switch (software version V4.0, or later)
  - Business Policy Switch 2000 (software version V1.1, or later)
- RADIUS server (Microsoft Windows XP Server)
- Client software that supports EAPOL (Microsoft Windows XP Client)

You must specify the Microsoft 2001 IAS server (or any generic RADIUS server that supports EAP) as the primary RADIUS server for these devices.

You must also configure your BayStack 350/410-24T/450 switches and BPS 2000 for port-based VLANs and EAPOL security. (For information on configuring the BPS 2000, refer to the Chapter 3, *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*, *Reference for the Business Policy Switch 2000 Management Software Version 2.5*, and *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5.* For information on configuring the BayStack switches, go to www.nortelnetworks.com/documentation on the Web, and find the switch. Scroll down to the documentation you need.)

EAPOL-based security configuration rules

The following configuration rules apply to your BPS 2000 when using EAPOL-based security:

- Before configuring your switch, you must configure the Primary RADIUS Server and Shared Secret fields.
- You cannot configure EAPOL-based security on ports that are currently configured for:
  - Shared segments
  - MultiLink Trunking

- MAC address-based security
- IGMP (Static Router Ports)
- Port mirroring

- You can connect only a single client on each port that is configured for EAPOL-based security. (If you attempt to add additional ports to a port, that port goes to Blocking mode.)

EAPOL-based security uses the RADIUS protocol to authenticate local console, Telnet, and EAPOL-authorized logins. Refer to "RADIUS-based network security" on page 80 for more information on using the RADIUS protocol.

Secure Shell

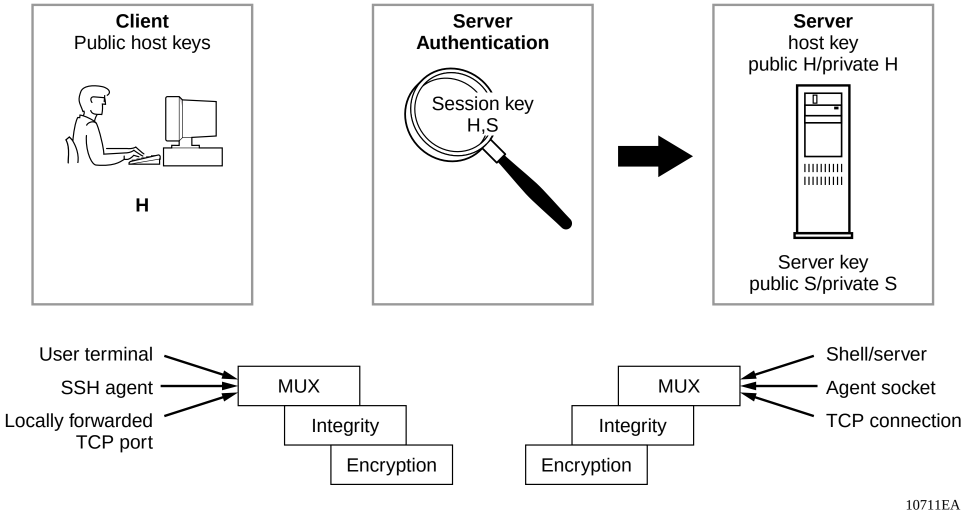
Note: Due to export restrictions on encryption software, the default BPS 2000 version 2.5 software image does not include SSH functionality. Refer to the release notes accompanying your software release for the latest information on how to download the SSH-enabled image. The SSH server is not available without the use of this image.

Secure Shell (SSH) is a client/server protocol that specifies the way to conduct secure communications over a network. When using other methods of remote access, such as telnet or ftp, the traffic generated by these utilities is not encrypted. Anyone that can see the network traffic can see all data, including passwords and user names. SSH can replace telnet, ftp and other remote logon utilities with an encrypted alternative.

In addition to standard username/password authentication, SSH supports a variety of the many different public/private key encryption schemes available. Using the public key of the host server, the client and server negotiate to generate a session key known only to the client and the server. This one-time key is then used to encrypt all traffic between the client and the server.

Figure 8 gives an overview of the SSH protocol.

Figure 8 Overview of the SSH protocol



Using a combination of host, server, and session keys, the SSH protocol can provide strong authentication and secure communication over an unsecure network, offering protection from the following security risks:

- IP Spoofing
- IP source routing
- DNS spoofing
- Man-in-the-middle/TCP hijacking attacks
- Eavesdropping/Password sniffing

Even if network security is compromised, traffic cannot be played back or decrypted, and the connection cannot be hijacked.

The secure channel of communication provided by SSH does not provide protection against break-in attempts or denial-of-service (DoS) attacks.

The SSH protocol supports the following security features:

— Authentication. This determines in a reliable way to identity the SSH client. During the login process the SSH client is queried for a digital proof of identity.

  Supported authentications are DSA and passwords.

  — Encryption. The SSH server uses encryption algorithms to scramble data and rendered it unintelligible except to the receiver.

  Supported encryption is 3DES only.

  — Integrity. This guarantees that the data is transmitted from the sender to the receiver without any alteration. If any third party captures and modifies the traffic, the SSH server will detect this alteration.

The implementation of the SSH server in the BPS 2000 enables the SSH client to make a secure connection to a BPS 2000 and will work with commercially available SSH clients.

SSH version 2 (SSH-2)

SSH protocol, version 2 (SSH-2) is a complete rewrite of the SSH-1 protocol. While SSH-1 contains multiple functions in a single protocol, in SSH-2 the functions are divided among three layers:

- SSH Transport Layer (SSH-TRANS)

  The SSH transport layer manages the server authentication and provides the initial connection between the client and the server. Once established, the transport layer provides a secure, full-duplex connection between the client and server.

- SSH Authentication Protocol (SSH-AUTH)

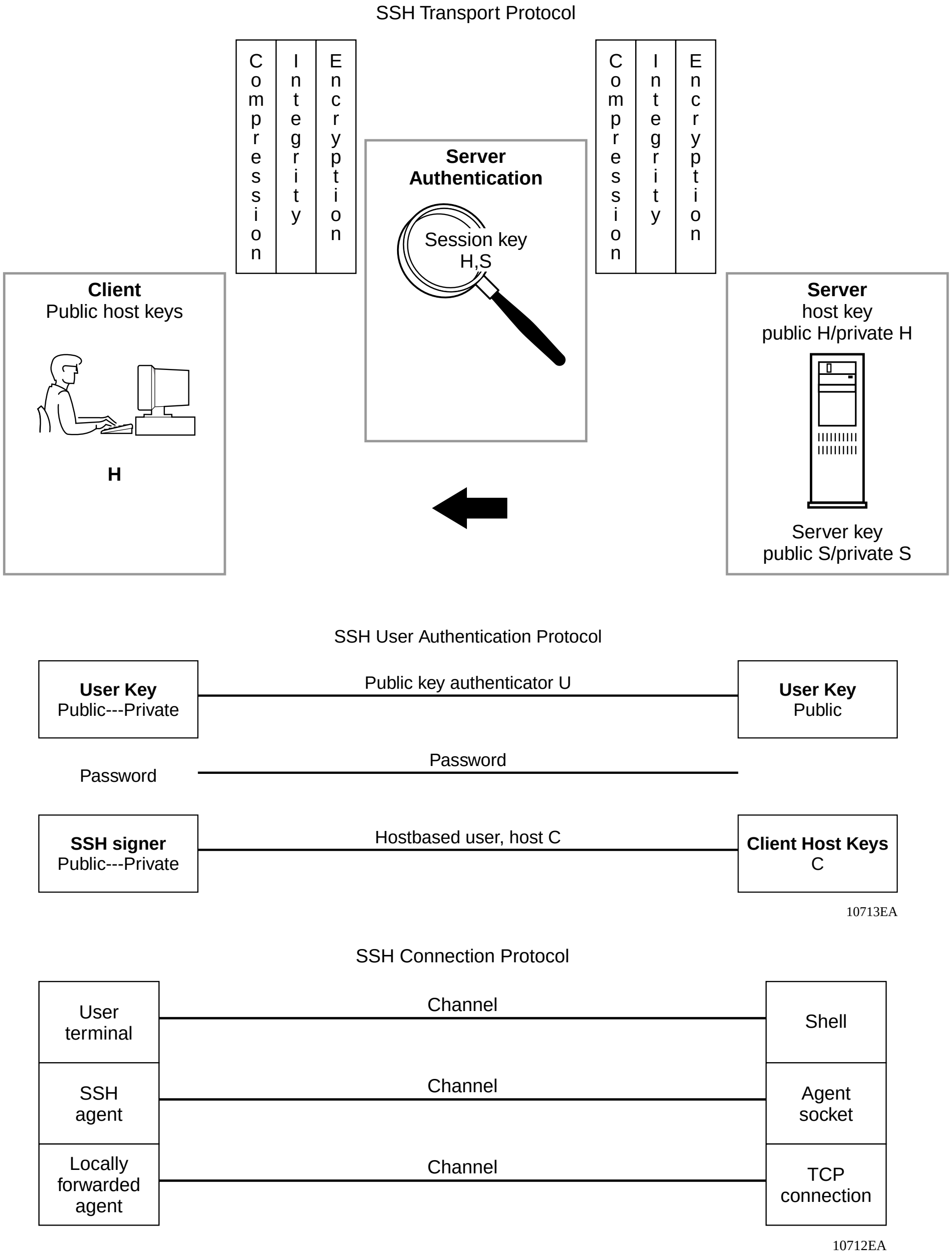
  The SSH authentication protocol runs on top of the SSH transport layer and authenticates the client-side user to the server. SSH-AUTH defines three authentication methods; public key, hostbased, and password. SSH-AUTH provides a single authenticated tunnel for the SSH connection protocol.

- SSH Connection Protocol (SSH-CONN)

  The SSH connection protocol runs on top of the SSH transport layer and user authentication protocols. SSH-CONN provides interactive login sessions, remote execution of commands, forwarded TCP/IP connections, and forwarded X11 connections. These richer services are multiplexed into the single encrypted tunnel provided by the SSH transport layer.

Figure 9 shows the three layers of the SSH-2 protocol.

Figure 9 Separate SSH version 2 protocols



The modular approach of SSH-2 improves on the security, performance, and portability of the SSH-1 protocol.

➡ **Note:** The SSH-1 and SSH-2 protocols are not compatible. The SSH implementation in the BPS 2000 only supports the more secure version, the SSH-2 protocol. Ensure that your SSH client supports the SSH-2 protocol.

Establishing a secure SSH connection

To establish a secure SSH connection to the Business Policy Switch 2000:

1 Configure and enable the SSH service on the switch.

To configure this feature, refer to *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5*. To use Device Manager (DM) to configure this feature, refer to *Reference for the Business Policy Switch 2000 Management Software Version 2.5*.

➡ **Note:** You must use the CLI to initially configure SSH. You can use Device Manager (DM) to change the SSH configuration parameters. However, Nortel Networks recommends using the CLI.

By default, the SSH service when enabled will listen for connections on port 22. It will allow up to 2 simultaneous SSH connections. In the default configuration, sessions can be authenticated by either password or public key authentication.

2 Connect to the switch using your SSH client.

Refer to the documentation that came with your selected SSH client for information on initiating a secure SSH connection to the switch.

a To connect to the switch using password authentication:

-- Enter either the Console Read-Only switch password (default is *user*) or the Console Read-Write switch password (default is *secure*) when asked to enter the password.

When using password authentication, the user name is not required.

Note: Using the Console Read-Only or Console Read-Write password does not set read-only or read-write privileges. Either password will work to establish a secure SSH connection to the device.

b To connect to the switch using DSA public key authentication:

-- Generate a DSA key pair (public and private keys) using your SSH client or key-gen tool and export your public key.

Refer to the documentation that came with your selected SSH client or key-gen tool for information on generating a DSA key pair and exporting the public key.

-- Download the DSA public key file to the switch via your TFTP server.

To download the public key file, refer to *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5*. To use Device Manager (DM) to download the key, refer to *Reference for the Business Policy Switch 2000 Management Software Version 2.5.*

-- Connect to the switch using DSA public key authentication.

Please refer to the documentation that came with your SSH client for information on establishing a secure SSH connection using DSA public key authentication.

Flash memory storage

Switch software image storage

The Business Policy Switch uses flash memory to store the switch software image. The flash memory allows you to update the software image with a newer version without changing the switch hardware (see Chapter 3). An in-band connection between the switch and the TFTP load host is required to download the software image.

Configuration parameters storage

All configuration parameters are stored in flash memory. These parameters are updated every 60 seconds (if a change occurs) or whenever a reset command is executed.

➡ **Note:** Do not power off the switch within 60 seconds of changing any configuration parameters. Powering down the switch within 60 seconds of changing configuration parameters can cause the changed configuration parameters to be lost.

MultiLink Trunking

➡ **Note:** For information on configuring VLANs, STGs, and MLTs, refer to "STG configuration guidelines" on page 62.

The MultiLink Trunking feature allows you to group multiple ports, two to four together, when forming a link to another switch or server, thus increasing aggregate throughput of the interconnection between two devices, up to 800 Mb/s in full-duplex mode. The Business Policy Switch can be configured with up to six MultiLink Trunks. The trunk members can be configured within a single unit in the stack or distributed between any of the units within the stack configuration (distributed trunking).

For more information about the MultiLink Trunking feature, refer to Chapter 2, "Network configuration."

For information on configuring MultiLink Trunks using the CI menus, refer to Chapter 3. To configure this feature using the Web-based management system, refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*. To use Device Manager (DM) to configure this feature, refer to *Reference for the Business Policy Switch 2000 Management Software Version 2.5***.** And, to configure this feature using CLI commands, refer to *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5*. book.

Port mirroring (conversation steering)

The port mirroring feature (sometimes referred to as *conversation steering*) allows you to designate a single switch port as a traffic monitor for up to two specified ports or two media access control (MAC) addresses. You can specify *port-based* monitoring, where all traffic on specified ports is monitored, or *address-based* monitoring, where traffic between specified MAC addresses is monitored. You can attach a probe device (such as a Nortel Networks StackProbe, or equivalent) to the designated monitor port

For more information about the port mirroring feature, refer to Chapter 2, "Network configuration."

Note: Use the CI menus, the CLI, or the Web-based management system to configure port mirroring.

For information on configuring port mirroring using the CI menus, refer to Chapter 3. To configure this feature using the Web-based management system, refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*. And, to configure this feature using CLI commands, refer to *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5* book.

Autosensing and autonegotiation

The Business Policy Switches are autosensing and autonegotiating devices:

- The term *autosense* refers to a port's ability to *sense* the speed of an attached device.
- The term *autonegotiation* refers to a standardized protocol (IEEE 802.3u) that exists between two IEEE 802.3u-capable devices. Autonegotiation allows the switch to select the best of both speed and duplex modes.

Autosensing is used when the attached device is not capable of autonegotiation or is using a form of autonegotiation that is not compatible with the IEEE 802.3u autonegotiation standard. In this case, because it is not possible to sense the duplex mode of the attached device, the Business Policy Switch reverts to half-duplex mode.

When autonegotiation-capable devices are attached to the Business Policy Switch, the ports negotiate down from 100 Mb/s speed and full-duplex mode until the attached device acknowledges a supported speed and duplex mode.

For more information about autosensing and autonegotiation modes, see Chapter 6, “Troubleshooting,” on page 361.

For information on configuring autonegoitation using the CI menus, refer to Chapter 3. To configure this feature using the Web-based management system, refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*. To use Device Manager (DM) to configure this feature, refer to *Reference for the Business Policy Switch 2000 Management Software Version 2.5*. And, to configure this feature using CLI commands, refer to *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5* book.

BootP automatic IP configuration/MAC address

Beginning with software version 1.2, you can retrieve the ASCII configuration file name and configuration server address using BootP.

With software 1.1 and a stack consisting *only* of BPS 2000 switches (Pure BPS 2000 Stack mode), you can perform BootP using the MAC address of the base unit.

The Business Policy Switch has a unique 48-bit hardware address, or MAC address, that is printed on a label on the back panel. You use this MAC address when you configure the network BootP server to recognize the Business Policy Switch BootP requests. A properly configured BootP server enables the switch to automatically learn its assigned IP address, subnet mask and the IP address of the default router (default gateway).

For information on a stack MAC address, see Chapter 2.

For more information and an example of a BootP configuration file, see Appendixes.

Configuration and switch management

The Business Policy Switch is shipped directly from the factory ready to operate in any 10BASE-T or 100BASE-TX standard network.

You must assign an IP address to the switch or stack, depending on the mode of operation. You can set both addresses by using the console port or BootP, which resides on the switch. You can manage the switch using:

- Console interface

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

  For information about the console interface, refer to Chapter 3.

- Web-based management

  You can manage the network from the World Wide Web. Access the Web-based graphical user interface (GUI) through the HTML-based browser located on your network. The GUI allows you to configure, monitor, and maintain your network through Web browsers. You can also download software using the Web.

  For information about Web-based management, refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*.

- Java-based Device Manager

  Device Manager is a Java-based set of graphical network management applications used to configure and manage a Business Policy Switch.

  Refer to *Reference for the Business Policy Switch 2000 Management Software Operations Software Version 2.5* for more information.

- Command Line Interface (CLI)—software version 1.2

With software version 1.2 and higher, the CLI is used to automate general management and configuration of the BPS 2000. Use the CLI through a Telnet connection or through the serial port on the console.

Refer to *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5* for complete information on using the CLI.

- Any generic SNMP-based network management software.

  You can use any generic SNMP-based network management software to configure and manage a Business Policy Switch.

- Nortel Networks Preside* Network Configuration System

  Allows you to configure the BayStack and Business Policy switches with a single system.

Multifield packet classification

Specify multifield packet classification based on header fields of data link, network, and transport layer protocols as you configure your policy criteria. Filters are populated with information needed to classify packets and determine the set of actions that need to be applied to classified packets.

See Chapter 4, “Policy-enabled networks” for more information.

SNMP MIB support

The Business Policy Switch supports an SNMP agent with industry-standard MIBs, as well as private MIB extensions, which ensures compatibility with existing network management tools. The switch supports the MIB-II (RFC 1213), Bridge MIB (RFC 1493), and the RMON MIB (RFC 1757), which provide access to detailed management statistics. With SNMP management, you can configure SNMP traps (on individual ports) to generate automatically for conditions such as an unauthorized access attempt or changes in a port’s operating status. Table 5 lists supported SNMP MIBs.

Table 5 SNMP MIB support

Application	Standard MIBs	Proprietary MIBs
S5 Chassis MIB		s5cha127.mib
S5 Agent MIB		s5age140.mib

Table 5 SNMP MIB support (continued)

Application	Standard MIBs	Proprietary MIBs
RMON	rfc2819.mib	
MLT		rcMLT
Common Open Policy Service (COPS) support	rfc.2940.mib	
Policy Management	Policy Info Base	pib802, pibFramework, pibIp, pibNtn, mibntqos, pibNtnEvol
SNMPv3 MIBs	RFCs 2570, 2571, 2572, 2573, 2574, 2575, 2576	
MIB2	rfc1213.mib	
IF-MIB	rfc2863.mib	
Etherlike MIB	rfc2665.mib	
Interface Extension MIB		s5ifx100.mib
Switch Bay Secure		s5sbs102.mib
IP Multicast (IGMP Snooping/ Proxy)		rcVlanIgmp
System Log MIB		bnlog.mib
S5 Autotopology MIB		s5emt104.mib
VLAN		rcVlan
Entity MIB	RFC 2737	
Spanning Tree	RFC1493 Bridge MIB	

SNMP trap support

The Business Policy Switch supports an SNMP agent with industry-standard SNMPv1 traps, as well as private SNMPv1 trap extensions (Table 6).

Table 6 Supported SNMP traps

Trap name	Configurable	Sent when
RFC 1215 (industry standard):		
linkUp	Per port	A port’s link state changes to up.
linkDown	Per port	A port’s link state changes to down.
authenticationFailure	System wide	There is an SNMP authentication failure.

Table 6 Supported SNMP traps (continued)

Trap name	Configurable	Sent when
coldStart	Always on	The system is powered on.
warmStart	Always on	The system restarts due to a management reset.
s5CtrMIB (Nortel proprietary traps):		
s5CtrUnitUp	Always on	A unit is added to an operational stack.
s5CtrUnitDown	Always on	A unit is removed from an operational stack.
s5CtrHotSwap	Always on	A unit is hot-swapped in an operational stack.
s5CtrProblem	Always on	An assigned base unit fails.
s5EtrSbsMacAccessViolation	Always on	A MAC address violation is detected.

For information on configuring SNMP using the CI menus, refer to Chapter 3, *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*, *Reference for the Business Policy Switch 2000, Command Line Interface Software Version 2.5*, and *Reference for the Business Policy Switch 2000 Management Software Version 2.5*.

Supported standards and RFCs

This section lists the standards and RFCs supported by the BPS 2000.

Standards

The following IEEE Standards contain information germane to the Business Policy Switch 2000:

- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.3 (Ethernet)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1p (Prioritizing)

RFCs

For more information about networking concepts, protocols, and topologies, consult the following RFCs:

- RFC 1213 (MIB-II)
- RFC 1493 (Bridge MIB)
- RFC 2863 (Interfaces Group MIB)
- RFC 2665 (Ethernet MIB)
- RFC 2737 (Entity MIBv2)
- RFC 2819 (RMON MIB)
- RFC 1757 (RMON)
- RFC 1271 (RMON)
- RFC 1157 (SNMP)
- RFC 2748 (COPS)
- RFC 2940 (COPS Clients)
- RFC 3084 (COPS Provisioning)
- RFC 2570 (SNMPv3)
- RFC 2571 (SNMP Frameworks)
- RFC 2573 (SNMPv3 Applications)
- RFC 2574 (SNMPv3 USM)
- RFC 2575 (SNMPv3 VACM)
- RFC 2572 (SNMP Message Processing)

Chapter 2
Network configuration

Use Business Policy Switches to connect workstations, personal computers (PCs), and servers to each other by connecting these devices directly to the switch, through a shared media hub connected to the switch or by creating a virtual LAN (VLAN) through the switch.

This chapter contains the following important information on configuring networks:

- "Compatibility with BayStack 450 switches," next
- "Network configuration examples" on page 102
- "Business Policy Switch stack operation" on page 107
- "IEEE 802.1Q VLAN workgroups" on page 118
- "IGMP snooping" on page 137
- "MultiLink Trunks" on page 144
- "Port mirroring" on page 154

Compatibility with BayStack 450 switches

The BPS 2000 software version 2.5 is compatible with BayStack 450 software version 4.1 and 4.2.

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

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

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

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

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

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

Network configuration examples

This section provides four network configuration examples using Business Policy Switches. In these examples, the packet classification feature can be used to prioritize the traffic of the network to ensure uninterrupted traffic of critical applications.

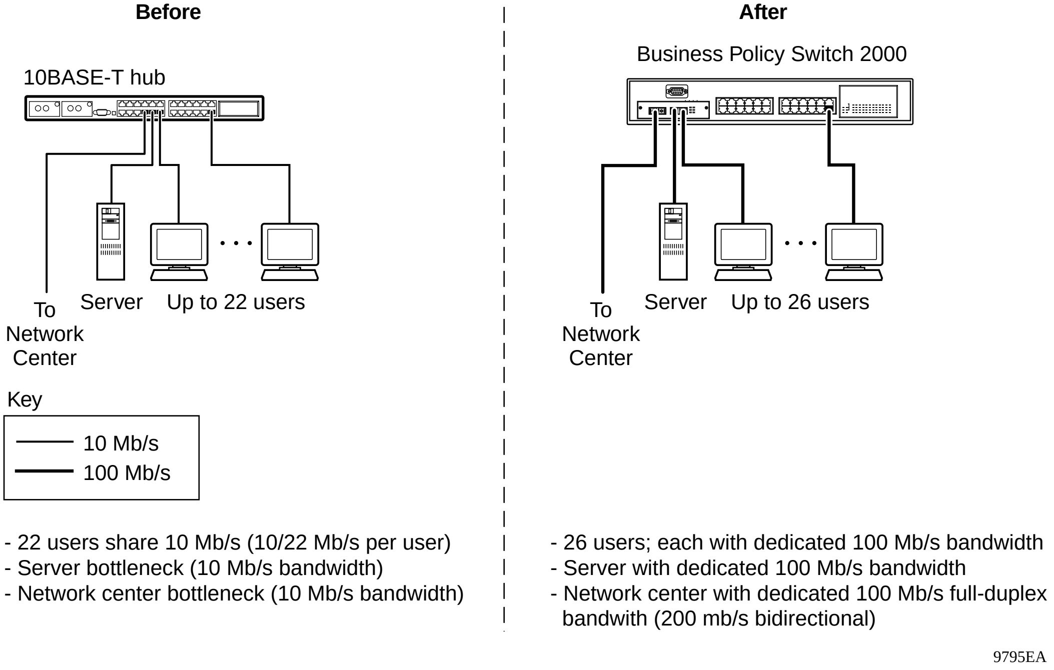
- Desktop switch application (this page)
- Segment switch application (page 103)
- High-density switched workgroup application (page 105)
- Fail-safe stack application (page 106)

Desktop switch application

Figure 10 shows a Business Policy Switch used as a desktop switch, where desktop workstations are connected directly to switch ports.

This configuration provides dedicated 100 Mb/s connections to the network center, the server, and as many as 26 users. This configuration uses the optional BPS2000-4TX MDA (10BASE-T/100BASE-TX MDA).

Figure 10 Business Policy Switch used as a desktop switch



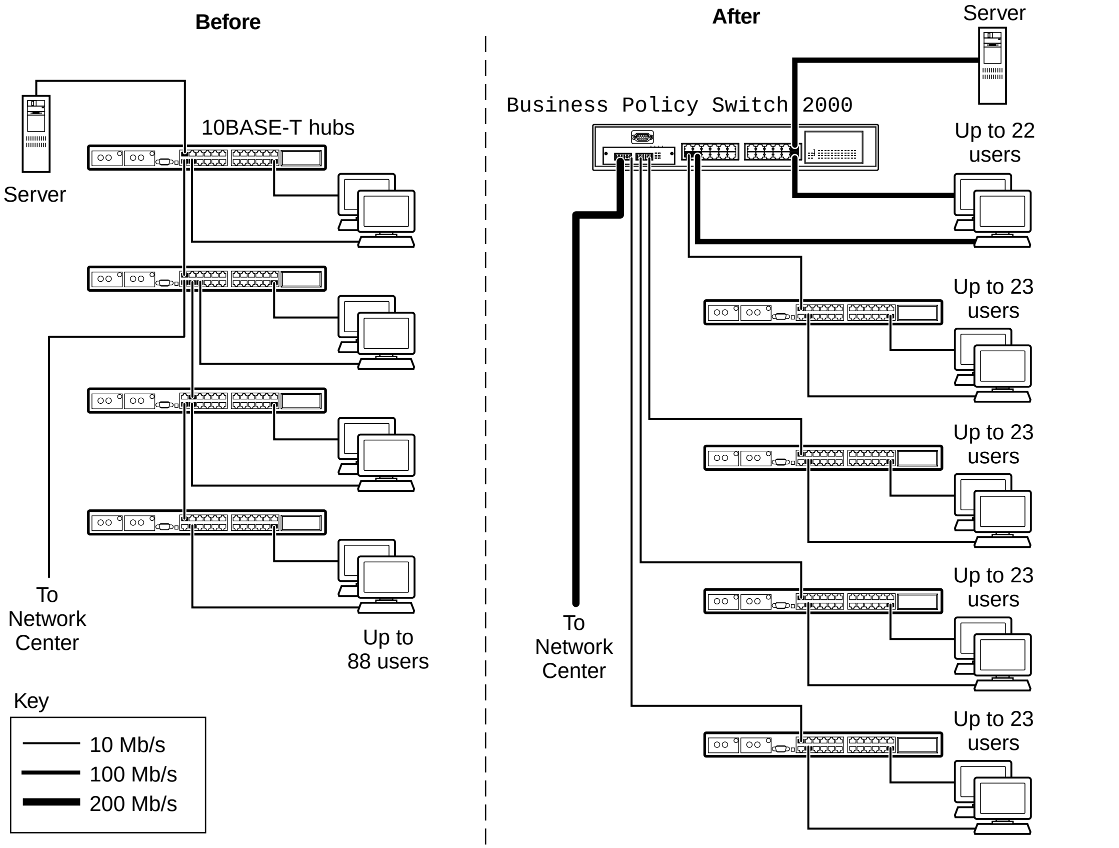
- 22 users share 10 Mb/s (10/22 Mb/s per user)
- Server bottleneck (10 Mb/s bandwidth)
- Network center bottleneck (10 Mb/s bandwidth)

- 26 users; each with dedicated 100 Mb/s bandwidth
- Server with dedicated 100 Mb/s bandwidth
- Network center with dedicated 100 Mb/s full-duplex bandwith (200 mb/s bidirectional)

Segment switch application

Figure 11 shows a Business Policy Switch used as a segment switch to alleviate user contention for bandwidth and eliminate server and network bottlenecks. Before segmentation, 88 users had a total bandwidth of only 10 Mb/s available. After segmentation, 92 users have 40 Mb/s, four times the previous bandwidth, while adding 22 dedicated 100 Mb/s connections. This configuration can be extended to add more segments without degrading performance.

Figure 11 Business Policy Switch used as a segment switch



- 88 users share 10 Mb/s (10/88 Mb/s per user)
- Server bottleneck (10 Mb/s bandwidth)
- Network center bottleneck (10 Mb/s bandwidth)
- Total of 88 users

- Four sets of 23 users; each set shares 10 Mb/s (10/23 Mb/s per user)
- Addition of 22 users; each with dedicated 100 Mb/s bandwidth
- Server with dedicated 100 Mb/s bandwidth
- Network center with dedicated 100 Mb/s full-duplex bandwidth (200 Mb/s bidirectional)
- Total of 114 users

9796EA

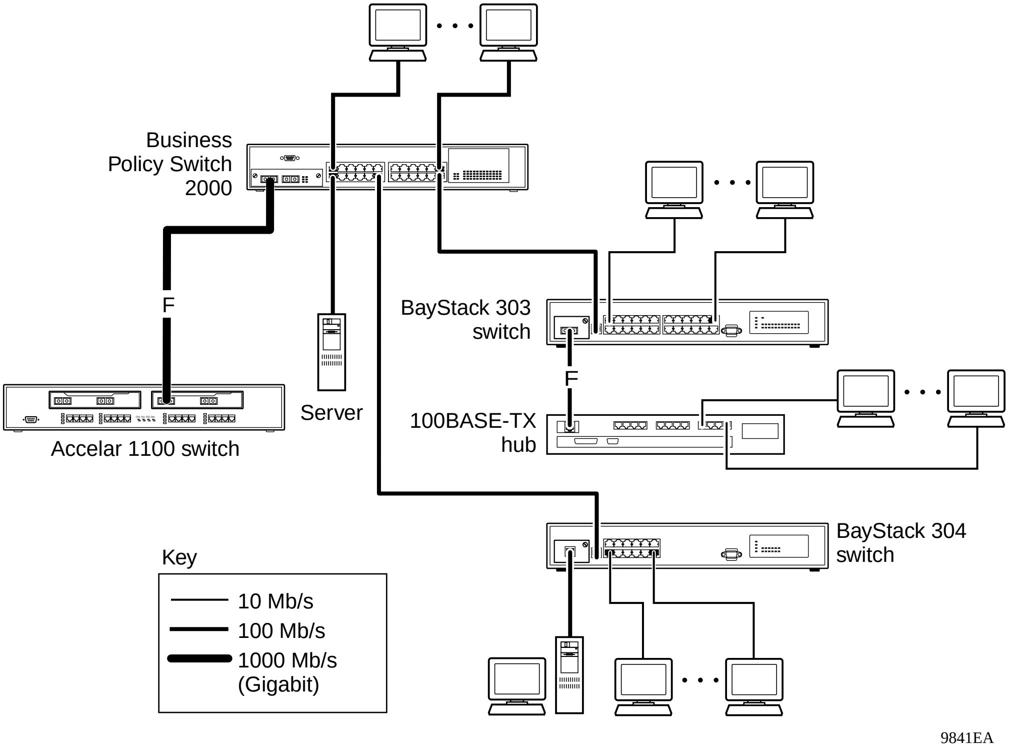
High-density switched workgroup application

Figure 12 shows an example of using a Business Policy Switch with a high-speed (gigabit) connection to a Nortel Networks Passport™ 1100 switch. BayStack 303 and BayStack 304 switches are also shown in this example of a high-density switched workgroup.

As shown in Figure 12, the Passport 1100 switch is used as a backbone switch, connecting to the Business Policy Switch with an optional gigabit (1000BASE-SX) MDA for maximum bandwidth. The BayStack 303 and BayStack 304 switches have 100 Mb/s connections to the Business Policy Switch, a 100BASE-TX hub, and a 100 Mb/s server as well as 10 Mb/s connections to DTE (data terminal equipment).

See the Nortel Networks library Web page www.nortelnetworks.com/documentation for online documentation about the Nortel Networks Passport 1100 switch and the BayStack 303 and BayStack 304 switches.

Figure 12 Configuring power workgroups and a shared media hub



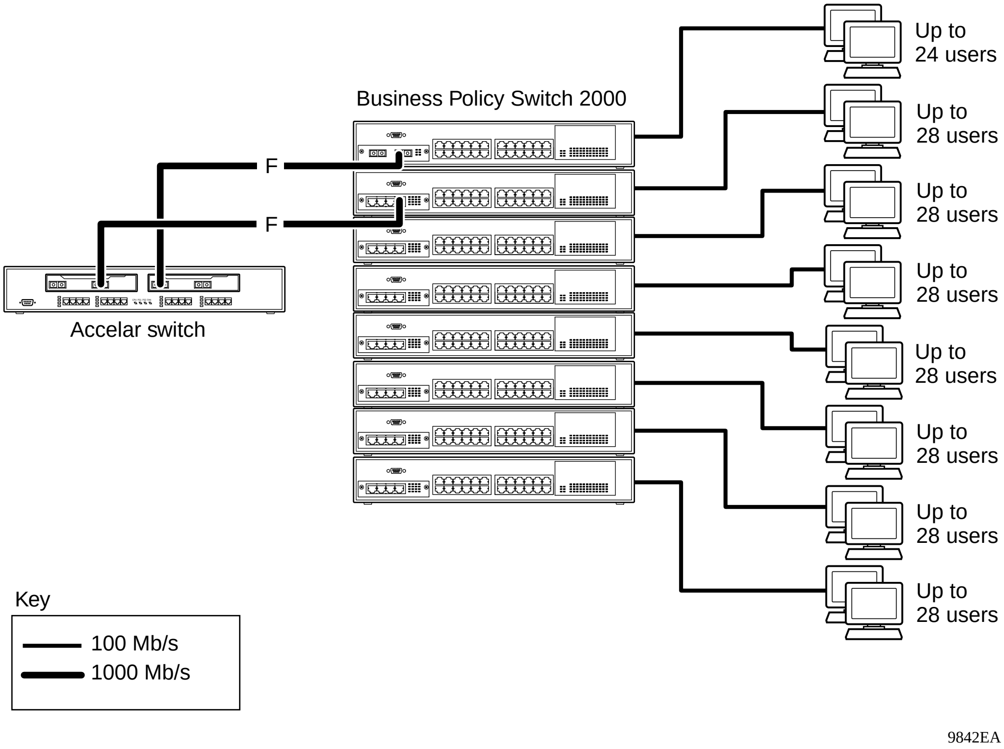
Fail-safe stack application

Figure 13 shows an example of eight Business Policy Switches that are stacked together as a single managed unit. If any single unit in the stack fails, the remaining stack remains operational, without interruption.

As shown in Figure 13, the Passport 1100 switch is used as a backbone switch, connecting to the Business Policy Switch with an optional gigabit (1000BASE-SX) MDA for maximum bandwidth. This configuration uses optional BayStack 400-ST1 Cascade Modules to connect the switches in the fail-safe stack.

For an overview of the fail-safe stacking feature that is available for the Business Policy Switches, see “Business Policy Switch stack operation.”

Figure 13 Fail-safe stack example



Business Policy Switch stack operation

BPS 2000 switches configured with Business Policy Switch software version 1.0 provide fail-safe stackability when you install the optional BayStack 400-ST1 Cascade Module. You can connect up to eight Business Policy Switches and BayStack 450 switches to provide uninterrupted connectivity for up to 224 ports (see “Fail-safe stack application.”). The entire stack is manageable as a single unit. Installation instructions are provided with the BayStack 400-ST1 Cascade Module (see your Nortel Networks sales representative for ordering information).

This section discusses the following stacking topics:

- “BayStack 400-ST1 Cascade Module” on page 108
- “Base unit” on page 110

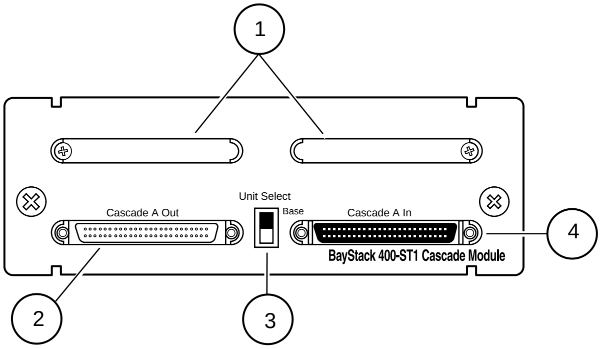
- "Stack configurations" on page 112
- "Redundant cascade stacking feature" on page 116

Note: If you are implementing a mixed stack with the Business Policy Switch and BayStack 450 and BayStack 410 switches, refer to Appendixes for configuration and interoperability information.

BayStack 400-ST1 Cascade Module

The front-panel components of the BayStack 400-ST1 Cascade Module are shown in Figure 14. Component descriptions follow the figure.

Figure 14 BayStack 400-ST1 Cascade Module front-panel components



1 = Blank connectors (unused)
2 = Cascade A Out connector
3 = Unit Select switch
4 = Cascade A In connector

BS0031B

Cascade A Out connector

Provides an attachment point for connecting this unit to another unit via the cascade cable. A *return* cable from another unit's Cascade A Out connector to this unit's Cascade A In connector completes the stack connection (see the example shown in Figure 15).

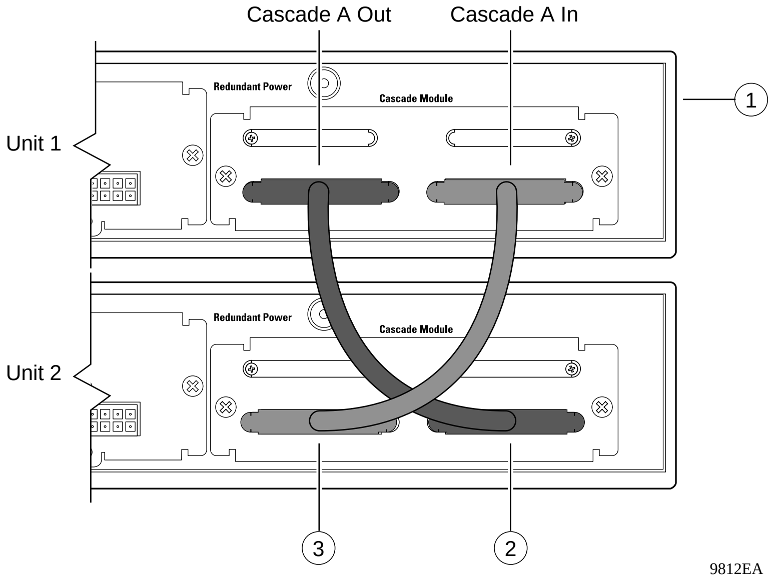
Unit Select switch

The Unit Select switch (up = Base) determines the *base unit* for the stack configuration (see “Base unit”). The Unit Select switch status is displayed on the Business Policy Switch LED display panel. When the Unit Select switch is in the Base (up) position, all other Unit Select switches in the stack configuration must be set to Off (down).

Cascade A In connector

Provides an attachment point for accepting a cascade cable connection from an adjacent unit in the stack. A *return* cable from this unit’s Cascade A Out connector to the adjacent unit’s Cascade A In connector completes the stack connection (see the example shown in Figure 15).

Figure 15 Connecting cascade cables



1	Base unit
2	303978-A cascade cable
3	303978-A cascade cable (used for return)

Base unit

Note: For stacking three or more units (maximum 8 units per stack), order the optional 1 meter (39.27 inch) cascade max-return cable (order number AL2018001).

The base unit is the unique stack unit that you configure with the Unit Select switch on the front panel of the BayStack 400-ST1 Cascade Module. One Business Policy Switch in the stack *must* be configured as the base unit; all other units in the stack *must* have their Unit Select switch set to Off (see "Unit Select switch"). You can assign any single Business Policy Switch as the base unit. If you are configuring a mixed stack, refer to Appendixes for base unit instructions.

The physical ordering of all of the other units in the stack is determined by the position of the base unit within the stack. This is important for management applications that view the physical ordering of the units within the stack.

Some characteristics of the base unit are described in the following sections.

Initial installation

During the *initial installation* of the stack, the software automatically determines the physical order of all units in the stack according to the position of the base unit within the stack. Thereafter, the individual units maintain their original unit numbering, even if you change the position of one or more units in the stack. (Refer to Chapter 3 for information on renumbering the units using the console interface (CI) menus and to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5* for renumbering the units using the Web-based management system).

For example, when you initially power up the stack, the base unit becomes unit 1 and the unit that the base unit connects to (via the Cascade A Out cable) becomes unit 2 (and the next unit is unit 3 and so on), until the maximum stack configuration (up to 8 units) is reached. If you change the base unit to another unit in the stack, the new base unit keeps its original unit number in the stack.

Stack MAC address

When the switch is participating in a stack configuration, a stack MAC address is automatically assigned during the stack initialization. The base unit's MAC address, with a software offset, is used for the stack MAC address.

For example, if the base unit's MAC address is 00-00-82-99-44-00, and the stack software offset is `1F,` then the stack MAC address becomes:

00-00-82-99-44-1F

If another unit in the stack is assigned as the base unit, the MAC address of the *new* base unit (with offset) now applies to the stack configuration. The original stack IP address still applies to the new base unit.

Temporary base unit

If an assigned base unit fails, the next unit in the stack order automatically becomes the new *temporary base unit.* This change is indicated by the base LED on the temporary base unit's LED display panel turning on (amber). For detailed information about the base LED, see Chapter 1.

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.

Note: If you do not reassign the temporary base unit as the new base unit, and 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.

Removing a unit from the stack

If a unit is removed from the stack (therefore operating in standalone mode), the following switch configuration settings revert back to the settings configured before the unit became a member of the stack:

- IP address
- Password: console, Web, Telnet, SNMP (including DM)
- Stack operational mode
- SNMP community strings

Stack configurations

As shown in Figure 16, the cascade connectors and cables on the BayStack 400-ST1 Cascade Module front panel provide the ability to stack up to 8 switches. With BPS-2000 MDAs installed in each switch, the stack can accommodate a maximum of 224 switch ports.

Because stack parameters are associated with the base unit (see “Base unit”), the physical stack order depends on the base unit’s position and whether the stack is configured *stack up* or *stack down*.

Stack up configurations

In Figure 16, data flows from the base unit (unit 1) to the next switch, which is assigned as unit 2, and continues until the last switch in the stack is assigned as unit 8. The physical order of the switches is *from bottom to top* (unit 1 to unit 8).

Figure 16 Stack up configuration example

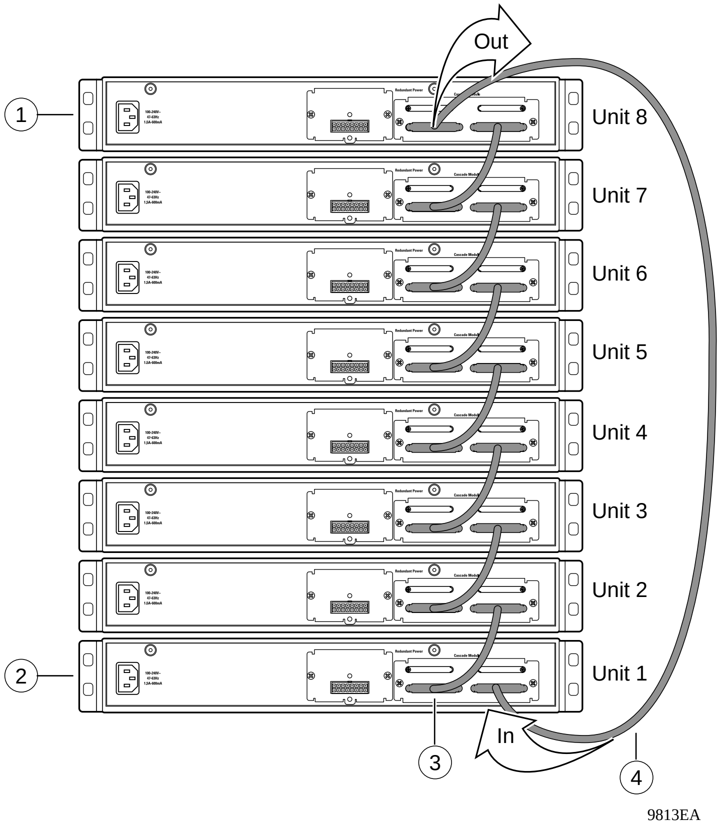


Table 7 describes the stack up configuration illustration references.

Table 7 Stack up configuration description

1	Last unit
2	Base unit
3	Cascade Cable (part number 303978-A)
4	Cascade Cable (part number 303979-A)

Stack down configurations

In Figure 17, data flows from the base unit (unit 1) to the next switch, which is assigned as unit 2, and continues until the last switch in the stack is assigned as unit 8. The physical order of the switches is *from top to bottom* (unit 1 to unit 8).

Figure 17 Stack down configuration example

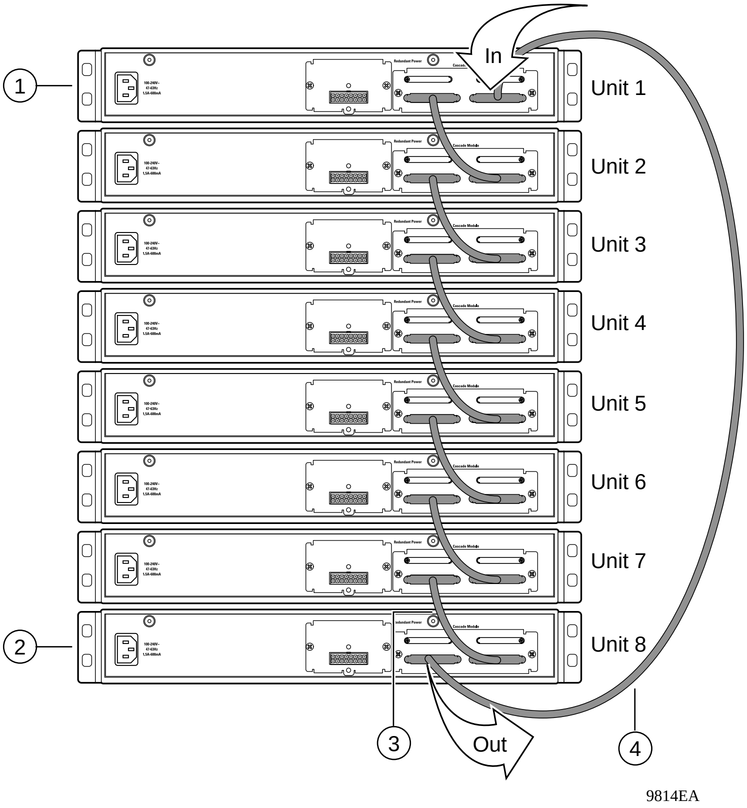


Table 8 describes the stack down configuration illustration references.

Table 8 Stack down configuration description

1	Base unit
2	Last unit
3	Cascade cable (part number 303978-A)
4	Cascade max-return cable (part number 303979-A)

Certain network management station (NMS) applications assume a stack down configuration for the graphical user interface (GUI) that represents the stack (see Figure 17).

➡ **Note:** For this reason, Nortel Networks recommends that you always configure the top unit in the stack as the base unit.

In any stack configuration, the following applies:

- When you apply power to the stack, the base unit initializes and the entire stack powers up as a single logical unit within 45 seconds.
- You can attach an RS-232 communications cable to the console port of any switch in the stack.
- You can downline upgrade the entire stack from any switch in the stack from the console interface, a Telnet session, the Web-based management interface, or any generic SNMP-based network management software.
- You can access and manage the stack using a Telnet connection, the Web-based management interface, or any generic SNMP management tool through any switch port that is part of the stack configuration.
- When stacking three or more switches, use the longer (1-meter) cascade max-return cable (part number 303979-A) to complete the link from the last unit in the stack to the base unit.

Redundant cascade stacking feature

Business Policy Switches allow you to connect up to 8 units into a redundant cascade stack. If any single unit fails or if a cable is accidently disconnected, other units in the stack remain operational, without interruption.

Figure 18 shows an example of how a stack configuration reacts to a failed or powered-down unit in the stack configuration:

1. As shown in Figure 18, unit 3 becomes nonoperational.

   This result can be due to a failed unit or simply because the unit was powered down.

2. Unit 2 and unit 4, directly upstream and downstream from unit 3, sense the loss of link signals from unit 3.

   a. Units 2 and 4 automatically loop their internal stack signals (A and B).

   b. The Cas Up LED for unit 2 and the Cas Dwn LED for unit 4 turn on (amber) to indicate that the stack signals are looped.

3. The remaining stack units remain connected.

Although the example shown in Figure 18 shows a failed unit causing the stack to loop signals at the points of failure (A and B), the system reacts the same way if a cable is removed.

Figure 18 Redundant cascade stacking feature

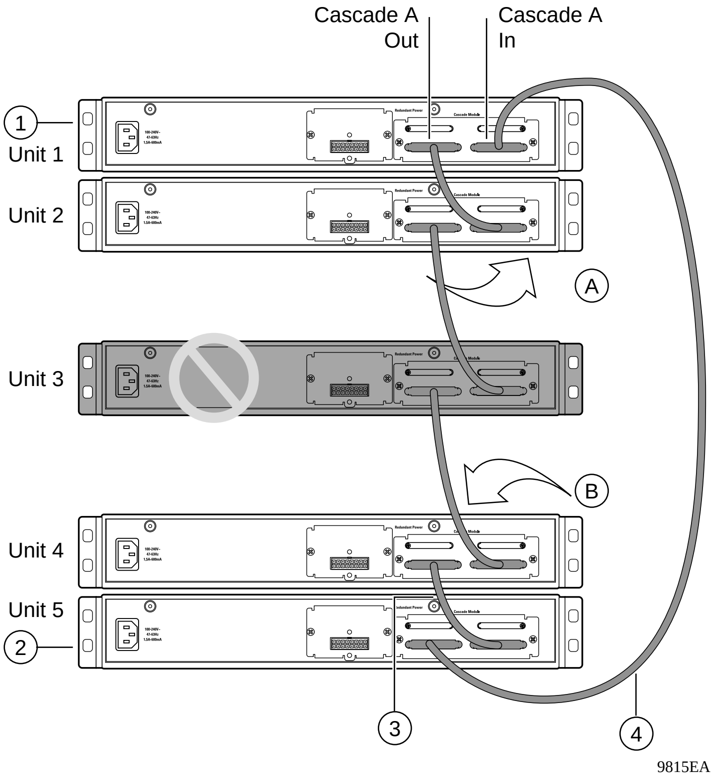


Table 9 describes the redundant cascade stacking illustration references.

Table 9 Redundant cascade stacking descriptions

1	Base unit
2	Last unit
3	Cascade cable (part number 303978-A)
4	Cascade max-return cable (part number 303979-A)

IEEE 802.1Q VLAN workgroups

➡ **Note:** For guidelines on configuring VLANs, STGs, and MLT, refer to Chapter 1.

Business Policy Switches support up to 64 VLANs (maximum of 48 MAC source address-based VLANs) with IEEE 802.1Q tagging available per port. With software version 1.2, the BPS 2000 supports up to 256 VLANs (maximum of 48 MAC source addressed-based VLANs.)

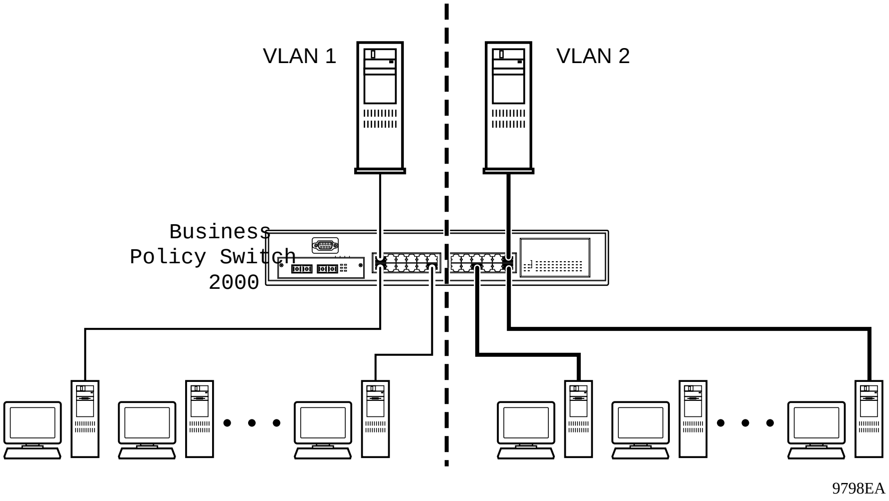
➡ **Note:** Only standalone or pure stacks of BPS 2000 support 256 VLANs. A mixed stack that consists of BPS 2000 and BayStack 450 switches has only 64 VLANs. Refer to Chapter 1 for more information on using 256 VLANs.

Ports are grouped into broadcast domains by assigning them to the same VLAN. Frames received in one VLAN can only be forwarded within that VLAN, and multicast frames and unknown unicast frames are flooded only to ports in the same VLAN.

Setting up virtual LANs (VLANs) is a way to segment networks to increase network capacity and performance without changing the physical network topology (Figure 19). With network segmentation, each switch port connects to a segment that is a single broadcast domain. When a switch port is configured to be a member of a VLAN, it is added to a group of ports (workgroup) that belong to one broadcast domain.

The Business Policy Switch allows you to assign ports to VLANs using the console, Telnet, Web-based management, CLI, or an appropriate SNMP-based application, such as the Device Manager. You can assign different ports (and therefore the devices attached to these ports) to different broadcast domains. This feature allows network flexibility because you can reassign VLANs to accommodate network moves, additions, and changes, eliminating the need to change physical cabling.

Figure 19 Port-based VLAN example



IEEE 802.1Q tagging

Business Policy Switches operate in accordance with the IEEE 802.1Q tagging rules. Important terms used with the 802.1Q tagging feature are:

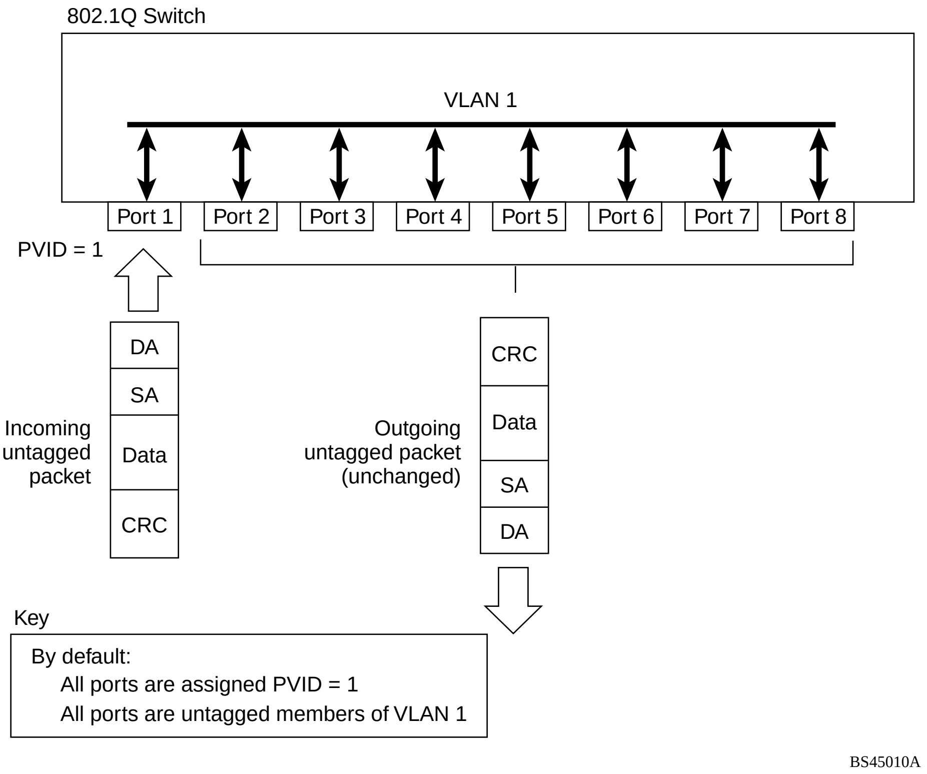
- VLAN identifier (VID)—the 12-bit portion of the VLAN tag in the frame header that identifies an explicit VLAN. When other types of VLANs are enabled, this default value can be overridden by the values enabled in the management interfaces. Refer to Chapter 3, *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5, Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5*, and *Reference for the Business Policy Switch 2000 Management Software Version 2.5* for information on overriding the default values.
- Port VLAN identifier (PVID)—a classification mechanism that associates a port with a specific VLAN. For example, a port with a PVID of 3 (PVID =3) assigns all untagged frames received on this port to VLAN 3.

  With software version 1.1, you can automatically assign the PVIDs.
- Tagged frame—the 32-bit field (VLAN tag) in the frame header that identifies the frame as belonging to a specific VLAN. Untagged frames are marked (tagged) with this classification as they leave the switch through a port that is configured as a tagged port.

- Untagged frame— a frame that does not carry any VLAN tagging information in the frame header.
- VLAN port members— a set of ports that form a broadcast domain for a specific VLAN. A port can be a member of one or more VLANs.
- Untagged member—a port that has been configured as an untagged member of a specific VLAN. When an untagged frame exits the switch through an untagged member port, the frame header remains unchanged. When a tagged frame exits the switch through an untagged member port, the tag is stripped and the tagged frame is changed to an untagged frame.
- Tagged member—a port that has been configured as a member of a specific VLAN. When an untagged frame exits the switch through a tagged member port, the frame header is modified to include the 32-bit tag associated with the PVID. When a tagged frame exits the switch through a tagged member port, the frame header remains unchanged (original VID remains).
- User priority—a three-bit field in the header of a tagged frame. The field is interpreted as a binary number, therefore has a value of 0 - 7. This field allows the tagged frame to carry the user-priority across bridged LANs where the individual LAN segments may be unable to signal priority information.
- Port priority—the priority level assigned to *untagged* frames received on a port. This value becomes the user priority for the frame. *Tagged* packets get their user priority from the value contained in the 802.1Q frame header.
- Unregistered packet—a tagged frame that contains a VID where the receiving port is not a member of that VLAN.
- Filtering database identifier (FID)—the specific filtering/forwarding database within the Business Policy Switch that is assigned to each VLAN. The current version of software assigns *all VLANs* to the same FID when it is running in the Hybrid Operational mode. This process is referred to as Shared VLAN Learning (SVL) in the IEEE 802.1Q specification. In the Pure BPS 2000 operational mode, a VLAN may either share its filtering database with other VLANs (SVL) or have its own filtering database, which is called independent VLAN learning (IVL).

The default configuration settings for Business Policy Switches have all ports set as untagged members of VLAN 1 with all ports configured as PVID = 1. Every VLAN is assigned a unique VLAN identifier (VID) that distinguishes it from all other VLANs. In the default configuration example shown in Figure 20, all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID =1). Untagged packets enter and leave the switch unchanged.

Figure 20 Default VLAN settings

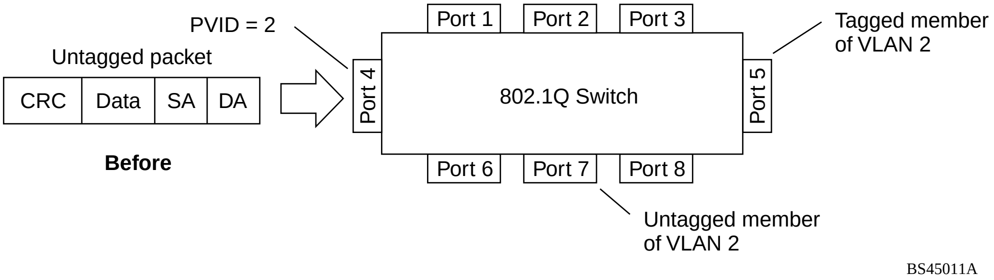


With software version 2.5, you can configure switch ports to transmit frames tagged on some VLANs, and untagged on other VLANs.

When you configure VLANs, you configure the egress tagging of each switch port as *Untag All*, *Untag PVID Only*, *Tag All* or *Tag PVID Only* (see Figure 21 through Figure 28).

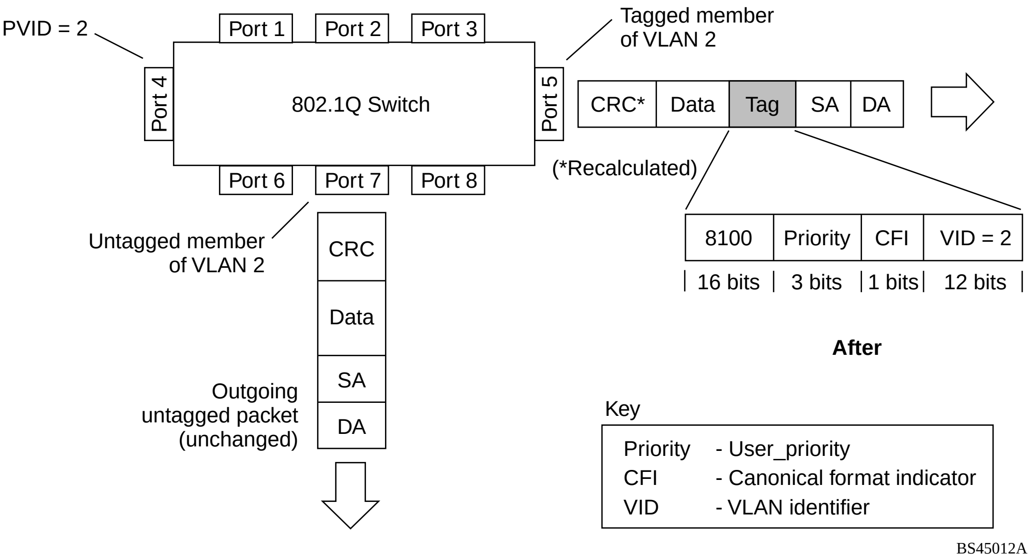
In Figure 21, untagged incoming packets are assigned directly to VLAN 2 (PVID = 2). Port 5 is configured as a *tagged* member of VLAN 2, and port 7 is configured as an *untagged* member of VLAN 2.

Figure 21 Port-based VLAN assignment



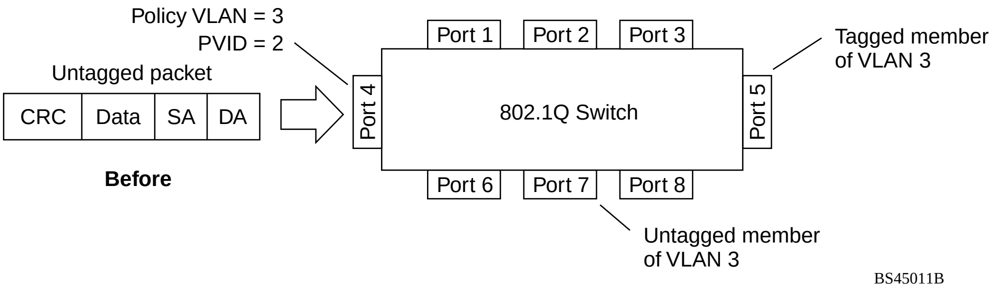
As shown in Figure 22, the untagged packet is marked (tagged) as it leaves the switch through port 5, which is configured as a tagged member of VLAN 2. The untagged packet remains unchanged as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.

Figure 22 802.1Q tagging (after port-based VLAN assignment)



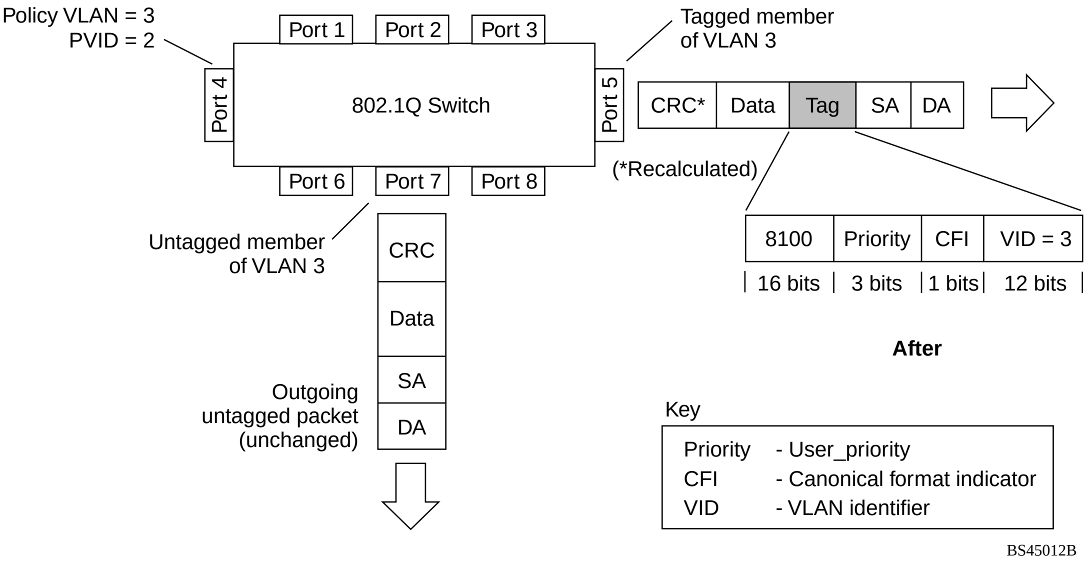
In Figure 23, untagged incoming packets are assigned to VLAN 3 (policy VLAN = 3, PVID = 2). Port 5 is configured as a *tagged* member of VLAN 3, and port 7 is configured as an *untagged* member of VLAN 3.

Figure 23 Policy-based VLAN assignment



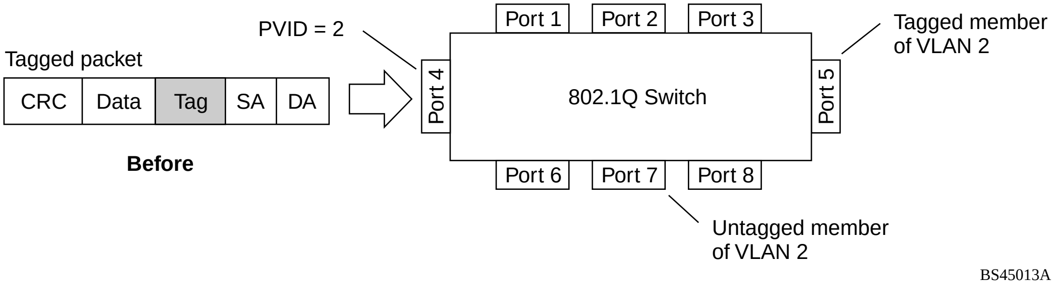
As shown in Figure 24, the untagged packet is marked (tagged) as it leaves the switch through port 5, which is configured as a tagged member of VLAN 3. The untagged packet remains unchanged as it leaves the switch through port 7, which is configured as an untagged member of VLAN 3.

Figure 24 802.1Q tagging (after policy-based VLAN assignment)



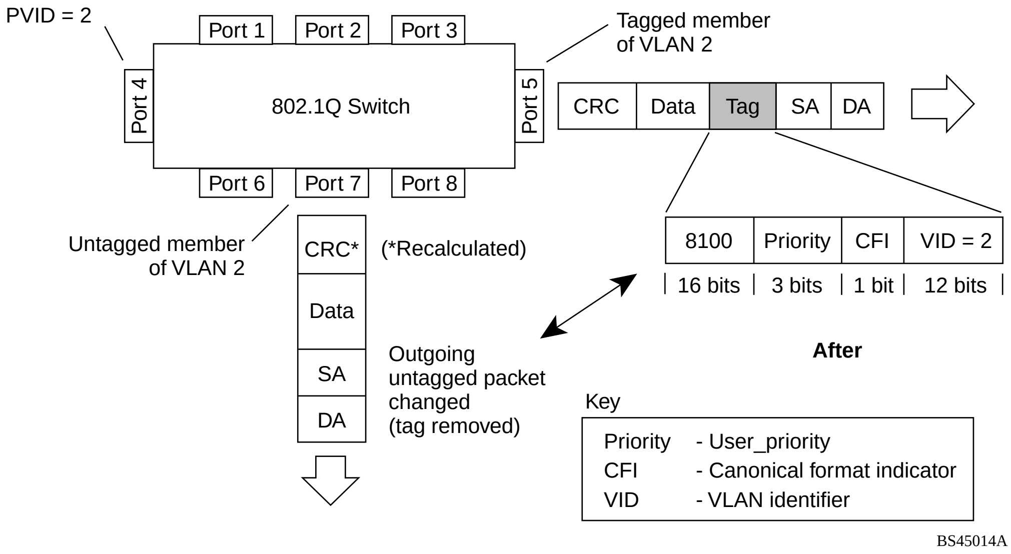
In Figure 25, tagged incoming packets are assigned directly to VLAN 2 because of the tag assignment in the packet. Port 5 is configured as a *tagged* member of VLAN 2, and port 7 is configured as an *untagged* member of VLAN 2.

Figure 25 802.1Q tag assignment



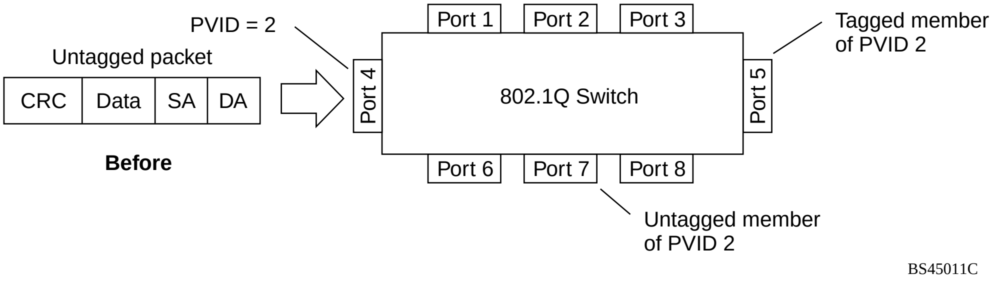
As shown in Figure 26, the tagged packet remains unchanged as it leaves the switch through port 5, which is configured as a tagged member of VLAN 2. However, the tagged packet is stripped (untagged) as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.

Figure 26 802.1Q tagging (after 802.1Q tag assignment)



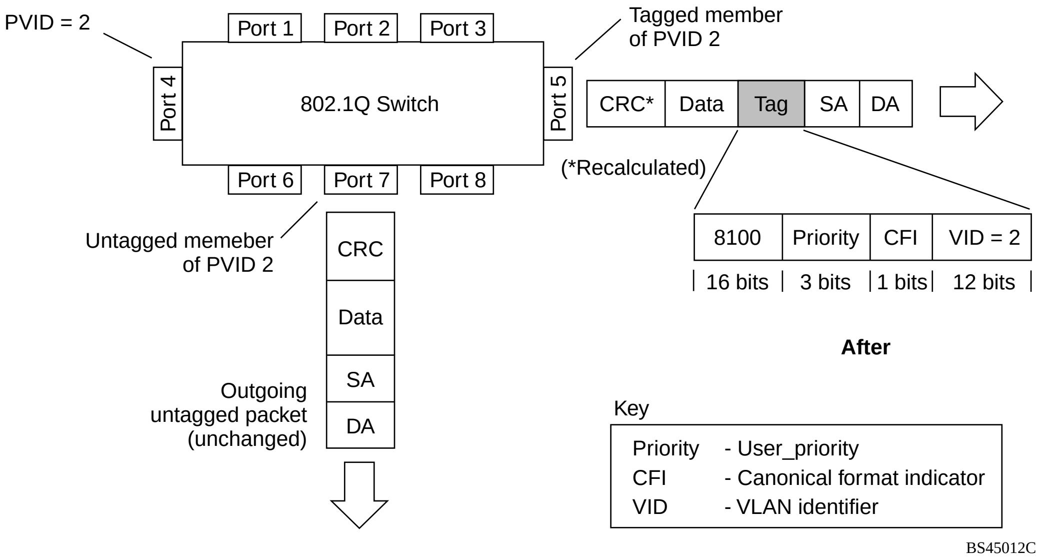
In Figure 27, untagged incoming packets are assigned directly to PVID = 2. Port 5 is configured as a *tagged* member of PVID 2, and port 7 is configured as an *untagged* member of PVID 2.

Figure 27 802.1Q tag assignment



As shown in Figure 28, the untagged packet is marked (tagged) as it leaves the switch through port 5, which is configured as a tagged member of PVID 2. The untagged packet remains unchanged as it leaves the switch through port 7, which is configured as an untagged member of PVID 2.

Figure 28 802.1Q tagging (after 802.1Q tag assignment)



VLANs spanning multiple switches

You can use VLANs to segment a network within a switch. When you connect multiple switches, it is possible to connect users of one VLAN with users of that same VLAN in another switch. However, the configuration guidelines depend on whether both switches support 802.1Q tagging.

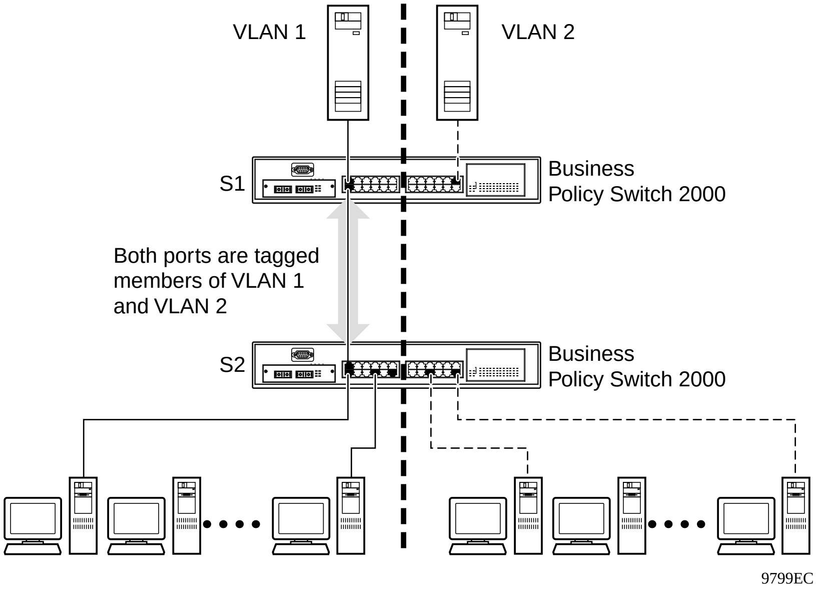
With 802.1Q tagging enabled on a port for a VLAN, all frames leaving the port for that VLAN are *marked* as belonging to that specific VLAN. You can assign specific switch ports as members of one or more VLANs that span multiple switches, without interfering with the Spanning Tree Protocol.

Refer to Chapter 1 for additional guidelines on configuring VLANs and spanning tree groups.

VLANs spanning multiple 802.1Q tagged switches

Figure 29 shows VLANs spanning two Business Policy Switches. The 802.1Q tagging is enabled on S1, port 2 and on S2, port 1 for VLAN 1 and VLAN 2. Both ports are tagged members of VLAN 1 and VLAN 2.

Figure 29 VLANs spanning multiple 802.1Q tagged switches



Because there is only one link between the two switches, the Spanning Tree Protocol (STP) treats this configuration as any other switch-to-switch connection. For this configuration to work properly, both switches must support the 802.1Q tagging protocol.

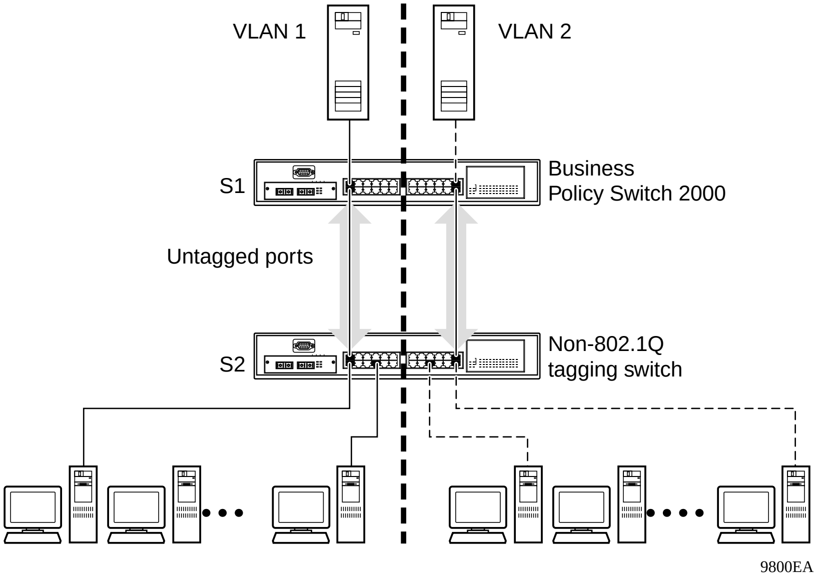
VLANS spanning multiple untagged switches

Figure 30 shows VLANs spanning multiple untagged switches. In this configuration, Switch S2 does not support 802.1Q tagging and you must use a single switch port on each switch for each VLAN.

For this configuration to work properly, you must set spanning tree participation to Disabled (the STP is not supported across multiple LANs).

Refer to Chapter 1 for additional guidelines on configuring VLANs and spanning tree groups.

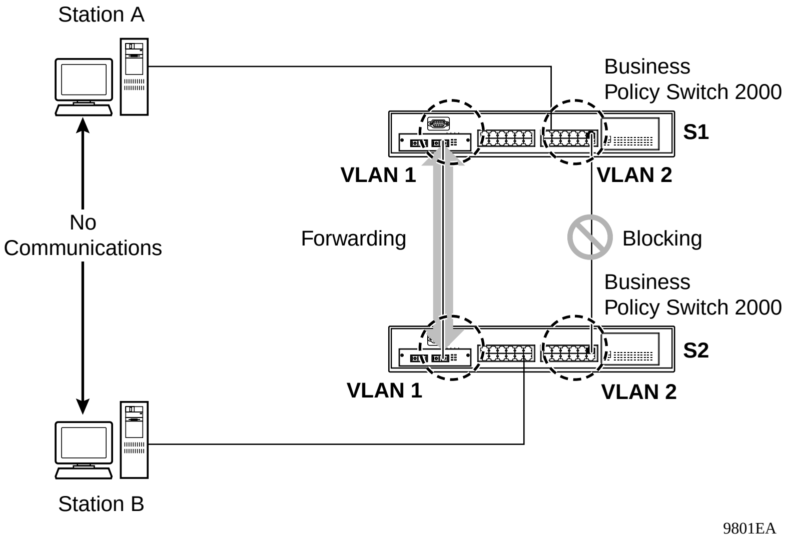
Figure 30 VLANs spanning multiple untagged switches



When the STP is enabled on these switches, only one link between each pair of switches will be forwarding traffic. Because each port belongs to only one VLAN at a time, connectivity on the other VLAN is lost. Exercise care when configuring the switches to ensure that the VLAN configuration does not conflict with spanning tree configuration.

To connect multiple VLANs across switches with redundant links, you must disable the STP on all participating switch ports. Figure 31 shows possible consequences of enabling the STP when using VLANs between untagged (non-802.1Q tagged) switches.

Figure 31 Possible problems with VLANs and Spanning Tree Protocol



As shown in Figure 31, with STP enabled, only one connection between Switch S1 and Switch S2 is forwarding at any time. Communications failure occurs between VLAN 2 of S1 and VLAN 2 of S2, blocking communications between Stations A and B.

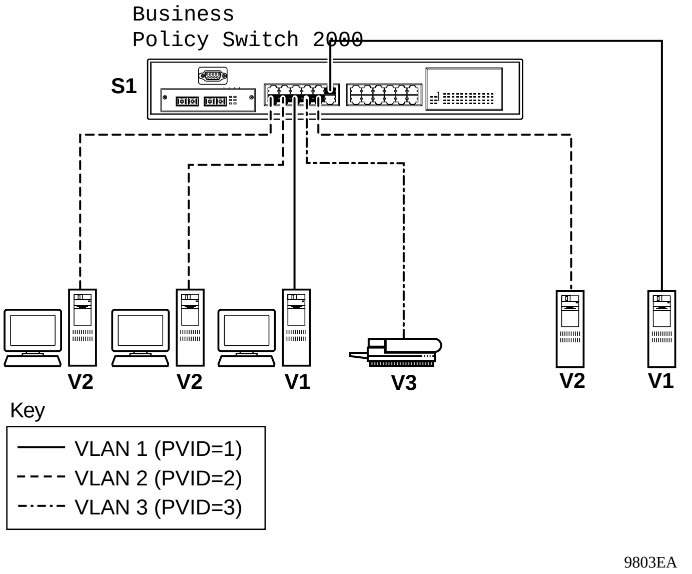
The STP selects the link connecting VLAN 1 on Switches S1 and S2 as the forwarding link based on port speed, duplex-mode, and port priority. Because the other link connecting VLAN 2 is in Blocking mode, stations on VLAN 2 in Switch S1 cannot communicate with stations in VLAN 2 on Switch S2. With multiple links only one link will be forwarding.

Shared servers

Business Policy Switches allow ports to exist in multiple VLANs for shared resources, such as servers, printers, and switch-to-switch connections. It is also possible to have resources exist in multiple VLANs on one switch as shown in Figure 32.

In this example, clients on different broadcast domains share resources. The broadcasts from ports configured in VLAN 3 can be seen by all VLAN port members of VLAN 3.

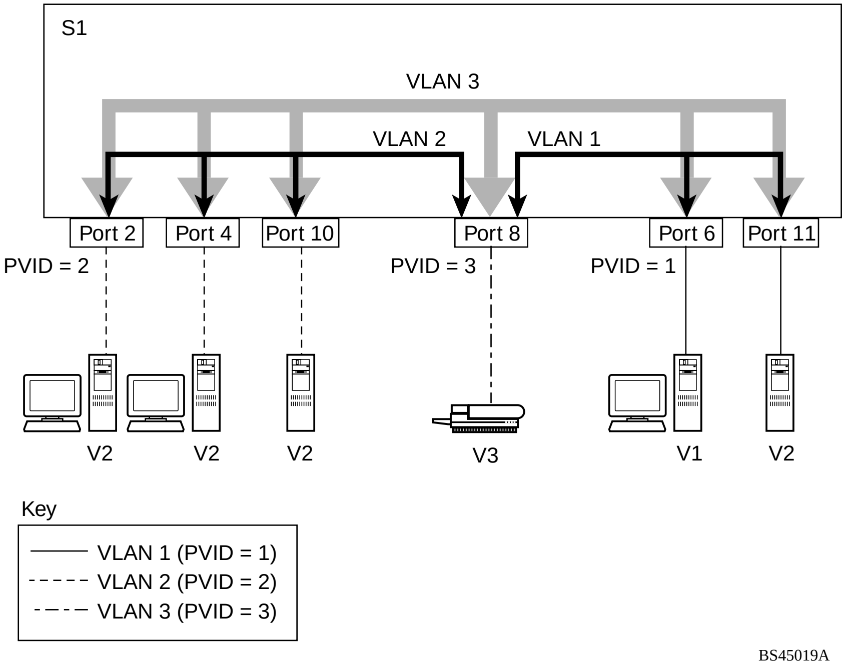
Figure 32 Multiple VLANs sharing resources



In the above configuration, all of the switch ports are set to participate as VLAN port members. This arrangement allows the switch to establish the appropriate broadcast domains within the switch (Figure 33).

Refer to Chapter 1 for additional guidelines on configuring VLANs and spanning tree groups.

Figure 33 VLAN broadcast domains within the switch



For example, to create a broadcast domain for each VLAN shown in Figure 33, configure each VLAN with a port membership, and each port with the appropriate PVID/VLAN association:

- Ports 8, 6, and 11 are untagged members of VLAN 1.
- The PVID/VLAN association for ports 6 and 11 is: PVID = 1.
- Ports 2, 4, 10, and 8 are untagged members of VLAN 2.
- The PVID/VLAN association for ports 2, 4, and 10 is: PVID = 2.
- Ports 2, 4, 10, 8, 6, and 11 are untagged members of VLAN 3.
- The PVID/VLAN association for port 8 is: PVID = 3.

The following steps show how to use the VLAN configuration screens to configure the VLAN 3 broadcast domain shown in Figure 33.

To configure the VLAN port membership for VLAN 1:

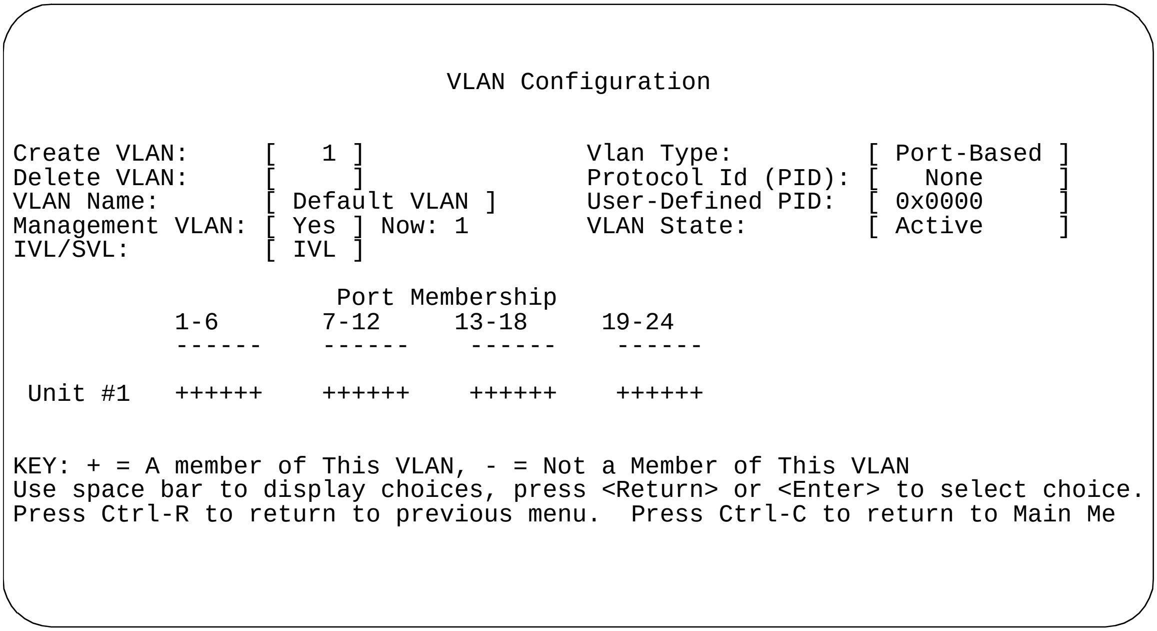
1 Select Switch Configuration from the Business Policy Switch Main Menu (or press w).

2 From the Switch Configuration Menu, select VLAN Configuration (or press v).

3 From the VLAN Configuration Menu select VLAN Configuration (or press v).

The default VLAN Configuration screen opens (Figure 34):

Figure 34 Default VLAN Configuration screen example



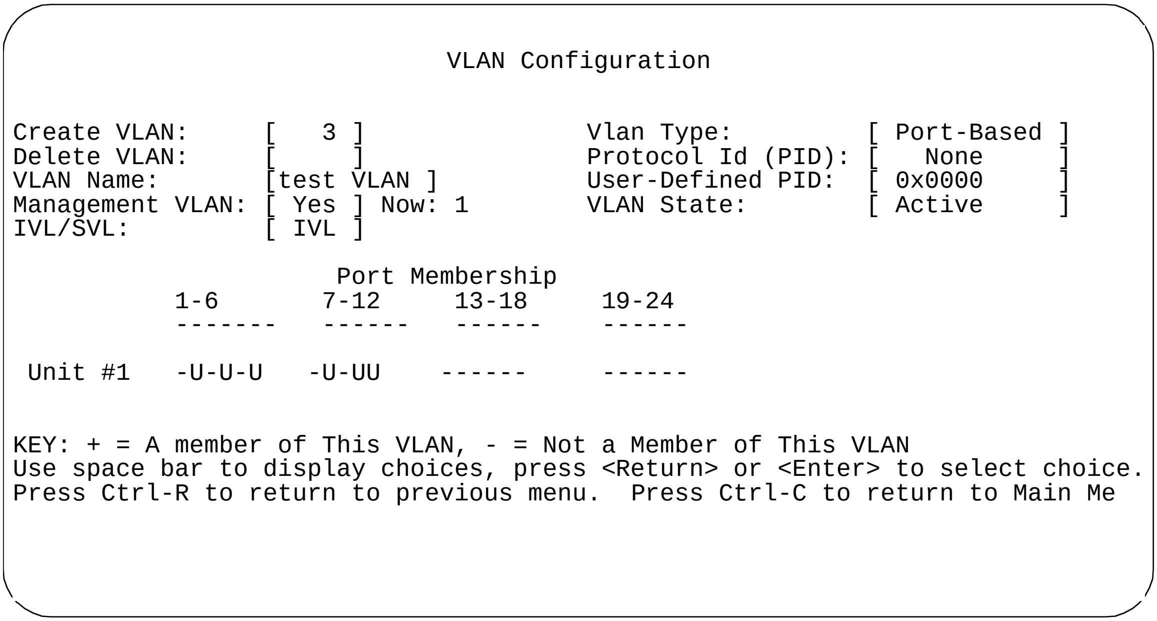
```
                             VLAN Configuration


Create VLAN:     [   1 ]               Vlan Type:         [ Port-Based ]
Delete VLAN:     [     ]               Protocol Id (PID): [   None     ]
VLAN Name:       [ Default VLAN ]      User-Defined PID:  [ 0x0000     ]
Management VLAN: [ Yes ] Now: 1        VLAN State:        [ Active     ]
IVL/SVL:         [ IVL ]

                      Port Membership
           1-6       7-12     13-18     19-24
           ------    ------    ------    ------

 Unit #1   ++++++    ++++++    ++++++    ++++++


KEY: + = A member of This VLAN, - = Not a Member of This VLAN
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Me
```

The VLAN Configuration screen settings shown in Figure 34 are default settings with all switch ports classified as *untagged* members of VLAN 1.

Figure 35 shows the VLAN Configuration screen after it is configured to support the VLAN 3 broadcast domain shown in Figure 33 (VLAN Name is optional).

Ports 2, 4, 6, 8, 10, and 11 are now untagged members of VLAN 3 as shown in Figure 33 on page 131.

Figure 35 VLAN Configuration screen example



```
                              VLAN Configuration


Create VLAN:     [   3 ]               Vlan Type:          [ Port-Based ]
Delete VLAN:     [     ]               Protocol Id (PID): [   None     ]
VLAN Name:       [test VLAN ]          User-Defined PID:  [ 0x0000     ]
Management VLAN: [ Yes ] Now: 1        VLAN State:        [ Active     ]
IVL/SVL:         [ IVL ]

                      Port Membership
           1-6       7-12      13-18     19-24
           -------   ------    ------    ------

 Unit #1   -U-U-U   -U-UU    ------     ------


KEY: + = A member of This VLAN, - = Not a Member of This VLAN
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Me
```

To configure the PVID (port VLAN identifier) for port 8:

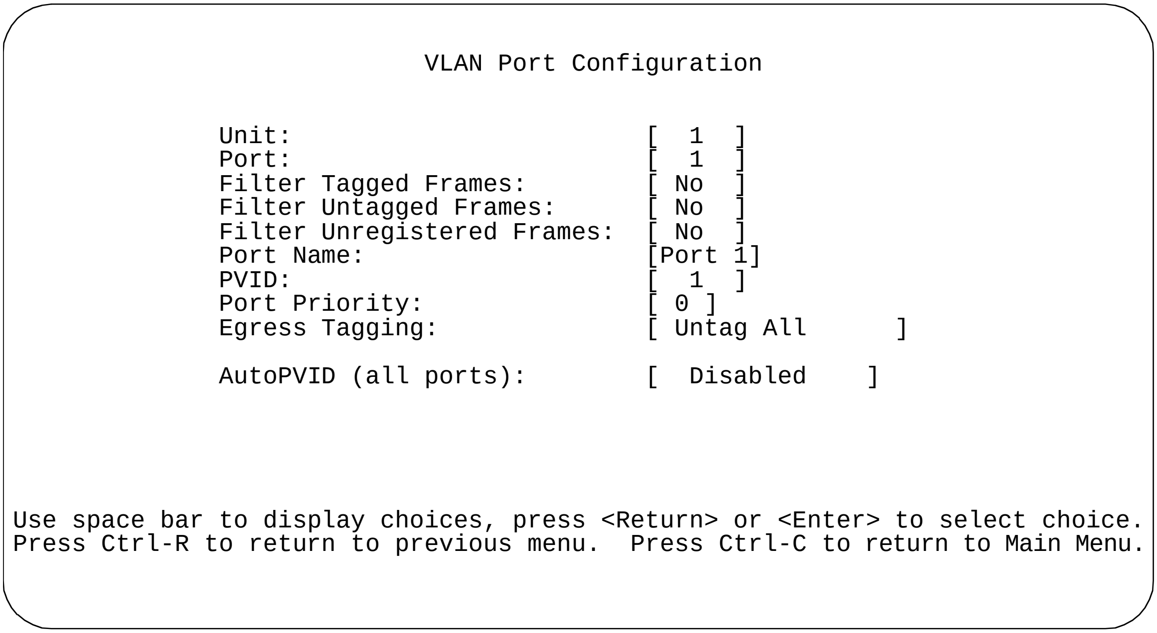
1 From the VLAN Configuration screen, press [Ctrl]-R to return to the VLAN Configuration Menu.

2 From the VLAN Configuration Menu, select VLAN Port Configuration (or press c).

The default VLAN Port Configuration screen opens (Figure 36).

The VLAN Port Configuration screen settings shown in Figure 36 are default settings.

Figure 36 Default VLAN Port Configuration screen example

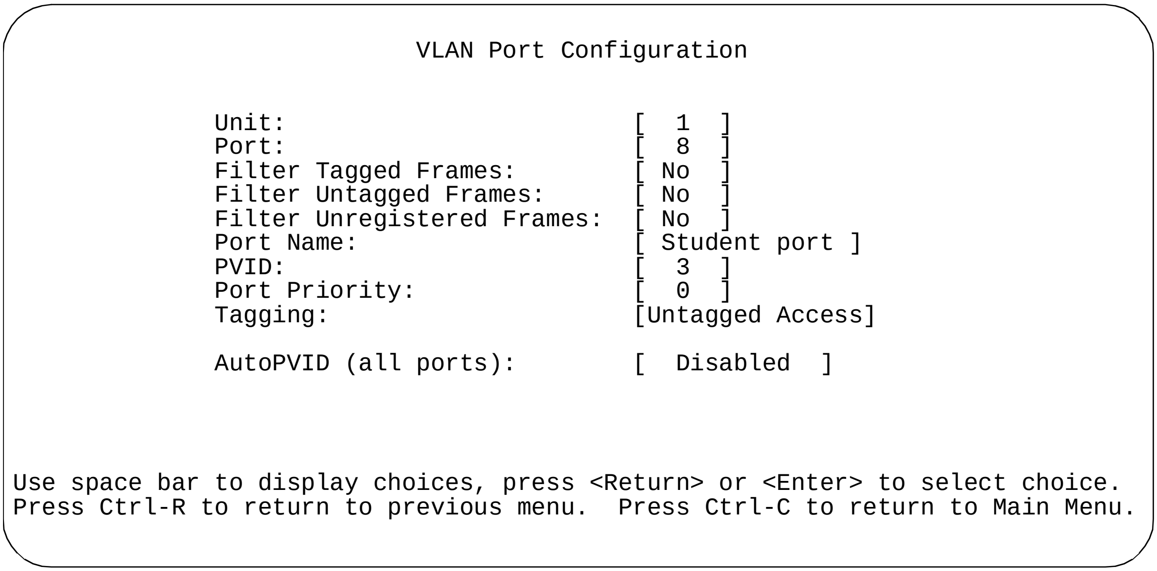


```
                            VLAN Port Configuration


              Unit:                        [  1  ]
              Port:                        [  1  ]
              Filter Tagged Frames:        [ No  ]
              Filter Untagged Frames:      [ No  ]
              Filter Unregistered Frames:  [ No  ]
              Port Name:                   [Port 1]
              PVID:                        [  1  ]
              Port Priority:               [ 0 ]
              Egress Tagging:              [ Untag All      ]

              AutoPVID (all ports):        [  Disabled    ]





Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Figure 37 shows the VLAN Port Configuration screen after it is configured to support the PVID assignment for port 8, as shown in Figure 33 (Port Name is optional).

The PVID/VLAN association for VLAN 3 is now PVID = 3.

Figure 37 VLAN Port Configuration screen example



```
                            VLAN Port Configuration


              Unit:                          [  1  ]
              Port:                          [  8  ]
              Filter Tagged Frames:          [ No  ]
              Filter Untagged Frames:        [ No  ]
              Filter Unregistered Frames:    [ No  ]
              Port Name:                     [ Student port ]
              PVID:                          [  3  ]
              Port Priority:                 [  0  ]
              Tagging:                       [Untagged Access]

              AutoPVID (all ports):          [  Disabled  ]




Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

VLAN workgroup summary

This section summarizes the VLAN workgroup examples discussed in the previous sections of this chapter.

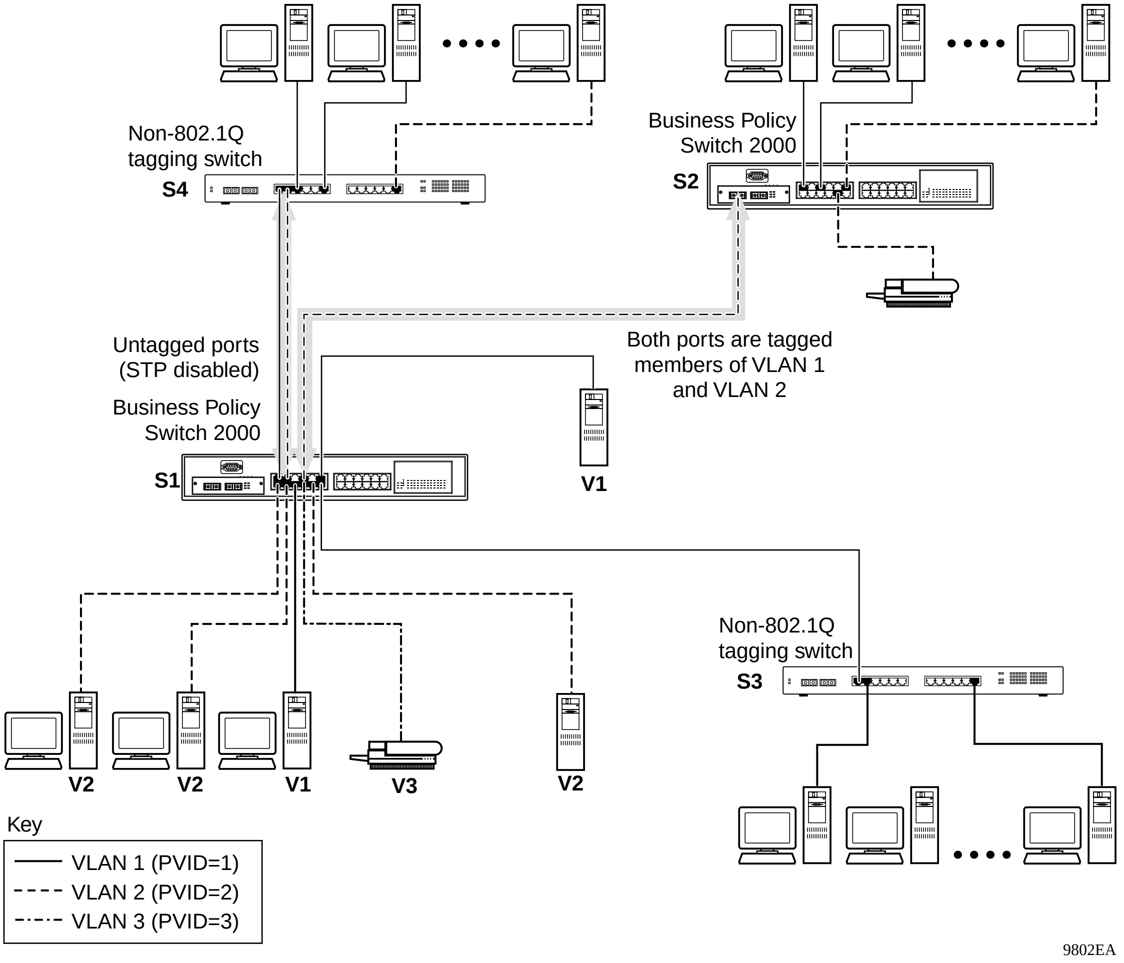
As shown in Figure 38, Switch S1 (Business Policy Switch) is configured with multiple VLANs:

- Ports 1, 6, 11, and 12 are in VLAN 1.
- Ports 2, 3, 4, 7, and 10 are in VLAN 2.
- Port 8 is in VLAN 3.

Because S4 does not support 802.1Q tagging, a single switch port on each switch must be used for each VLAN (see "VLANS spanning multiple untagged switches).

The connection to S2 requires only one link between the switches because S1 and S2 are both Business Policy Switches that support 802.1Q tagging (see "VLANs spanning multiple 802.1Q tagged switches).

Figure 38 VLAN configuration spanning multiple switches



VLAN configuration rules

VLANs operate according to specific configuration rules. When creating VLANs, consider the following rules that determine how the configured VLAN reacts in any network topology:

- You must be in the Pure BPS 2000 Stack mode and using software version 1.2 to be able to configure between 65 and 256 VLANs. (You can configure up to 64 VLANs in Hybrid mode.)
- All ports that are involved in port mirroring must have memberships in the same VLANs. If a port is configured for port mirroring, the port's VLAN membership cannot be changed.
- If a port is a trunk group member, all trunk members are added or deleted from the VLAN.
- All ports involved in trunking and port mirroring must have the same VLAN configuration. If a port is on a trunk with a mirroring port, the VLAN configuration cannot be changed.
- VLANs are not dependent on Rate Limiting settings.
- If a port is an IGMP member on any VLAN, and is removed from a VLAN, the port's IGMP membership is also removed.
- If a port is added to a different VLAN, and it is already configured as a static router port, the port is configured as an IGMP member on that specific VLAN.

For more information about configuring VLANs, refer to Chapter 1 for additional guidelines on configuring VLANs and spanning tree groups and Chapter 3.

See also the Appendixes for configuration flowcharts that can help you use this feature.

IGMP snooping

Business Policy Switches can sense Internet Group Management Protocol (IGMP) host membership reports from attached stations and use this information to set up a dedicated path between the requesting station and a local IP Multicast router. After the pathway is established, the Business Policy Switch blocks the IP

Multicast stream from exiting any other port that does not connect to another host member, thus conserving bandwidth. The following section describes how Business Policy Switches provide the same benefit as IP Multicast routers, but in the local area.

IGMP is used by IP Multicast routers to learn about the existence of host group members on their directly attached subnets (see RFC 2236). The IP Multicast routers get this information by broadcasting IGMP queries and listening for IP hosts reporting their host group memberships. This process is used to set up a client/server relationship between an IP Multicast source that provides the data streams and the clients that want to receive the data.

Figure 39 shows how IGMP is used to set up the path between the client and server. As shown in this example, the IGMP host provides an IP Multicast stream to designated routers that forward the IP Multicast stream on their local network only if there is a recipient.

The client/server path is set up as follows:

1 The designated router sends out a host membership query to the subnet and receives host membership reports from end stations on the subnet.

2 The designated routers then set up a path between the IP Multicast stream source and the end stations.

3 Periodically, the router continues to query end stations on whether or not to continue participation.

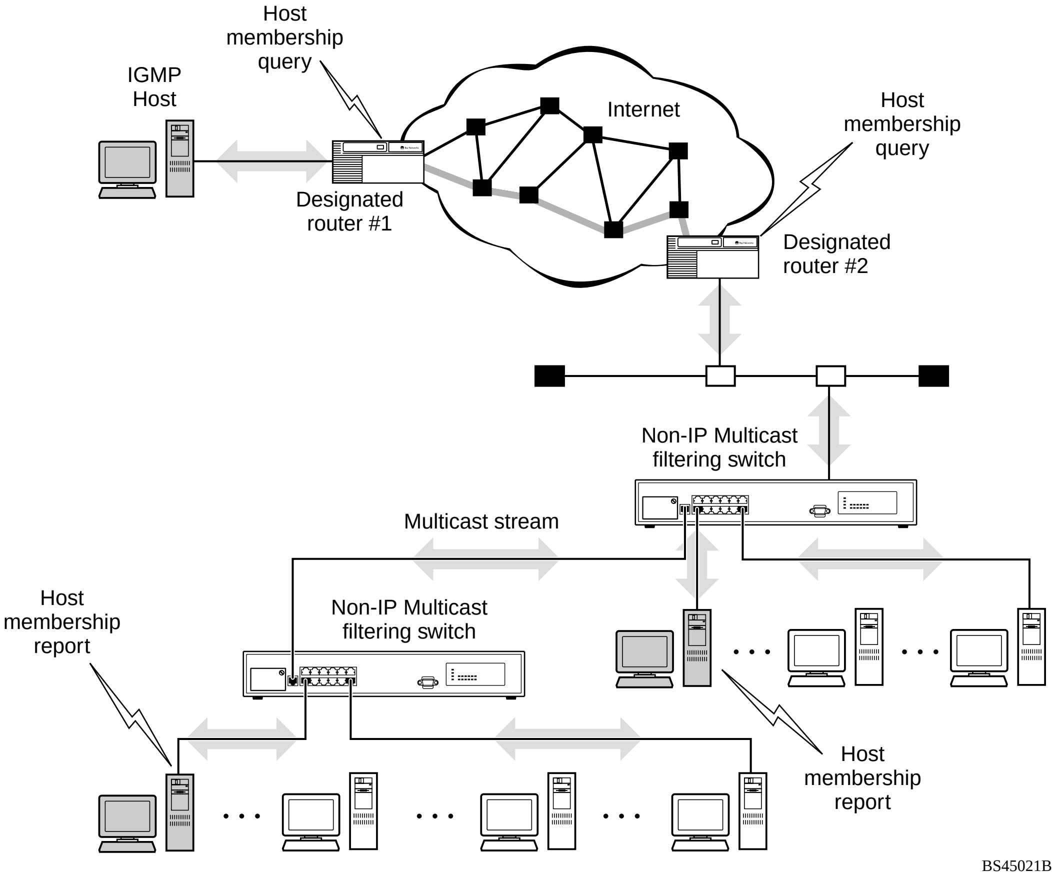
4 As long as any client continues to participate, all clients, including nonparticipating end stations on that subnet, receive the IP Multicast stream.

Note: Although the nonparticipating end stations can filter the IP Multicast traffic, the IP Multicast traffic still exists on the subnet and consumes bandwidth.

IP Multicast can be optimized in a LAN by using IP Multicast filtering switches, such as the Business Policy Switch.

As shown in Figure 39, a non-IP Multicast filtering switch causes IP Multicast traffic to be sent to all segments on the local subnet.

Figure 39 IP Multicast propagation with IGMP routing

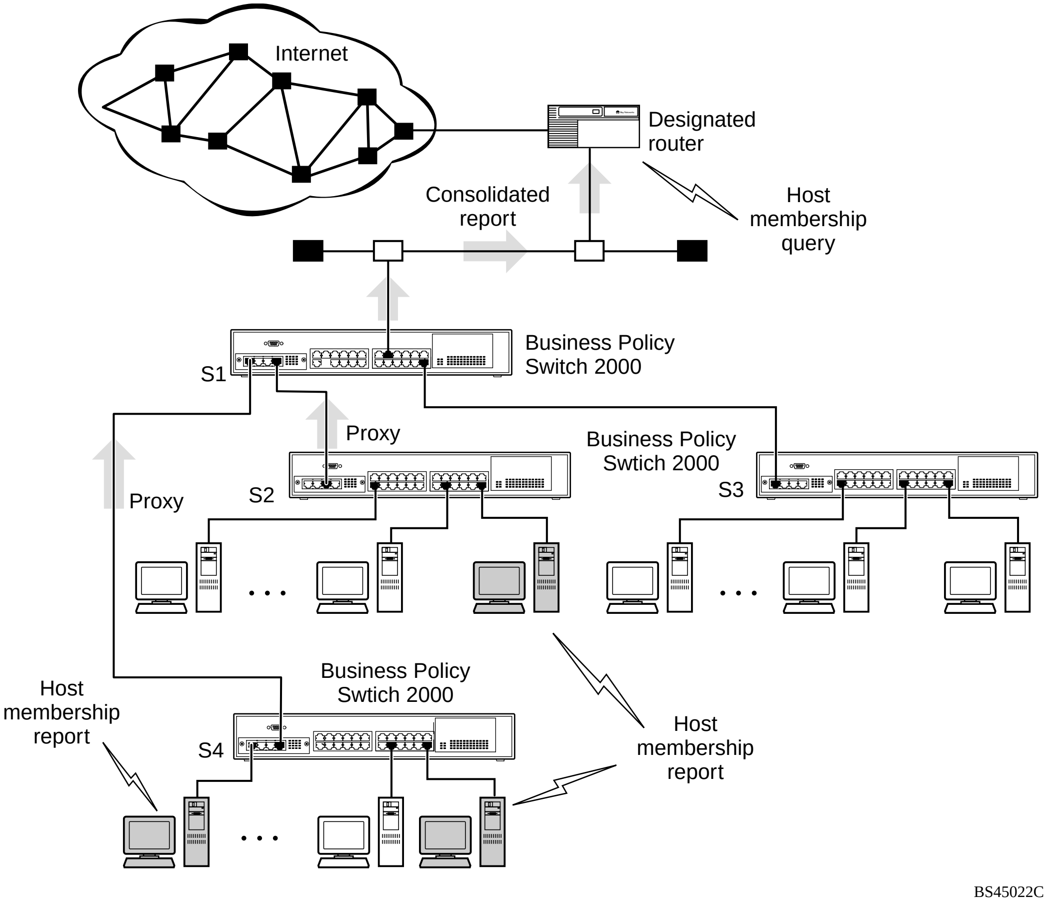


The Business Policy Switch can automatically set up IP Multicast filters so the IP Multicast traffic is only directed to the participating end nodes (see Figure 40).

In Figure 40, switches S1 to S4 represent a LAN connected to an IP Multicast router. The router periodically sends Host Membership Queries to the LAN and listens for a response from end stations. All of the clients connected to switches S1 to S4 are aware of the queries from the router.

One client, connected to S2, responds with a host membership report. Switch S2 intercepts the report from that port, and generates a *proxy* report to its upstream neighbor, S1. Also, two clients connected to S4 respond with host membership reports, causing S4 to intercept the reports and to generate a *consolidated proxy report* to its upstream neighbor, S1.

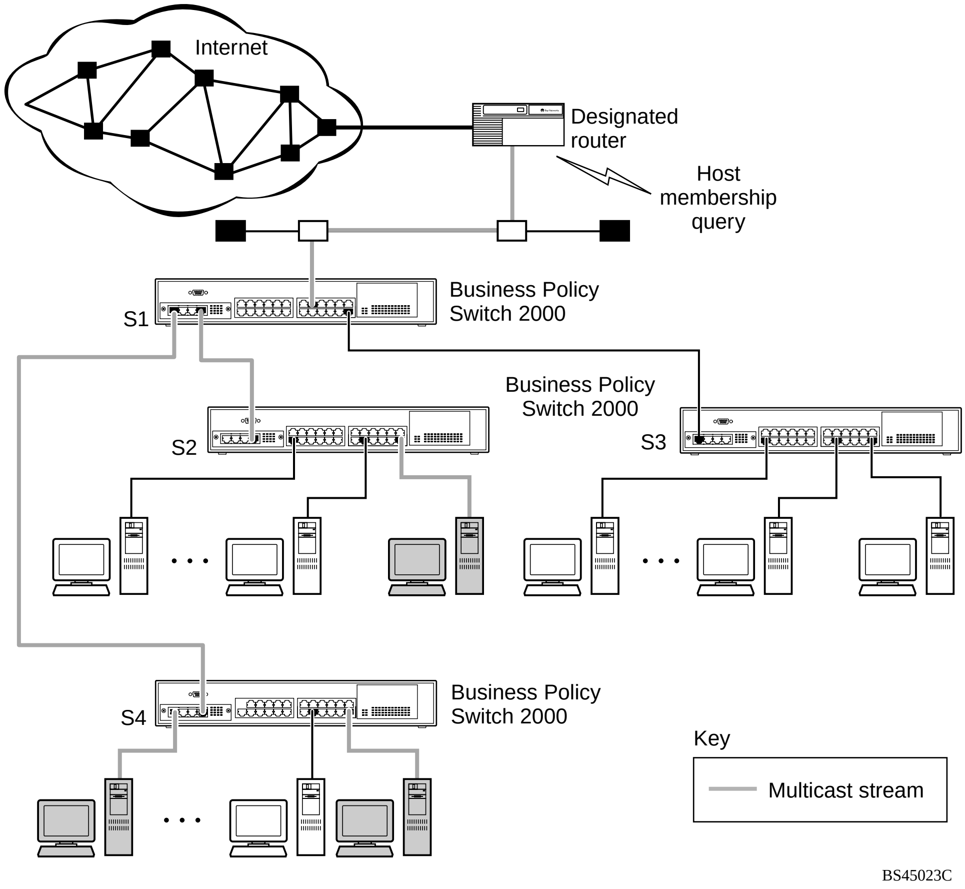
Figure 40 Business Policy Switch filtering IP multicast streams (1 of 2)



Switch S1 treats the consolidated proxy reports from S2 and S4 as if they were reports from any client connected to its ports, and generates a consolidated proxy report to the designated router. In this way, the router receives a single consolidated report from that entire subnet.

After the switches learn which ports are requesting access to the IP Multicast stream, all other ports not responding to the queries are blocked from receiving the IP Multicast (Figure 41).

Figure 41 Business Policy Switch filtering IP multicast streams (2 of 2)



The consolidated proxy report generated by the switch remains transparent to layer 3 of the International Organization for Standardization, Open Systems Interconnection (ISO/OSI) model. (The switch IP address and MAC address are not part of proxy report generation.) The last reporting IGMP group member in each VLAN represents all of the hosts in that VLAN and IGMP group.

IGMP snooping configuration rules

The IGMP snooping feature operates according to specific configuration rules. When configuring your switch for IGMP snooping, consider the following rules that determine how the configuration reacts in any network topology:

- A port that is configured for port mirroring cannot be configured as a static router port.
- If a MultiLink Trunk member is configured as a static router port, all of the MultiLink trunk members are configured as static router ports. Also, if a static router port is removed, and it is a MultiLink Trunk member, all MultiLink trunk members are removed as static router port members, automatically.
- Static router ports must be port members of at least one VLAN.
- If a port is configured as a static router port, it is configured as a static router port for all VLANs on that port. The IGMP configuration is propagated through all VLANs of that port.
- If a static router port is removed, the membership for that port is removed from all VLANs of that port.
- The IGMP snooping feature is not STP-dependent.
- The IGMP snooping feature is not Rate Limiting-dependent.
- The snooping field must be enabled for the proxy field to have any valid meaning.
- Static router ports are configured per VLAN and per IGMP Version.

Note: Because IGMP snooping is set up per VLAN, all IGMP changes are implemented according to the VLAN configuration for the specified ports.

For more information about using the IGMP snooping feature, refer to Chapter 1 for additional guidelines on configuring VLANs, IGMP, and spanning tree groups and Chapter 3.

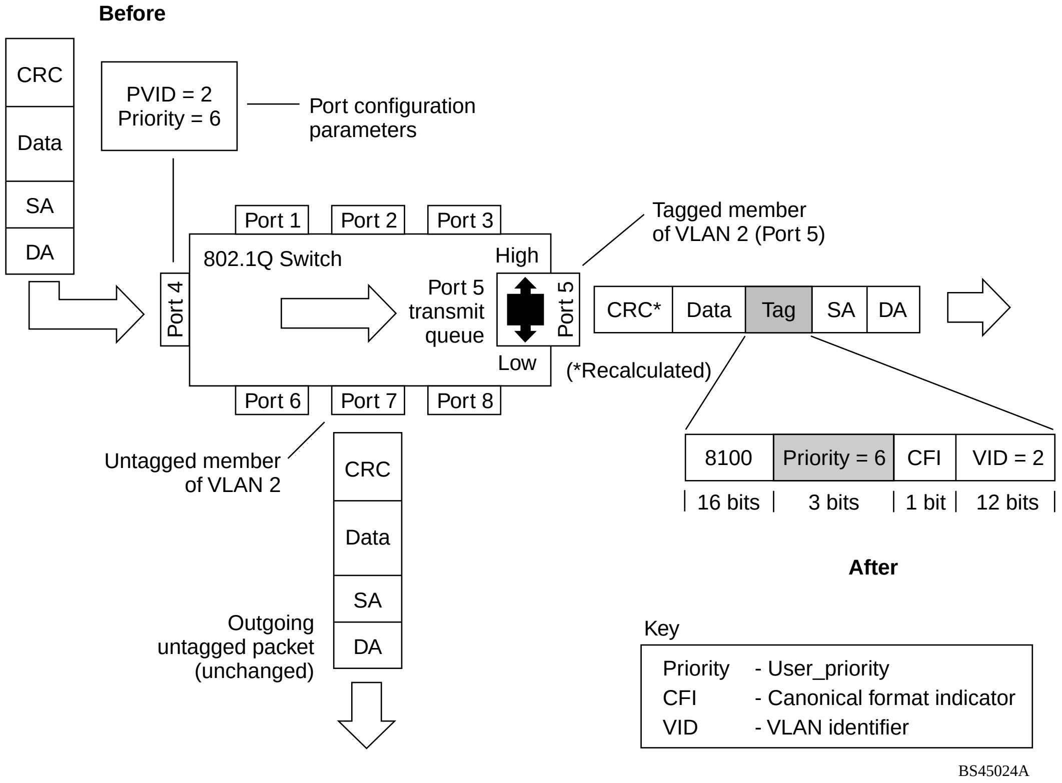
See also appendixes for configuration flowcharts that can help you use this feature.

IEEE 802.1p prioritizing

For more information on prioritizing traffic, refer to Chapter 4, “Policy-enabled networks.”

You can use the VLAN Configuration screens to prioritize the order in which the switch forwards packets, on a per-port basis. For example, if messages from a specific segment are crucial to your operation, you can set the switch port connected to that segment to a higher priority level (by default, all switch ports are set to low priority). Untagged packets received by the switch on that port are tagged according to the priority level you assign to the port (see Figure 42).

Figure 42 Prioritizing packets



The newly tagged frame is read within the switch and sent to the port’s high or low transmit queue for disposition.

MultiLink Trunks

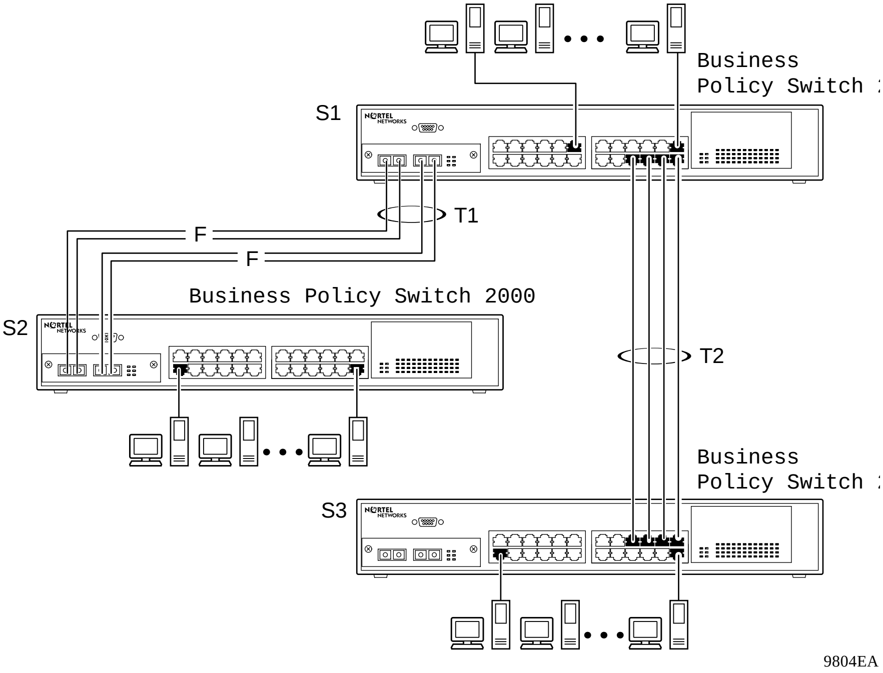
Note: For guidelines on configuring VLANs, STGs, and MLT, refer to Chapter 1.

MultiLink Trunks allow you to group up to four switch ports together to form a link to another switch or server, thus increasing aggregate throughput of the interconnection between the devices (up to 800 Mb/s in full-duplex mode). You can configure up to six MultiLink Trunks. The trunk members can reside on a single unit or on multiple units within the same stack configuration as a *distributed trunk*. MultiLink Trunking software detects misconfigured (or broken) trunk links and redirects traffic on the misconfigured or broken trunk link to other trunk members within that trunk.

You can use the Trunk Configuration screen with the CI menus, the Web-based management system, the CLI, or DM to create switch-to-switch and switch-to-server MultiLink Trunk links.

Figure 43 shows two trunks (T1 and T2) connecting Switch S1 to switches S2 and S3.

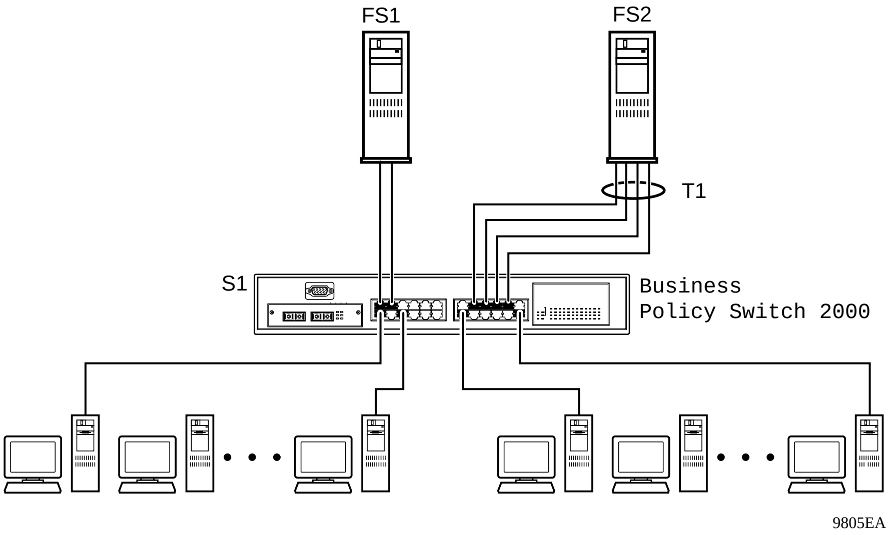
Figure 43 Switch-to-switch trunk configuration example



You can configure each of the trunks shown in Figure 43 with up to four switch ports to provide up to 800 Mb/s aggregate bandwidth through each trunk, in full-duplex mode. As shown in this example, when traffic between switch-to-switch connections approaches single port bandwidth limitations, creating a MultiLink Trunk can supply the additional bandwidth required to improve the performance.

Figure 44 shows a typical switch-to-server trunk configuration. In this example, file server FS1 uses dual MAC addresses, using one MAC address for each network interface card (NIC). For this reason, FS1 does not require a trunk assignment. FS2 is a single MAC server (with a four-port NIC) and is set up as trunk configuration T1.

Figure 44 Switch-to-server trunk configuration example



Client/server configuration using MultiLink Trunks

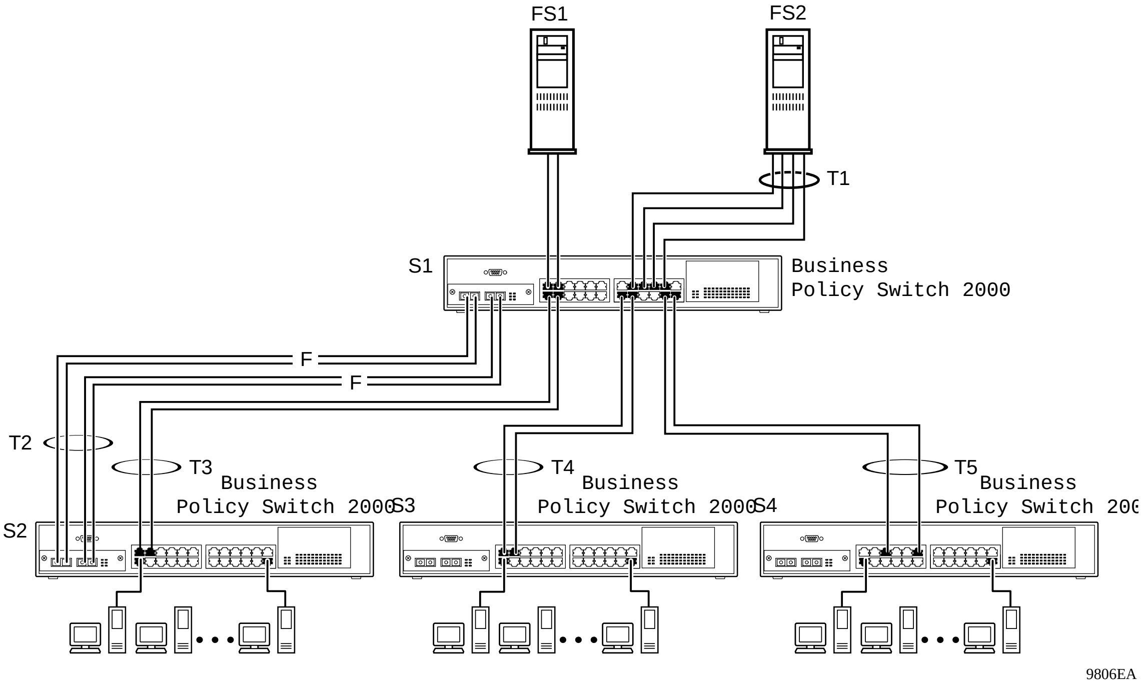
Figure 45 shows an example of how MultiLink Trunking can be used in a client/server configuration. In this example, both servers connect directly to Switch S1. FS2 is connected through a trunk configuration (T1). The switch-to-switch connections are through trunks (T2, T3, T4, and T5).

Clients accessing data from the servers (FS1 and FS2) are provided with maximized bandwidth through trunks T1, T2, T3, T4, and T5. Trunk members (the ports making up each trunk) do not have to be consecutive switch ports; you can select ports randomly, as shown by T5.

With spanning tree *enabled*, one of the trunks (T2 or T3) acts as a redundant (backup) trunk to Switch S2. With spanning tree *disabled*, you must configure trunks T2 and T3 into separate VLANs for this configuration to function properly

For more information on configuration guidelines for spanning tree, VLANs, and MultiLink Trunking, refer to Chapter 1 and "IEEE 802.1Q VLAN workgroups."

Figure 45 Client/server configuration example


FS1
FS2
T1
S1
Business Policy Switch 2000
F
F
T2
T3
Business Policy Switch 2000
S2
T4
Business Policy Switch 2000
S3
T5
Business Policy Switch 200
S4
9806EA

For detailed information about configuring trunks, see Chapter 3.

Before you configure trunks

When you create and enable a trunk, the trunk members (switch ports) take on certain settings necessary for correct operation of the MultiLink Trunking feature.

Before you configure your MultiLink Trunk, you must consider these settings, along with specific configuration rules, as follows:

1. Read the configuration rules provided in the next section, "MultiLink Trunking configuration rules."
2. Determine which switch ports (up to four) are to become *trunk members* (the specific ports making up the trunk). A minimum of two ports are required for each trunk.

Ensure that the chosen switch ports are set to Enabled, using either the Port Configuration screen (see Chapter 3) or other network management system.

Trunk member ports must have the same VLAN configuration.

3 All network cabling should be complete and stable before configuring any trunks, to avoid configuration errors.

4 Consider how the existing spanning tree will react to the new trunk configuration (see "Spanning tree considerations for MultiLink Trunks" and Chapter 1 for spanning tree group configuration guidelines).

5 Consider how existing VLANs will be affected by the addition of a trunk.

MultiLink Trunking configuration rules

The MultiLink Trunking feature is deterministic; that is, it operates according to specific configuration rules. When creating trunks, consider the following rules that determine how the MultiLink Trunk reacts in any network topology:

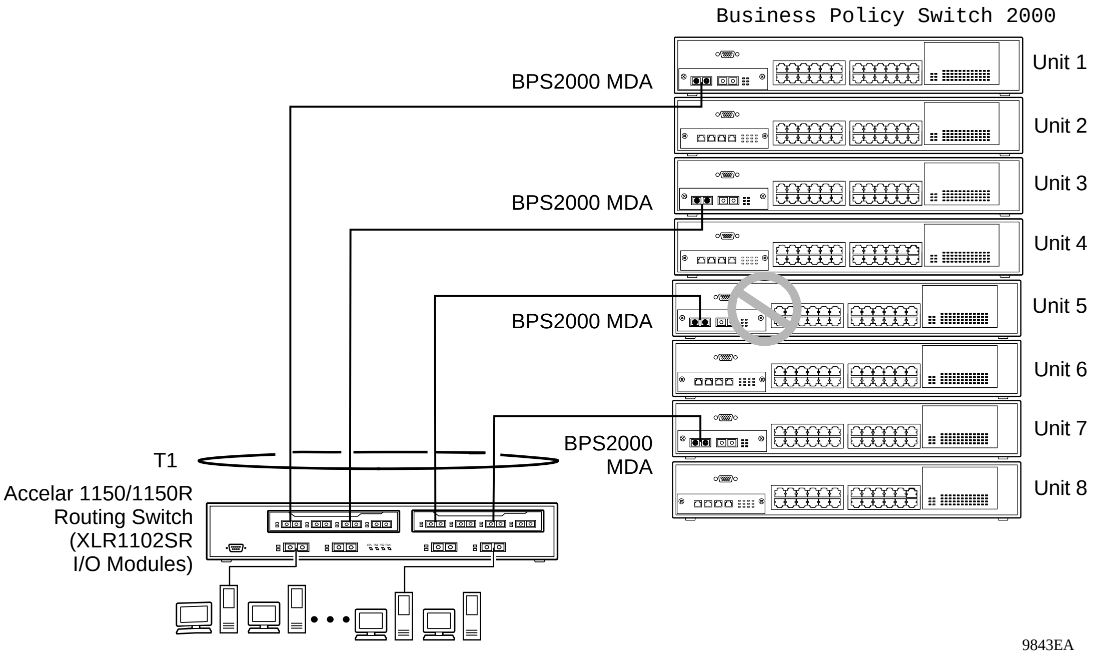
- Any port that participates in MultiLink Trunking must be an active port (set to Enabled via the Port Configuration screen or through network management).
- All trunk members must have the same VLAN configuration before the Trunk Configuration screen's Trunk Status field can be set to Enabled using CI menus (see Chapter 3).
- When an active port is configured in a trunk, the port becomes a *trunk member* when you set the Trunk Status field to Enabled. The spanning tree parameters for the port then change to reflect the new trunk settings.
- All trunk members must be in the same spanning tree group and can belong to only one spanning tree group.
- If you change the spanning tree participation of any trunk member to Enabled or Disabled, the spanning tree participation of all members of that trunk changes similarly (see "Spanning tree considerations for MultiLink Trunks" and Chapter 1 for spanning tree group configuration guidelines).
- When a trunk is enabled, the trunk spanning tree participation setting takes precedence over that of any trunk member.
- If you change the VLAN settings of any trunk member, the VLAN settings of all members of that trunk change similarly.

- When you set any trunk member to Disabled (not active) through the Port Configuration screen or through network management, the trunk member is removed from the trunk. The trunk member has to be reconfigured to rejoin the trunk through the Trunk Configuration screen on the CI menus, or another management system. A screen prompt precedes this action when you are using CI menus. A trunk member cannot be disabled if there are only two trunk members on the trunk.
- You cannot configure a trunk member as a monitor port (see Chapter 3).
- Trunks cannot be monitored by a monitor port; however, trunk members can be monitored (see "Port-based mirroring configuration").
- All trunk members must have identical IGMP configurations.
- If you change the IGMP snooping configuration for any trunk member, the IGMP snooping settings for all trunk members change.
- Nortel Networks recommends that you do not enable MAC Address Security (or BaySecure) on trunk ports.

How the MultiLink Trunk reacts to losing distributed trunk members

If your MultiLink Trunk (Figure 46) spans separate units in a stack configuration and any of those units (or trunked MDAs) becomes inactive from a loss of power or unit failure, the unaffected trunk members remain operational.

Figure 46 Loss of distributed trunk members



However, until you correct the cause of the failure or change the trunk Status field to Disabled, you will be unable to modify any of the following parameters for the affected trunk:

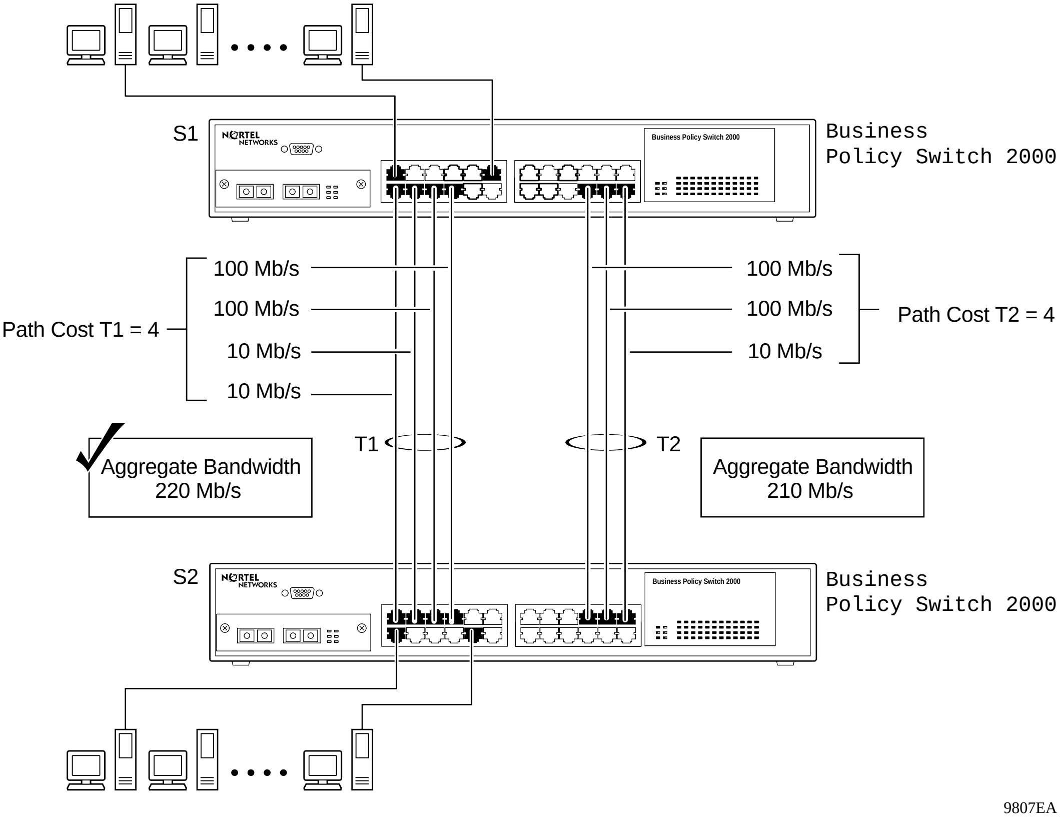
- VLAN configuration
- Spanning Tree configuration
- Port Mirroring configuration
- Port configuration
- IGMP configuration
- Rate Limiting configuration

Spanning tree considerations for MultiLink Trunks

The spanning tree Path Cost parameter is recalculated based on the aggregate bandwidth of the trunk. For example, Figure 47 shows a four-port trunk (T1) with two port members operating at 100 Mb/s and two at 10 Mb/s. Trunk T1 provides an aggregate bandwidth of 220 Mb/s. The Path Cost for T1 is 4 (Path Cost = 1000/

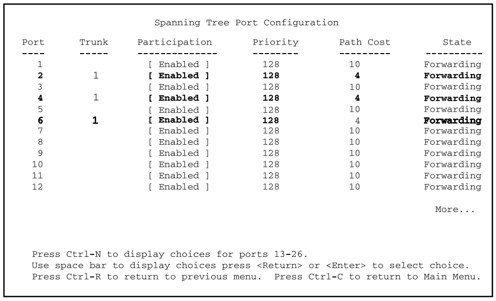
LAN speed, in Mb/s). Another three-port trunk (T2) is configured with an aggregate bandwidth of 210 Mb/s, with a comparable Path Cost of 4. When the Path Cost calculations for both trunks are equal, the software chooses the trunk with the larger aggregate bandwidth (T1) to determine the most efficient path. Also, the trunk cannot span multiple spanning tree groups.

Figure 47 Path Cost arbitration example



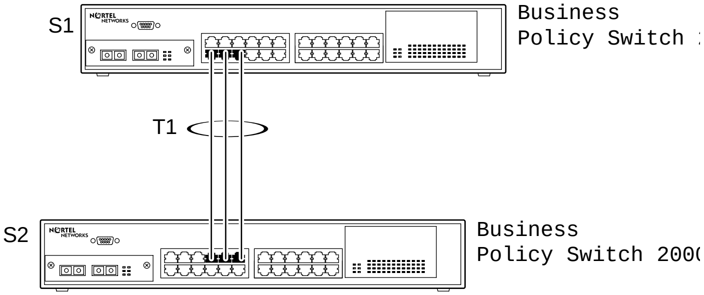
The switch can also detect trunk member ports that are physically misconfigured. For example, in Figure 48, trunk member ports 2, 4, and 6 of Switch S1 are configured *correctly* to trunk member ports 7, 9, and 11 of Switch S2. The Spanning Tree Port Configuration screen for each switch shows the port state field for each port in the Forwarding state.

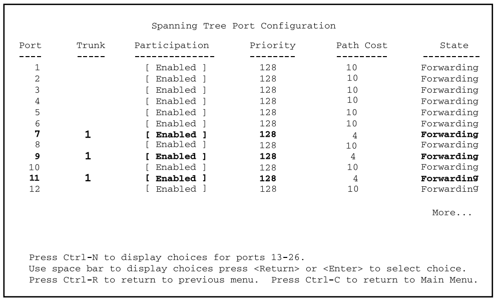
Figure 48 Example 1: correctly configured trunk



```
                     Spanning Tree Port Configuration

Port        Trunk      Participation       Priority      Path Cost         State
----        -----      --------------      --------      ---------      ----------
  1                     [ Enabled ]          128            10          Forwarding
  2           1         [ Enabled ]          128             4          Forwarding
  3                     [ Enabled ]          128            10          Forwarding
  4           1         [ Enabled ]          128             4          Forwarding
  5                     [ Enabled ]          128            10          Forwarding
  6           1         [ Enabled ]          128             4          Forwarding
  7                     [ Enabled ]          128            10          Forwarding
  8                     [ Enabled ]          128            10          Forwarding
  9                     [ Enabled ]          128            10          Forwarding
 10                     [ Enabled ]          128            10          Forwarding
 11                     [ Enabled ]          128            10          Forwarding
 12                     [ Enabled ]          128            10          Forwarding

                                                                           More...


  Press Ctrl-N to display choices for ports 13-26.
  Use space bar to display choices press <Return> or <Enter> to select choice.
  Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

S1 Port Configuration screen





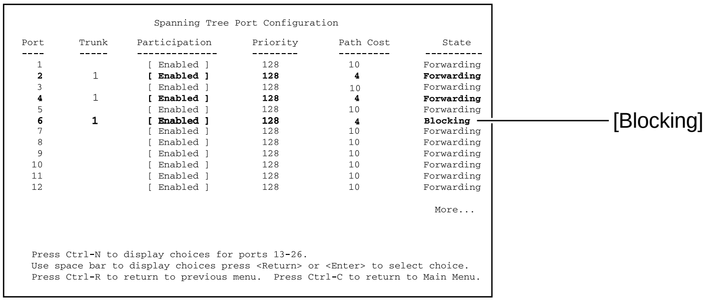
```
                     Spanning Tree Port Configuration

Port        Trunk      Participation       Priority      Path Cost         State
----        -----      --------------      --------      ---------      ----------
  1                     [ Enabled ]          128            10          Forwarding
  2                     [ Enabled ]          128            10          Forwarding
  3                     [ Enabled ]          128            10          Forwarding
  4                     [ Enabled ]          128            10          Forwarding
  5                     [ Enabled ]          128            10          Forwarding
  6                     [ Enabled ]          128            10          Forwarding
  7           1         [ Enabled ]          128             4          Forwarding
  8                     [ Enabled ]          128            10          Forwarding
  9           1         [ Enabled ]          128             4          Forwarding
 10                     [ Enabled ]          128            10          Forwarding
 11           1         [ Enabled ]          128             4          Forwarding
 12                     [ Enabled ]          128            10          Forwarding

                                                                           More...


  Press Ctrl-N to display choices for ports 13-26.
  Use space bar to display choices press <Return> or <Enter> to select choice.
  Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

S2 Port Configuration screen

9808EA

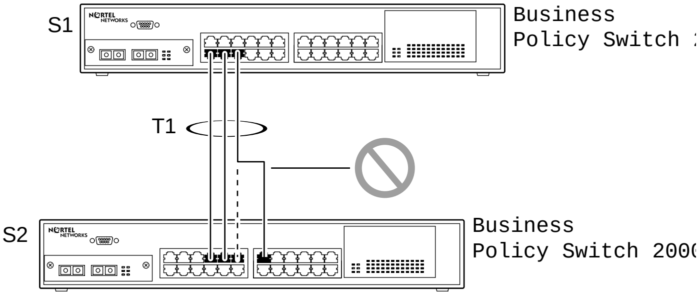
If Switch S2’s trunk member port 11 is physically disconnected and then reconnected to port 13, the Spanning Tree Port Configuration screen for Switch S1 changes to show port 6 in the Blocking state (Figure 49).

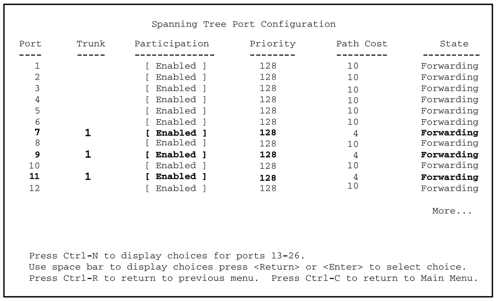
Figure 49 Example 2: detecting a misconfigured port



```
                    Spanning Tree Port Configuration

Port      Trunk     Participation       Priority       Path Cost        State
----      -----     --------------      --------       ---------      ----------
  1                  [ Enabled ]          128             10          Forwarding
  2         1        [ Enabled ]          128              4          Forwarding
  3                  [ Enabled ]          128             10          Forwarding
  4         1        [ Enabled ]          128              4          Forwarding
  5                  [ Enabled ]          128             10          Forwarding
  6         1        [ Enabled ]          128              4          Blocking
  7                  [ Enabled ]          128             10          Forwarding
  8                  [ Enabled ]          128             10          Forwarding
  9                  [ Enabled ]          128             10          Forwarding
 10                  [ Enabled ]          128             10          Forwarding
 11                  [ Enabled ]          128             10          Forwarding
 12                  [ Enabled ]          128             10          Forwarding

                                                                        More...


   Press Ctrl-N to display choices for ports 13-26.
   Use space bar to display choices press <Return> or <Enter> to select choice.
   Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

S1 Port Configuration screen





```
                    Spanning Tree Port Configuration

Port      Trunk     Participation       Priority       Path Cost        State
----      -----     --------------      --------       ---------      ----------
  1                  [ Enabled ]          128             10          Forwarding
  2                  [ Enabled ]          128             10          Forwarding
  3                  [ Enabled ]          128             10          Forwarding
  4                  [ Enabled ]          128             10          Forwarding
  5                  [ Enabled ]          128             10          Forwarding
  6                  [ Enabled ]          128             10          Forwarding
  7         1        [ Enabled ]          128              4          Forwarding
  8                  [ Enabled ]          128             10          Forwarding
  9         1        [ Enabled ]          128              4          Forwarding
 10                  [ Enabled ]          128             10          Forwarding
 11         1        [ Enabled ]          128              4          Forwarding
 12                  [ Enabled ]          128             10          Forwarding

                                                                        More...


   Press Ctrl-N to display choices for ports 13-26.
   Use space bar to display choices press <Return> or <Enter> to select choice.
   Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

S2 Port Configuration screen

9809EA

Additional tips about the MultiLink Trunking feature

When you create a MultiLink Trunk, the individual trunk members (the specific ports that make up the trunk) logically connect and react as a single entity. For example, if you change spanning tree parameters for *any* trunk member, the spanning tree parameters for *all* trunk members change.

All configured trunks are indicated in the Spanning Tree Configuration screen. The Trunk field lists the active trunks, adjacent to the port numbers that correspond to the specific trunk member for that trunk.

When a trunk is active, you can disable spanning tree participation using the Trunk Configuration screen or using the Spanning Tree Configuration screen.

When a trunk is not active, the spanning tree participation setting in the Trunk Configuration screen does not take effect until you set the Trunk Status field to Enabled.

The trunk is also viewed by management stations as a single spanning tree port. The spanning tree port is represented by the trunk member with the lowest port number. For example, if ports 13, 14, 15, and 16 are trunk members of trunk T1, the management station views trunk T1 as spanning tree port 13.

For more information on configuring MultiLink Trunking, VLANs, and spanning tree groups, refer to Chapter 1 for guidelines on configuring spanning tree groups.

For more information about using the MultiLink Trunking feature, see Chapter 3.

See also Appendixes for configuration flowcharts that can help you use this feature.

Port mirroring

You can designate one of your switch ports to monitor traffic on any two specified switch ports (port-based) or to monitor traffic to or from any two specified addresses that the switch has learned (address-based).

Note: A probe device, such as the Nortel Networks StackProbe™ or equivalent, must be connected to the designated monitor port to use this feature (contact your Nortel Networks sales agent for details about the StackProbe).

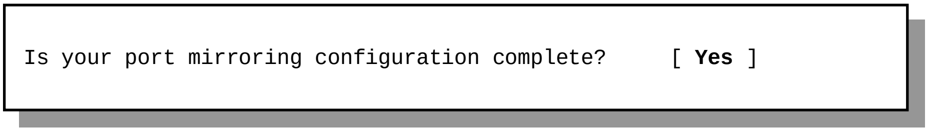
The following sections provide sample configurations for both monitoring modes available with the Port Mirroring feature:

- Port-based mirroring
- Address-based mirroring

A sample Port Mirroring Configuration screen accompanies each network configuration example. Note that the displayed screens do not show all of the screen prompts that precede some actions.

Note: Use the CI menus, the CLI, or the Web-based management system to configure port mirroring.

For example, when you configure a switch for port mirroring or when you modify an existing port mirroring configuration, the new configuration does not take effect until you respond [Yes] to the following screen prompt:



```
Is your port mirroring configuration complete?     [ Yes ]
```

Port-based mirroring configuration

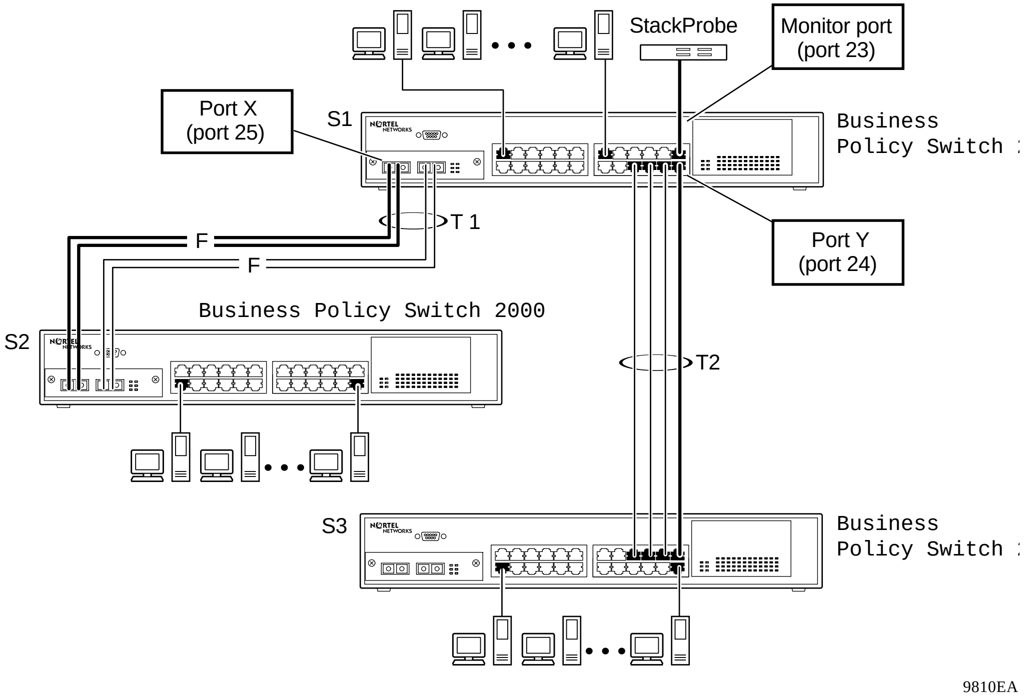
Figure 50 shows an example of a port-based mirroring configuration where port 23 is designated as the monitor port for ports 24 and 25 of Switch S1. Although this example shows ports 24 and 25 monitored by the monitor port (port 23), any of the trunk members of T1 and T2 can also be monitored.

In this example, Figure 50 shows port X and port Y as members of Trunk T1 and Trunk T2. Port X and port Y are not required to always be members of Trunk T1 and Trunk T2.

Note: Trunks cannot be monitored and trunk members cannot be configured as monitor ports (see “MultiLink Trunking configuration rules”).

Figure 50 shows the Port Mirroring Configuration screen setup for this example.

Figure 50 Port-based mirroring configuration example



In the configuration example shown in Figure 50, the designated monitor port (port 23) can be set to monitor traffic in any of the following modes:

- Monitor all traffic received by port X.
- Monitor all traffic transmitted by port X.
- Monitor all traffic received and transmitted by port X.
- Monitor all traffic received by port X or transmitted by port Y.
- Monitor all traffic received by port X (destined to port Y) and then transmitted by port Y.
- Monitor all traffic received/transmitted by port X and transmitted/received by port Y (conversations between port X and port Y).

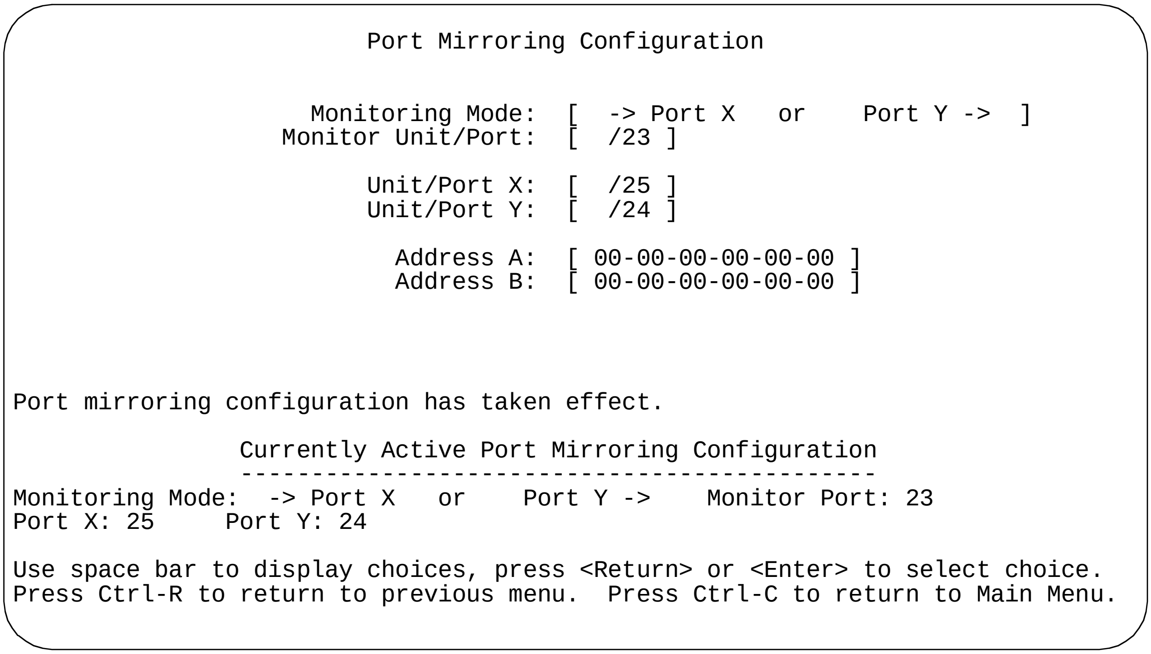
As shown in the Port Mirroring Configuration screen example (Figure 51), port 23 is designated as the Monitor Port for ports 24 and 25 in Switch S1.

Note: The Unit value (in the Unit/Port field) is not configurable when the switch is operating standalone. For detailed information about the Port Mirroring screen fields, see Chapter 3.

The Monitoring Mode field [**-** > Port X or Port Y **-** >] indicates that all traffic received by port X *or* all traffic transmitted by port Y is currently being monitored by the StackProbe attached to Monitor Port 23.

The screen data displayed at the bottom of the screen shows the currently active port mirroring configuration.

Figure 51 Port Mirroring Configuration port-based screen example

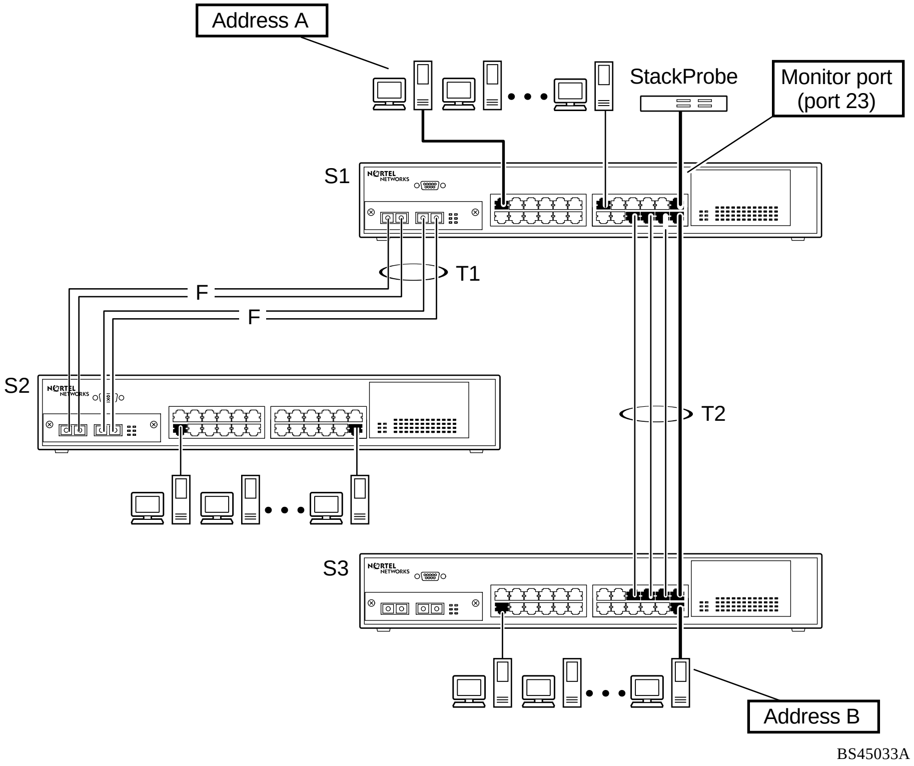


```
                         Port Mirroring Configuration


                     Monitoring Mode:  [  -> Port X   or    Port Y ->  ]
                   Monitor Unit/Port:  [  /23 ]

                         Unit/Port X:  [  /25 ]
                         Unit/Port Y:  [  /24 ]

                           Address A:  [ 00-00-00-00-00-00 ]
                           Address B:  [ 00-00-00-00-00-00 ]




Port mirroring configuration has taken effect.

                Currently Active Port Mirroring Configuration
                ---------------------------------------------
Monitoring Mode:  -> Port X   or    Port Y ->    Monitor Port: 23
Port X: 25     Port Y: 24

Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Address-based mirroring configuration

Figure 52 shows an example of an address-based mirroring configuration where port 23, the designated monitor port for Switch S1, is monitoring traffic occurring between address A and address B.

Figure 52 Address-based mirroring configuration example



In this configuration, the designated monitor port (port 23) can be set to monitor traffic in any of the following modes:

- Monitor all traffic transmitted from address A to any address.
- Monitor all traffic received by address A from any address.
- Monitor all traffic received by or transmitted by address A.
- Monitor all traffic transmitted by address A to address B.

- Monitor all traffic between address A and address B (conversation between the two stations).

Figure 53 shows the Port Mirroring Configuration screen setup for this example.

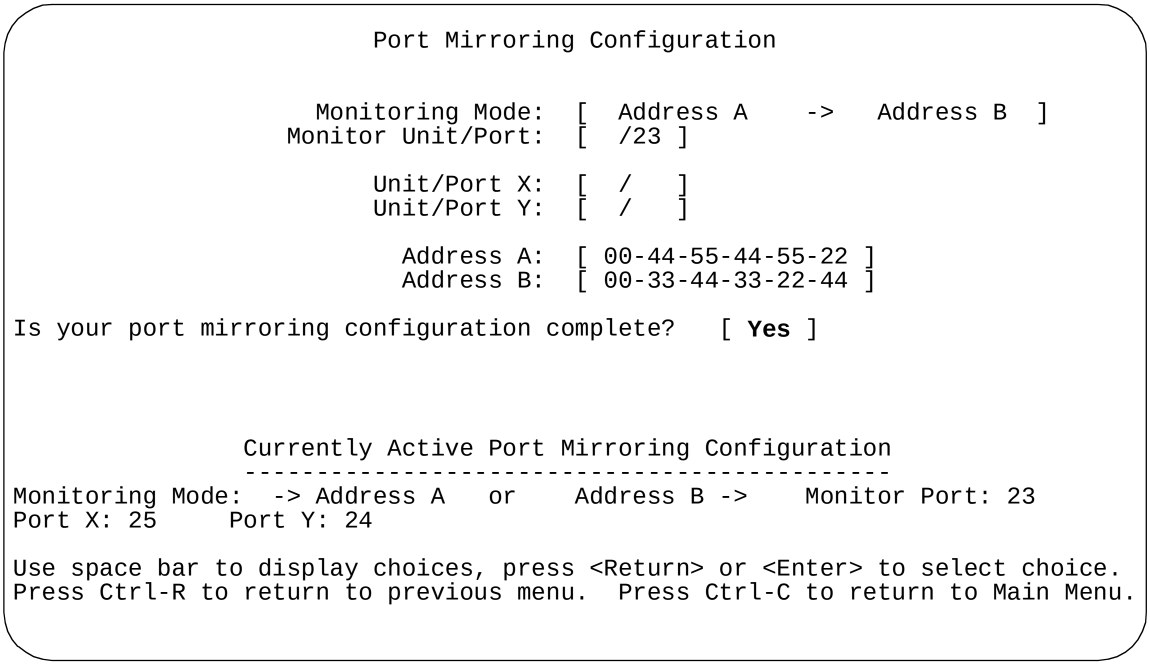
In this example, port 23 becomes the designated Monitor Port for Switch S1 when you press Enter in response to the [Yes] screen prompt.

Note: The screen data displayed at the bottom of the screen changes to show the *new* currently active port mirroring configuration *after* you press Enter.

The Monitoring Mode field [Address A -> Address B] indicates that all traffic transmitted by address A to address B will be monitored by the StackProbe attached to Monitor Port 23.

Note: When you enter MAC addresses in this screen, they are also displayed in the MAC Address Table screen (see Chapter 3).

Figure 53 Port Mirroring Configuration address-based screen example



```
                         Port Mirroring Configuration


                     Monitoring Mode:  [  Address A    ->   Address B  ]
                   Monitor Unit/Port:  [  /23 ]

                         Unit/Port X:  [  /   ]
                         Unit/Port Y:  [  /   ]

                           Address A:  [ 00-44-55-44-55-22 ]
                           Address B:  [ 00-33-44-33-22-44 ]

Is your port mirroring configuration complete?   [ Yes ]




                Currently Active Port Mirroring Configuration
                ---------------------------------------------
Monitoring Mode:  -> Address A   or    Address B ->    Monitor Port: 23
Port X: 25     Port Y: 24

Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Port mirroring configuration rules

The following configuration rules apply to any port mirroring configuration:

- You cannot configure a monitor port as a trunk member or IGMP member.
- A monitor port cannot be used for normal switch functions.
- When you configure a port as a monitor port, the port is automatically disabled from participating in the spanning tree. When you reconfigure the port as a standard switch port (no longer a monitor port), the port is enabled for spanning tree participation.
- When you create a *port-based* port mirroring configuration, be sure that the monitor port and both of the mirrored ports, port X and port Y, have the same configuration. Use the VLAN Configuration screen to configure the VLAN (see Chapter 3).

- VLAN configuration settings for any ports configured for port-based mirroring cannot be changed. Use the Port Mirroring Configuration screen to disable port mirroring (or reconfigure the port mirroring ports), then change the VLAN configuration settings.
- For port-based monitoring of traffic, use one of the following modes for monitoring broadcast, IP Multicast, or unknown DA frames:
  - Monitor all traffic received by port X.
  - Monitor all traffic transmitted by port X.
  - Monitor all traffic received and transmitted by port X.

For more information about using the Port Mirroring feature, see Chapter 3.

See also appendixes for configuration flowcharts that can help you use this feature.

Chapter 3
Using the console interface

This chapter describes how to configure and manage the Business Policy Switch using the menu-driven console interface (CI).

This chapter covers the following topics:

- "Compatibility with BayStack 450 switches," next
- "Accessing the CI menus and screens" on page 164
- "Using the CI menus and screens" on page 165
- "Main Menu" on page 168

Note: If you choose to install the BPS 2000 software version 2.5 that includes support for Secure Shell, the console interface will be unavailable. You must use one of the other management interfaces to configure the Business Policy Switch 2000.

Compatibility with BayStack 450 switches

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

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

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

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

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

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

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

Accessing the CI menus and screens

You can access the CI menus and screens locally through a console terminal attached to your Business Policy Switch, remotely through a dial-up modem connection, or in-band through a Telnet session (see Chapter 1). You can connect your console cable into any unit in a Business Policy Switch-only stack (Pure BPS 2000 Stack mode) for a unified stack interface. For the mixed stack (Hybrid Stack mode) management functions to become fully operational, you must connect your console terminal into a Business Policy Switch port within your mixed stack.

Note: If you have a properly configured BootP server in your network, it detects the IP address; you will not need to configure the IP address.

For information about SNMP, see your network management documentation. You can also manage the BPS 2000 using the command line interface (CLI), the Web-based management system, or Device Manager. For more information on using these management systems, consult the “Related Publications” in the Preface.

Using the CI menus and screens

The CI menus and screens provide options that allow you to configure and manage Business Policy Switches. Help prompts at the bottom of each menu and screen explain how to enter data in the highlighted field and how to navigate the menus and screens.

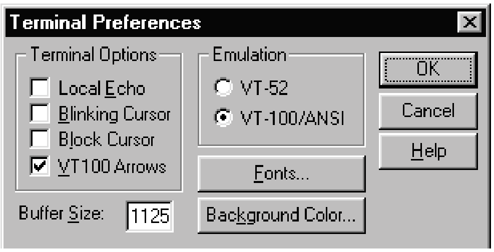
The Console Port default settings are: 9600 baud with eight data bits, one stop bit, and no parity as the communications format, with flow control set to disabled.

Some CI screen options allow you to toggle among several possible values; other options allow you to set or modify a parameter.

Using Telnet to access the CI menus and screens

When you use Telnet to access the CI menus and screens, set the terminal Preferences to VT100 Arrows and VT-100/ANSI and as shown in Figure 54.

Figure 54 Terminal preference settings



Terminal Preferences

Terminal Options

□ Local Echo
□ Blinking Cursor
□ Block Cursor
☑ VT100 Arrows

Emulation

○ VT-52
● VT-100/ANSI

Buffer Size: 1125

Navigating the CI menus and screens

Use the following methods to navigate the CI menus and screens.

To select a menu option:

1. Use the arrow keys to highlight the option name.
2. Press [Enter].

   The option takes effect immediately after you press [Enter].

   Alternatively, you can press the key corresponding to the underlined letter in the option name. For example, to select the Switch Configuration option in the main menu, press the w key. Note that the text characters are not case-sensitive.

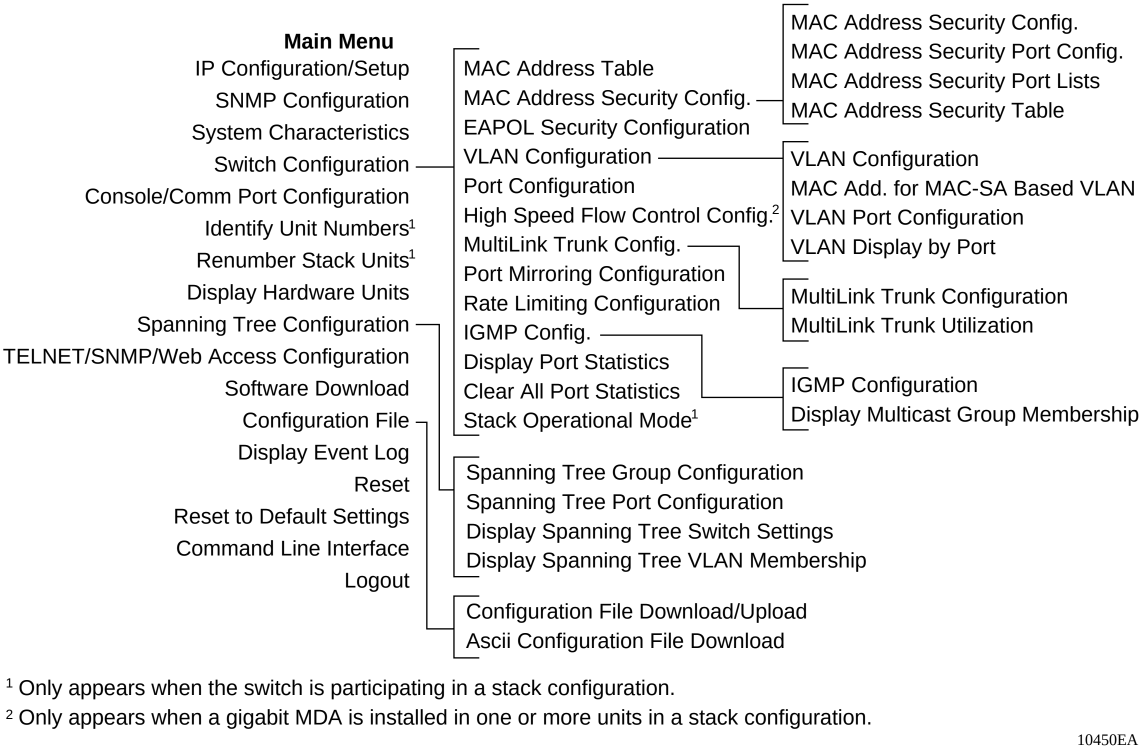
Additional navigation aids follow:

- To toggle between values in a form:
  - Use the spacebar to highlight the value.
  - Press [Enter].
- To clear a string field:
  - Position the cursor in the string field.
  - Press [Ctrl]-K.
- To return to the previous menu, press [Ctrl]-R.
- To go to the next screen in a series, press [Ctrl]-N.
- To return to the main menu at any time, press [Ctrl]-C.
- Press [Backspace] to delete entered text.
- Options that appear in brackets (for example, [Enabled]) are user-settable options.

Screen fields and descriptions

Figure 55 shows a map of the CI screens. The remainder of this chapter describes the CI screens and their fields, beginning with the main menu.

Figure 55 Map of console interface screens


Main Menu
IP Configuration/Setup
SNMP Configuration
System Characteristics
Switch Configuration
Console/Comm Port Configuration
Identify Unit Numbers[1]
Renumber Stack Units[1]
Display Hardware Units
Spanning Tree Configuration
TELNET/SNMP/Web Access Configuration
Software Download
Configuration File
Display Event Log
Reset
Reset to Default Settings
Command Line Interface
Logout
MAC Address Table
MAC Address Security Config.
EAPOL Security Configuration
VLAN Configuration
Port Configuration
High Speed Flow Control Config.[2]
MultiLink Trunk Config.
Port Mirroring Configuration
Rate Limiting Configuration
IGMP Config.
Display Port Statistics
Clear All Port Statistics
Stack Operational Mode[1]
MAC Address Security Config.
MAC Address Security Port Config.
MAC Address Security Port Lists
MAC Address Security Table
VLAN Configuration
MAC Add. for MAC-SA Based VLAN
VLAN Port Configuration
VLAN Display by Port
MultiLink Trunk Configuration
MultiLink Trunk Utilization
IGMP Configuration
Display Multicast Group Membership
Spanning Tree Group Configuration
Spanning Tree Port Configuration
Display Spanning Tree Switch Settings
Display Spanning Tree VLAN Membership
Configuration File Download/Upload
Ascii Configuration File Download
10450EA

[1] Only appears when the switch is participating in a stack configuration.

[2] Only appears when a gigabit MDA is installed in one or more units in a stack configuration.

The CI screens for your specific switch model will show the correct model name in the main menu screen title and the correct number of ports and port types in the Port Configuration screen.

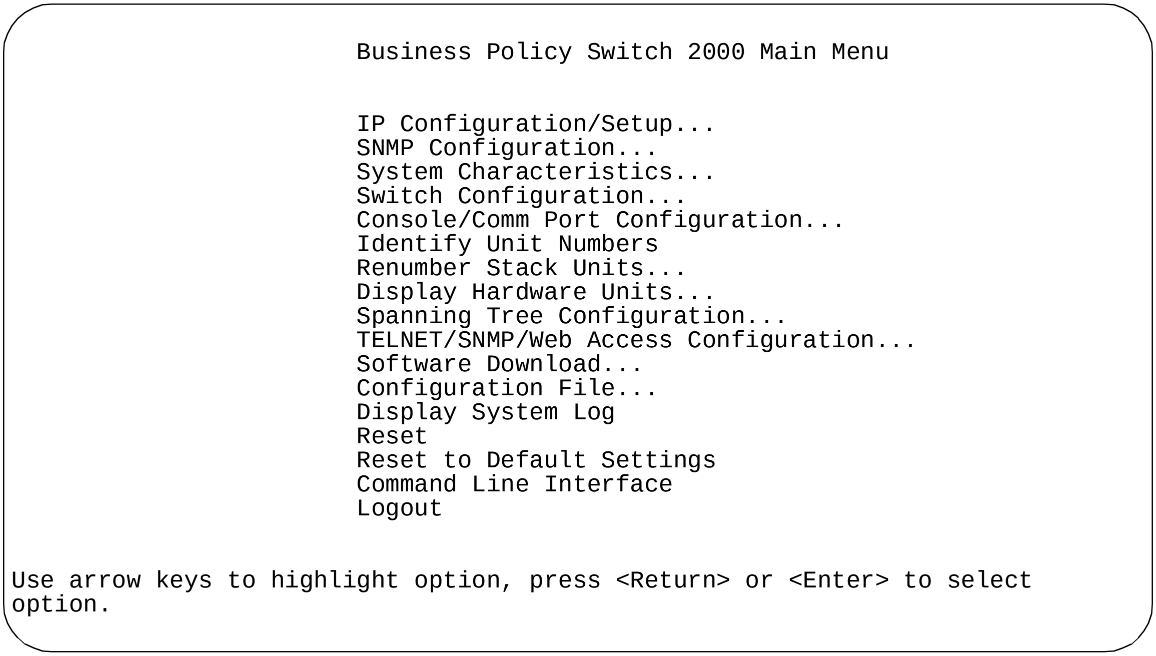
Note: The field values shown in the CI screens in this section are provided as examples only.

Main Menu

This section describes the options available from the CI main menu (Figure 56). The CI screens and submenus for these options are described in the following sections.

Note: Some menu options shown in this main menu example and in other screen examples in this chapter may not appear on your screen, depending on the switch options installed. However, the full menu options are shown in the screen examples and described in the following sections.

Figure 56 Console interface main menu



```
                         Business Policy Switch 2000 Main Menu


                         IP Configuration/Setup...
                         SNMP Configuration...
                         System Characteristics...
                         Switch Configuration...
                         Console/Comm Port Configuration...
                         Identify Unit Numbers
                         Renumber Stack Units...
                         Display Hardware Units...
                         Spanning Tree Configuration...
                         TELNET/SNMP/Web Access Configuration...
                         Software Download...
                         Configuration File...
                         Display System Log
                         Reset
                         Reset to Default Settings
                         Command Line Interface
                         Logout


Use arrow keys to highlight option, press <Return> or <Enter> to select
option.
```

Table 10 describes the CI main menu options

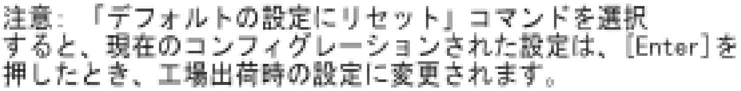
Table 10 Console interface Main Menu options

Option	Description
IP Configuration/ Setup...	Displays the IP Configuration/Setup screen (see "IP Configuration/Setup screen" on page 172). This screen allows you to set or modify IP configuration parameters and to ping other network devices.
SNMP Configuration...	Displays the SNMP Configuration screen (see "SNMP Configuration screen" on page 177). This screen allows you to set or modify the SNMP read-only community and read-write community strings, enable or disable the authentication trap and the link Up/down trap, set the IP address of trap receivers, and set the trap community strings.
System Characteristics...	Displays the System Characteristics screen (see "System Characteristics screen" on page 179). This screen allows you to view switch characteristics, including number of resets, power status, hardware and software version, and MAC address. This screen also contains three user-configurable fields: sysContact, sysName, and sysLocation. When the switch is part of a stack configuration, this screen also displays the base unit identification, the number of units configured in the stack, and the local unit stack number.
Switch Configuration...	Displays the Switch Configuration Menu screen (see "Switch Configuration Menu screen" on page 181). This menu provides the following configuration options: MAC Address Table, MAC Address-Based Security, EAPOL Security Configuration, VLAN Configuration, Port Configuration, High Speed Flow Control, MultiLink Trunk Configuration, Port Mirroring Configuration, Rate Limiting Configuration, IGMP Configuration, Display Port Statistics, Clear All Port Statistics, and Stack Operational Mode.
Console/Comm Port Configuration...	Displays the Console/Comm Port Configuration screen (see "Console/Comm Port Configuration screen" on page 249). This screen allows you to configure and modify the console/Comm port parameters, including the console port speed and password settings for the switch and stack operation.
Spanning Tree Configuration...	Displays the Spanning Tree Configuration Menu (see "Spanning Tree Configuration Menu screen" on page 258). This menu provides the following options: Spanning Tree Group Configuration, Spanning Tree Port Configuration, Display Spanning Tree Switch Settings, and Display Spanning Tree VLAN Membership.
TELNET/SNMP/Web Access Configuration...	Displays the TELNET/SNMP/Web Access Configuration screen (see "TELNET/SNMP/Web Access Configuration screen" on page 272). This screen allows you to set your switch to enable a user at a remote console terminal to communicate with the Business Policy Switch as if the console terminal were directly connected to it. You can have up to four active Telnet sessions running at one time in either a standalone switch or a stack configuration. You can use the Command Line Interface (CLI), DM, or Web-based management system or these menus with a Telnet session. This screen also allows you to set the switch to allow up to 10 IP addresses to access the switch using either these management systems or SNMP access

Table 10 Console interface Main Menu options (continued)

Option	Description
Software Download...	Displays the Software Download screen (see "Software Download screen" on page 275). This screen allows you to revise the Business Policy Switch software image that is located in nonvolatile flash memory (NVRAM).
Configuration File...	Displays the Configuration File Menu screen (see "Configuration File Menu screen" on page 284). This menu provides the following options: Configuration File Download/Upload and ASCII Configuration File Download.
Display System Log	Displays the System Log screen (see "System Log screen" on page 292).
Reset	Resets the switch with the current configuration settings. This option is followed by a screen prompt that precedes the action. Enter Yes to reset the switch; enter No to abort the option: • If the switch is participating in a stack configuration, additional prompts allow you to choose to reset a specific unit in the stack or the entire stack. • When you select this option, the switch resets, runs a self-test, then displays the Nortel Networks logo screen. Press [Ctrl]-Y to access the Business Policy Switch main menu.
Reset to Default Settings	Resets the switch to the factory default configuration settings. This option is followed by a screen prompt that precedes the action. Enter Yes to reset the switch to the factory default configuration settings; enter No to abort the option: • If the switch is participating in a stack configuration, additional prompts allow you to choose to reset a specific unit in the stack or the entire stack. • When you select this option, the switch resets, runs a self-test, then displays the Nortel Networks logo screen. Press [Ctrl]-Y to access the Business Policy Switch main menu. **NOTE**: The following items do NOT reset: Stack Operational Mode, Reset Count, and Reason for Last Reset.
	⛔ **Caution:** If you choose the Reset to Default Settings option, all of your configured settings will be replaced with factory default settings when you press [Enter]
	⛔ **Achtung:** Bei Auswahl des Befehls zur Rücksetzung auf die Standardeinstellungen werden alle von Ihnen konfigurierten Einstellungen durch die werkseitigen Standardeinstellungen ersetzt, wenn Sie die Eingabetaste drücken.
	⛔ **Attention:** Si vous restaurez la configuration usine, votre configuration courante sera remplacée par la configuration usine dès que vous appuierez sur [Entrée].
	⛔ **Precaución:** Si selecciona el comando Restaurar valores predeterminados, todos los valores de configuración se sustituirán por las valores predeterminados en fábrica al pulsar [Intro].

Table 10 Console interface Main Menu options (continued)

Option	Description
	Attenzione: Nel caso in cui si selezioni la reimpostazione dei valori di default, tutte le impostazioni configurate verranno sostituite dai default di fabbrica premendo il tasto [Invio].
	 注意：「デフォルトの設定にリセット」コマンドを選択すると、現在のコンフィグレーションされた設定は、[Enter]を押したとき、工場出荷時の設定に変更されます。
Command Line Interface	Allows a properly authorized user to initiate a CLI management session. Refer to *Reference for the Business Policy Switch 2000 Command Line Interface Release 2.5* for information on using the CLI.
Logout	Allows a user in a Telnet session or a user working at a password-protected console terminal to terminate the session.

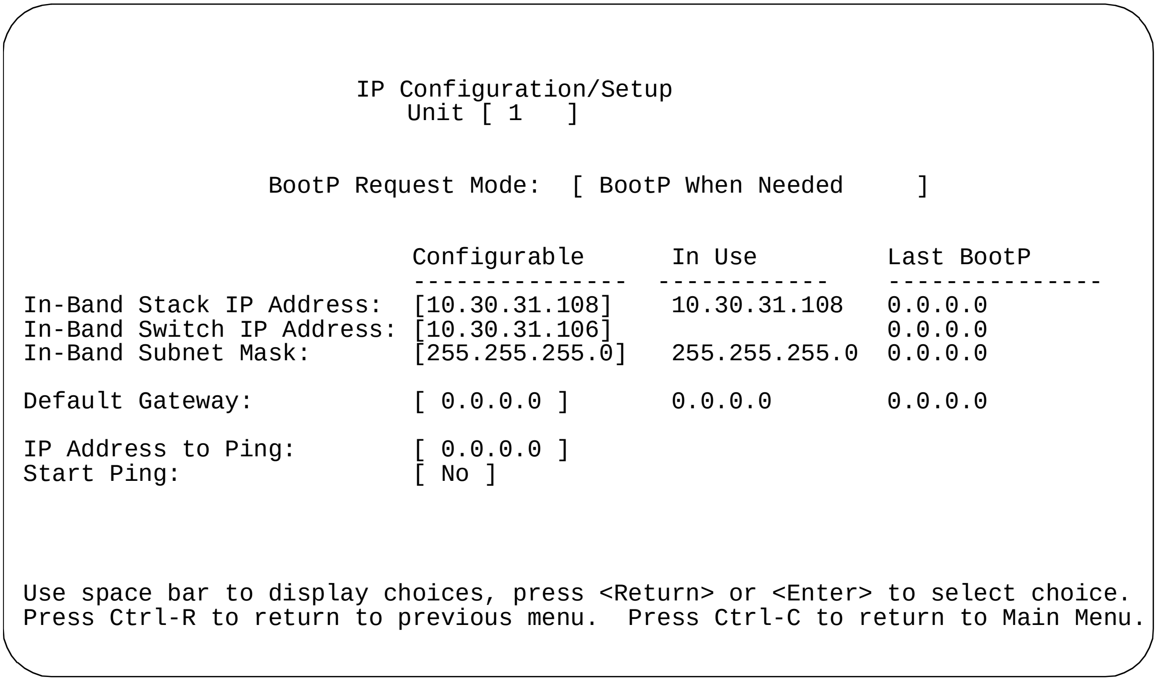
IP Configuration/Setup screen

The IP Configuration/Setup screen (Figure 57) allows you to set or modify the Business Policy Switch IP configuration parameters. Data that you enter in the user-configurable fields takes effect as soon as you press [Enter].

To open the IP Configuration/Setup screen:

➨ Choose IP Configuration/Setup (or press i) from the main menu.

Figure 57 IP Configuration/Setup screen



```
                       IP Configuration/Setup
                           Unit [ 1   ]


                 BootP Request Mode:  [ BootP When Needed     ]


                           Configurable      In Use          Last BootP
                           ---------------  ------------    ---------------
In-Band Stack IP Address:  [10.30.31.108]    10.30.31.108    0.0.0.0
In-Band Switch IP Address: [10.30.31.106]                    0.0.0.0
In-Band Subnet Mask:       [255.255.255.0]   255.255.255.0   0.0.0.0

Default Gateway:           [ 0.0.0.0 ]       0.0.0.0         0.0.0.0

IP Address to Ping:        [ 0.0.0.0 ]
Start Ping:                [ No ]




Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 11 describes the IP Configuration/Setup screen fields.

Note: The read-only fields in this screen are updated based on the BootP mode specified in the BootP Request Mode field. (See “Choosing a BootP request mode” on page 174 for more information.)

Table 11 IP Configuration/Setup screen fields

Field	**Description**
Unit	To view or configure an IP address for a specific unit, choose that unit number.
BootP Request Mode	One of four modes of operation for BootP. (See "Choosing a BootP request mode" on page 174 for details about the four modes.) Default Value — BootP Disabled Range — BootP Disabled, BootP When Needed, BootP Always, BootP or Last Address
Configurable	Column header for the user-configurable IP configuration fields in this screen.
In Use	Column header for the read-only fields in this screen. The read-only data displayed in this column represents IP configuration that is currently in use.
Last BootP	Column header for the read-only fields in this screen. The read-only data displayed in this column represents IP configuration obtained from the last BootP reply received.
In-Band Stack IP Address	The in-band *stack* IP address field. This field is not required for the operation of the standalone switch. Default Value — 0.0.0.0 (no IP address assigned) Range — Four-octet dotted-decimal notation, where each octet is represented as a decimal value, between 0 and 255, separated by a decimal point
In-Band Switch IP Address	The in-band IP address of the switch. This field is not required for the operation of the stack. This field *cannot* use the same IP address used for the stack. Default Value — 0.0.0.0 (no IP address assigned) Range — Four-octet dotted-decimal notation, where each octet is represented as a decimal value, between 0 and 255, separated by a decimal point **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.

Table 11 IP Configuration/Setup screen fields (continued)

Field	Description	
In-Band Subnet Mask	The subnet address mask associated with the in-band IP address shown on the screen (see In-Band Switch IP Address field). Network routers use the subnet mask to determine the network or subnet address portion of a host's IP address. The bits in the IP address that contain the network address (including the subnet) are set to 1 in the address mask, and the bits that contain the host identifier are set to 0.	
	Default Value	0.0.0.0 (no subnet mask assigned)
	Range	Four-octet dotted-decimal notation, where each octet is represented as a decimal value, between 0 and 255, separated by a decimal point
Default Gateway	The IP address of the default gateway.	
	Default Value	0.0.0.0 (no IP address assigned)
	Range	Four-octet dotted-decimal notation, where each octet is represented as a decimal value, between 0 and 255, separated by a decimal point
IP Address to Ping	The IP address of the network device you want to ping. This field is not required for the operation of the stack. This field *cannot* use the same IP address used for the stack.	
	Default Value	0.0.0.0 (no IP address assigned)
	Range	Four-octet dotted-decimal notation, where each octet is represented as a decimal value, between 0 and 255, separated by a decimal point
Start Ping	Pings the selected network device when you choose Yes.	
	Default Value	No
	Range	No, Yes

Choosing a BootP request mode

The BootP Request Mode field in the IP Configuration screen allows you to choose which method the switch uses to broadcast BootP requests:

- BootP When Needed
- BootP Always
- BootP Disabled

- BootP or Last Address

Note: Whenever the switch is broadcasting BootP requests, the BootP process will eventually time out if a reply is not received. 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
- BootP or Last Address.

BootP When Needed

Allows the switch to request an IP address if one has not already been set from the console terminal. When selected, this mode operates as follows:

- When the IP data is entered from the console terminal, the data becomes the in-use address of the switch and BootP requests are not broadcast. The switch can be managed using this in-band IP address.
- When the in-band IP address is not set from the console terminal, the switch broadcasts BootP requests until it receives a BootP reply containing an IP address. If the switch does not receive a BootP reply that contains an IP address, the switch cannot be managed in-band.

If an IP address is *not* currently in use, these actions take effect immediately. If an IP address *is* currently in use, these actions take effect only after the switch is reset or power cycled.

BootP Always

Allows the switch to be managed only when configured with the IP address obtained from the BootP server. When selected, this mode operates as follows:

- The switch continues to broadcast BootP requests, regardless of whether an in-band IP address is set from the console terminal.
- If the switch receives a BootP reply that contains an in-band IP address, the switch uses this new in-band IP address.
- If the switch does not receive a BootP reply, the switch cannot be managed using the in-band IP address set from the console terminal.

If an IP address is *not* currently in use, these actions take effect immediately. If an IP address *is* currently in use, these actions take effect only after the switch is reset or power cycled.

BootP Disabled

Allows the switch to be managed only by using the IP address set from the console terminal. When selected, this mode operates as follows:

- The switch does not broadcast BootP requests, regardless of whether an IP address is set from the console terminal.
- The switch can be managed only by using the in-band switch IP address set from the console terminal.

These actions take effect after the switch is reset or power cycled, even if an IP address is not currently in use.

BootP or Last Address

Allows the switch to be managed even if a BootP server is not reachable. When selected, this mode operates as follows:

- When the IP data is entered from the console terminal, the data becomes the in-band address of the switch and BootP requests are not broadcast. The switch can be managed using this in-band IP address.
- When the in-band IP address is not set from the console terminal, the switch broadcasts BootP requests until it receives a BootP reply containing an in-band IP address. If the switch does not receive a BootP reply that contains an in-band IP address within 10 minutes, the switch uses the last in-band IP address it received from a BootP server. This IP information is displayed in the Last BootP column.

If an IP address is *not* currently in use, these actions take effect immediately. If an IP address *is* currently in use, these actions take effect only after the switch is reset or power cycled.

With software 1.1 and a stack consisting *only* of BPS 2000 switches (Pure BPS 2000 Stack mode), you can perform BootP using the MAC address of the base unit.

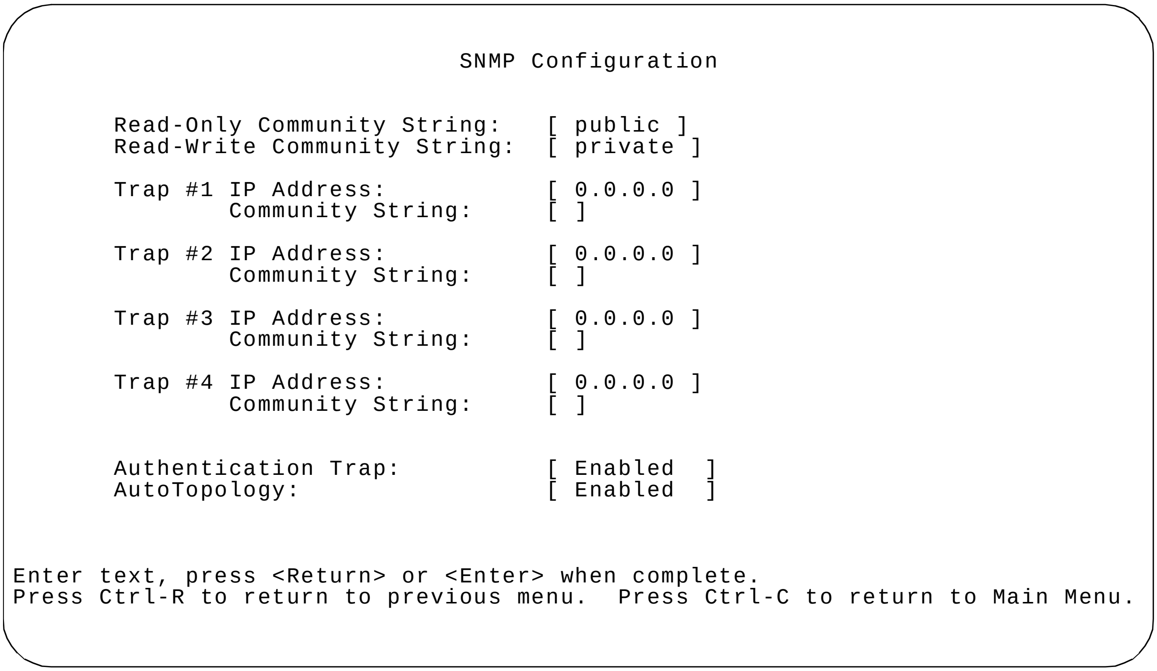
SNMP Configuration screen

The SNMP Configuration screen (Figure 58) allows you to set or modify the SNMP configuration parameters.

To open the SNMP Configuration screen:

➨ Choose SNMP Configuration (or press m) from the main menu.

Figure 58 SNMP Configuration screen



```
                               SNMP Configuration

       Read-Only Community String:   [ public ]
       Read-Write Community String:  [ private ]

       Trap #1 IP Address:           [ 0.0.0.0 ]
               Community String:     [ ]

       Trap #2 IP Address:           [ 0.0.0.0 ]
               Community String:     [ ]

       Trap #3 IP Address:           [ 0.0.0.0 ]
               Community String:     [ ]

       Trap #4 IP Address:           [ 0.0.0.0 ]
               Community String:     [ ]


       Authentication Trap:          [ Enabled  ]
       AutoTopology:                 [ Enabled  ]


Enter text, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 12 describes the SNMP Configuration screen fields.

Table 12 SNMP Configuration screen fields

Field	Description
Read-Only Community String	The community string used for in-band read-only SNMP operations. Default Value public Range Any ASCII string of up to 32 printable characters
Read-Write Community String	The community string used for in-band read-write SNMP operations. Default Value private Range Any ASCII string of up to 32 printable characters
Trap #1 IP Address*	Number one of four trap IP addresses. Successive trap IP address fields are numbered 2, 3, and 4. Each trap address has an associated community string (see Community String). Default Value 0.0.0.0 (no IP address assigned) Range Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
Community String	The community string associated with one of the four trap IP addresses (see Trap #1 IP Address). Default Value Zero-length string Range Any ASCII string of up to 32 printable characters
Authentication Trap	Determines whether a trap will be sent when there is an SNMP authentication failure. Default Value Enabled Range Enabled, Disabled
Autotopology	Allows you to enable or disable the switch participation in Autotopology, which allows network topology mapping of other switches in your network. Default Value Enabled Range Disabled

* The Trap IP Address and Community String fields can be set using a MIB table (in a Nortel Networks proprietary MIB). The status of the row in the MIB table can be set to Ignore. If the row status is set to Ignore, the fields appear to be set when viewed from the console terminal; however, no traps will be sent to that address until the row status is set to Valid.

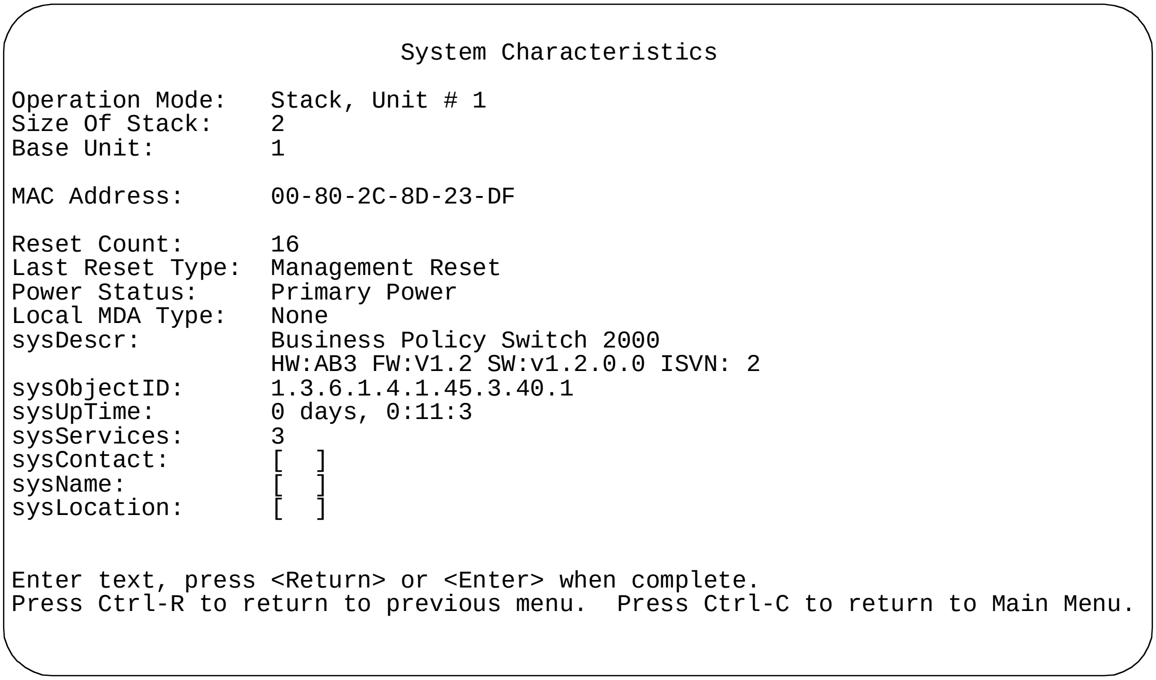
System Characteristics screen

The System Characteristics screen (Figure 59) allows you to view system characteristics and contains three user-configurable fields: sysContact, sysName, and sysLocation.

To open the System Characteristics screen:

➨ Choose System Characteristics (or press s) from the main menu.

Figure 59 System Characteristics screen



```
                              System Characteristics

Operation Mode:   Stack, Unit # 1
Size Of Stack:    2
Base Unit:        1

MAC Address:      00-80-2C-8D-23-DF

Reset Count:      16
Last Reset Type:  Management Reset
Power Status:     Primary Power
Local MDA Type:   None
sysDescr:         Business Policy Switch 2000
                  HW:AB3 FW:V1.2 SW:v1.2.0.0 ISVN: 2
sysObjectID:      1.3.6.1.4.1.45.3.40.1
sysUpTime:        0 days, 0:11:3
sysServices:      3
sysContact:       [  ]
sysName:          [  ]
sysLocation:      [  ]


Enter text, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 13 describes the System Characteristics screen fields.

Table 13 System Characteristics screen fields

Field	Description
Operation Mode	Read-only field that indicates the operation mode of the unit, for example: • When the unit is part of a stack configuration, the (read-only) field indicates the unit is operational in a stack, and lists the current unit number of this switch. In this example (see Figure 59 on page 179), the current unit number is Unit 2. • When the unit is *not* part of a stack configuration (operating standalone), the read-only field indicates the unit is operating as a switch. When in this operation mode, the Size of Stack and Base Unit fields (see following description) do not appear.
Size of Stack	This read-only field only appears when the switch is participating in a stack configuration. This field indicates the number of units configured in the stack configuration (1 to 8 units maximum).
Base Unit	This read-only field only appears when the switch is participating in a stack configuration. This field indicates the unit number of the switch that is currently operating as the base unit.
MAC Address	The MAC address of the switch or, when the switch is participating in a stack configuration, the MAC address of the stack configuration.
Reset Count	A read-only field that indicates the number of resets since the operational firmware was first loaded on the switch. Default Value 1 Range 0 to 2^{32} -1 (4,294,967,295)
Last Reset Type	A read-only field that indicates the last type of reset. Default Value Power Cycle Range Power Cycle, Software Download, Management Reset, Management Factory Reset
Power Status	A read-only field that indicates the current power source (primary, RPSU, or both). Default Value Primary Power Range Primary Power, Redundant Power, Primary and Redundant Power
Local MDA Type	A read-only field that indicates the MDA type that is configured in this unit.
sysDescr	A read-only field that specifies hardware and software versions.
sysObjectID	A read-only field that provides a unique identification of the switch, which contains the vendor's private enterprise number.
sysUpTime	A read-only field that shows the length of time since the last reset. Note that this field is updated when the screen is redisplayed.
sysServices	A read-only field that indicates the switch's physical and data link layer functionality.

Table 13 System Characteristics screen fields (continued)

Field	**Description**	
sysContact	The name and phone number of the person responsible for the switch.	
	Default Value	Zero-length string
	Range	Any ASCII string of up to 56 printable characters*
sysName	A name that uniquely identifies the switch.	
	Default Value	Zero-length string
	Range	Any ASCII string of up to 56 printable characters*
sysLocation	The physical location of the switch.	
	Default Value	Zero-length string
	Range	Any ASCII string of up to 56 printable characters

* Although this field can be set to up to 255 characters from a Network Management Station (NMS), only 56 characters are displayed on the console terminal.

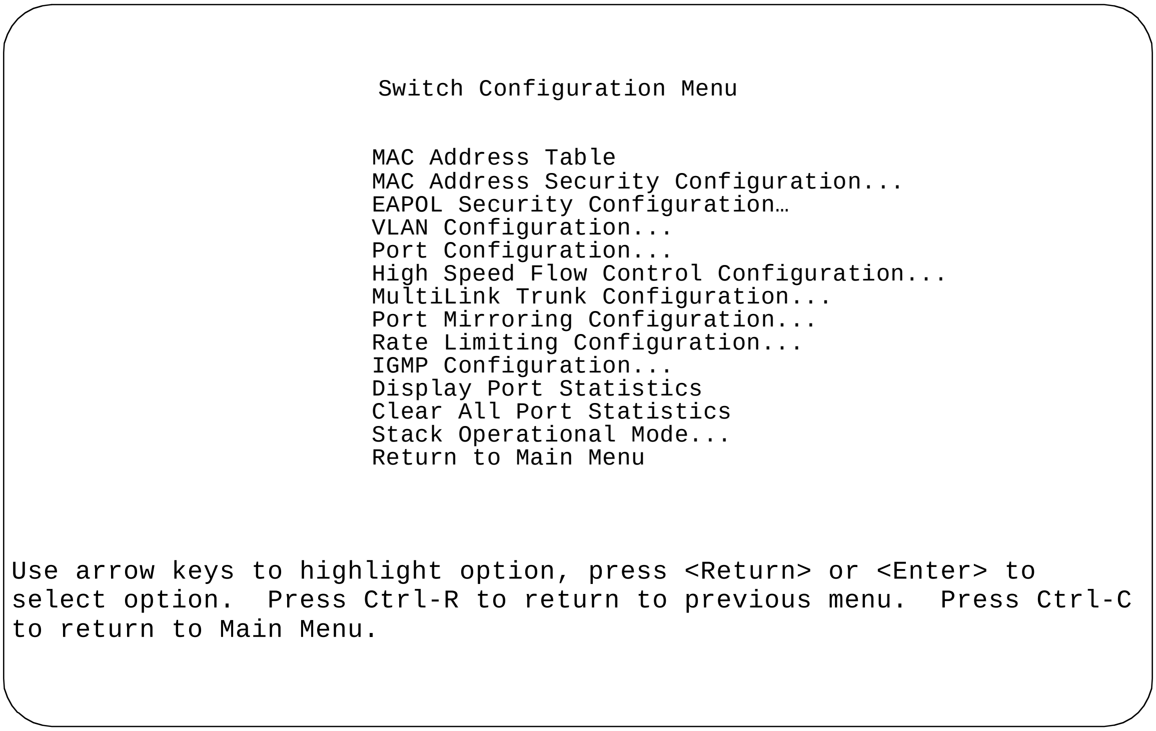
Switch Configuration Menu screen

The Switch Configuration Menu screen (Figure 60) allows you to set or modify your switch configuration.

Note: The High Speed Flow Control Configuration option only appears when an optional Gigabit MDA is installed.

Choose Switch Configuration (or press w) from the main menu to open the Switch Configuration Menu screen (Table 14).

Figure 60 Switch Configuration Menu screen



```
                          Switch Configuration Menu


                         MAC Address Table
                         MAC Address Security Configuration...
                         EAPOL Security Configuration…
                         VLAN Configuration...
                         Port Configuration...
                         High Speed Flow Control Configuration...
                         MultiLink Trunk Configuration...
                         Port Mirroring Configuration...
                         Rate Limiting Configuration...
                         IGMP Configuration...
                         Display Port Statistics
                         Clear All Port Statistics
                         Stack Operational Mode...
                         Return to Main Menu



Use arrow keys to highlight option, press <Return> or <Enter> to
select option.  Press Ctrl-R to return to previous menu.  Press Ctrl-C
to return to Main Menu.
```

Table 14 describes the Switch Configuration Menu screen options.

Table 14 Switch Configuration Menu screen options

Option	Description
MAC Address Table	Displays the MAC Address Table screen (see "MAC Address Table screen" on page 184). This screen allows you to view all MAC addresses and their associated port or trunk that the switch has learned, or to search for a particular MAC address (to see if the switch has learned the address).
MAC Address Security Configuration...	Displays the MAC Address Security Configuration menu (see "MAC Address Security Configuration Menu screen on page 186). This screen allows you to set up the MAC address security feature and provides the following options: MAC Address Security Configuration, MAC Address Security Port Configuration, MAC Address Security Port Lists, and MAC Address Security Table. This menu allows you to enable and disable security features on the port and trunk levels.

Table 14 Switch Configuration Menu screen options (continued)

Option	Description
EAPOL Security Configuration...	Displays the EAPOL Security Configuration menu (see "EAPOL Security Configuration screen" on page 201). This screen allows you to set up Extensible Authentication Protocol over LAN (EAPOL)-based security.
VLAN Configuration...	Displays the VLAN Configuration Menu (see "VLAN Configuration Menu screen" on page 205). This menu provides the following options: VLAN Configuration, MAC Addresses for MAC-SA Based VLAN, VLAN Port Configuration, and VLAN Display by Port. This menu allows you to create and modify VLANs and to enable the automatic PVID feature.
Port Configuration...	Displays the Port Configuration screen (see "Port Configuration screen" on page 219). This screen allows you to configure a specific switch port, all switch ports or, when in a stack configuration, all stack ports.
High Speed Flow Control Configuration...	Only appears when an optional Gigabit MDA is installed in the Uplink Module slot. When the Gigabit MDA is installed, selecting this option displays the High Speed Flow Control Configuration screen (see "High Speed Flow Control Configuration screen" on page 222).
MultiLink Trunk Configuration...	Displays the MultiLink Trunk Configuration Menu (see "MultiLink Trunk Configuration Menu screen"on page 225). This menu provides the following options: MultiLink Trunk Configuration and MultiLink Trunk Utilization. This menu allows you to create and modify trunks, and to monitor the bandwidth utilization of configured trunks.
Port Mirroring Configuration...	Displays the Port Mirroring Configuration screen (see "Port Mirroring Configuration screen"on page 231). This screen allows you to designate a single switch port as a traffic monitor for up to two specified ports or addresses.
Rate Limiting Configuration...	Displays the Rate Limiting Configuration screen (see "Rate Limiting Configuration screen"on page 234). This screen allows you to limit the forwarding rate of broadcast and multicast packets.
IGMP Configuration...	Displays the IGMP Configuration screen (see "IGMP Configuration screen" on page 239). This screen allows you to optimize multicast traffic by setting up IGMP port memberships that filter multicast on a per port basis (see Chapter 1 for more information about this feature).
Display Port Statistics	Displays the Port Statistics screen (see "Port Statistics screen" on page 244). This screen allows you to view detailed information about any switch port.

Table 14 Switch Configuration Menu screen options (continued)

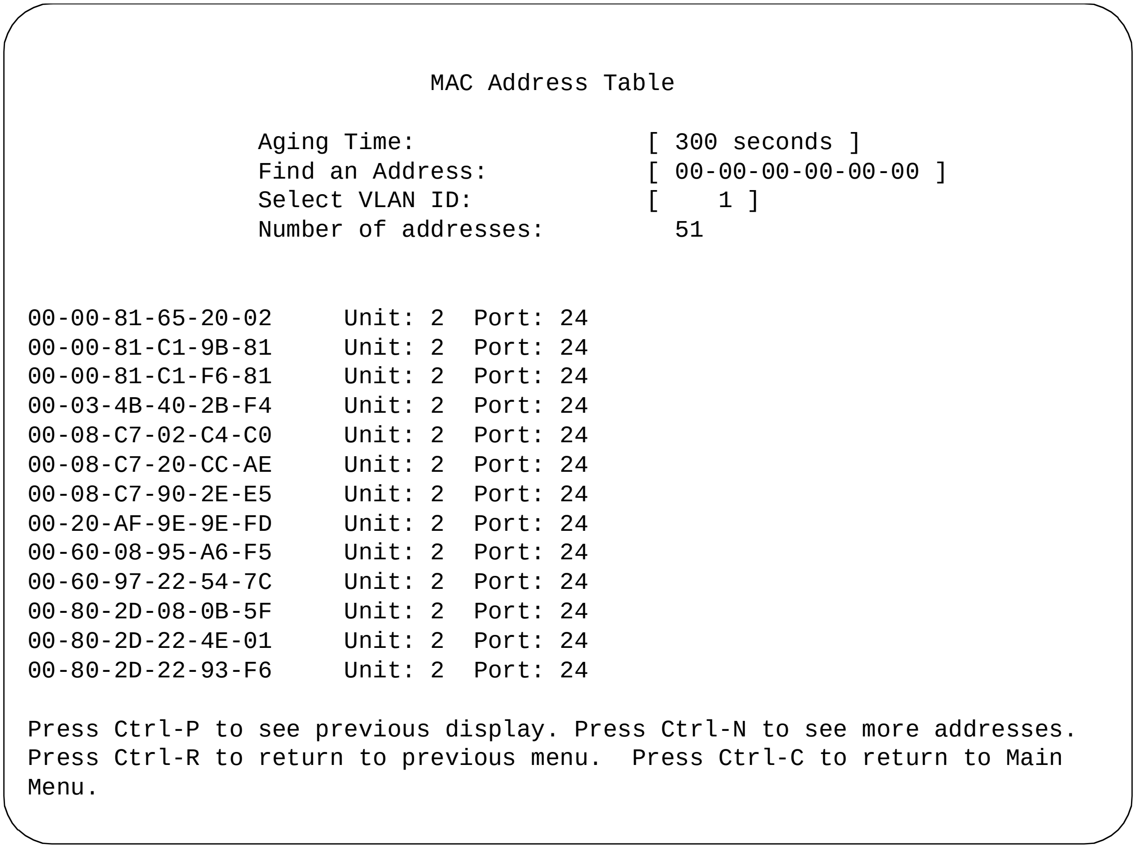
Option	Description
Clear All Port Statistics	Allows you to clear all port statistics. This option is followed by screen prompts that precede a choice of the actions: • If the switch is operating *standalone*, choose one of the following: • Yes, to clear all port statistics for all switch ports • No, to abort the option • If the switch is *participating in a stack configuration*, choose one of the following: • Clear all port statistics for a specific unit in the stack • Clear all port statistics for the entire stack • No, to abort the option
Stack Operational Mode	Displays the stack operational mode screen, which provides information about the types of switches in your stack. See "Stack Operational Mode screen" on page 248 for details. • The Pure BPS 2000 Stack Mode field indicates that your stack contains only Business Policy Switches. • The Hybrid Stack Mode field indicates that your stack consists of switches other than, or in addition to, Business Policy Switch(es).

MAC Address Table screen

The MAC Address Table screen (Figure 61) allows you to view MAC addresses that the switch has discovered or to search for a specific MAC address.

➨ Choose MAC Address Table (or press m) from the Switch Configuration Menu screen to open the MAC Address Table screen (Figure 61).

Figure 61 MAC Address Table Screen



```
                            MAC Address Table

                Aging Time:                    [ 300 seconds ]
                Find an Address:               [ 00-00-00-00-00-00 ]
                Select VLAN ID:                [     1 ]
                Number of addresses:             51


00-00-81-65-20-02     Unit: 2  Port: 24
00-00-81-C1-9B-81     Unit: 2  Port: 24
00-00-81-C1-F6-81     Unit: 2  Port: 24
00-03-4B-40-2B-F4     Unit: 2  Port: 24
00-08-C7-02-C4-C0     Unit: 2  Port: 24
00-08-C7-20-CC-AE     Unit: 2  Port: 24
00-08-C7-90-2E-E5     Unit: 2  Port: 24
00-20-AF-9E-9E-FD     Unit: 2  Port: 24
00-60-08-95-A6-F5     Unit: 2  Port: 24
00-60-97-22-54-7C     Unit: 2  Port: 24
00-80-2D-08-0B-5F     Unit: 2  Port: 24
00-80-2D-22-4E-01     Unit: 2  Port: 24
00-80-2D-22-93-F6     Unit: 2  Port: 24

Press Ctrl-P to see previous display. Press Ctrl-N to see more addresses.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main
Menu.
```

Table 15 describes the MAC Address Table screen fields.

Table 15 MAC Address Table screen fields

Field	Description
Aging Time	Specifies how long a learned MAC address remains in the switch's forwarding database. If an entry is inactive for a period of time that exceeds the specified aging time, the address is removed. Default Value 300 seconds Range 10 to 1,000,000 seconds

Table 15 MAC Address Table screen fields (continued)

Field	Description
Find an Address	Allows the user to search for a specific MAC address. Default Value 00-00-00-00-00-00 (no MAC address assigned) Range 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF
Select VLAN ID	Enter the VLAN ID number you want to display the MAC addresses for. Default Value 1 Range 1-4094
Number of addresses	Displays the total number of MAC addresses currently learned by the specified VLAN. This number updates dynamically when you press [Ctrl]-P or [Ctrl]-N to scroll through the list.

MAC Address Security Configuration Menu screen

The MAC Address Security Configuration Menu screen (Figure 62) allows you to specify a range of system responses to unauthorized network access to your switch. The system response can range from sending a trap to disabling the port. The network access control is based on the MAC addresses of the authorized stations. You can specify a list of up to 448 MAC addresses that are authorized to access the switch. You can also specify the ports that each MAC address is allowed to access. The options for allowed port access include: NONE, ALL, and single or multiple ports that are specified in a list, for example, 1-4, 6, 9, etc. You must also include the MAC address of any router connected to any secure ports.

In addition, with software version 2.5, you can configure the BPS 2000 to drop all packets with specified MAC destination addresses (DA). You can enter up to 10 specific MAC DAs you want filtered. The packet with the specified MAC DA will be dropped regardless of the ingress port, source address (SA) intrusion, or VLAN membership.

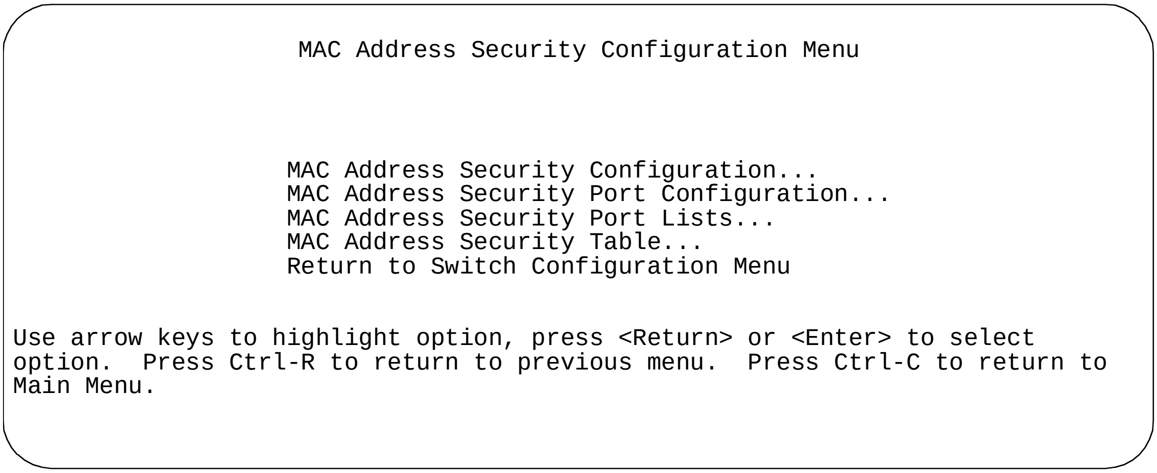
Note: You must use either the Web-based management system or the CLI to configure MAC DA filtering. Also, this feature is available only on BPS2000 software version 2.0 or higher.

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

To open the MAC Address Security Configuration screen:

➨ Choose MAC Address Security Configuration from the Switch Configuration Menu.

Figure 62 MAC Address Security Configuration Menu screen



```
                    MAC Address Security Configuration Menu



                   MAC Address Security Configuration...
                   MAC Address Security Port Configuration...
                   MAC Address Security Port Lists...
                   MAC Address Security Table...
                   Return to Switch Configuration Menu


Use arrow keys to highlight option, press <Return> or <Enter> to select
option.  Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to
Main Menu.
```

Table 16 describes the MAC Address Security Configuration Menu options.

Table 16 MAC Address Security Configuration Menu Options

Option	**Description**
MAC Address Security Configuration...	Displays the MAC Address Security Configuration screen (see "MAC Address Security Configuration Menu screen" on page 186). This screen allows you to Enable or Disable the MAC Address Security feature.
MAC Address Security Port Configuration...	Displays the MAC Address Security Port Configuration screen (see "MAC Address Security Port Configuration screen" on page 191"). This screen allows you to Enable or Disable MAC Security for each port.

Table 16 MAC Address Security Configuration Menu Options (continued)

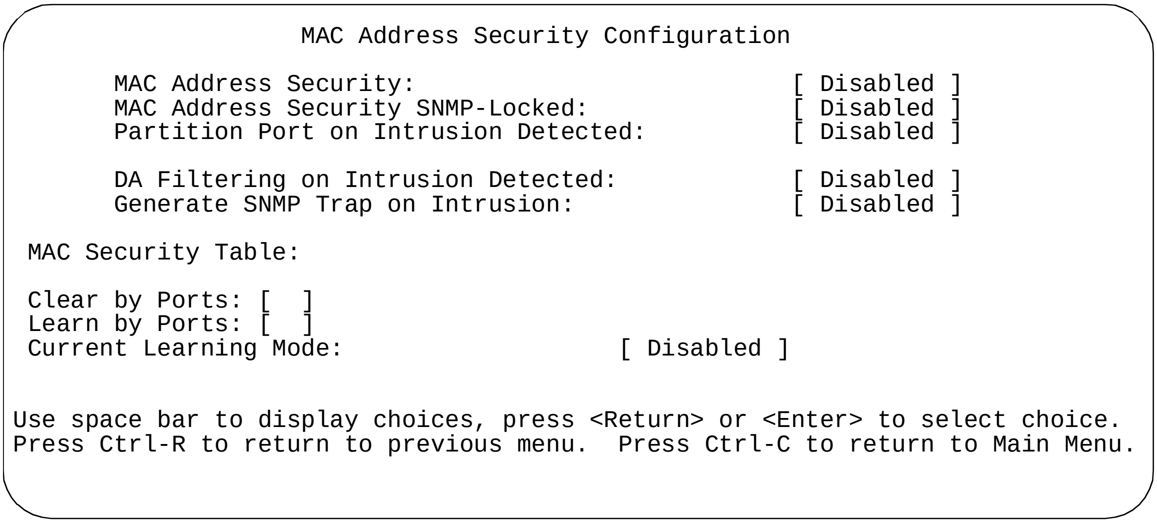
Option	Description
MAC Address Security Port Lists...	Displays the MAC Address Security Port Lists screen (see "MAC Address Security Port Lists screens" on page 194). This screen allows you to create port lists that can be used as an *allowed source port list* for a MAC address in the MAC Address Security Table screen.
MAC Address Security Table...	Displays the MAC Address Security Table screen (see "MAC Address Security Table screens" on page 199). This screen allows you to specify the MAC addresses that are allowed to access the switch.

MAC Address Security Configuration screen

The MAC Address Security Configuration screen (Figure 63) allows you to enable or disable the MAC address security feature and to specify the appropriate system responses to any unauthorized network access to your switch.

➨ Choose MAC Address Security Configuration from the MAC Address Security Configuration Menu to open the MAC Address Security Configuration screen.

Figure 63 MAC Address Security Configuration screen



```
                    MAC Address Security Configuration

       MAC Address Security:                          [ Disabled ]
       MAC Address Security SNMP-Locked:              [ Disabled ]
       Partition Port on Intrusion Detected:          [ Disabled ]

       DA Filtering on Intrusion Detected:            [ Disabled ]
       Generate SNMP Trap on Intrusion:               [ Disabled ]

 MAC Security Table:

 Clear by Ports: [  ]
 Learn by Ports: [  ]
 Current Learning Mode:                   [ Disabled ]


Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 17 describes the MAC Address Security Configuration screen fields.

Table 17 MAC Address Security Configuration fields

Field	Description
MAC Address Security	When this field is set to enabled, the software checks source MAC addresses of packets that arrive on secure ports against MAC addresses listed in the MAC Address Security Table for allowed membership. If the software detects a source MAC address that is not an allowed member, the software registers a MAC intrusion event. Default Disabled Range Disabled, Enabled
MAC Address Security SNMP-Locked	When this field is set to enabled, the MAC address security screens cannot be modified using SNMP (SNMP includes the DM management system). Default Disabled Range Disabled, Enabled
Partition Port on Intrusion Detected	This field value determines how the switch reacts to an intrusion event. When an intrusion even is detected (see MAC Address Security field description) the specified switch port is set to Disabled (partitioned from other switch ports). When the field is set to: • Disabled - the port remains enabled, even if an intrusion event is detected. • Enabled - the port becomes disabled, then automatically resets to enabled depending on the value set in the Partition Time field. • Forever - the port becomes disabled, and remains disabled (partitioned). The Partition Time field cannot be used to automatically to reset the port to Enabled if you set this field to Forever. You can always manually set the port's status field to enabled using the Port Configuration screen (see "Port Configuration screen" on page 219). Default Disabled Range Disabled, Enabled, Forever
Partition Time	This field appears only when the Partition Port on Intrusion Detected field is set to enabled. This field determines the length of time a partitioned port remains disabled. This field is not operational when the Partition Port on Intrusion Detected field is set to Forever. Default 1 second (the value 0 indicates forever) Range 0-65536 seconds

Table 17 MAC Address Security Configuration fields (continued)

Field	Description
DA Filtering on Intrusion Detected	When set to enabled, this field isolates the intruding node by filtering (discarding) packets sent to that MAC address. Default Disabled Range Disabled, Enabled
Generate SNMP Trap on Intrusion	When set to enabled and a MAC intrusion event is detected, the software issues an SNMP trap message to all registered SNMP trap addresses (see "SNMP Configuration screen" on page 177). Default Disabled Range Disabled, Enabled
Clear by Ports	This field clears the specified port (or ports) that are listed in the Allowed Source Port(s) field of the MAC Address Security Table screen (see "MAC Address Security Table screens" on page 199). When you specify a port (or ports) to be cleared using this field, the specific port (or ports) will be cleared for each of the entries listed in the MAC Address Security Table. If you totally clear the allowed Source Port(s) field (leaving a blank field) for an entry, the associated MAC address for that entry is also cleared. Default NONE Range NONE, ALL, a port number list (for example, 1/1, 2/6, etc.)
Learn by Ports	All source MAC addresses of any packets received on the specified port (or ports) are added to the MAC Security Table when the Current Learning Mode field is set to Enabled. You cannot include any of the port values you have chosen for the secure ports field. Default NONE Range NONE, ALL, a port number list (for example, 1/1, 2/6, etc.)
Current Learning Mode	Indicates the current learning mode for the switch ports. When this field is set to Learning in Progress, all source MAC addresses of any packets received on the specified port (or ports) are added to the MAC Security Table (maximum of 448 MAC address entries allowed). If you exceed the limit of 448 entries, the system prompts you with an alert message. Default Disabled Range Enabled, Disabled

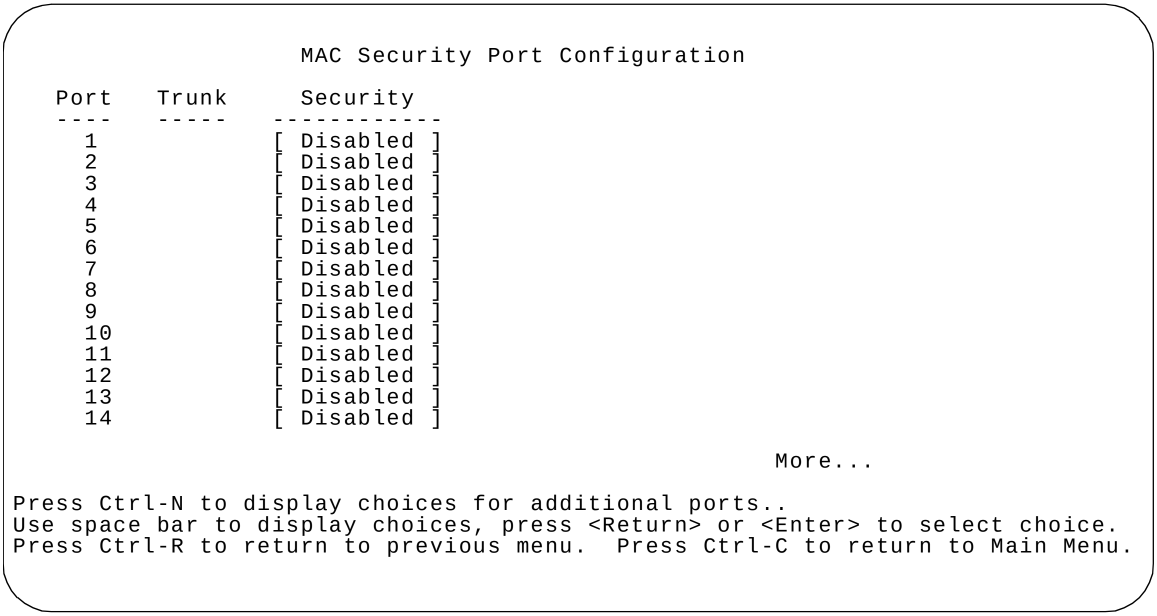
MAC Address Security Port Configuration screen

The MAC Address Security Port Configuration screens (Figure 64 and Figure 65) allow you to set or modify your MAC address port security configuration on a per port basis.

To open the MAC Address Security Port Configuration screen:

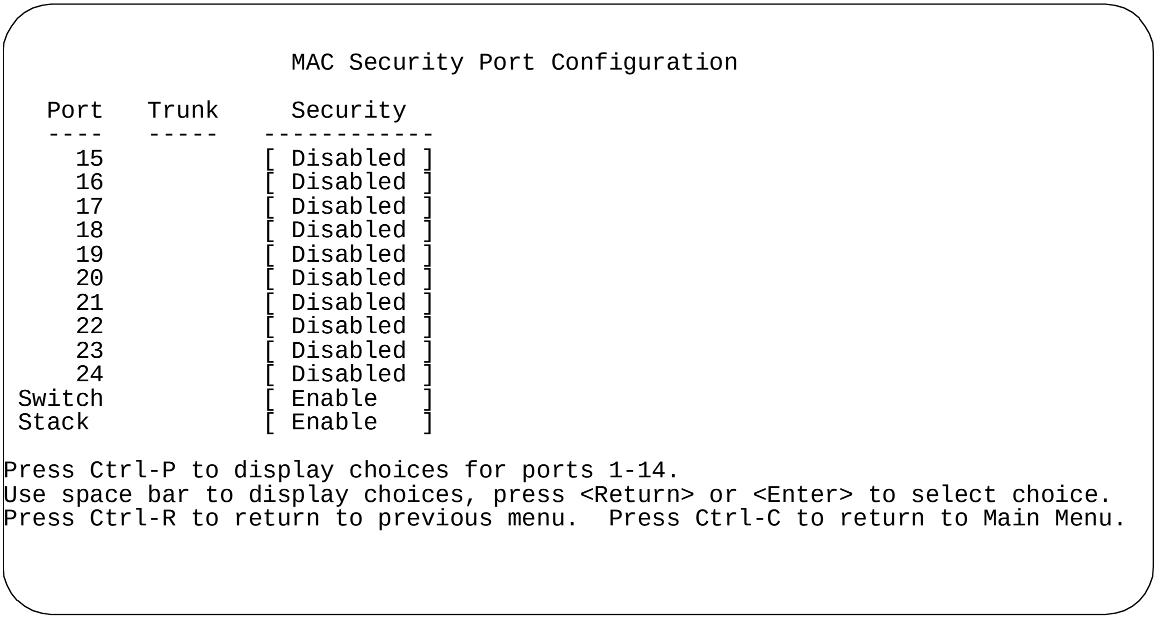
➨ Choose MAC Address Security Port Configuration from the MAC Address Security Configuration Menu.

Figure 64 MAC Security Port Configuration screen (1 of 2)



```
                     MAC Security Port Configuration

   Port   Trunk     Security
   ----   -----   ------------
     1            [ Disabled ]
     2            [ Disabled ]
     3            [ Disabled ]
     4            [ Disabled ]
     5            [ Disabled ]
     6            [ Disabled ]
     7            [ Disabled ]
     8            [ Disabled ]
     9            [ Disabled ]
     10           [ Disabled ]
     11           [ Disabled ]
     12           [ Disabled ]
     13           [ Disabled ]
     14           [ Disabled ]

                                                        More...

Press Ctrl-N to display choices for additional ports..
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Figure 65 MAC Security Port Configuration screen (2 of 2)



```
                     MAC Security Port Configuration

   Port   Trunk     Security
   ----   -----   ------------
     15           [ Disabled ]
     16           [ Disabled ]
     17           [ Disabled ]
     18           [ Disabled ]
     19           [ Disabled ]
     20           [ Disabled ]
     21           [ Disabled ]
     22           [ Disabled ]
     23           [ Disabled ]
     24           [ Disabled ]
 Switch           [ Enable   ]
 Stack            [ Enable   ]

Press Ctrl-P to display choices for ports 1-14.
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 18 describes the MAC Security Port Configuration screen fields.

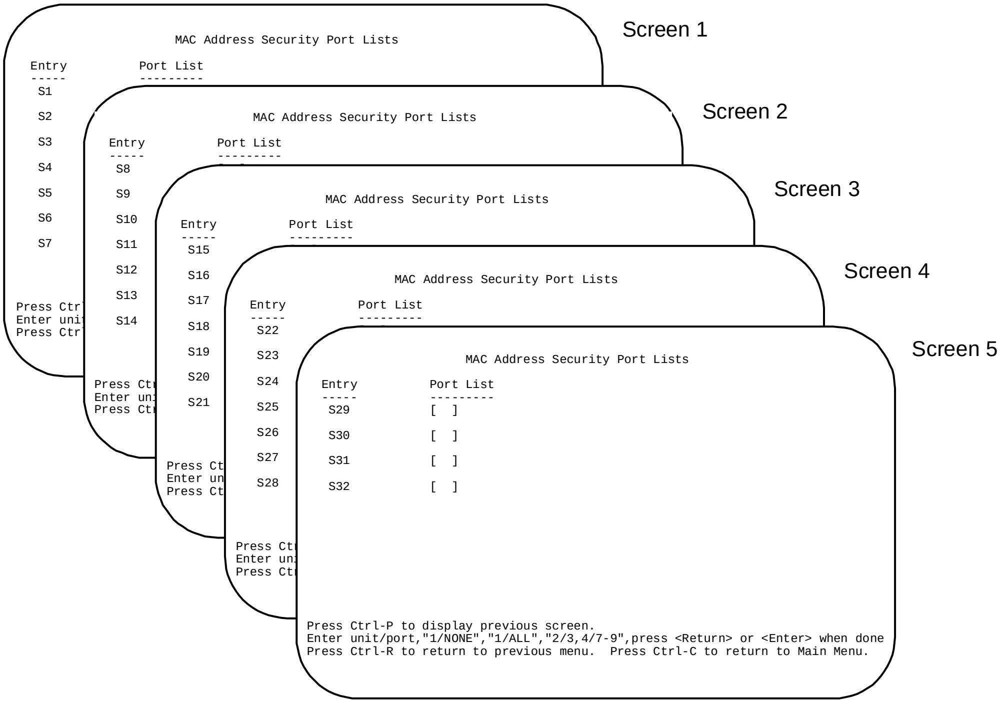
Table 18 MAC Security Port Configuration screen fields

Field	Description	
Port	Displays a numbered port list.	
Trunk	Displays the trunk number if the port is a member of that trunk.	
	Default	blank field
Security	This field value determines whether or not security is enabled or disabled on the port level or switch level.	
	Default	Disabled
	Range	Disabled, Enabled

MAC Address Security Port Lists screens

The MAC Address Security Port Lists screens allow you to create port lists that can be used as *allowed source port lists* for a specified MAC address in the MAC Address Security Table screen. You can create as many as 32 port lists, using up to five MAC Address Security Port Lists screens (see Figure 66).

Figure 66 MAC Address Security Port Lists screens



```
                MAC Address Security Port Lists

 Entry          Port List
 -----          ---------
  S1
  S2
  S3
  S4
  S5
  S6
  S7

Press Ctr
Enter uni
Press Ctr
```

```
                MAC Address Security Port Lists

 Entry          Port List
 -----          ---------
  S8
  S9
  S10
  S11
  S12
  S13
  S14

Press Ct
Enter uni
Press Ctr
```

```
                MAC Address Security Port Lists

 Entry          Port List
 -----          ---------
  S15
  S16
  S17
  S18
  S19
  S20
  S21

Press Ct
Enter un
Press Ct
```

```
                MAC Address Security Port Lists

 Entry          Port List
 -----          ---------
  S22
  S23
  S24
  S25
  S26
  S27
  S28

Press Ct
Enter uni
Press Ct
```

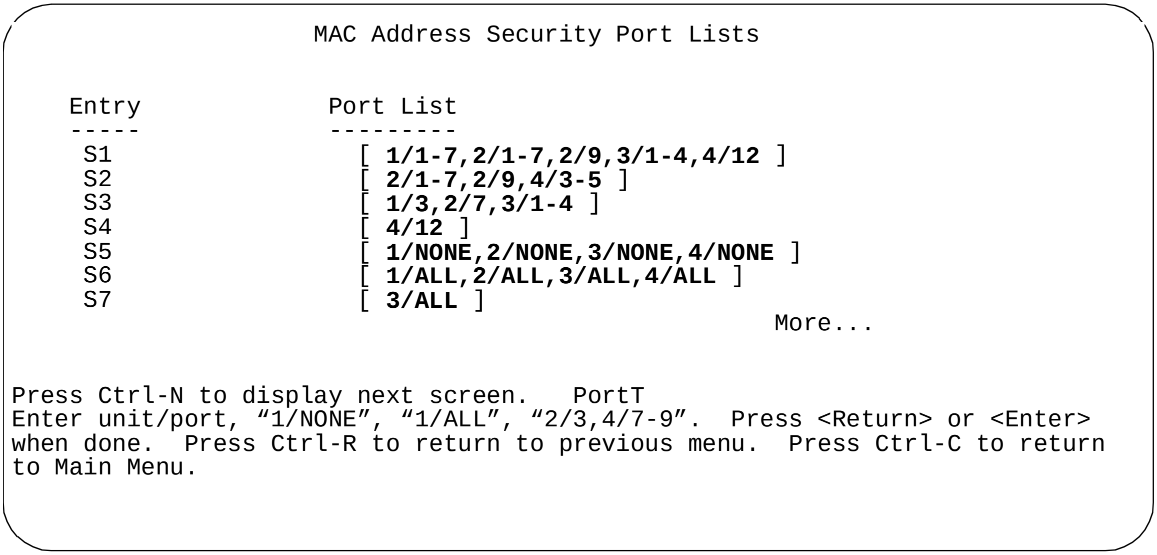
```
                     MAC Address Security Port Lists

  Entry          Port List
  -----          ---------
   S29           [  ]
   S30           [  ]
   S31           [  ]
   S32           [  ]






Press Ctrl-P to display previous screen.
Enter unit/port,"1/NONE","1/ALL","2/3,4/7-9",press <Return> or <Enter> when done
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

To open the MAC Address Security Lists screen:

➨ Choose MAC Address Security Lists from the MAC Address Security Configuration Menu.

The options for allowed port access include: NONE, ALL, and ports that are specified in a list (for example, 1/1, 2/6, etc.). Refer to Port List syntax for more information.

Figure 67 MAC Address Security Port Lists screen



```
                     MAC Address Security Port Lists


    Entry                 Port List
    -----                 ---------
     S1                     [ 1/1-7,2/1-7,2/9,3/1-4,4/12 ]
     S2                     [ 2/1-7,2/9,4/3-5 ]
     S3                     [ 1/3,2/7,3/1-4 ]
     S4                     [ 4/12 ]
     S5                     [ 1/NONE,2/NONE,3/NONE,4/NONE ]
     S6                     [ 1/ALL,2/ALL,3/ALL,4/ALL ]
     S7                     [ 3/ALL ]
                                                     More...


Press Ctrl-N to display next screen.   PortT
Enter unit/port, “1/NONE”, “1/ALL”, “2/3,4/7-9”.  Press <Return> or <Enter>
when done.  Press Ctrl-R to return to previous menu.  Press Ctrl-C to return
to Main Menu.
```

Table 19 describes the MAC Address Security Port Lists screen fields.

Table 19 MAC Address Security Port Lists screen fields

Field	Description
Entry	This field indicates the port list number (S1 to S32) that corresponds to the values you set in the Port List field.
Port List	This field allows you to create a port list that you can use as an “Allowed Source” in the MAC Address Security Table screen.

Port list syntax

When you enter a port list in a stack configuration, you must specify either a unit/port list, NONE, or ALL. In a stack configuration, ALL indicates all of the stack port; whereas, in a standalone scenario, ALL indicates all of the switch ports.

Note: NONE and ALL must be entered in uppercase characters as shown in the screen prompt.

A unit/port number list is composed of one or more list items, each of which can be a single number or a range of numbers (where the numbers represents one or more ports). If a list item is preceded by a number and then a slash (/), the number represents a stack unit.

For example, 1/1-7,2/1-7,2/9,3/1-4,4/12 is a valid unit/port number list (see entry S1 in Figure 67 on page 196). It represents the following port order:

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

Accelerator keys for repetitive tasks

You can use certain keystrokes as “accelerator keys” to help speed up repetitive tasks. For example, suppose you want to modify the Port List field in the MAC Address Security Port List screen (Figure 67 on page 196). You can modify the port list in any of the following ways:

- Add a new port to an existing port number list.
- Remove a port from an existing port number list.
- Copy an existing field into an adjacent field.

Adding a new port to an existing port number list

In the example shown in Figure 67 on page 196, S3 shows the Port List field values as:

1/3,2/7,3/1-4

If you want to add another port (for example, port 2/9) to the existing port number list, you could highlight the field and then type another port list, including the new port number 1/3,2/7,**2/9**,3/1-4 [Return]. This method can be cumbersome.

As an alternative method instead, you can highlight the field and then enter +2/9 [Return]. The existing field keeps the previous list and adds the new port number (2/9) between ports 2/7 and 3/14.

(If you choose to add port 2/8 to the existing port number list, the field accepts the new port 2/8 but shows the new port number list field as: 1/3,2/7-8,3/1-4.)

Removing a port from an existing port number list

To remove a port from the port number list, use the minus sign (-) character instead of the plus sign (+) character as described above.

Copying an existing field into and adjacent field

You can use the period (.) character to copy a previously entered field value into the field directly next to it. For example, to copy the Allowed Source S3 (shown in Figure 67 on page 196) into the next field (entry 6):

1. Enter a MAC address into the next MAC address field.
2. Highlight the (blank) Allowed Source field.
3. Enter the period (.) character and click Return.

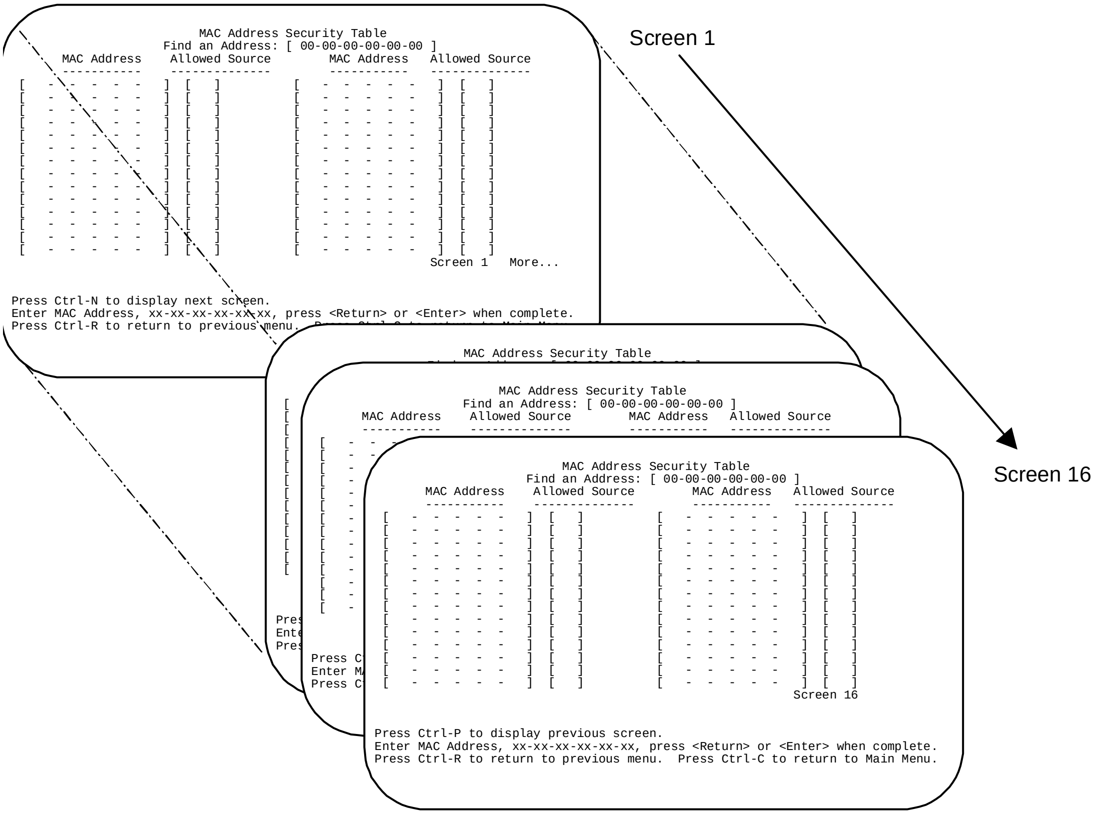
The port number list from the previous entry is copied into the new field.

MAC Address Security Table screens

The MAC Address Security Table screens allow you specify the ports that each MAC address is allowed to access. You must also include the MAC addresses of any routers that are connected to any secure ports.

There are 16 available MAC Address Security Table screens (Figure 68) that you can use to create up to 448 MAC address entries (28 per screen).

Figure 68 MAC Address Security Table screens

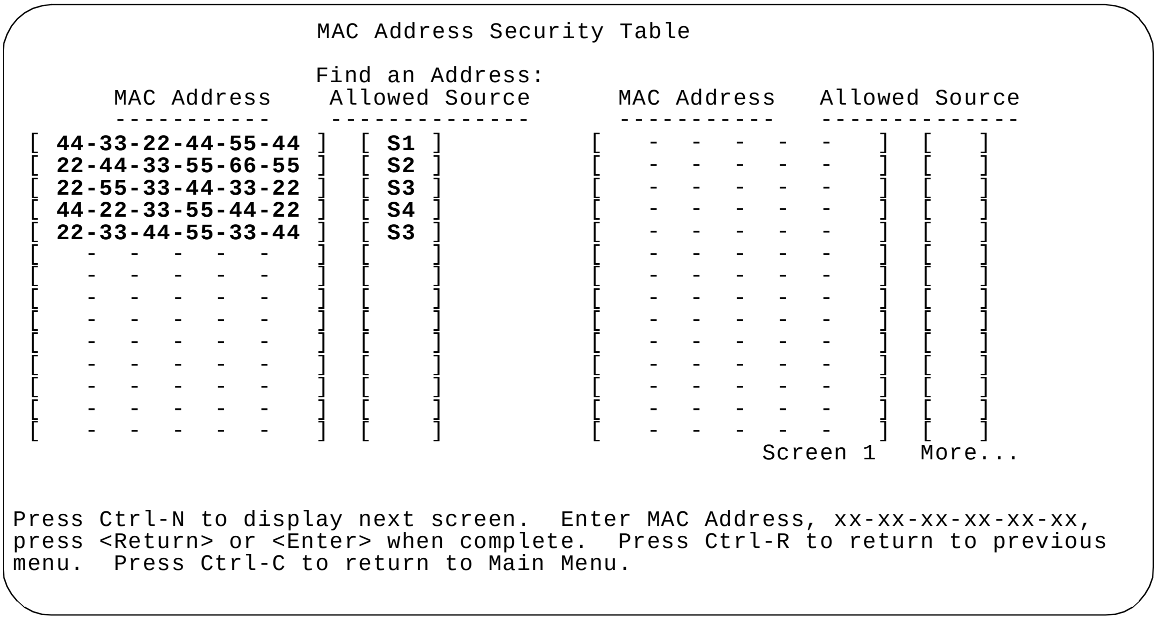


```
                      MAC Address Security Table
                 Find an Address: [ 00-00-00-00-00-00 ]
      MAC Address    Allowed Source         MAC Address    Allowed Source
      -----------    --------------         -----------    --------------
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
                                                     Screen 1    More...


Press Ctrl-N to display next screen.
Enter MAC Address, xx-xx-xx-xx-xx-xx, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu.
```

```
                      MAC Address Security Table
                 Find an Address: [ 00-00-00-00-00-00 ]
      MAC Address    Allowed Source         MAC Address    Allowed Source
      -----------    --------------         -----------    --------------
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
 [   - - - - - -  ] [   ]            [   - - - - - -  ] [   ]
                                                     Screen 16

Press Ctrl-P to display previous screen.
Enter MAC Address, xx-xx-xx-xx-xx-xx, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

➨ Choose MAC Address Security Table from the MAC Address Security Configuration Menu to open the MAC Address Security Table screen (Figure 69).

Figure 69 MAC Address Security Table screen



```
                     MAC Address Security Table

                     Find an Address:
       MAC Address    Allowed Source      MAC Address   Allowed Source
       -----------    --------------      -----------   --------------
 [ 44-33-22-44-55-44 ]  [ S1 ]          [   -  -  -  -  -   ]  [   ]
 [ 22-44-33-55-66-55 ]  [ S2 ]          [   -  -  -  -  -   ]  [   ]
 [ 22-55-33-44-33-22 ]  [ S3 ]          [   -  -  -  -  -   ]  [   ]
 [ 44-22-33-55-44-22 ]  [ S4 ]          [   -  -  -  -  -   ]  [   ]
 [ 22-33-44-55-33-44 ]  [ S3 ]          [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [    ]          [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [    ]          [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [    ]          [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [    ]          [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [    ]          [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [    ]          [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [    ]          [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [    ]          [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [    ]          [   -  -  -  -  -   ]  [   ]
                                                    Screen 1   More...


Press Ctrl-N to display next screen.  Enter MAC Address, xx-xx-xx-xx-xx-xx,
press <Return> or <Enter> when complete.  Press Ctrl-R to return to previous
menu.  Press Ctrl-C to return to Main Menu.
```

Table 20 describes the MAC Address Security Table screen fields.

Table 20 MAC Address Security Table Screen Fields

Field	Description
Find an Address	Allows you to search for a specific MAC address that is used in any of the MAC Address Security Table screens.
MAC Address	Allows you to specify up to 448 MAC addresses that are authorized to access the switch. You can specify the ports that each MAC address is allowed to access using the Allowed Source field (see next field description). The specified MAC address does not take effect until the Allowed Source field is set to some value (a single unit/port number or a port list value that you previously configured in the MAC Address Security Port Lists screen). You can clear an existing MAC address field by entering zero (0) in the field and pressing [Enter]. Default - - - - - (no address assigned) Range A range of 6 Hex Octets, separated by dashes (multicast* and broadcast addresses are not allowed).

Table 20 MAC Address Security Table Screen Fields (continued)

Field	Description
Allowed Source	Allows you to specify the ports that each MAC address is allowed to access. The options for the Allowed Source field include a single unit/port number or a port list value that you have previously configured in the MAC Address Security Port Lists screen. Default - (Blank field) Range A single unit/port or a port list value (for example, 1/3, 1/6, 3/4, S1, S5, etc.).

* Multicast address -- Note that the first octet of any multicast address will always be an odd number.

EAPOL Security Configuration screen

The EAPOL Security Configuration screen (Figure 70) allows you to selectively limit access to the switch based on an authentication mechanism that uses Extensible Authentication Protocol (EAP) to exchange authentication information between the switch and an authentication server.

Note: Before you use the EAPOL Security Configuration screen, you must configure your Primary RADIUS Server and RADIUS Shared Secret.

You will also need to set up specific user accounts on your RADIUS server:

- User names
- Passwords
- VLAN IDs
- Port priority

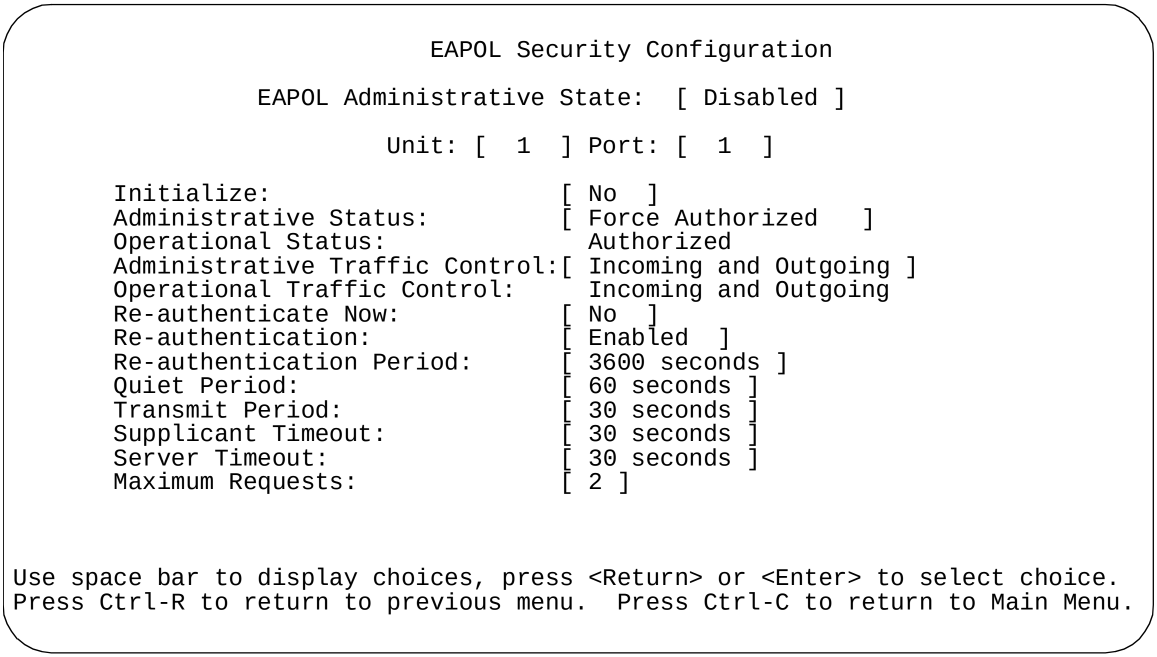
You can set up these parameters directly on your RADIUS server. For detailed instructions about configuring your RADIUS server, refer to your RADIUS server documentation.

Note: Do not enable EAPOL security on the switch port that is connected to the RADIUS server.

To open the EAPOL Security Configuration screen:

➨ Choose EAPOL Security Configuration (or press e) from the Switch Configuration Menu.

Figure 70 EAPOL Security Configuration screen



```
                             EAPOL Security Configuration

                 EAPOL Administrative State:  [ Disabled ]

                          Unit: [  1  ] Port: [  1  ]

       Initialize:                    [ No  ]
       Administrative Status:         [ Force Authorized   ]
       Operational Status:              Authorized
       Administrative Traffic Control:[ Incoming and Outgoing ]
       Operational Traffic Control:     Incoming and Outgoing
       Re-authenticate Now:           [ No  ]
       Re-authentication:             [ Enabled  ]
       Re-authentication Period:      [ 3600 seconds ]
       Quiet Period:                  [ 60 seconds ]
       Transmit Period:               [ 30 seconds ]
       Supplicant Timeout:            [ 30 seconds ]
       Server Timeout:                [ 30 seconds ]
       Maximum Requests:              [ 2 ]



Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 21 describes the EAPOL Security Configuration screen options.

Table 21 EAPOL security configuration screen options

Option	Description
EAPOL Administrative State	Allows you to enable or disable EAPOL for your switch or stack. When this field is set to disabled (the default state), the Operational Status for all of the switch/stack ports is set to Authorized (no security restriction). Default Disabled Range Disabled, Enabled

Table 21 EAPOL security configuration screen options (continued)

Option	Description
Unit	Allows you to select the unit number (when stacking is configured) to view or configure. To view or configure another unit, type its unit number and press [Enter], or press the spacebar to toggle the unit numbers. If you set this field value to All, other screen field values you modify apply to *all* stack ports. Default 1 Range 1,2,3,4,5,6,7,8,ALL
Port	Allows you to select a specified unit's (see preceding Unit field) port number to view or configure. To view or configure another port, type its port number and press [Enter], or press the spacebar to toggle the port numbers. If you set this field value to All, other screen field values you modify apply to *all* ports for the specified unit. The All value is also useful when you want to apply modified field values to most of, but not all of, your switch's ports. For example, if you want to apply modified field values to 23 of your switch's 24 ports, it may be easier to apply the All value in the Port field, and then reconfigure the single port back to its original values. Default 1 Range 1 to 28,ALL
Initialize	Allows you to activate EAPOL authentication for the specified unit/port. Default No Range No,Yes
Administrative Status	Allows you to set the EAPOL authorization status for the specified unit/port. Default Force Authorized Range Force Authorized,Force Unauthorized,Auto • Force Authorized means the specified unit/port authorization status is *always* authorized. • Force Unauthorized means the specified unit/port authorization status is *always* Unauthorized. • Auto means the specified unit/port authorization status depends on the EAP authentication results.
Operational Status	A read-only field that shows the current authorization status for the specified unit/port. This read-only field does not appear when the Unit/Port field value is set to All. Default Authorized Range Authorized,Unauthorized

Table 21 EAPOL security configuration screen options (continued)

Option	Description
Administrative Traffic Control	Allows you to choose whether EAPOL authentication is set for incoming and outgoing traffic or for incoming traffic only. For example, if you set the specified unit/port field value to Incoming and Outgoing, and the EAPOL authentication fails, then both incoming and outgoing traffic on the specified unit/port is blocked. Default Incoming and Outgoing Range Incoming and Outgoing,Incoming Only
Operational Traffic Control	A read-only field that indicates the current administrative traffic control configuration for the specified unit/port (see preceding field description). This read-only field does not appear when the Unit/Port field value is set to All. Default Incoming and Outgoing Range Incoming and Outgoing,Incoming Only
Re-authenticate Now	Allows you to activate EAPOL authentication for the specified unit/port immediately, without waiting for the Re-Authentication Period to expire. Default No Range No,Yes
Re-authentication	Allows you to repeat EAPOL authentication for the specified unit/port according to the time interval value configured in the Re-Authentication Period field (see next field description). Default Enabled Range Enabled,Disabled
Re-authentication Period	When the Re-Authentication field value (see preceding field) is set to enabled, this field allows you to specify the time period between successive EAPOL authentications for the specified unit/port. Default 3600 seconds Range 1 to 604800 seconds
Quiet Period	Allows you to specify the time period between any single EAPOL authentication failure and the start of a new EAPOL authentication attempt. Default 60 seconds Range 0 to 65535 seconds
Transmit Period	Allows you to specify how long the switch waits for the supplicant to respond to EAP Request/Identity packets. Default 30 seconds Range 1 to 65535 seconds
Supplicant Timeout	Allows you to specify how long the switch waits for the supplicant to respond to all EAP packets, except EAP Request/Identity packets.

Table 21 EAPOL security configuration screen options (continued)

Option	Description
	Default 30 seconds Range 1 to 65535 seconds
Server Timeout	Allows you to specify how long the switch waits for the RADIUS server to respond to all EAP packets. Default 30 seconds Range 1 to 65535 seconds
Maximum Requests	Allows you to specify the number of times the switch attempts to resend EAP packets to a supplicant. Default 2 attempts Range 1 to 10 attempts

VLAN Configuration Menu screen

With software version 1.2, the VLAN Configuration Menu screen (Figure 71) allows you to select the appropriate screen to configure up to 256 VLANs. VLAN 1 is port-based by default. You can configure the remaining 255 VLANs to be of any appropriate combination of types, although you have a maximum of 48 MAC SA-based VLANs.

You can configure as many as 255 protocol-based VLANs, with up to 14 different protocols**.** The number of different protocols you can configure depends on the number of hexadecimal values (PID values) associated with the protocol type. Some protocol types use more than one PID value. Refer to "Predefined Protocol Identifier (PID) description" on page 212. A port may not be a member of more than one protocol-based VLAN with the same PID. (Untagged ports cannot belong to different VLANs of the same protocol type; however, tagged ports can.)

Note: Only standalone or pure stacks of BPS 2000 support 256 VLANs. A mixed stack that consists of BPS 2000 and BayStack 450 switches has only 64 VLANs. Refer to "Using 356 VLANs" in Chapter 1 for more information on using 256 VLANs.

You can configure up to 48 MAC SA-based VLANs. Up to 48 MAC addresses can be used with the existing MAC SA-based VLANs. Due to hardware limitations, it is possible that some MAC address cannot be entered, depended on the values of MAC addresses previously entered.

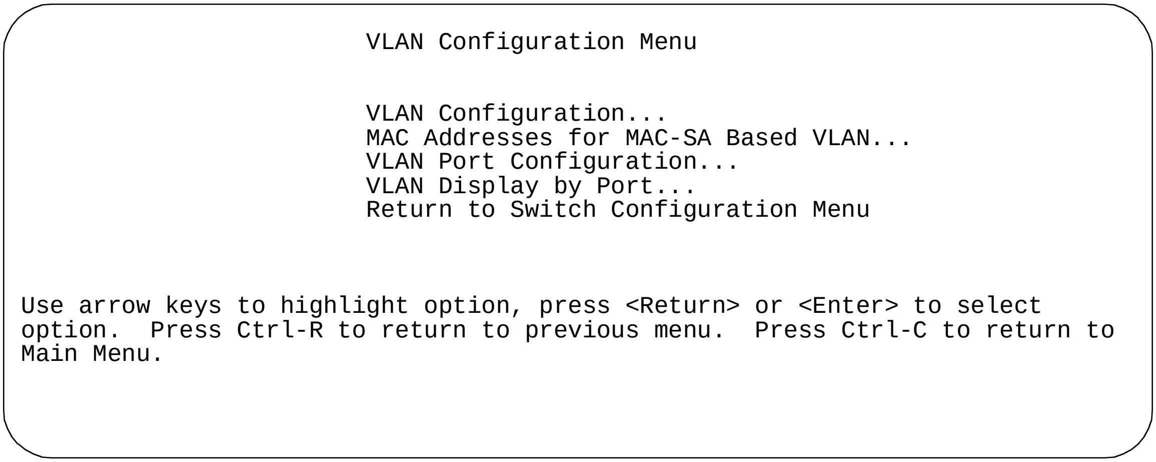
When you create VLANs, you can assign various ports (and therefore the devices attached to these ports) to different broadcast domains. Creating VLANs increases network flexibility by allowing you to reassign devices to accommodate network moves, additions, and changes, eliminating the need to change physical cabling.

Note: Refer to Chapters 1 and 2 for detailed information about configuring VLANs.

To open the VLAN Configuration Menu:

➨ Choose VLAN Configuration (or press v) from the Switch Configuration Menu screen.

Figure 71 VLAN Configuration Menu screen



```
                         VLAN Configuration Menu


                         VLAN Configuration...
                         MAC Addresses for MAC-SA Based VLAN...
                         VLAN Port Configuration...
                         VLAN Display by Port...
                         Return to Switch Configuration Menu



Use arrow keys to highlight option, press <Return> or <Enter> to select
option.  Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to
Main Menu.
```

Table 22 describes the VLAN Configuration Menu screen options.

Table 22 VLAN Configuration Menu Screen options

Option	Description
VLAN Configuration...	Displays the VLAN Configuration screen (see "VLAN Configuration screen" on page 207). This screen allows you to set up VLAN workgroups.
MAC Addresses for MAC-SA Based VLAN	Allows you to configure MAC source address-based VLANs. (see "MAC Address Configuration for MAC-SA-Based VLAN screen" on page 214)
VLAN Port Configuration...	Displays the VLAN Port Configuration screen (see "VLAN Port Configuration screen" on page 215). This screen allows you to set up a specific switch port.
VLAN Display by Port...	Displays the VLAN Display by Port screen (see "VLAN Display by Port screen" on page 218).

VLAN Configuration screen

The VLAN Configuration screen (Figure 72) allows you to create and assign VLAN port memberships to standalone or stacked unit ports. You can create port-based and policy-based VLANs for the following purposes:

- IEEE 802.1Q port-based VLANs allow you to explicitly configure switch ports as VLAN port members.

  When you create a port-based VLAN, you assign a Port VLAN Identifier (PVID) and specify which ports belong to the VLAN.

- Policy-based VLANs allow you to configure your switch ports as members of a broadcast domain, based on the information within a packet. Policy-based VLANs can localize broadcast traffic and assure that only the policy-based VLAN ports are flooded with the specified packets.

When you configure ports as VLAN port members, they become part of a set of ports that form a broadcast domain for a specific VLAN. You can assign switch ports, whether standalone or stacked unit ports, as VLAN port members of one or more VLANs.

Note: Refer to Chapter 1 and guidelines for configuring spanning tree groups for more information on configuring VLANs.

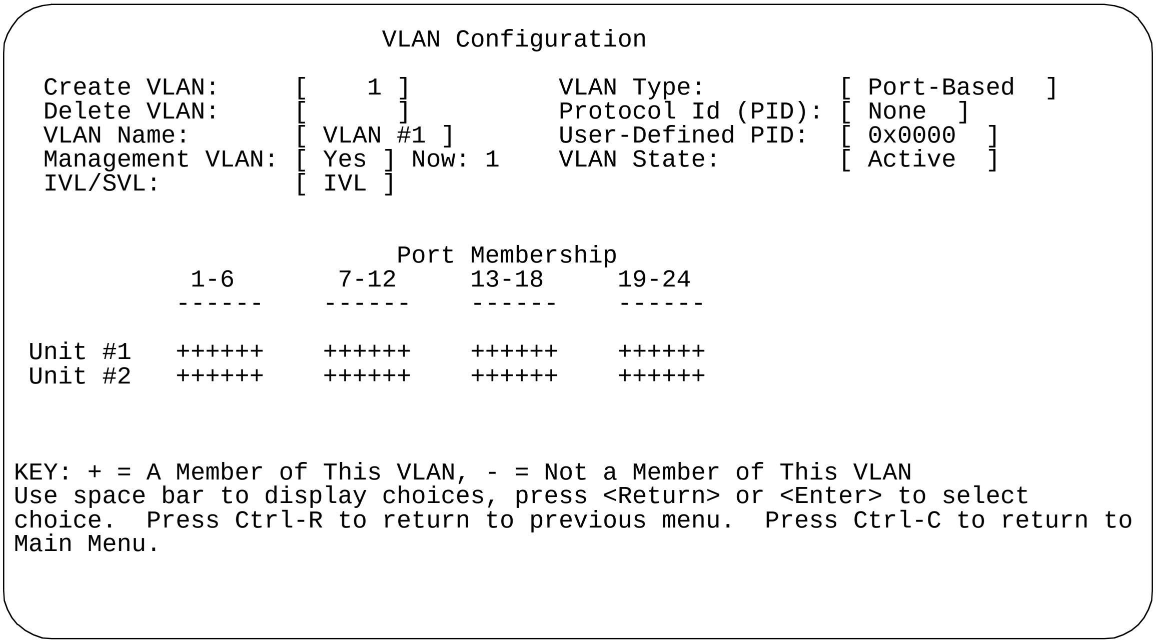
You can add or remove port members from a VLAN in accordance with the IEEE 802.1Q tagging rules. Refer to Chapter 2 for a description of important terms used with 802.1Q VLANs.

You can also use this screen to create and to delete specific VLANs, to assign VLAN names, and to assign any VLAN as the management VLAN.

To open the VLAN Configuration screen:

➨ Choose VLAN Configuration (or press v) from the VLAN Configuration Menu screen.

Figure 72 VLAN Configuration screen



```
                         VLAN Configuration

  Create VLAN:     [    1 ]          VLAN Type:         [ Port-Based  ]
  Delete VLAN:     [      ]          Protocol Id (PID): [ None  ]
  VLAN Name:       [ VLAN #1 ]       User-Defined PID:  [ 0x0000  ]
  Management VLAN: [ Yes ] Now: 1    VLAN State:        [ Active  ]
  IVL/SVL:         [ IVL ]


                          Port Membership
            1-6       7-12     13-18     19-24
           ------    ------    ------    ------

 Unit #1   ++++++    ++++++    ++++++    ++++++
 Unit #2   ++++++    ++++++    ++++++    ++++++



KEY: + = A Member of This VLAN, - = Not a Member of This VLAN
Use space bar to display choices, press <Return> or <Enter> to select
choice.  Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to
Main Menu.
```

Table 23 describes the VLAN Configuration screen fields.

Table 23 VLAN Configuration screen fields

Field	**Description**
Create VLAN	Allows you to set up or view configured VLAN workgroups. Enter the number of the new VLAN you want to create or view, then press [Return]. The Port Membership fields indicate the corresponding VLAN workgroup configuration, if configured. Dashes (-) indicate no VLAN Members are configured. Alternatively, you can use the space bar to toggle through the various configured VLAN workgroups. You can create up to 255 different VLANs (except VLAN #1). Default 1 Range 2 to 4094
Delete VLAN	Allows you to delete specified VLANs, except the assigned management VLAN (See Management VLAN field). Enter the number of the VLAN you want to delete, then press [Return], or use the space bar to toggle through the selection until you reach the VLAN you want to delete, then press [Return].

Table 23 VLAN Configuration screen fields (continued)

Field	**Description**
	The specified VLAN is deleted as soon as you press [Return]. The software does not prompt you to reconsider this action. If you delete a VLAN, all configuration parameters that are associated with that VLAN are deleted also. You cannot delete VLAN 1. By default, all switch ports are assigned as untagged members of VLAN 1 with all ports configured as PVID = 1. See Chapter 1 for more information. Default Blank Range 2 to 4094
VLAN Name	Allows you to assign a name field to configured VLANs. Default VLAN # (*VLAN number*) Range Any ASCII string of up to 16 printable characters
Management VLAN	Allows you to assign any VLAN 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. Default No Range Yes, No
IVL/SVL	Allows you to select either Shared VLAN Learning (SVL), multiple VLANs using a single forwarding database, or Independent VLAN Learning (IVL), each VLAN using a unique forwarding database. To set this field, the VLAN State field value must be Inactive. IVL is a Business Policy Switch-only feature. The IVL option is enabled only in Pure BPS 2000 Stack mode. The SVL option is enabled in the Hybrid Stack mode. See "Stack Operational Mode screen" on page 248. Default SVL (in a mixed stack or hybrid stack) IVL (in a pure Business Policy Switch stack or standalone switch) Range IVL, SVL
VLAN Type	Allows you to select the type of VLAN (port-based, protocol-based, or MAC SA-based) to create. To set this field, the VLAN State field value must be Inactive. Default Port-based Range Port-based, Protocol-based, MAC-SA-based
Protocol ID (PID)	Allows you to set the protocol type of your VLAN (to set this field, the VLAN State field value must be Inactive). You can choose from any of 14 predefined supported protocols (see "Predefined Protocol Identifier (PID) description" on page 212), or you can create your own user-defined protocol-based VLAN (see the User-defined PID field description for more information).
	Default None

Table 23 VLAN Configuration screen fields (continued)

Field	**Description**	
	Range	None, IP Ether2, Ipx 802.3, Ipx 802.2, Ipx Snap, Ipx Ether2, AplTk Ether2Snap, Declat Ether2, DecOth Ether2, Sna 802.2, Sna Ether2, NetBios 802.2, Xns Ether2,Vines Ether2, Ipv6 Ether2, User-Defined, Rarp Ether2
User-Defined PID	Allows you to create your own user-defined VLAN where you specify the Protocol Identifier (PID) for the VLAN. To set this field, the VLAN State field must be set to Inactive. Some restrictions apply. "User-Defined Protocol Identifier Description" on page 213.	
	Default	0x0000
	Range	Any 16-bit hexadecimal value (for example, 0xABCD)
VLAN State	Allows you to activate your newly created VLAN. The following field values: VLAN Type, Protocol Id (PID), or User-defined PID must be configured appropriately before this field can be set to active. After you set the VLAN State field value to Active, you cannot change the VLAN State, VLAN Type, Protocol Id, or User-defined PID field values, unless you delete the VLAN. If you delete a VLAN, all configuration parameters that are associated with that VLAN are also deleted.	
	Default	Inactive
	Range	Inactive, Active
Port Membership	Allows you to assign VLAN port memberships to *standalone* or *stacked unit* ports. The ports can be configured in one or more VLANs. To set this field, you must set the VLAN State field to Active. Certain restrictions apply for the BayStack 450-1GBIC, 450-SR, 450-1SX, 450-1LR, 450-1LX MDA sand BayStack 410 ports (see "Port restrictions" on page 215). This field is dependent on the Tagging field value in the VLAN Port Configuration screen (see the Tagging field description in "VLAN Port Configuration screen fields" on page 216). For example: • When the Tagging field is set to *Untagged Access*, you can set the Port Membership field as an untagged port member (U) 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 (T) or as a non-VLAN port member (-).	
	The Port Membership fields are displayed in six-port groups (for example, 1-6, 7-12, 13-18). The number of ports displayed depends on the switch model or type of optional MDA installed in the Uplink Module slot.	
	Default	U (All ports are assigned as untagged members of VLAN 1.)
	Range	U, T, and -

Predefined Protocol Identifier (PID) description

Table 24 defines the standard protocol-based VLANs and PID types that are supported by the Business Policy Switch and BayStack 450 and BayStack 410 switches.

Table 24 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
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 (see "Predefined Protocol Identifier (PID) description" below, for more information).
RARP Ether2	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 Protocol Identifier Description

In addition to the standard predefined protocols, user-defined protocol-based VLANs are supported. For user-defined protocol-based VLANs, you specify the protocol identifier (PID) for the VLAN. 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

The following PIDs (Table 25) are reserved and are not available for user-defined PIDs.

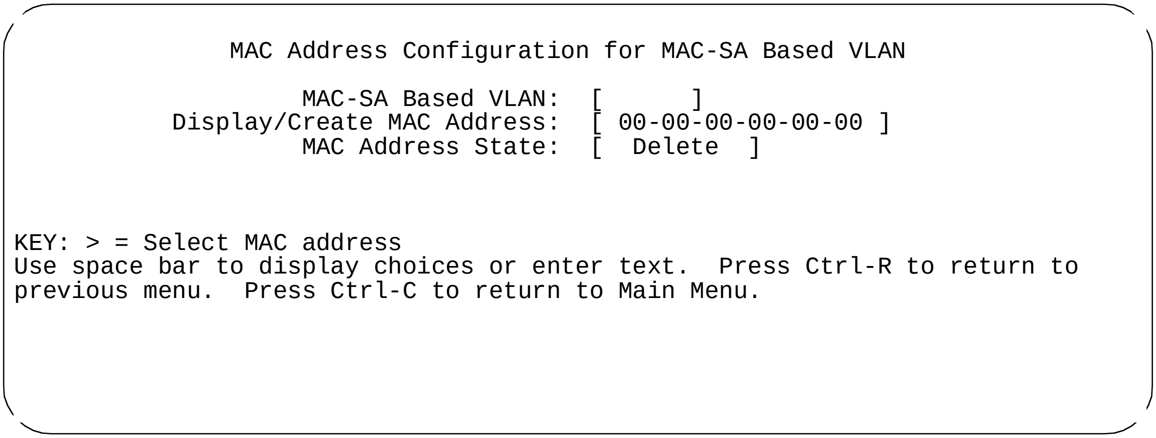
Table 25 Reserved PIDs

PID Value (hex)	**Comments**
04**, **04	Sna 802.2
F0**, **F0	NetBIOS 802.2
AAAA	SNAP
0 - 05DC	Overlaps with 802.3 frame length
0600, 0807	Xns Ether2
0BAD	Vines Ether2
4242	IEEE 802.1D BPDUs
6000 - 6009, 8038	Dec
0800, 0806	Ip Ether2 (including ARP)
8035	RARP Ether2
809B, 80F3	AplTk Ether2Snap
8100	IEEE 802.1Q for tagged frames
8137, 8138	Ipx
80D5	SNA Ether2
86DD	Ipv6 Ether2
8808	Ipx 802.3
Ipx 802.3	Ethernet 802.2
Ipx 802.2	Ethernet 802.

MAC Address Configuration for MAC-SA-Based VLAN screen

The MAC Address Configuration for MAC-SA Based VLAN screen (Figure 73) allows you to configure specific MAC SA-based VLANs. This screen allows you to select a MAC SA-based VLAN.

Figure 73 MAC Address Configuration for MAC-SA Based VLAN screen



```
               MAC Address Configuration for MAC-SA Based VLAN

                    MAC-SA Based VLAN:  [      ]
           Display/Create MAC Address:  [ 00-00-00-00-00-00 ]
                    MAC Address State:  [  Delete  ]



KEY: > = Select MAC address
Use space bar to display choices or enter text.  Press Ctrl-R to return to
previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 26 describes the MAC Address Configuration for MAC-SA Based VLAN screen fields.

Table 26 MAC Address Configuration for MAC-SA Based VLAN screen fields

Field	Description	
MAC-SA Based VLAN	Allows you to select a MAC SA-based VLAN.	
	Default	The least-valued active MAC-SA based VLAN will be displayed.
	Range	2 to 4094 (must be a currently active MAC-SA based VLAN)
Display/Create MAC Address	Allows you to enter a MAC address. If the address is already present in the selected MAC-SA based VLAN, its state is displayed. Otherwise, that address will be activated in the MAC-SA based VLAN.	
MAC Address State	Displays current state (Active) or allows you to delete a MAC address (Delete).	

Port restrictions

Ports on the BayStack 450-1GBIC, 450-1SR, 450-1SX, 450-1LR, 450-1LX MDAs and BayStack 410 ports do not have the ability to assign incoming untagged frames to a protocol-based VLAN.

To allow these ports to participate in protocol-based VLANs, you must set the Tagging field value in the VLAN Port Configuration screen to Tagged Trunk. Incoming untagged frames will be assigned to the PVID VLAN.

VLAN Port Configuration screen

The VLAN Port Configuration screen (Figure 74) allows you to configure specified switch ports with the appropriate PVID/VLAN association that enables the creation of VLAN broadcast domains (see Chapters 1 and 2 for more information about setting up VLAN broadcast domains).

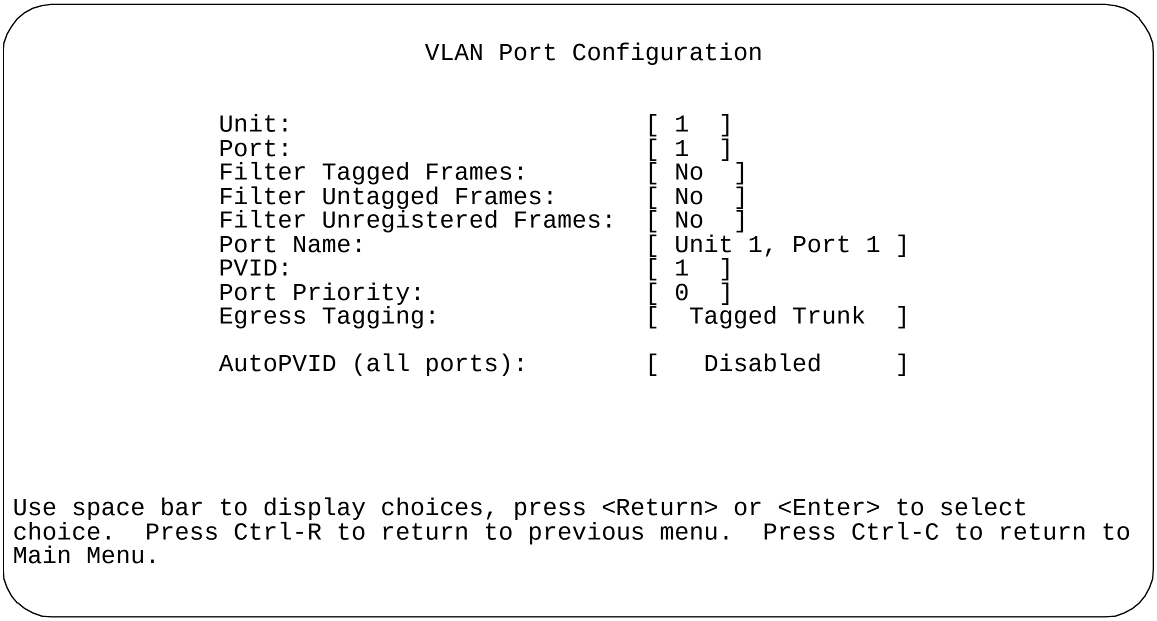
You can configure specified switch ports to filter (discard) all received tagged frames, untagged frames, or unregistered frames (see Chapters 1 and 2). Refer to the guidelines for configuring spanning tree groups in Chapter 1 for more information on configuring ports for tagged or untagged frames.

You can also prioritize the order in which the switch forwards packets, on a per-port basis (see Chapters 1 and 2). Refer to Chapter 4 “Policy-enabled networks,” for more information on prioritizing traffic.

To open the VLAN Port Configuration screen:

➨ Choose VLAN Port Configuration (or press c) from the VLAN Configuration Menu screen.

Figure 74 VLAN Port Configuration screen



```
                              VLAN Port Configuration


              Unit:                            [ 1  ]
              Port:                            [ 1  ]
              Filter Tagged Frames:            [ No  ]
              Filter Untagged Frames:          [ No  ]
              Filter Unregistered Frames:      [ No  ]
              Port Name:                       [ Unit 1, Port 1 ]
              PVID:                            [ 1  ]
              Port Priority:                   [ 0  ]
              Egress Tagging:                  [  Tagged Trunk  ]

              AutoPVID (all ports):            [   Disabled     ]





Use space bar to display choices, press <Return> or <Enter> to select
choice.  Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to
Main Menu.
```

Table 27 describes the VLAN Port Configuration screen fields.

Table 27 VLAN Port Configuration screen fields

Field	Description
Unit	Allows you to select a switch in your stack. To view another switch, type its switch number and press [Enter], or press the spacebar to toggle the switch numbers.
Port	Allows you to select the number of the port you want to view or configure. To view another port, type its port number and press [Enter], or press the spacebar to toggle the port numbers.
Filter Tagged Frames	Allows you to set this port to filter (discard) all received tagged packets. Default No Range No, Yes
Filter Untagged Frames	Sets this port to filter (discard) all received untagged frames. Default No Range No, Yes

Table 27 VLAN Port Configuration screen fields (continued)

Field	Description
Filter Unregistered Frames	Sets this port to filter (discard) all received unregistered packets. The Business Policy Switch does not support the Yes option. Default No Range No, Yes
Port Name	The default port name (with associated stack unit number when configured) assigned to this port. You can change this field to any name that is up to 16 characters long. Default Unit *x*, Port *x* Range Any ASCII string of up to 16 printable characters
PVID	Associates this port with a specific VLAN. For example, a port with a PVID of 3 assigns all untagged frames received on this port to VLAN 3. Default 1 Range 1 to 4094
Port Priority	Prioritizes the order in which the switch forwards packets received on specified ports. Default 0 Range 0 to 7
Egress Tagging	Allows you to assign VLAN Port Membership tagging options to this port, as follows: • Untag All: Any VLAN that this port is a member of *will not* be 802.1Q tagged. • Tag All: Any VLAN that this port is a member of will be 802.1Q tagged. • Tag PVID Only: Only frames whose VLAN ID match the PVID value assigned to the egress port will be tagged. • Untag PVID Only: All frames are tagged except those whose VLAN ID matches the PVID value assigned to the egress port. **Restriction:** If this port is a BayStack 450-1GBC, 450-1SR, 450-1SX, 450-1LR, 450-1LX MDA or a BayStack 410-24T switch port that is a protocol-based VLAN member, you cannot set this field value to Untag All. This restriction also applies if this port is a MultiLink trunk member with a BayStack 450-1GBC, 450-1SR, 450-1SX, 450-1LR, 450-1LX MDA port or a BayStack 410-24T switch port that is a protocol-based VLAN member. Setting this field value on any port to Tag All causes incoming untagged packets to be assigned to the PVID VLAN. They will no longer be classified based on the information within the packet, even if they are members of a policy-based VLAN.

Table 27 VLAN Port Configuration screen fields (continued)

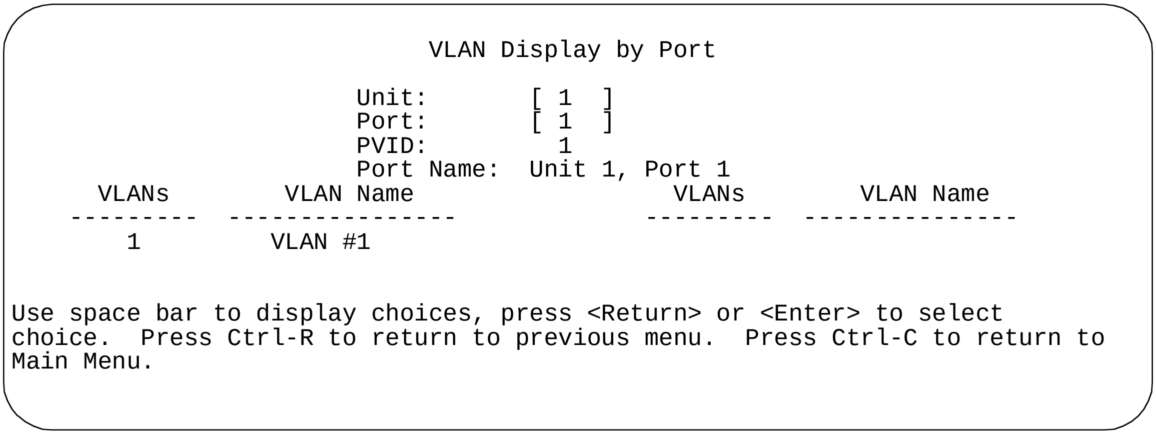
Field	Description
	Default Untag All Range Untag All, Tag All, Tag PVID Only, Untag PVID Only
AutoPVID	Automatically associates this PVID specific VLAN. Default Disabled Range Enabled, Disabled

VLAN Display by Port screen

The VLAN Display by Port screen (Figure 75) allows you to view VLAN characteristics associated with a specified switch port.

Choose VLAN Display by Port (or press d) from the VLAN Configuration Menu screen to open the VLAN Display by Port screen.

Figure 75 VLAN Display by Port screen



```
                             VLAN Display by Port

                        Unit:       [ 1  ]
                        Port:       [ 1  ]
                        PVID:         1
                        Port Name:  Unit 1, Port 1
      VLANs        VLAN Name                   VLANs        VLAN Name
    ---------   ----------------             ---------   ---------------
        1         VLAN #1


Use space bar to display choices, press <Return> or <Enter> to select
choice.  Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to
Main Menu.
```

Table 28 describes the VLAN Display by Port screen fields.

Table 28 VLAN Display by Port screen fields

Field	Description
Unit	Allows you to select a switch in your stack. To view another switch, type its switch number and press [Enter], or press the spacebar to toggle the switch numbers.
Port	Allows you to select the number of the port you want to view. To view another port, type its port number and press [Enter], or press the spacebar on your keyboard to toggle the port numbers.
PVID	Read-only field that indicates the PVID setting for the specified port.
Port Name	Read-only field that indicates the port name assigned to the specified port.
VLANs	Column header for the read-only fields listing the VLANs associated with the specified port.
VLAN Name	Column header for the read-only fields listing the VLAN Names associated with the specified port.

Port Configuration screen

The Port Configuration screen (Figures 76 and 77) allows you to configure specific switch ports or all switch ports. You can enable or disable the port status of specified switch ports, set the switch ports to autonegotiate for the highest available speed of the connected station, or set the speed for selected switch ports (autonegotiation is not supported on fiber optic ports).

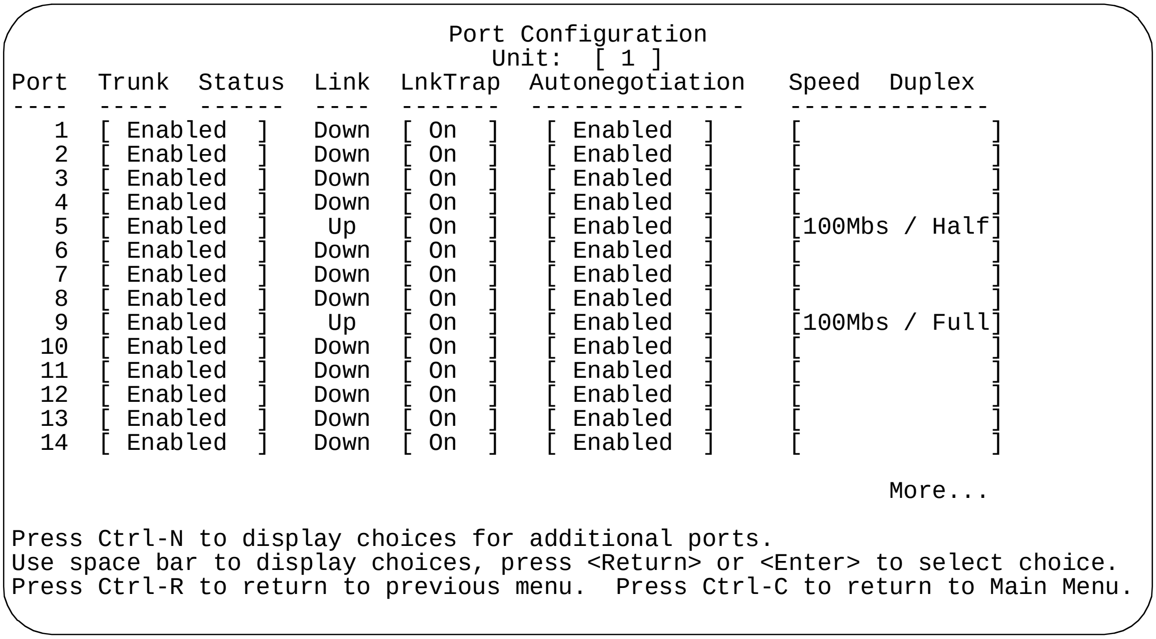
You can disable switch ports that are trunk members; however, the screen prompts for verification of the request before completing the action. Choosing [Yes] disables the port and removes it from the trunk.

Note: The Autonegotiation fields, the Speed fields, and the Duplex fields are independent of MultiLink Trunking, rate limiting, VLANs, IGMP Snooping, and the STP.

To open the Port Configuration screen:

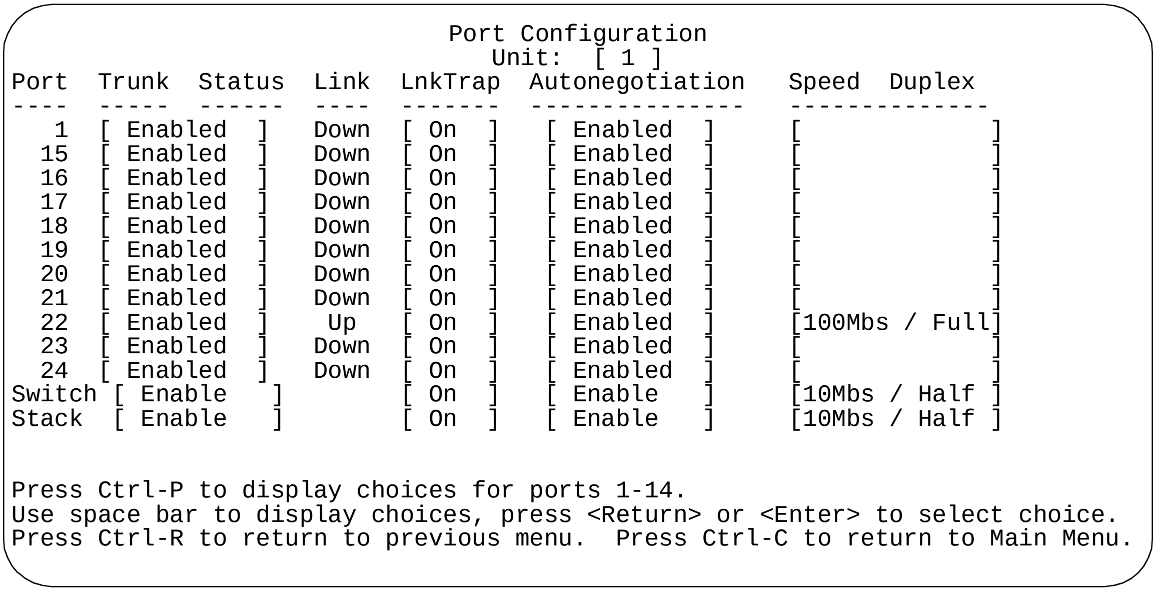
➨ Choose Port Configuration (or press p) from the Switch Configuration Menu screen.

Figure 76 Port Configuration screen (1 of 2)



```
                              Port Configuration
                                 Unit:  [ 1 ]
Port  Trunk  Status  Link  LnkTrap  Autonegotiation   Speed  Duplex
----  -----  ------  ----  -------  ---------------   --------------
   1  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
   2  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
   3  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
   4  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
   5  [ Enabled  ]    Up   [ On  ]   [ Enabled  ]     [100Mbs / Half]
   6  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
   7  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
   8  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
   9  [ Enabled  ]    Up   [ On  ]   [ Enabled  ]     [100Mbs / Full]
  10  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
  11  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
  12  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
  13  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
  14  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]

                                                             More...

Press Ctrl-N to display choices for additional ports.
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Figure 77 Port Configuration screen (2 of 2)



```
                              Port Configuration
                                 Unit:  [ 1 ]
Port  Trunk  Status  Link  LnkTrap  Autonegotiation   Speed  Duplex
----  -----  ------  ----  -------  ---------------   --------------
   1  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
  15  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
  16  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
  17  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
  18  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
  19  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
  20  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
  21  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
  22  [ Enabled  ]    Up   [ On  ]   [ Enabled  ]     [100Mbs / Full]
  23  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
  24  [ Enabled  ]   Down  [ On  ]   [ Enabled  ]     [             ]
Switch [ Enable   ]        [ On  ]   [ Enable   ]     [10Mbs / Half ]
Stack  [ Enable   ]        [ On  ]   [ Enable   ]     [10Mbs / Half ]


Press Ctrl-P to display choices for ports 1-14.
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

➡ **Note:** When a gigabit MDA is installed, only the Status field for that MDA port is configurable. See "High Speed Flow Control Configuration screen" on page 222 to set the autonegotiation field for the gigabit MDA port.

Table 29 describes the Port Configuration screen fields.

Table 29 Port Configuration screen fields

Field	Description
Port	Indicates the switch port numbers that correspond to the field values in that row of the screen (for example, the field values in row 2 apply to switch port 2). The values that you set in the *Switch* row will affect all switch ports and, when the switch is part of a stack, the values that you set in the *Stack* row will affect all ports in the entire stack (except the Gigabit MDA ports or fiber optic ports, when installed).
Trunk	The read-only data displayed in this column indicates the trunks that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen (see "MultiLink Trunk Configuration Menu screen" on page 225).
Status	Allows you to disable any of the switch ports. You can also use this field to control access to any switch port. Default Value Enabled Range Enabled, Disabled
Link	A read-only field that indicates 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.
LnkTrap	Allows you to control whether link up/link down traps are sent to the configured trap sink from the switch. Default Value On Range On, Off
Autonegotiation	When enabled, sets the corresponding port speed to match the best service provided by the connected station, up to 100 Mb/s in full-duplex mode. **NOTE:** This field is disabled for all fiber optic ports. Autonegotiation *cannot* be disabled with the ports on the BPS2000-1GT and BPS2000-2GT MDAs. Use the High Speed Flow Control Configuration screen (next) to set autonegotiation for all gigabit ports. Default Value Enabled Range Enabled, Disabled

Table 29 Port Configuration screen fields (continued)

Field	Description
Speed/Duplex*	Allows you to manually configure any port to support an Ethernet speed of 10 Mb/s or 100 Mb/s, in half- or full-duplex mode. This field is set (by default) to 1000 Mb/s, full-duplex for gigabit ports only. **NOTE**: Use the High Speed Flow Control Configuration screen (next) to set autonegotiation for all gigabit ports. Default Value 100Mbs/Half (when Autonegotiation is Disabled) Range 10Mbs/Half, 10Mbs/Full, 100Mbs/Half, 100Mbs/Full

* Fiber optic ports can only be set to 100 Mb/s/Half or 100 Mb/s Full.

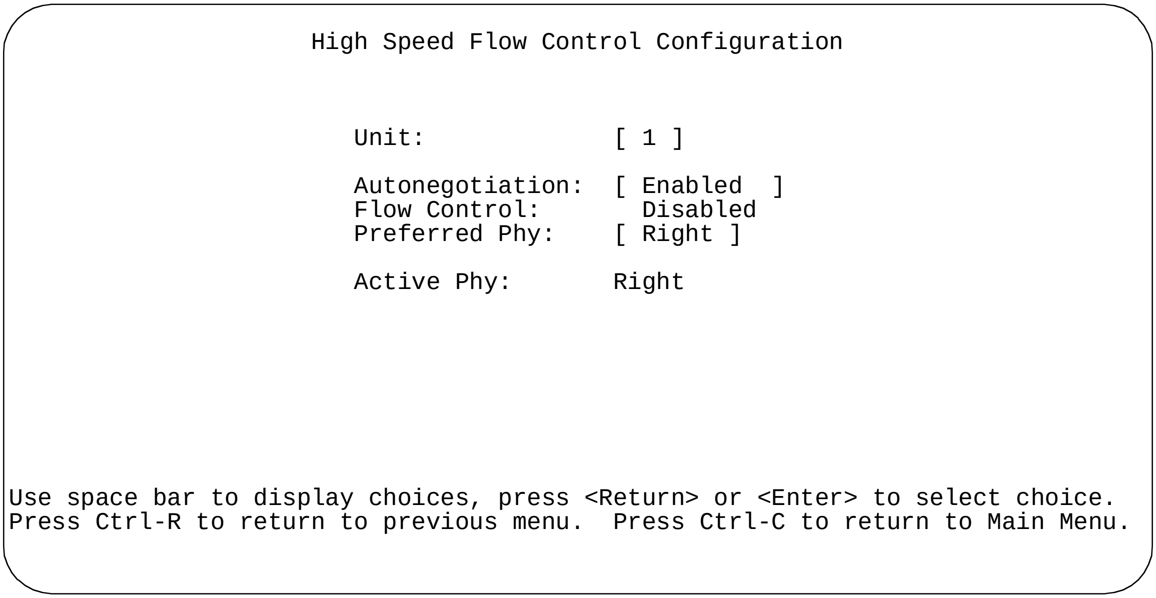
High Speed Flow Control Configuration screen

The High Speed Flow Control Configuration screen (Figure 78) allows you to set the port parameters for installed gigabit MDAs. Use this screen to set autonegotiation for all gigabit ports.

➡ **Note:** This screen only appears when an optional gigabit MDA is installed in the Uplink Module slot.

➨ Choose High Speed Flow Control Configuration (or press h) from the Switch Configuration Menu screen to open the High Speed Flow Control Configuration screen.

Figure 78 High Speed Flow Control Configuration



```
                     High Speed Flow Control Configuration



                        Unit:              [ 1 ]

                        Autonegotiation:   [ Enabled  ]
                        Flow Control:        Disabled
                        Preferred Phy:     [ Right ]

                        Active Phy:        Right









Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 30 describes the High Speed Flow Control Configuration screen fields.

Table 30 High Speed Flow Control Configuration Screen Fields

Field	Description
Unit	Allows you to select the unit number (when stacking is configured) to view or configure. To view or configure another unit, type its unit number and press [Enter], or press the spacebar to toggle the unit numbers (the system only displays a screen for units that are configured with a Gigabit MDA).
Autonegotiation	When enabled, the port only advertises support for 1000 Mb/s operation, in full-duplex mode. **NOTE:** This field is disabled for all fiber optic ports. Autonegotiation *cannot* be disabled with the ports on the BPS2000-1GT and BPS2000-2GT. Default Value Enabled Range Enabled, Disabled

Table 30 High Speed Flow Control Configuration Screen Fields (continued)

Field	Description
Flow Control	Allows you to control traffic and avoid congestion on the Gigabit MDA port. Two modes are available (see "Choosing a high speed flow control mode" for details about the two modes). The Flow Control field cannot be configured unless you set the Autonegotiation field value to Disabled. Default Value Disabled Range Disabled, Symmetric, Asymmetric
Preferred Phy	**Note:** The following two fields only appear when a single MAC MDA (450-1LR-MDA or 450-1SR MDA) with a separate redundant Phy port is installed. Allows you to choose a preferred Phy port; the other Phy port reverts to backup. Default Value Right Range Right, Left
Active Phy	Indicates the operational Phy port. Default Value: None Range: None, Right, Left

Choosing a high speed flow control mode

The high speed flow control feature allows you to control traffic and avoid congestion on the Gigabit full-duplex link. If the receive port buffer becomes full, the Business Policy Switch issues a flow-control signal to the device at the other end of the link to suspend transmission. When the receive buffer is no longer full, the switch issues a signal to resume the transmission. You can choose Symmetric or Asymmetric flow control mode.

Symmetric mode

This mode allows both the Gigabit MDA port and its link partner to send flow control *pause* frames to each other.

When a pause frame is received (by either the Gigabit MDA port or its link partner), the port suspends transmission of frames for a number of slot times specified in the control frame or until a pause-release control frame is received. Both devices on the link must support this mode when it is selected.

Asymmetric mode

This mode allows the link partner to send flow control pause frames to the Gigabit MDA port. When a pause frame is received, the receiving port suspends transmission of frames for a number of slot times specified in the control frame or until a pause-release control frame is received.

In this mode, the Gigabit MDA port is disabled from transmitting pause frames to its link partner. Use this mode when the Gigabit MDA port is connected to a buffered repeater device.

MultiLink Trunk Configuration Menu screen

The MultiLink Trunk Configuration Menu screen (Figure 79) allows you to select the appropriate screen to configure up to six MultiLink Trunks (you can group up to four switch ports together to form each trunk).

You can configure up to six MultiLink Trunks in each stack, with trunk members in either a single unit or distributed between units within the stack configuration (distributed trunking).

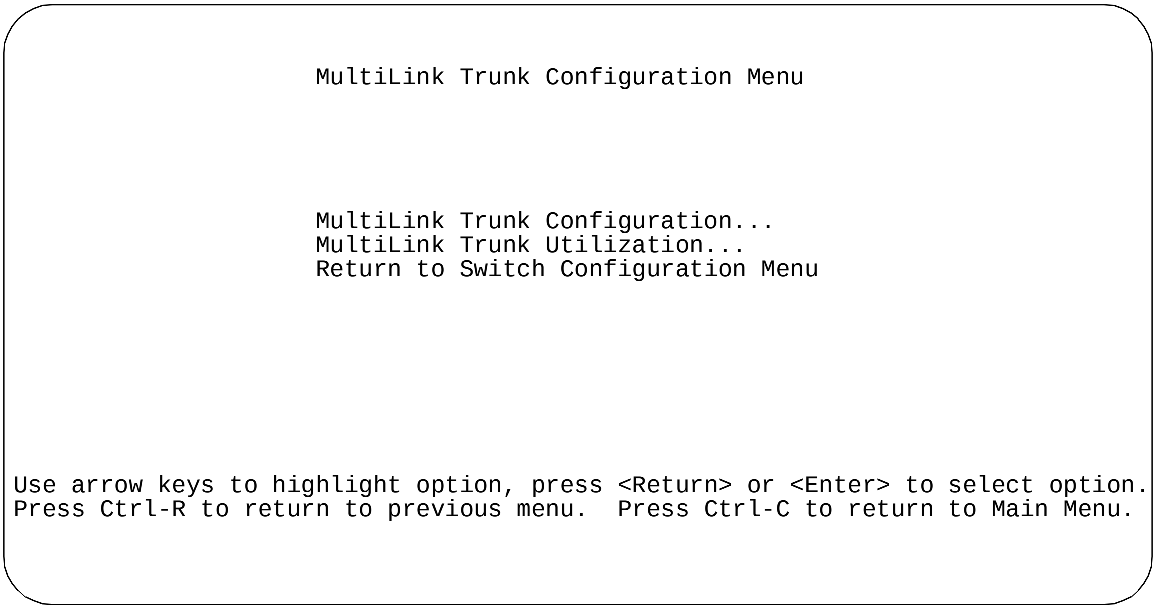
You can monitor the bandwidth usage for the trunk member ports within each trunk. For more information about configuring MultiLink Trunks, see Chapters 1 and 2.

➡ **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.

To open the MultiLink Trunk Configuration Menu screen:

➨ Choose MultiLink Trunk Configuration (or press t) from the Switch Configuration Menu screen.

Figure 79 MultiLink Trunk Configuration Menu screen



```
                     MultiLink Trunk Configuration Menu




                     MultiLink Trunk Configuration...
                     MultiLink Trunk Utilization...
                     Return to Switch Configuration Menu







Use arrow keys to highlight option, press <Return> or <Enter> to select option.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 31 describes the MultiLink Trunk Configuration Menu screen options.

Table 31 MultiLink Trunk Configuration Menu screen options

Option	Description
MultiLink Trunk Configuration...	Displays the MultiLink Trunk Configuration screen (Figure 80). This screen allows you to configure up to six MultiLink Trunks within a standalone switch or within a stack configuration. You can group up to four switch ports together to form each trunk.
MultiLink Trunk Utilization...	Displays the MultiLink Trunk Utilization screen (Figure 81 and Figure 82). This screen allows you to monitor the bandwidth utilization of the configured trunks.

MultiLink Trunk Configuration screen

The MultiLink Trunk Configuration screen (Figure 80) allows you to configure up to six trunks in a standalone switch or stack. In a stack configuration, trunk members can be distributed between any of the units within the same stack configuration.

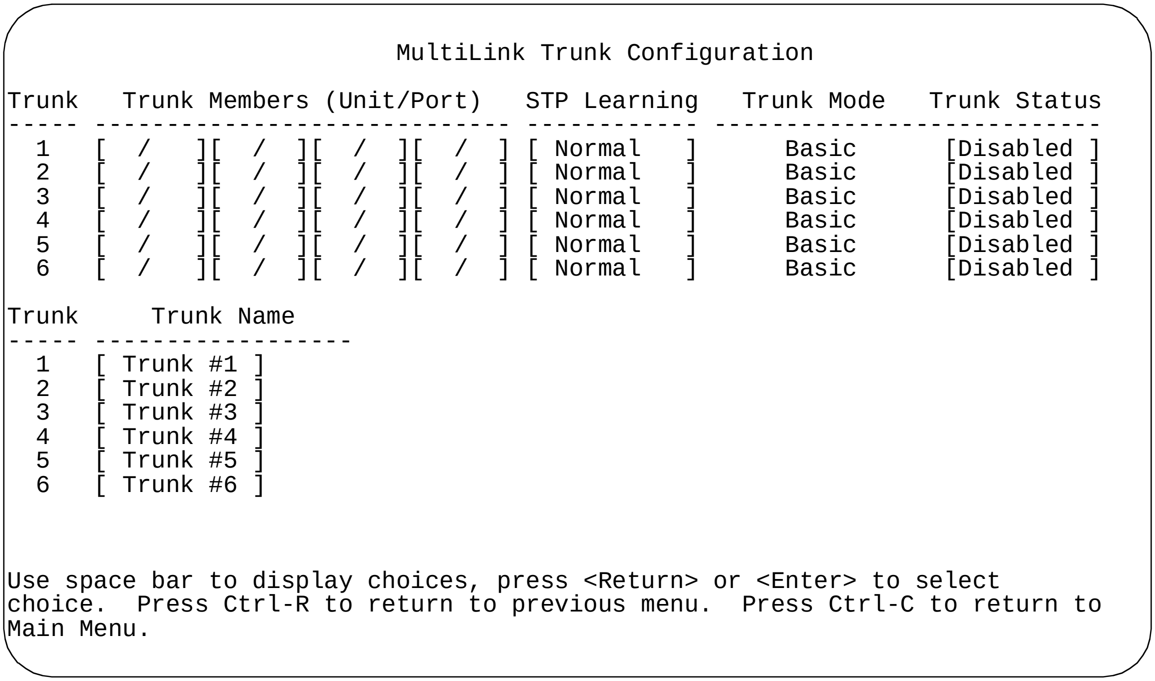
Any mix of up to eight Business Policy Switches *and* BayStack 450 and BayStack 410 switches can be stacked to provide a total of 224 ports (when all MDA slots are configured with the maximum port availability). See Appendix B, for more information about a mixed stack configuration.

When the trunks are enabled, the trunk members take on default settings necessary for correct operation of the MultiLink Trunking feature. These default settings can affect the correct operation of your configured network. If you disable a trunk, you may need to reconfigure the specific trunk members switch ports to return to the previous switch configuration. See Chapter 1 for more information.

To open the MultiLink Trunk Configuration screen:

➨ Choose Trunk Configuration (or press t) from the MultiLink Trunk Configuration Menu screen.

Figure 80 MultiLink Trunk Configuration screen



```
                            MultiLink Trunk Configuration

Trunk   Trunk Members (Unit/Port)   STP Learning   Trunk Mode   Trunk Status
----- ---------------------------- ------------ --------------------------
  1   [  /   ][  /  ][  /  ][  /  ] [ Normal   ]     Basic      [Disabled ]
  2   [  /   ][  /  ][  /  ][  /  ] [ Normal   ]     Basic      [Disabled ]
  3   [  /   ][  /  ][  /  ][  /  ] [ Normal   ]     Basic      [Disabled ]
  4   [  /   ][  /  ][  /  ][  /  ] [ Normal   ]     Basic      [Disabled ]
  5   [  /   ][  /  ][  /  ][  /  ] [ Normal   ]     Basic      [Disabled ]
  6   [  /   ][  /  ][  /  ][  /  ] [ Normal   ]     Basic      [Disabled ]

Trunk     Trunk Name
----- -----------------
  1   [ Trunk #1 ]
  2   [ Trunk #2 ]
  3   [ Trunk #3 ]
  4   [ Trunk #4 ]
  5   [ Trunk #5 ]
  6   [ Trunk #6 ]



Use space bar to display choices, press <Return> or <Enter> to select
choice.  Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to
Main Menu.
```

Table 32 describes the MultiLink Trunk Configuration screen fields.

Table 32 MultiLink Trunk Configuration screen fields

Field	Description
Trunk	Column header for the read-only fields in this screen. The read-only data displayed in the Trunk column indicates the trunk (1 to 6) that corresponds to the switch ports specified in the user-configurable Trunk Members fields.
Trunk Members (Unit/Port)	The Trunk Members 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. Default Value Blank Range 1 to 8 or 1 to 28 (depending on model type)
STP Learning	The STP Learning column contains a single field for each row that, when enabled, allows the specified trunk to participate in the spanning tree. This setting overrides those of the individual trunk members. Fast is the same as Normal, except that the state transition timer is shortened to two seconds. Default Value Normal Range Normal, Fast, Disabled
Trunk Mode	The Trunk Mode column contains a single read only field for each row that indicates the default operating mode for the switch. **Basic:** Basic mode is the default mode for the switch. When in this mode, source MAC addresses are dynamically assigned to specific trunk members for flooding and forwarding, which allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.
Trunk Status	The Trunk Status column contains a single field for each row that allows users to enable or disable any of the trunks. Default Value Disabled Range Enabled, Disabled
Trunk Name	The Trunk Name column contains a single optional field in each row that can be used to assign names to the corresponding configured trunks. The names chosen for this example can provide meaningful information to the user (for example, S1:T1 to FS2 indicates Trunk 1, in switch S1 connects to File Server 2).

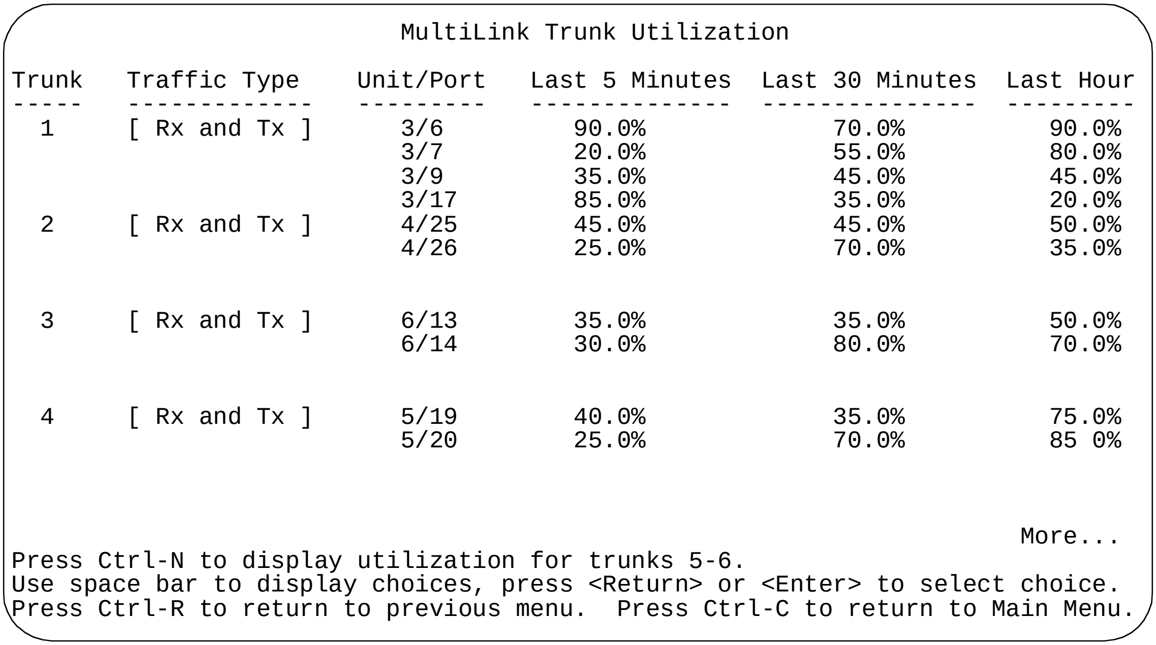
MultiLink Trunk Utilization screen

The MultiLink Trunk Utilization screen (Figure 81 and Figure 82) allows you to monitor the percentage of bandwidth used by configured trunk members. You can choose the type of traffic to monitor.

Figure 81 shows an *example* of bandwidth utilization rates for trunk member ports. Because two screens are necessary to show all of the configured trunks (up to six), the screen prompts you to Press [Ctrl]-N to view trunks five and six.

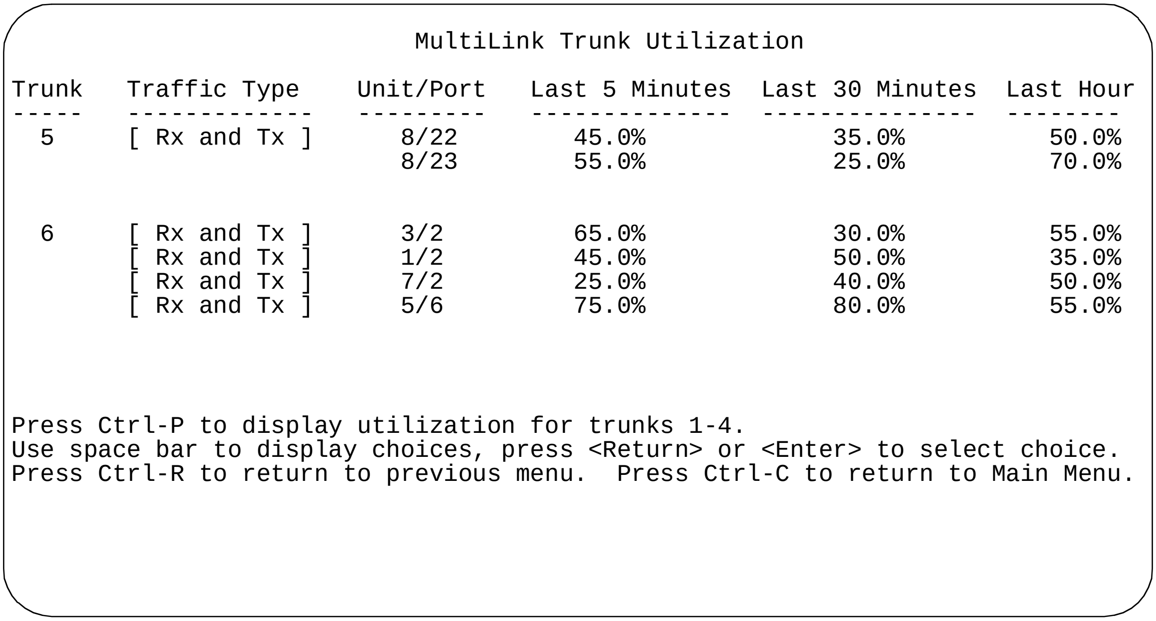
➨ Choose MultiLink Trunk Utilization (or press u) from the MultiLink Trunk Configuration Menu screen to open the MultiLink Trunk Utilization screen.

Figure 81 MultiLink Trunk Utilization screen (1 of 2)



```
                           MultiLink Trunk Utilization

Trunk   Traffic Type    Unit/Port   Last 5 Minutes  Last 30 Minutes  Last Hour
-----   -------------   ---------   --------------  ---------------  ---------
  1     [ Rx and Tx ]      3/6         90.0%             70.0%          90.0%
                           3/7         20.0%             55.0%          80.0%
                           3/9         35.0%             45.0%          45.0%
                           3/17        85.0%             35.0%          20.0%
  2     [ Rx and Tx ]      4/25        45.0%             45.0%          50.0%
                           4/26        25.0%             70.0%          35.0%


  3     [ Rx and Tx ]      6/13        35.0%             35.0%          50.0%
                           6/14        30.0%             80.0%          70.0%


  4     [ Rx and Tx ]      5/19        40.0%             35.0%          75.0%
                           5/20        25.0%             70.0%          85 0%




                                                                      More...
Press Ctrl-N to display utilization for trunks 5-6.
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Figure 82 MultiLink Trunk Utilization screen (2 of 2)



```
                                MultiLink Trunk Utilization

Trunk   Traffic Type    Unit/Port   Last 5 Minutes  Last 30 Minutes  Last Hour
-----   -------------   ---------   --------------  ---------------  --------
  5     [ Rx and Tx ]      8/22        45.0%              35.0%          50.0%
                           8/23        55.0%              25.0%          70.0%


  6     [ Rx and Tx ]      3/2         65.0%              30.0%          55.0%
        [ Rx and Tx ]      1/2         45.0%              50.0%          35.0%
        [ Rx and Tx ]      7/2         25.0%              40.0%          50.0%
        [ Rx and Tx ]      5/6         75.0%              80.0%          55.0%




Press Ctrl-P to display utilization for trunks 1-4.
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 33 describes the MultiLink Trunk Utilization screen fields.

Table 33 MultiLink Trunk Utilization screen fields

Field	Description
Trunk	Column header for the read-only fields in this screen. The read-only data displayed in this column indicates the trunk (1 to 6) that corresponds to the switch ports specified in the Port field.
Traffic Type	Allows you to choose the traffic type to be monitored for percent of bandwidth utilization (see Range). Default Value Rx and Tx Range Rx and Tx, Rx, Tx
Unit/Port	Lists the trunk member ports that correspond to the trunk specified in the Trunk column. The (Unit/) extension to the Port column name only appears when the switch (unit) is part of a stack configuration. It indicates that the ports in this row are associated with the specified unit number configured in the Unit field.
Last 5 Minutes	This read-only field indicates the percentage of packets (of the type specified in the Traffic Type field) utilized by the port in the last 5 minutes. This field provides a running average of network activity and is updated every 15 seconds.

Table 33 MultiLink Trunk Utilization screen fields (continued)

Field	Description
Last 30 Minutes	This read-only field indicates the percentage of packets (of the type specified in the Traffic Type field) utilized 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	This read-only field indicates the percentage of packets (of the type specified in the Traffic Type field) utilized by the port in the last 60 minutes. This field provides a running average of network activity and is updated every 15 seconds.

Port Mirroring Configuration screen

The Port Mirroring Configuration screen allows you to configure a specific switch port to monitor up to two specified ports or two MAC addresses. You can specify port-based monitoring or address-based monitoring. In a stack configuration, you can monitor ports that reside on different units within the stack.

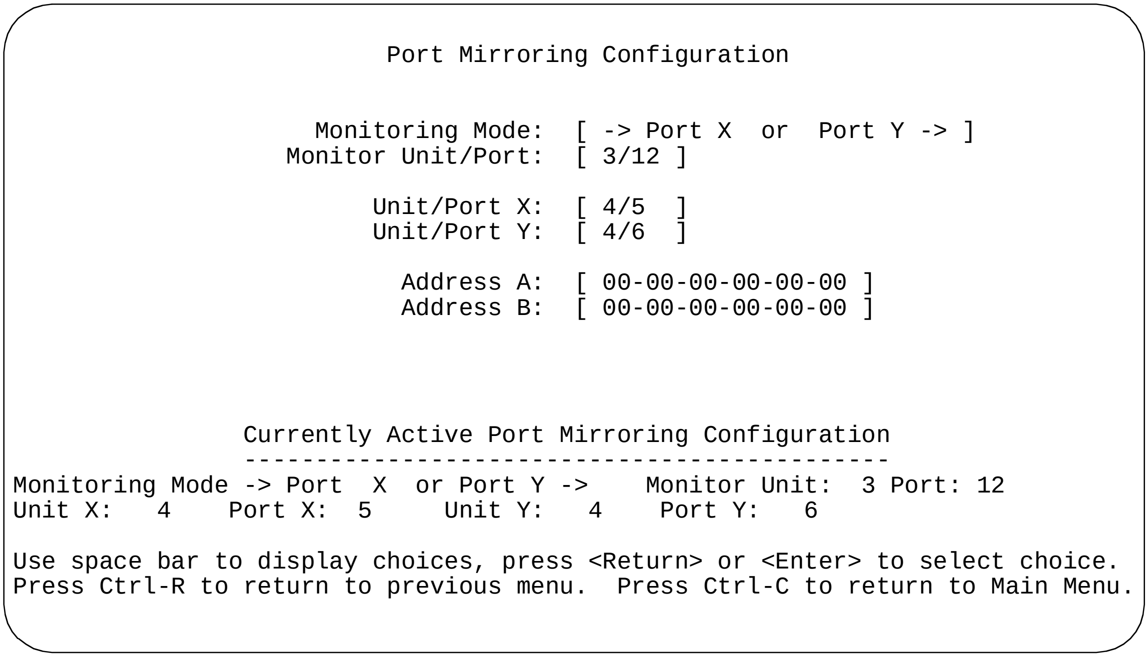
For more information about the port mirroring feature, see Chapter 1.

Figure 83 shows an example of a Port Mirroring Configuration screen, in a stack configuration, where port 12 (in stack unit 3) is designated as the monitoring port for ports 5 and 6 of stack unit 4. When installed as a standalone switch, the screen does not display the (Unit/) field designation.

To open the Port Mirroring Configuration screen:

➨ Choose Port Mirroring Configuration (or press i) from the Switch Configuration Menu screen.

Figure 83 Port Mirror Configuration screen



```
                          Port Mirroring Configuration


                     Monitoring Mode:  [ -> Port X  or  Port Y -> ]
                   Monitor Unit/Port:  [ 3/12 ]

                         Unit/Port X:  [ 4/5  ]
                         Unit/Port Y:  [ 4/6  ]

                           Address A:  [ 00-00-00-00-00-00 ]
                           Address B:  [ 00-00-00-00-00-00 ]




                Currently Active Port Mirroring Configuration
                ---------------------------------------------
Monitoring Mode -> Port  X  or Port Y ->    Monitor Unit:  3 Port: 12
Unit X:   4    Port X:  5     Unit Y:   4    Port Y:   6

Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 34 describes the Port Mirroring Configuration screen fields.

Table 34 Port Mirroring Configuration screen fields

Field	Description
Monitoring Mode	Allows a user to select any one of six port-based monitoring modes or any one of five address-based monitoring modes (see Table 35). Selecting any one of the six *port-based modes* activates the port X and port Y screen fields, where a user can choose up to two ports to monitor. Selecting any one of the five *address-based modes* activates the Address A and Address B screen fields, where a user can specify MAC addresses to monitor. Default Value Disabled Range See Table 35
Monitor Unit/Port	Indicates the port number (of the specified unit) that is designated as the monitor port. Default Value Zero-length string Range 1 to 8/ 1 to 28 (depending on model type)

Table 34 Port Mirroring Configuration screen fields (continued)

Field	Description
Unit/Port X	Indicates one of the ports (of the specified unit) that will be monitored by the designated port monitor when one of the port-based monitoring modes is selected. This port will be monitored according to the value of Port X in the Monitoring Mode field (see Table 35). Default Value Zero-length string Range 1 to 8/ 1 to 28 (depending on model type)
Unit/Port Y	Indicates one of the ports (of the specified unit) that will be monitored by the designated port monitor when one of the port-based monitoring modes is selected. When installed as a standalone switch, the screen does not display the (Unit/) field designation. This port will be monitored according to the value of Port Y in the Monitoring Mode field (see Table 35). Default Value Zero-length string Range 1 to 8/ 1 to 28 (depending on model type)
Address A	Indicates the MAC addresses that will be monitored by the designated port monitor when one of the address-based monitoring modes is selected. This port will be monitored according to the value of Address A in the selected Monitoring Mode field (see Table 35). Default Value 00-00-00-00-00-00 (no MAC address assigned) Range 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF
Address B	Indicates the MAC addresses that will be monitored by the designated port monitor when one of the address-based monitoring modes is selected. This port will be monitored according to the value of Address B in the selected Monitoring Mode field (see Table 35). Default Value 00-00-00-00-00-00 (no MAC address assigned) Range 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF

Table 35 describes the various monitoring modes available from the Port Mirroring Configuration screen.

Table 35 Monitoring modes

Field	Description
Port-based:	
Disabled	Default value for this feature.
-> Port X	Monitor all traffic received by Port X.
Port X ->	Monitor all traffic transmitted by Port X.
<-> Port X	Monitor all traffic received and transmitted by Port X.
-> Port X or Port Y ->	Monitor all traffic received by Port X or transmitted by Port Y. Note: Do not use this mode for broadcast or multicast traffic.
-> Port X and Port Y ->	Monitor all traffic received by Port X (destined to Port Y) and then transmitted by Port Y. Note: Do not use this mode for broadcast or multicast traffic
<-> Port X and Port Y <->	Monitor all traffic received/transmitted by Port X and received/ transmitted by Port Y. Note: Do not use this mode for broadcast or multicast traffic
Address-based:	
Disabled	Default value for this feature.
Address A -> any Address	Monitor all traffic transmitted from Address A to any address.
any Address -> Address A	Monitor all traffic received by Address A from any address.
<-> Address A	Monitor all traffic received by or transmitted by Address A.
Address A -> Address B	Monitor all traffic transmitted by Address A to Address B.
Address A <-> Address B	Monitor all traffic between Address A and Address B (conversation between the two stations).

Rate Limiting Configuration screen

The Rate Limiting Configuration screen allows you to limit the forwarding rate of broadcast and multicast packets.

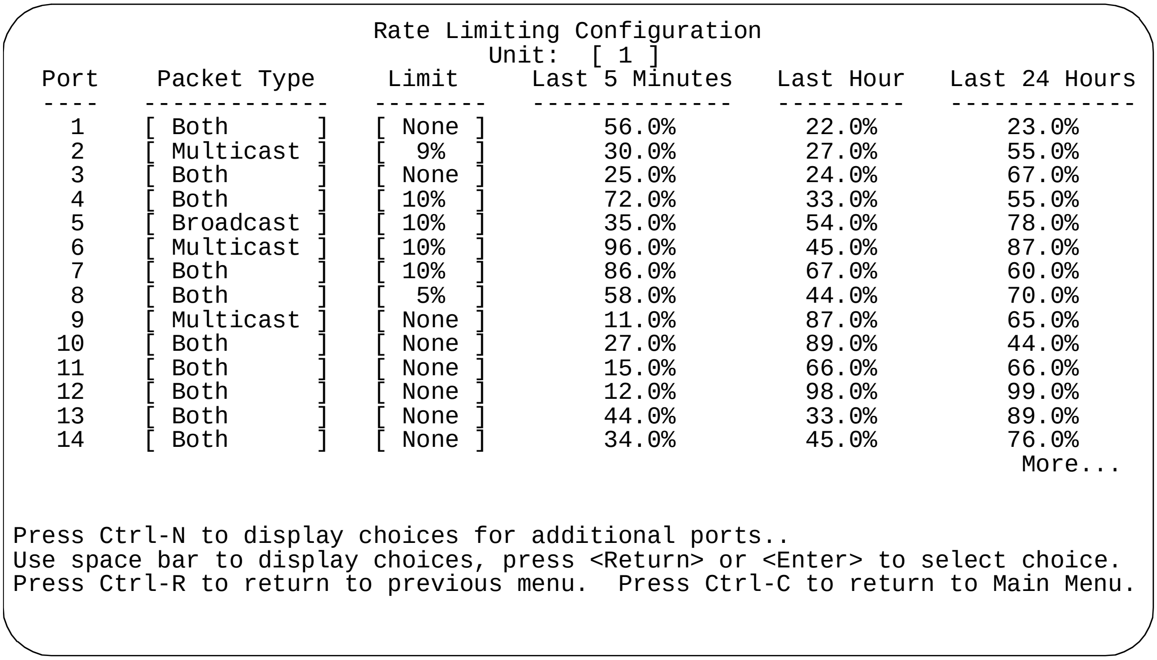
Figures 84 and 85 show sample rate limiting values for the two Rate Limiting Configuration screens.

➡ **Note:** If a port is configured for rate limiting, and it is a MultiLink Trunk member, all trunk member ports implement rate limiting. Also, if a trunk member is implementing rate limiting and the port is disabled from rate limiting, all trunk members are disabled from rate limiting.

To open the Rate Limiting Configuration screen:

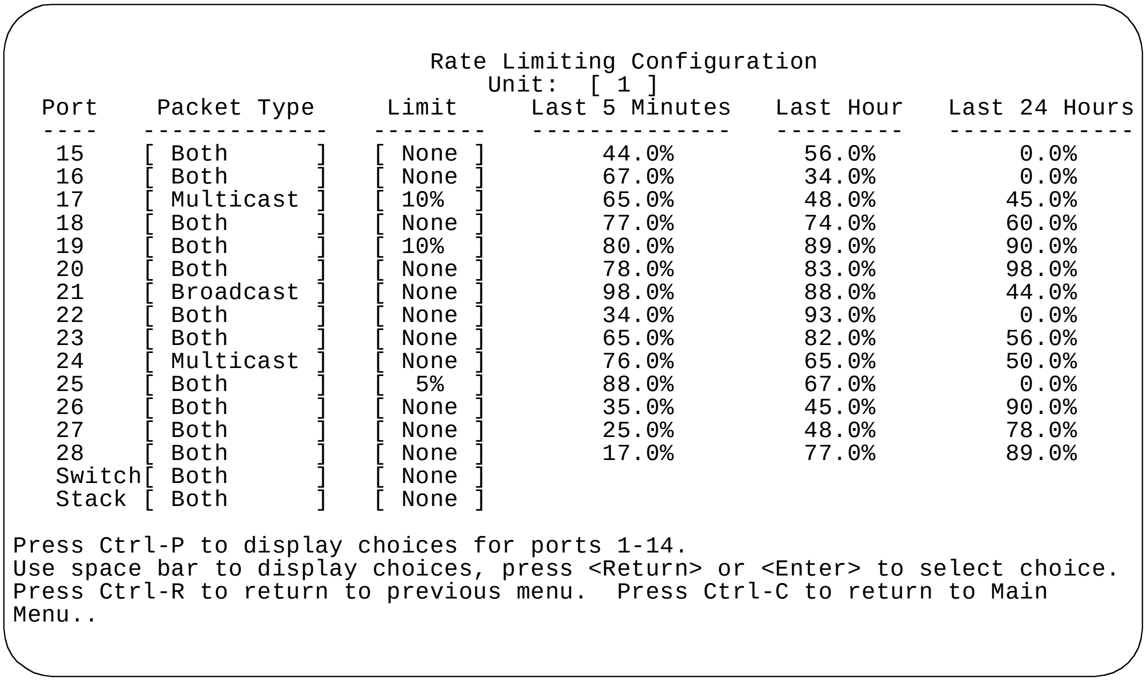
➨ Choose Rate Limiting Configuration (or press l) from the Switch Configuration Menu screen.

Figure 84 Rate Limiting Configuration screen (1 of 2)



```
                         Rate Limiting Configuration
                                 Unit:  [ 1 ]
  Port    Packet Type     Limit     Last 5 Minutes   Last Hour   Last 24 Hours
  ----   -------------   --------   --------------   ---------   -------------
    1    [ Both      ]   [ None ]        56.0%         22.0%         23.0%
    2    [ Multicast ]   [  9%  ]        30.0%         27.0%         55.0%
    3    [ Both      ]   [ None ]        25.0%         24.0%         67.0%
    4    [ Both      ]   [ 10%  ]        72.0%         33.0%         55.0%
    5    [ Broadcast ]   [ 10%  ]        35.0%         54.0%         78.0%
    6    [ Multicast ]   [ 10%  ]        96.0%         45.0%         87.0%
    7    [ Both      ]   [ 10%  ]        86.0%         67.0%         60.0%
    8    [ Both      ]   [  5%  ]        58.0%         44.0%         70.0%
    9    [ Multicast ]   [ None ]        11.0%         87.0%         65.0%
   10    [ Both      ]   [ None ]        27.0%         89.0%         44.0%
   11    [ Both      ]   [ None ]        15.0%         66.0%         66.0%
   12    [ Both      ]   [ None ]        12.0%         98.0%         99.0%
   13    [ Both      ]   [ None ]        44.0%         33.0%         89.0%
   14    [ Both      ]   [ None ]        34.0%         45.0%         76.0%
                                                                      More...


Press Ctrl-N to display choices for additional ports..
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Figure 85 Rate Limiting Configuration screen (2 of 2)



```
                           Rate Limiting Configuration
                               Unit:  [ 1 ]
  Port    Packet Type     Limit     Last 5 Minutes   Last Hour   Last 24 Hours
  ----   -------------   --------   --------------   ---------   -------------
   15    [ Both      ]   [ None ]       44.0%          56.0%          0.0%
   16    [ Both      ]   [ None ]       67.0%          34.0%          0.0%
   17    [ Multicast ]   [ 10%  ]       65.0%          48.0%         45.0%
   18    [ Both      ]   [ None ]       77.0%          74.0%         60.0%
   19    [ Both      ]   [ 10%  ]       80.0%          89.0%         90.0%
   20    [ Both      ]   [ None ]       78.0%          83.0%         98.0%
   21    [ Broadcast ]   [ None ]       98.0%          88.0%         44.0%
   22    [ Both      ]   [ None ]       34.0%          93.0%          0.0%
   23    [ Both      ]   [ None ]       65.0%          82.0%         56.0%
   24    [ Multicast ]   [ None ]       76.0%          65.0%         50.0%
   25    [ Both      ]   [  5%  ]       88.0%          67.0%          0.0%
   26    [ Both      ]   [ None ]       35.0%          45.0%         90.0%
   27    [ Both      ]   [ None ]       25.0%          48.0%         78.0%
   28    [ Both      ]   [ None ]       17.0%          77.0%         89.0%
   Switch[ Both      ]   [ None ]
   Stack [ Both      ]   [ None ]

Press Ctrl-P to display choices for ports 1-14.
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main
Menu..
```

You can use this screen to view the percentage of either packet type (or both packet types) received on each port.

When the volume of either packet type 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. The percentage you set refers to the total available bandwidth, not to a percentage of current traffic. Table 36 describes the Rate Limiting Configuration screen fields.

Table 36 Rate Limiting Configuration screen fields

Field	Description
Port	Indicates the switch port numbers that correspond to the field values in that row of the screen (for example, the field values in row 2 apply to switch port 2). Note that the values applied in the Switch or Stack row (last 2 rows) affect all standalone switch ports or all switch ports in a stack.
Packet Type	Allows you to select the packet types for rate-limiting or viewing. Default Value Both Range Both, Multicast, Broadcast
Limit	Sets the percentage of port bandwidth allowed for forwarding the packet types specified in the Packet Type field. When the threshold is exceeded, any additional packets (specified in the Packet Type field) are discarded*. Default Value None Range None, 10%, 9%, 8%, 7%, 6%, 5%, 4%, 3%, 2%, 1%
Last 5 Minutes	This read-only field indicates the percentage of packets (of the type specified in the Packet Type field) received by the port in the last 5 minutes. This field provides a running average of network activity and is updated every 15 seconds. Note that this field indicates the receiving port's view of network activity, regardless of the rate-limiting setting.
Last Hour	This read-only field indicates the percentage of packets (of the type specified in the Packet Type field) received by the port in the last hour. This field provides a running average of network activity and is updated every 5 minutes. Note that this field indicates the receiving port's view of network activity, regardless of the rate-limiting setting.
Last 24 Hours	This read-only field indicates the percentage of packets (of the type specified in the Packet Type field) received by the port in the last 24 hours. This field provides a running average of network activity and is updated every hour. Note that this field indicates the receiving port's view of network activity, regardless of the rate-limiting setting.

* 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.

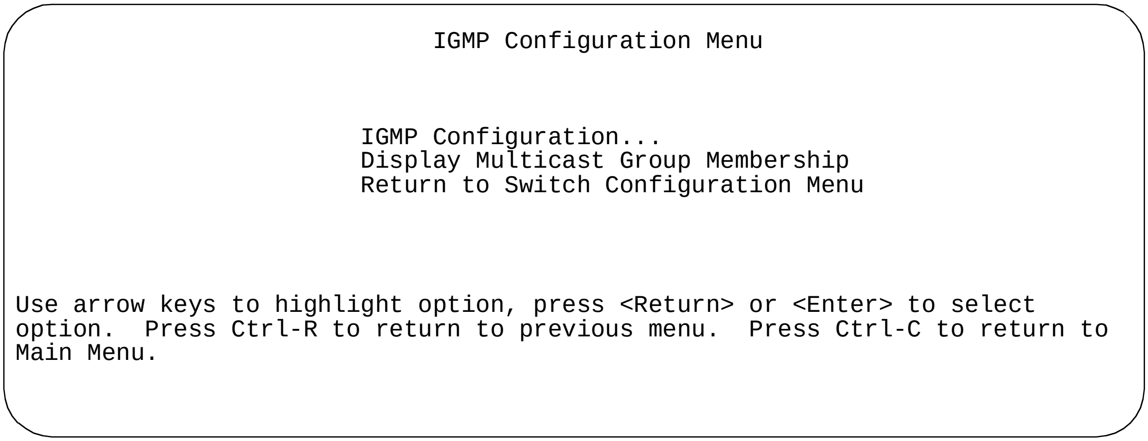
IGMP Configuration Menu screen

The IGMP Configuration Menu screen (Figure 86) allows you to select the appropriate screen to optimize IP Multicast packets in a bridged Ethernet environment (see Chapter 1).

To open the IGMP Configuration Menu screen:

➨ Choose IGMP Configuration (or press g) from the Switch Configuration Menu screen.

Figure 86 IGMP Configuration Menu screen



```
                              IGMP Configuration Menu


                         IGMP Configuration...
                         Display Multicast Group Membership
                         Return to Switch Configuration Menu




Use arrow keys to highlight option, press <Return> or <Enter> to select
option.  Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to
Main Menu.
```

Table 37 describes the IGMP Configuration Menu screen options.

Table 37 IGMP Configuration Menu screen options

Option	Description
IGMP Configuration...	Displays the IGMP Configuration screen (see "IGMP Configuration screen" on page 239). This screen allows you to set up IGMP VLAN configurations.
Display Multicast Group Membership...	Displays the Multicast Group Membership screen (see"Multicast Group Membership screen" on page 242. This screen allows you to view all IP Multicast addresses that are active in the current LAN.

IGMP Configuration screen

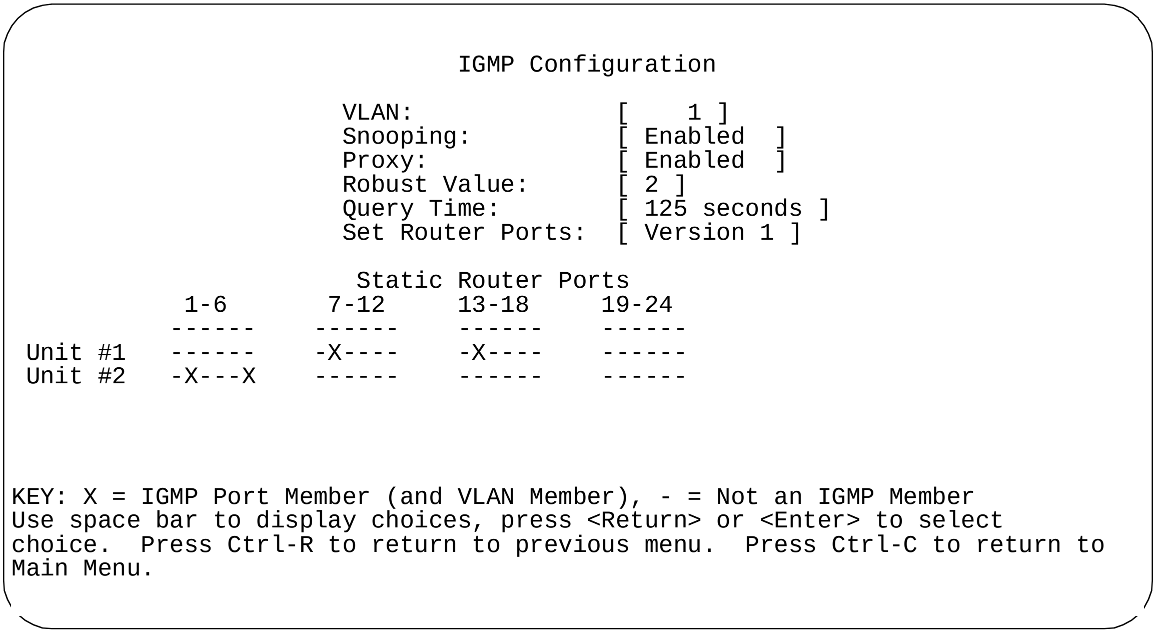
Figure 87 shows an example of the IGMP Configuration screen in a stacked configuration. When installed as a standalone switch, the screen does not display the Unit # field designation.

In this example, switch ports 8 and 14 of unit 1, ports 2 and 6 of unit 2, and port 16 of unit 4 are set to receive/transmit multicast from the local multicast router. The configured ports are VLAN port members of VLAN 5.

To open the IGMP Configuration screen:

➨ Choose IGMP Configuration (or press g) from the Switch Configuration Menu screen.

Figure 87 IGMP Configuration screen



```
                               IGMP Configuration

                       VLAN:               [    1 ]
                       Snooping:           [ Enabled  ]
                       Proxy:              [ Enabled  ]
                       Robust Value:       [ 2 ]
                       Query Time:         [ 125 seconds ]
                       Set Router Ports:   [ Version 1 ]

                        Static Router Ports
            1-6       7-12     13-18     19-24
           ------    ------    ------    ------
 Unit #1   ------    -X----    -X----    ------
 Unit #2   -X---X    ------    ------    ------




KEY: X = IGMP Port Member (and VLAN Member), - = Not an IGMP Member
Use space bar to display choices, press <Return> or <Enter> to select
choice.  Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to
Main Menu.
```

Table 38 describes the IGMP Configuration screen fields.

Table 38 IGMP Configuration screen fields

Field	Description
VLAN	Allows you to set up or view IGMP VLAN configurations on specified VLANs. You can use the space bar to toggle to any *existing* IGMP VLAN configurations (the maximum number of VLANs that can be displayed is 256). Default 1 Range 1 to 4094
Snooping	Allows you to enable or disable IGMP Snooping. This field affects all VLANs (for example, if you disable snooping on the VLAN specified in the screen's VLAN field, ALL VLANs are disabled for snooping). Default Value Enabled Range Enabled, Disabled

Table 38 IGMP Configuration screen fields (continued)

Field	Description	
Proxy	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. This field affects all VLANs (for example, if you disable proxy on the VLAN specified in the screen’s VLAN field, ALL VLANs are disabled for proxy). The Proxy field cannot be disabled unless the Snooping field is enabled.	
	Default Value	Enabled
	Range	Enabled, Disabled
Robust Value	Allows a user 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. This field affects only the VLAN specified in the screen’s VLAN field (for example, if you change the robust value on the VLAN specified in the screen’s VLAN field, other VLANs are not affected).	
	Default Value	2
	Range	1 to 256
Query Time	Allows a user to control the number of IGMP messages allowed on the subnet by varying the *Query Interval* (the Query Interval is the interval between general queries sent by the multicast router). This field affects only the VLAN specified in the screen’s VLAN field (for example, if you change the Query Time value field on the VLAN specified in the screen’s VLAN field, other VLANs are not affected).	
	Default Value	125 seconds
	Range	1 to 512 seconds
Set Router Ports	Selects the IGMP version according to the IGMPv1 (Version 1) or IGMPv2 (Version 2) standard (see RFC 2236). Use this field in conjunction with the Static Router Ports field (see next field description) to select the IGMP version to set. You can also use this field to view which static router ports are set to Version 1 or to Version 2. Use the space bar to toggle between the two versions and view the static router ports settings. This field affects all VLANs (for example, if you change the value of the Set Router Ports field on the VLAN specified in the screen’s VLAN field, ALL VLANs are affected).	
	Default Value	Version 1
	Range	Version 1, Version 2

Table 38 IGMP Configuration screen fields (continued)

Field	Description
Static Router Ports	Allows a user to assign switch ports to any port that has a path to a multicast router. When the unit is part of a stack configuration, the screen displays the unit numbers of the switches configured in the stack, along with the corresponding ports. The configured ports do not filter any IP Multicast traffic. The Static Router Ports fields are displayed in six-port groups (for example, 1-6, 7-12, 13-18). The number of ports displayed depends on the switch model or type of optional MDA that is installed in the Uplink Module slot. This field affects all VLANs (for example, if you assign a port as a static router port in this screen, the port becomes a static router port for the VLAN specified in the screen's VLAN field, and also for any other VLAN where this port is a member). Default Value - Range -, X

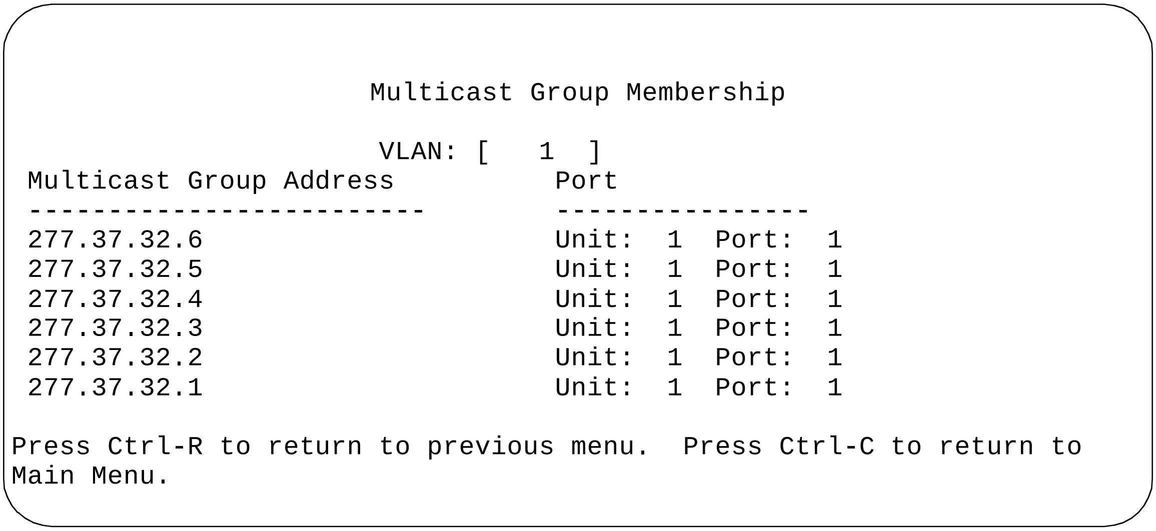
Multicast Group Membership screen

The Multicast Group Membership screen allows you to view configured IP Multicast group addresses for specific VLANs. The screen displays the IP Multicast group addresses associated with ports that are configured within a standalone switch or a stack of switches. The displayed addresses are dynamic and can change as clients join (or leave) the various IP Multicast groups.

To open the Multicast Group Membership screen:

➨ Choose Display Multicast Group Membership (or press d) from the IGMP Configuration Menu screen.

Figure 88 Multicast Group Membership screen



```
                       Multicast Group Membership

                        VLAN: [   1  ]
 Multicast Group Address          Port
 -------------------------        ----------------
 277.37.32.6                      Unit:  1  Port:  1
 277.37.32.5                      Unit:  1  Port:  1
 277.37.32.4                      Unit:  1  Port:  1
 277.37.32.3                      Unit:  1  Port:  1
 277.37.32.2                      Unit:  1  Port:  1
 277.37.32.1                      Unit:  1  Port:  1

Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to
Main Menu.
```

Table 39 describes the Multicast Group Membership screen options.

Table 39 Multicast Group Membership screen options

Option	Description
VLAN	Allows you to view multicast group addresses on specified VLANs. You can use the space bar to view group addresses for any existing IGMP VLAN configurations (the maximum number of VLANs that can be displayed is 256).
Multicast Group Address	Displays all of the IP Multicast group addresses that are currently active on the associated port.
Port	Displays the port numbers that are associated with the IP Multicast group addresses displayed in the IP Multicast group address field.

Port Statistics screen

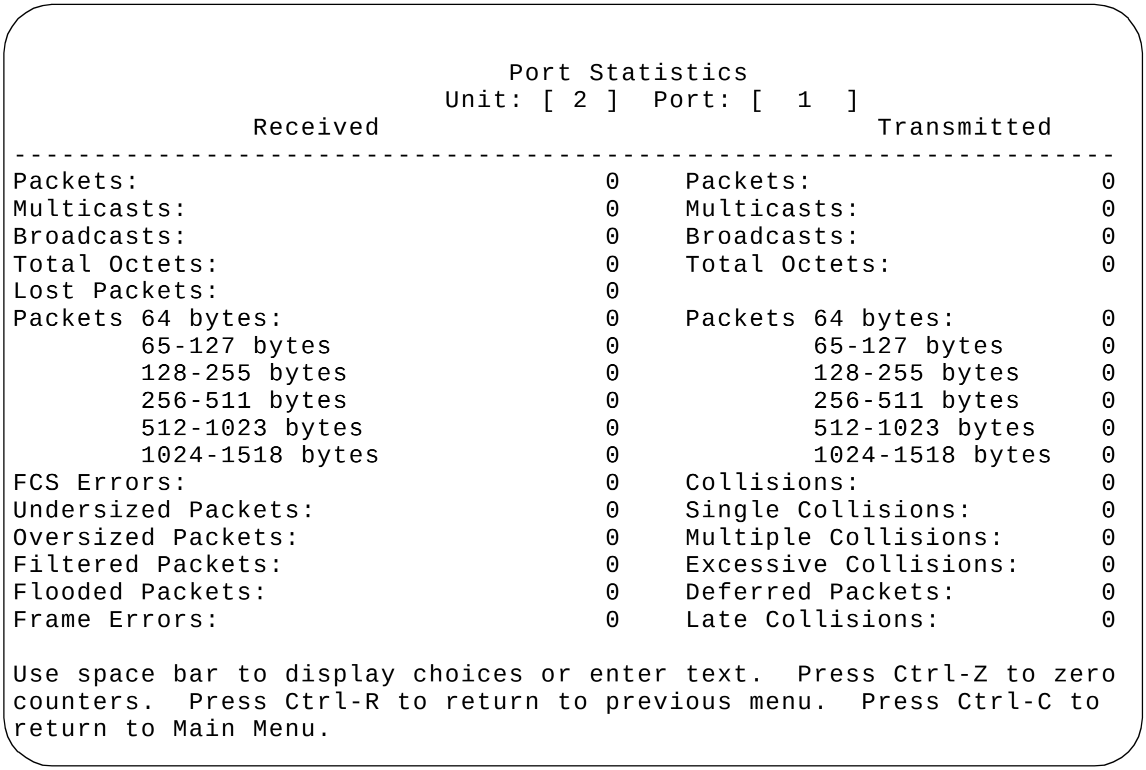
The Port Statistics screen (Figure 89) allows you to view detailed information about any switch or port in a stacked or standalone configuration. The screen is divided into two sections (Received and Transmitted) so that you can compare and evaluate throughput or other port parameters. All screen data is updated approximately every 2 seconds.

You can use the Port Statistics screen to clear (reset to zero) port counters for a specific switch or port. Alternatively, you can use the Clear All Port Statistics option to clear port counters for all switches or ports (see "Switch Configuration Menu screen" on page 181).

To open the Port Statistics screen:

➨ Choose Display Port Statistics (or press d) from the Switch Configuration Menu screen.

Figure 89 Port Statistics screen



```
                               Port Statistics
                           Unit: [ 2 ]  Port: [  1  ]
               Received                               Transmitted
---------------------------------------------------------------------
Packets:                             0    Packets:                  0
Multicasts:                          0    Multicasts:               0
Broadcasts:                          0    Broadcasts:               0
Total Octets:                        0    Total Octets:             0
Lost Packets:                        0
Packets 64 bytes:                    0    Packets 64 bytes:         0
        65-127 bytes                 0            65-127 bytes      0
        128-255 bytes                0            128-255 bytes     0
        256-511 bytes                0            256-511 bytes     0
        512-1023 bytes               0            512-1023 bytes    0
        1024-1518 bytes              0            1024-1518 bytes   0
FCS Errors:                          0    Collisions:               0
Undersized Packets:                  0    Single Collisions:        0
Oversized Packets:                   0    Multiple Collisions:      0
Filtered Packets:                    0    Excessive Collisions:     0
Flooded Packets:                     0    Deferred Packets:         0
Frame Errors:                        0    Late Collisions:          0

Use space bar to display choices or enter text.  Press Ctrl-Z to zero
counters.  Press Ctrl-R to return to previous menu.  Press Ctrl-C to
return to Main Menu.
```

Table 40 describes the Port Statistics screen fields.

Note: In a stacked configuration, the Port Statistics screen appears in a slightly different format when the port selected in the Unit/Port field is configured with a Gigabit MDA.

Table 40 Port Statistics screen fields

Field	Description
Unit	Only appears if the switch is participating in a stack configuration. The field allows you to select the number of the unit you want to view or configure. To view or configure another unit, type its unit number and press [Enter], or press the spacebar on your keyboard to toggle the unit numbers.
Port	Allows you to select the number of the port you want to view or reset to zero. To view another port, type its port number and press [Enter], or press the spacebar on your keyboard to toggle the port numbers.
Packets	Received column: Indicates the total number of packets received on this port, including bad packets, broadcast packets, and multicast packets. Transmitted column: Indicates the total number of packets transmitted successfully on this port, including broadcast packets and multicast packets.
Multicasts	Received column: Indicates the total number of good multicast packets received on this port, excluding broadcast packets. Transmitted column: Indicates the total number of multicast packets transmitted successfully on this port, excluding broadcast packets.
Broadcasts	Received column: Indicates the total number of good broadcast packets received on this port. Transmitted column: Indicates the total number of broadcast packets transmitted successfully on this port.
Total Octets	Received column: Indicates the total number of octets of data (including data in bad packets) received on this port, excluding framing bits but including FCS octets. Transmitted column: Indicates the total number of octets of data transmitted successfully on this port, including FCS octets.
Lost Packets	Received column: Indicates the total number of packets lost (discarded) when the capacity of the port receive buffer was exceeded. Transmitted column: Indicates the total number of packets lost (discarded) when the capacity of the port transmit buffer was exceeded.
Packets 64 bytes	Received column: Indicates the total number of 64-byte packets received on this port. Transmitted column: Indicates the total number of 64-byte packets transmitted successfully on this port.
65-127 bytes	Received column: Indicates the total number of 65-byte to 127-byte packets received on this port. Transmitted column: Indicates the total number of 65-byte to 127-byte packets transmitted successfully on this port.

Table 40 Port Statistics screen fields (continued)

Field	Description
128-255 bytes	Received column: Indicates the total number of 128-byte to 255-byte packets received on this port. Transmitted column: Indicates the total number of 128-byte to 255-byte packets transmitted successfully on this port.
256-511 bytes	Received column: Indicates the total number of 256-byte to 511-byte packets received on this port. Transmitted column: Indicates the total number of 256-byte to 511-byte packets transmitted successfully on this port.
512-1023 bytes	Received column: Indicates the total number of 512-byte to 1023-byte packets received on this port. Transmitted column: Indicates the total number of 512-byte to 1023-byte packets transmitted successfully on this port.
1024-1518 bytes	Received column: Indicates the total number of 1024-byte to 1518-byte packets received on this port. Transmitted column: Indicates the total number of 1024-byte to 1518-byte packets transmitted successfully on this port.
Frame Errors	Indicates the total number of valid-size packets that were received but discarded because of CRC errors and improper framing.
Undersized Packets	Indicates the total 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	Indicates the total number of packets received on this port with more than 1518 bytes and with proper CRC and framing (also known as oversized frames).
Filtered Packets	Indicates the number of packets filtered (not forwarded) by this port.
Flooded Packets	Indicates the total number of packets flooded (forwarded) through this port because the destination address was not in the address database.
FCS Errors	Indicates the total number of valid-size packets that were received with proper framing but discarded because of cyclic redundancy check (CRC) errors.
Collisions	Indicates the total number of collisions detected on this port.
Single Collisions	Indicates the total number of packets that were transmitted successfully on this port after a single collision.
Multiple Collisions	Indicates the total number of packets that were transmitted successfully on this port after more than one collision.
Excessive Collisions	Indicates the total number of packets lost on this port due to excessive collisions.
Deferred Packets	Indicates the total number of frames that were delayed on the first transmission attempt, but never incurred a collision.
Late Collisions	Indicates the total number of packet collisions that occurred after a total length of time that exceeded 512 bit-times of packet transmission.

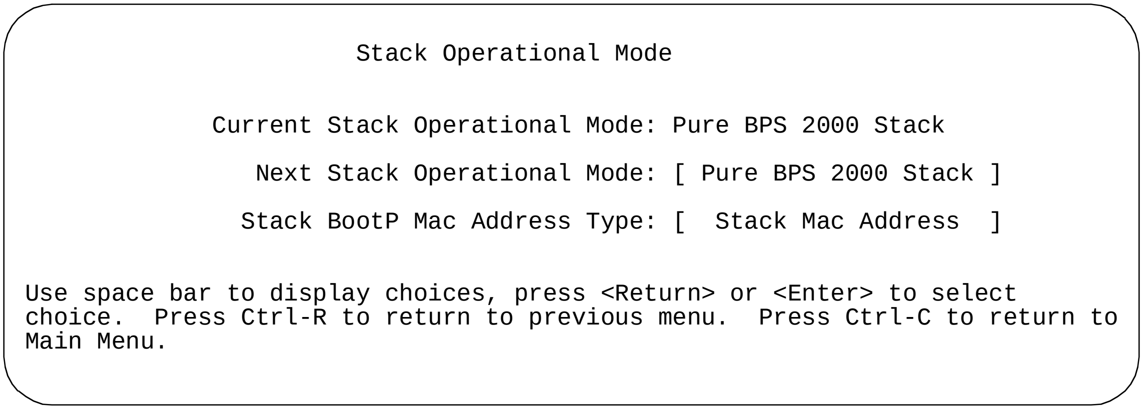
Table 40 Port Statistics screen fields (continued)

Field	Description
The following field values appear only when the port selected in the Unit/Port field is configured with a Gigabit MDA.	
Pause Frames	Transmitted column: Indicates the total number of pause frames transmitted on this port. Pause frames cause the transmitting port to temporarily suspend the transmission of packets when the receiving port's frame buffer is full (Gigabit ports only). Received column: Indicates the total number of pause frames received on this port. Pause frames cause the transmitting port to temporarily suspend the transmission of packets when the receiving port's frame buffer is full (Gigabit ports only).

Stack Operational Mode screen

The Stack Operational Mode screen (Figure 90) displays the current configuration mode for the Business Policy Switch or mixed stack configuration. When the BPS 2000 is reset to factory default settings, the Stack Operational Mode will not be reset. You must especially be aware of this when moving the switch between different stacks.

Figure 90 Stack Operational Mode screen



```
                        Stack Operational Mode


              Current Stack Operational Mode: Pure BPS 2000 Stack

                 Next Stack Operational Mode: [ Pure BPS 2000 Stack ]

                Stack BootP Mac Address Type: [  Stack Mac Address  ]


Use space bar to display choices, press <Return> or <Enter> to select
choice.  Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to
Main Menu.
```

Table 41 describes the Stack Operational Mode screen fields.

Table 41 Stack Operational Mode screen fields

Field	Description
Current Stack Operational Mode	A read-only field that indicates the current mode of your stack. This field identifies a stack that contains only Business Policy Switches or a stack that contains a variety of switches. Default Pure BPS 2000 Stack Range Hybrid Stack, Pure BPS 2000 Stack
Next Stack Operational Mode	Allows you to set the configuration modes of your stack. Press the spacebar to toggle between Hybrid Stack and Pure BPS 2000 Stack options. Reboot the system to implement the change. Default Pure BPS 2000 Stack Range Hybrid Stack, Pure BPS 2000 Stack
Stack BootP Mac Address Type	Allows you to set the location for the BootP MAC address. (The Base Unit Mac Address option is available *only* with Pure BPS 2000 Stack options.) Default Stack Mac Address Range Stack Mac Address, Base Unit Mac Address

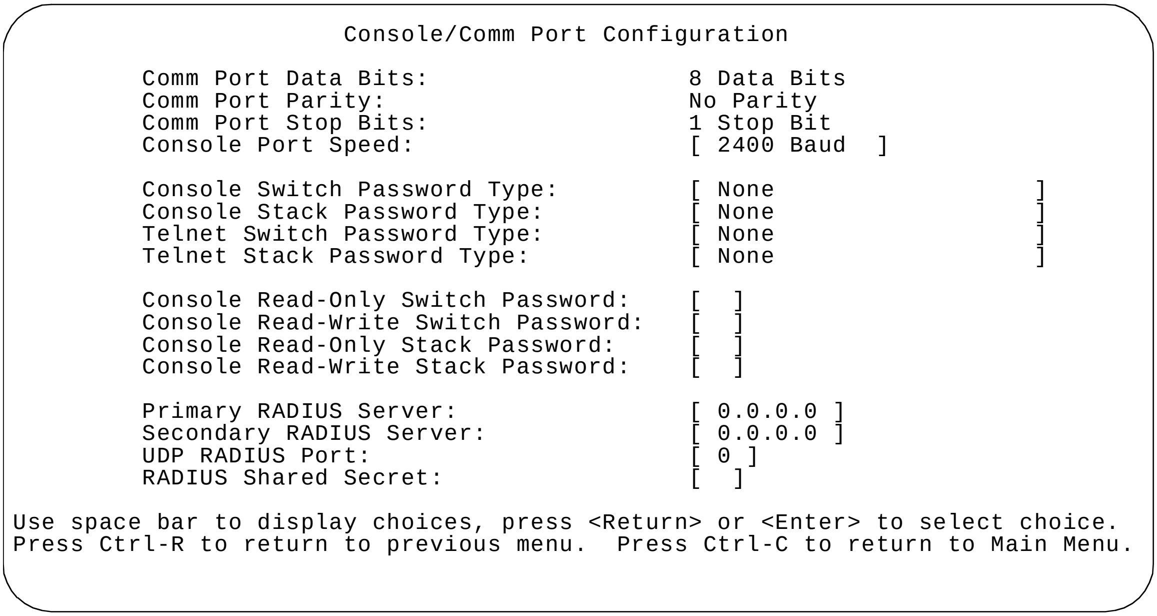
Console/Comm Port Configuration screen

The Console/Comm Port Configuration screen (Figure 91) allows you to configure and modify the console/comm port parameters and security features of a standalone switch or any participating switch in a stack configuration.

To open the Console/Comm Port Configuration screen:

➨ Choose Console/Comm Port Configuration (or press o) from the main menu.

Figure 91 Console/Comm Port Configuration screen



```
                       Console/Comm Port Configuration

         Comm Port Data Bits:                  8 Data Bits
         Comm Port Parity:                     No Parity
         Comm Port Stop Bits:                  1 Stop Bit
         Console Port Speed:                   [ 2400 Baud  ]

         Console Switch Password Type:         [ None                  ]
         Console Stack Password Type:          [ None                  ]
         Telnet Switch Password Type:          [ None                  ]
         Telnet Stack Password Type:           [ None                  ]

         Console Read-Only Switch Password:    [  ]
         Console Read-Write Switch Password:   [  ]
         Console Read-Only Stack Password:     [  ]
         Console Read-Write Stack Password:    [  ]

         Primary RADIUS Server:                [ 0.0.0.0 ]
         Secondary RADIUS Server:              [ 0.0.0.0 ]
         UDP RADIUS Port:                      [ 0 ]
         RADIUS Shared Secret:                 [  ]

Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 42 describes the Console/Comm Port Configuration screen fields.

Table 42 Console/Comm Port Configuration screen fields

Field	Description
Comm Port Data Bits	A read-only field that indicates the current console/comm port data bit setting.
Comm Port Parity	A read-only field that indicates the current console/comm port parity setting.
Comm Port Stop Bits	A read-only field that indicates the current console/comm port stop bit setting.
Console Port Speed	Allows you to set the console/comm port baud rate to match the baud rate of the console terminal. Default Value: 9600 Baud Range: 2400 Baud, 4800 Baud, 9600 Baud, 19200 Baud, 38400 Baud
	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 press [Enter]. If communication is lost, set your console terminal to match the new service port setting.

Table 42 Console/Comm Port Configuration screen fields (continued)

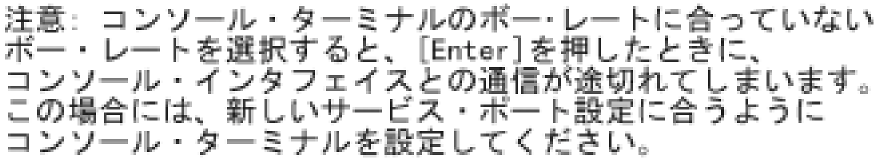
Field	**Description**
	Achtung: Bei Auswahl einer Baud rate, die nicht mit der Baudrate des Konsolenterminals übereinstimmt, geht die Kommunikation mit der Konsolenschnittstelle verloren, wenn Sie die Eingabetaste drücken. Stellen Sie in diesem Fall das Konsolenterminal so ein, daß es mit der neuen Einstellung der Service-Schnittstelle übereinstimmt.
	Attention: Si vous sélectionnez un débit différent de celui de votre terminal, vous perdrez le contact avec l'interface de votre console dès que vous appuierez sur [Entrée]. Pour restaurer la communication, alignez le débit de votre terminal sur le nouveau débit de votre port de service.
	Precaución: Si selecciona una velocidad de transmisión que no coincide con la velocidad de transmisión del terminal de la consola, perderá la comunicación con el interfaz de la consola al pulsar [Intro]. Si se pierde la comunicación, ajuste el terminal de la consola para que coincida con el nuevo valor del puerto de servicio.
	Attenzione: Nel caso in cui si scelga una velocità di trasmissione non corrispondente a quella del terminale della console, la comunicazione con l'interfaccia della console cadrà premendo il tasto [Invio]. Se la comunicazione cade, impostare il terminale della console in modo tale che corrisponda alla nuova impostazione della porta di servizio.
 注意： コンソール・ターミナルのボー・レートに合っていないボー・レートを選択すると、[Enter]を押したときに、コンソール・インタフェイスとの通信が途切れてしまいます。この場合には、新しいサービス・ポート設定に合うようにコンソール・ターミナルを設定してください。	
Console Switch Password Type	Enables password protection for accessing the console interface (CI) of a *standalone switch* through a console terminal. If you set this field to Required, you can use the Logout option to restrict access to the CI. Thereafter, you will need to specify the correct password at the console-terminal prompt. See Console Read-Only Switch Password and Console Read-Write Switch Password for more information. Default Value None Range None, Local Password, RADIUS Authentication

Table 42 Console/Comm Port Configuration screen fields (continued)

Field	Description
Console Stack Password Type	Enables password protection for accessing the console interface (CI) of *any participating switch in a stack configuration* through a console terminal. If you set this field to Required, you can use the Logout option to restrict access to the CI of any stack unit. Thereafter, you will need to specify the correct password at the console-terminal prompt when accessing the stack. See Console Read-Only Stack Password and Console Read-Write Stack Password for more information. Default Value None Range None, Local Password, RADIUS Authentication
TELNET Switch Password Type	Enables password protection for accessing the console interface (CI) of a *standalone switch* through a Telnet session. If you set this field to Required, you can use the Logout option to restrict access to the CI. Thereafter, you will need to specify the correct password at the console-terminal prompt. See Console Read-Only Switch Password and Console Read-Write Switch Password descriptions for more information. Default Value None Range None, Local Password, RADIUS Authentication
TELNET Stack Password Type	Enables password protection for accessing the console interface (CI) of *any participating switch in a stack configuration*, through a Telnet session. If you set this field to Required, you can use the Logout option to restrict access to the CI of any stack unit. Thereafter, you will need to specify the correct password at the console-terminal prompt when accessing the stack. See Console Read-Only Stack Password and Console Read-Write Stack Password for more information. Default Value None Range None, Local Password, RADIUS Authentication
Console Read-Only Switch Password	When the Console Switch Password field is set to Required (for Telnet, for Console, or for Both), this field allows read-only password access to the CI of a *standalone switch*. Users can access the CI using the correct password (see default), but cannot change parameters or use the Reset option or Reset to Default option. Default Value user Range An ASCII string of up to 15 printable characters
Console Read-Write Switch Password	When the Console Switch Password field is set to Required (for Telnet, for Console, or for Both), this field allows read-write password access to the CI of a *standalone switch*. Users can log in to the CI using the correct password (see default) and can change any parameter, except the stack passwords. You can change the default passwords for read-only access and read-write access to a private password.

Table 42 Console/Comm Port Configuration screen fields (continued)

Field	Description
	Default Value: secure Range: Any ASCII string of up to 15 printable characters
	⛔ **Caution:** If you change the system-supplied default passwords, be sure to write the new passwords down and keep them in a safe place. If you forget the new passwords, you cannot access the console interface. In that case, contact Nortel Networks for help.
	⛔ **Achtung:** Wenn Sie die für das System standardmäßig eingestellten Paßwörter ändern, notieren Sie sich die neuen Paßwörter, und bewahren Sie sie an einem sicheren Ort auf. Falls Sie die neuen Paßwörter vergessen, können Sie nicht mehr auf die Konsolenschnittstelle zugreifen. Wenden Sie sich in diesem Fall an Nortel Networks, um Unterstützung zu erhalten.
	⛔ **Attention:** Si vous changez les mots de passe par défaut du système, assurez-vous de bien noter vos nouveaux mots de passe et de les conserver dans un endroit sûr. Si vous perdez vos nouveaux mots de passe, vous ne pourrez plus accéder à votre interface. Le cas échéant, veuillez contacter Nortel Networks.
	⛔ **Precaución:** Si modifica las contraseñas predeterminadas asignadas por el sistema, asegúrese de anotar las nuevas contraseñas y guárdelas en un lugar seguro. Si olvida las nuevas contraseñas, no podrá acceder al interfaz de la consola. En ese caso, póngase en contacto con Nortel Networks para obtener ayuda al respecto.
	⛔ **Attenzione:** In caso di modifica delle password predefinite nel sistema, assicurarsi di annotare le nuove password e di conservarle in un luogo sicuro. Nel caso in cui le nuove password vengano dimenticate, non sarà possibile accedere all'interfaccia della console. In tal caso, contattare la Nortel Networks per avere assistenza.
⛔	注意：システム装備したデフォルトのパスワードを変更する場合、必ず新しいパスワードを書き留めて安全な場所に保管してください。新しいパスワードを忘れてしまうと、コンソール・インタフェイスにアクセスできません。この場合は、Bay Networksまでご連絡ください。

Table 42 Console/Comm Port Configuration screen fields (continued)

Field	Description
Console Read-Only Stack Password	When the Console Switch Password field is set to Required (for Telnet, for Console, or for Both), this field allows read-only password access to the CI of *any participating switch in a stack configuration*. Users can access the CI using the correct password (see default), but cannot change any parameters or use the Reset option or Reset to Default option. Default Value user Range An ASCII string of up to 15 printable characters
Console Read-Write Stack Password	When the Console Switch Password field is set to Local Password (for Telnet, for Console, or for Both), this field allows read-write password access to the CI of *any participating switch in a stack configuration*. Users can log in to the CI using the correct password (see default), and can change any parameter, except the switch password. You can change the default passwords for read-only access and read-write access to a private password. Default Value: secure Range: Any ASCII string of up to 15 printable characters
	Caution: you change the system-supplied default passwords, be sure to write the new passwords down and keep them in a safe place. If you forget the new passwords, you cannot access the console interface. In that case, contact Nortel Networks for help.
	Achtung: Wenn Sie die für das System standardmäßig eingestellten Paßwörter ändern, notieren Sie sich die neuen Paßwörter, und bewahren Sie sie an einem sicheren Ort auf. Falls Sie die neuen Paßwörter vergessen, können Sie nicht mehr auf die Konsolenschnittstelle zugreifen. Wenden Sie sich in diesem Fall an Nortel Networks, um Unterstützung zu erhalten.
	Attention: Si vous changez les mots de passe par défaut du système, assurez-vous de bien noter vos nouveaux mots de passe et de les conserver dans un endroit sûr. Si vous perdez vos nouveaux mots de passe, vous ne pourrez plus accéder à votre interface. Le cas échéant, veuillez contacter Nortel Networks.
	Precaución: Si modifica las contraseñas predeterminadas asignadas por el sistema, asegúrese de anotar las nuevas contraseñas y guárdelas en un lugar seguro. Si olvida las nuevas contraseñas, no podrá acceder al interfaz de la consola. En ese caso, póngase en contacto con Nortel Networks para obtener ayuda al respecto.

Table 42 Console/Comm Port Configuration screen fields (continued)

Field	Description
	⛔ **Attenzione:** In caso di modifica delle password predefinite nel sistema, assicurarsi di annotare le nuove password e di conservarle in un luogo sicuro. Nel caso in cui le nuove password vengano dimenticate, non sarà possibile accedere all'interfaccia della console. In tal caso, contattare la Nortel Networks per avere assistenza.
⛔	注意：システム装備したデフォルトのパスワードを変更する場合、必ず新しいパスワードを書き留めて安全な場所に保管してください。新しいパスワードを忘れてしまうと、コンソール・インタフェイスにアクセスできません。この場合は、Bay Networksまでご連絡ください。
Primary RADIUS Server	The IP address of the Primary RADIUS server. Default 0.0.0.0 (no IP address assigned) Range Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
Secondary RADIUS Server	The IP address of the Secondary RADIUS server. Default 0.0.0.0 (no IP address assigned) Range Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
RADIUS UPD Port	The user datagram protocol (UDP) port for the RADIUS server. Default 1645 Range 0 to 65536
RADIUS Shared Secret	Your special switch security code that provides authentication to the RADIUS server. Default Null string (which will not authenticate) Range Any contiguous ASCII string that contains at least 1 printable character, up to a maximum of 35

Identify Unit Numbers

When you choose Identify Unit Numbers from the main menu, the console returns the message:

```
Port LEDs lit on the front panel of the switch correspond to
its unit number.
```

Renumber Stack Units screen

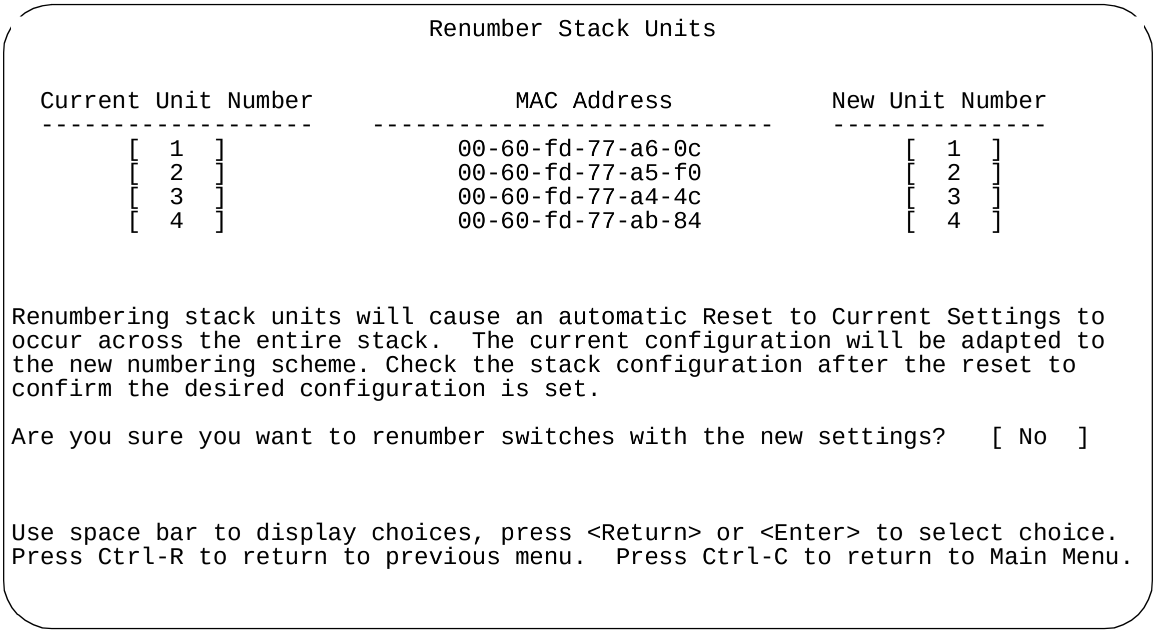
The Renumber Stack Units screen (Figure 92) allows you to renumber the units configured in the stack. When selected, this option identifies the unit number of each unit in the stack configuration by lighting the corresponding number of (100 Mb/s port) LEDs on each unit for approximately 10 seconds. For example, unit 3 will display three LEDs.

Note: This menu option and screen appears only when the switch is participating in a stack configuration.

To open the Renumber Stack Units screen:

➨ Choose Renumber Stack Units (or press n) from the main menu.

Figure 92 Renumber Stack Units screen



```
                              Renumber Stack Units


  Current Unit Number                 MAC Address                New Unit Number
  -------------------        ----------------------------        ---------------
        [  1  ]                    00-60-fd-77-a6-0c                  [  1  ]
        [  2  ]                    00-60-fd-77-a5-f0                  [  2  ]
        [  3  ]                    00-60-fd-77-a4-4c                  [  3  ]
        [  4  ]                    00-60-fd-77-ab-84                  [  4  ]



Renumbering stack units will cause an automatic Reset to Current Settings to
occur across the entire stack.  The current configuration will be adapted to
the new numbering scheme. Check the stack configuration after the reset to
confirm the desired configuration is set.

Are you sure you want to renumber switches with the new settings?   [ No  ]



Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 43 describes the Renumber Stack Units screen options.

Table 43 Renumber Stack Units screen options

Option	Description
Current Unit Number	Read-only fields listing the current unit number of each of the configured stack units. 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	Read-only field listing the MAC address of the corresponding unit listed in the Current Unit Number field.
New Unit Number	User-settable field showing the current unit number of each unit in the stack. You can change any of the fields, as required. You can also delete entries by typing zero (0) or using the space bar to clear the field. Default Value Current stack order Range 1 to 8
Renumber units with new setting?	Specifies whether to start the renumbering process (default is No). Use the spacebar to toggle the selection to Yes. Renumbering resets the switch with the current configuration values. When you select this option, the switch resets, runs a self-test, then displays the Nortel Networks logo screen. After you press [Ctrl]-Y at the screen prompt, the console screen temporarily displays the (standalone) Business Policy Switch main menu. Then, within 20 seconds, the console screen refreshes and displays the main menu screen for the stack configuration. The Unit LEDs display the new numbering order. Default Value No Range No, Yes

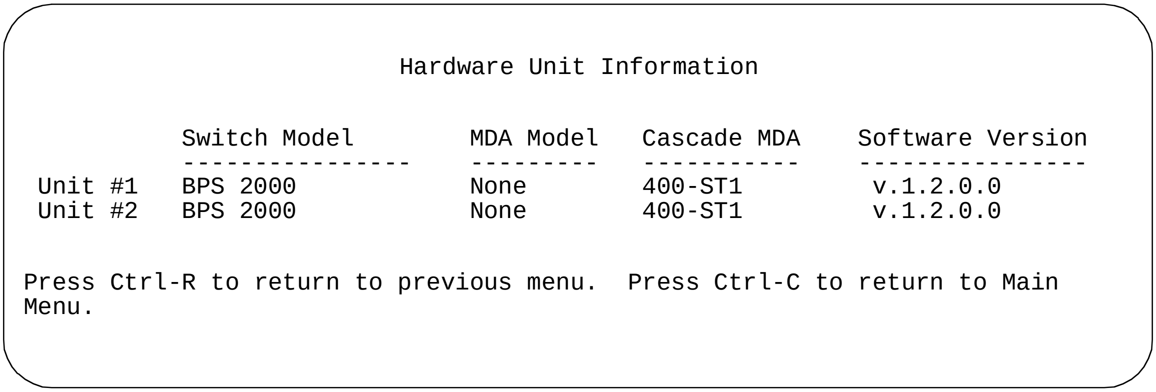
Hardware Unit Information screen

The Hardware Unit Information screen (Figure 93) lists the switch models, including any installed MDA and Cascade modules, that are configured in your standalone or stack configuration. In addition, this screen displays the software version running on the hardware.

To open the Hardware Unit Information screen:

➨ Choose Display Hardware Units (or press h) from the main menu.

Figure 93 Hardware Unit Information screen



```
                            Hardware Unit Information


           Switch Model          MDA Model    Cascade MDA     Software Version
           ----------------      ---------    -----------     ----------------
 Unit #1   BPS 2000              None         400-ST1          v.1.2.0.0
 Unit #2   BPS 2000              None         400-ST1          v.1.2.0.0


Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main
Menu.
```

Spanning Tree Configuration Menu screen

Note: Before configuring spanning tree groups, refer to Chapters 1 and 2 for guidelines and interactions with VLANs and MLT.

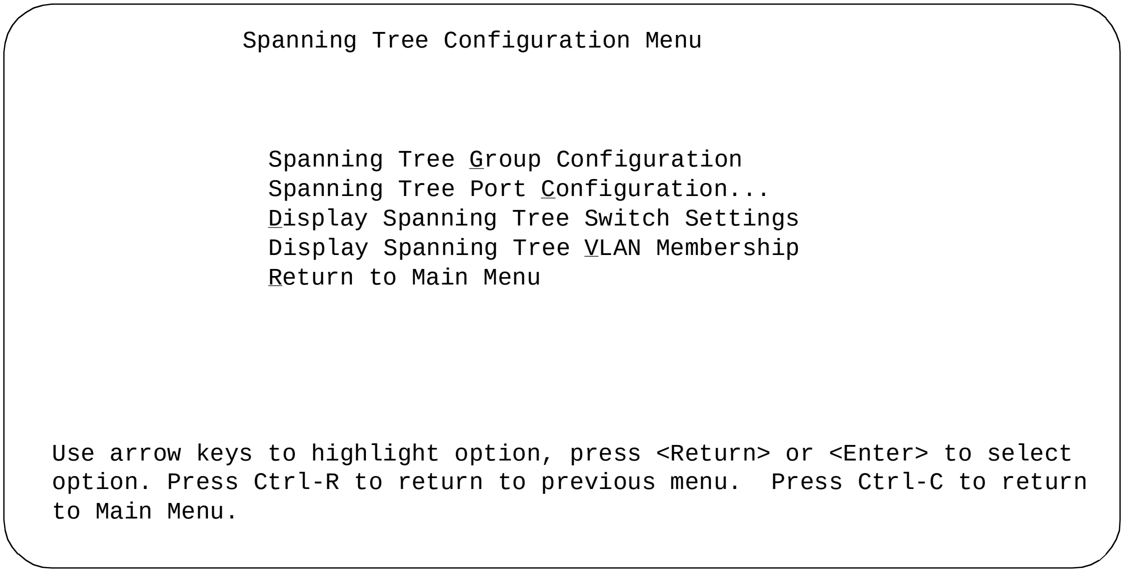
The Spanning Tree Configuration Menu screen (Figure 94) allows you to view spanning tree parameters and configure multiple spanning tree groups (STGs).

Note: You must use either the Command Line Interface (CLI) or Device Manager (DM) if you want to configure individual port values for path cost and priority.

To open the Spanning Tree Configuration Menu screen:

➨ Choose Spanning Tree Configuration (or press p) from the main menu.

Figure 94 Spanning Tree Configuration Menu



```
                Spanning Tree Configuration Menu



                  Spanning Tree Group Configuration
                  Spanning Tree Port Configuration...
                  Display Spanning Tree Switch Settings
                  Display Spanning Tree VLAN Membership
                  Return to Main Menu






   Use arrow keys to highlight option, press <Return> or <Enter> to select
   option. Press Ctrl-R to return to previous menu.  Press Ctrl-C to return
   to Main Menu.
```

Table 44 describes the Spanning Tree Configuration Menu screen options

.

Table 44 Spanning Tree Configuration Menu screen options

Option	Description
Spanning Tree Group Configuration...	Displays the Spanning Tree Group Configuration screen (see "Spanning Tree Group Configuration screen" on page 260).
Spanning Tree Port Configuration...	Displays the Spanning Tree Port Configuration screen (see "Spanning Tree Port Configuration screen" on page 263).
Display Spanning Tree Switch Settings	Allows you to display the Spanning Tree Switch Settings screen (see "Spanning Tree Switch Settings screen" on page 266).
Display Spanning Tree VLAN Membership	Allows you to display the Spanning Tree VLAN Membership screen (see "Spanning Tree VLAN Membership screen" on page 266).

Note: Because multiple STGs are available only in Pure BPS 2000 Stack mode, the first and fourth menu items do not appear when you work in Hybrid Stack, or mixed stack, mode.

Spanning Tree Group Configuration screen

The Spanning Tree Group Configuration screen allows you to create and configure spanning tree groups (STGs).

Multiple STGs, up to 8, are available with software version 1.2 and higher. The STGs are available only in Pure BPS 2000 Stack mode. In Hybrid Stack mode, you have only 1 STG, which is the default STG1. Beginning with software version 2.0, you can configure the VLAN for tagged BPDUs. Beginning with software version 2.0.5, you set the STG multicast MAC address.

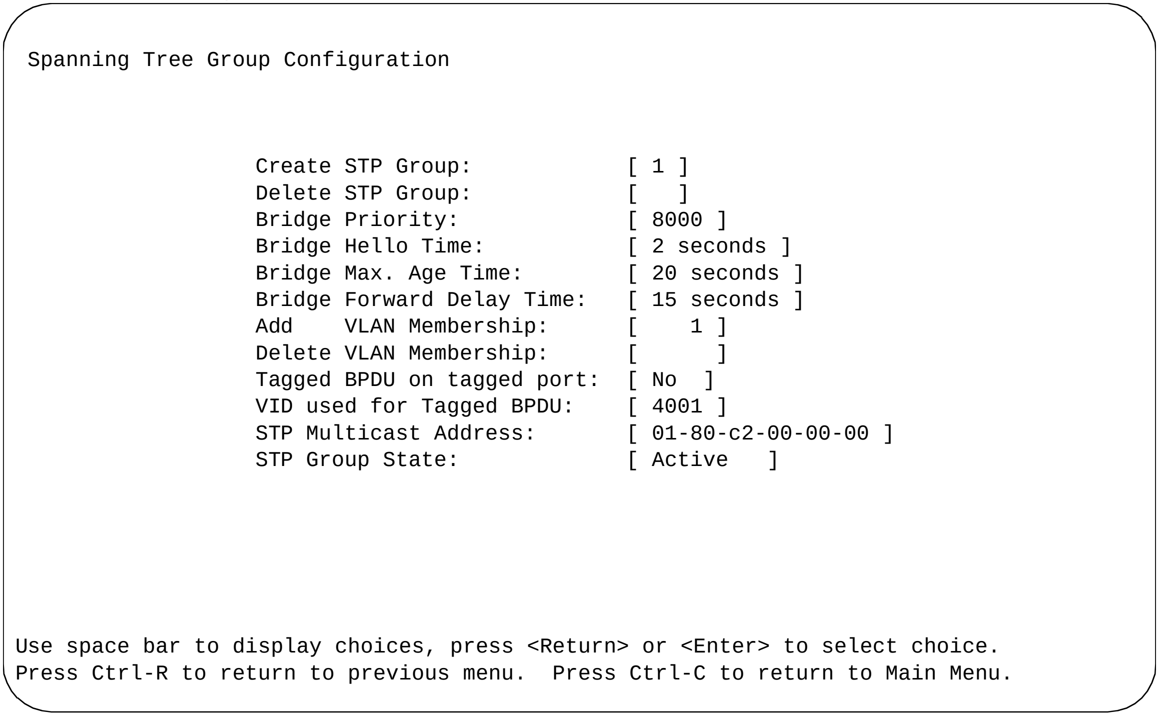
Note: When you change the Stack Operational Mode from Pure BPS 2000 Stack mode to Hybrid Stack mode, you lose all STGs above 1 (the default STG).

To open the Spanning Tree Group Configuration screen:

➨ Choose Spanning Tree Group Configuration (or press g) from the Spanning Tree Configuration Menu screen.

Figure 95 shows the Spanning Tree Group Configuration menu.

Figure 95 Spanning Tree Group Configuration menu



```
Spanning Tree Group Configuration



                  Create STP Group:             [ 1 ]
                  Delete STP Group:             [   ]
                  Bridge Priority:              [ 8000 ]
                  Bridge Hello Time:            [ 2 seconds ]
                  Bridge Max. Age Time:         [ 20 seconds ]
                  Bridge Forward Delay Time:    [ 15 seconds ]
                  Add    VLAN Membership:       [    1 ]
                  Delete VLAN Membership:       [      ]
                  Tagged BPDU on tagged port:   [ No  ]
                  VID used for Tagged BPDU:     [ 4001 ]
                  STP Multicast Address:        [ 01-80-c2-00-00-00 ]
                  STP Group State:              [ Active   ]






Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 45 describes the Spanning Tree Group Configuration parameters.

Table 45 Spanning Tree Group Configuration parameters

Parameter	Description
Create STP Group	Allows you to create a spanning tree group. Default Value 1 Range 1 to 8
Delete STP Group	Allows you to delete a spanning tree group. Default Value Blank Range 1 to 8; only created STP Groups are available

Table 45 Spanning Tree Group Configuration parameters (continued)

Parameter	Description	
Bridge Priority	For the STP Group, indicates the management-assigned priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. The 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.	
	Default Value	0x8000
	Range	0 to 0xFFFF
Bridge Hello Time	For the STP Group, indicates the Hello Interval (the amount of time between transmissions of BPDUs) specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge. Note that, although you can set the Hello Interval for a bridge using bridge management software, once the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network. See also Hello Time.	
	Default Value	2 seconds
	Range	1 to 10 seconds
Bridge Max. Age Time	For the STP Group, specifies the maximum age (in seconds) that a Hello message can attain before it is discarded. This parameter, specified by management for this bridge, takes effect only when the bridge becomes the root bridge. Note that, if this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. See also Maximum Age Time.	
	Default Value	20 seconds
	Range	6 to 40 seconds
Bridge Forward Delay Time	For the STP Group indicates the Forward Delay parameter value specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge. The Forward Delay parameter value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. Note that all bridges participating in the spanning tree network use the root bridge's Forward Delay parameter value. See also Forward Delay.	
	Default Value	15 seconds
	Range	4 to 30 seconds

Table 45 Spanning Tree Group Configuration parameters (continued)

Parameter	**Description**
Add VLAN Membership	Allows you to add a VLAN to the specified spanning tree group. Default Value 1 Range 1 to 4094 **NOTE**: Beginning with BPS 2000 software version 1.2, the system displays the following message when you add a VLAN to a spanning tree group: `Vlan X removed from STP A. Vlan X added to STP B.`
Delete VLAN Membership	Allows you to delete a VLAN from the specified spanning tree group. Default Value Blank Range 1 to 4094; but only configured ones are available **NOTE**: You cannot remove VLAN 1 from STP Group 1.
Tagged BPDU on tagged port	Allows you to choose to send either tagged or untagged BPDUs from a tagged port. Default Value STP Group 1: No; Other STP Groups: Yes Range No or Yes
VID used for tagged BPDU	Allows you to select the VLAN ID (VID) for tagged BPDU for the specified spanning tree group. Default Value 4001-4008 for STGs 1-8, respectively Range 1-4094
STP Multicast Address	Allows you to set the STG multicast MAC address. Default Value 01-80-c2-00-00-00
STP Group State	Allows you to make the STP Group active or inactive. Note that you cannot set the default STG, STG1, to InActive. Default Value Active for STG1; InActive for STGs 2 to 8. Range Active or InActive

Spanning Tree Port Configuration screen

Note: Use either the Web-based management system, CLI, or DM to set the spanning tree path cost or priority for individual ports.

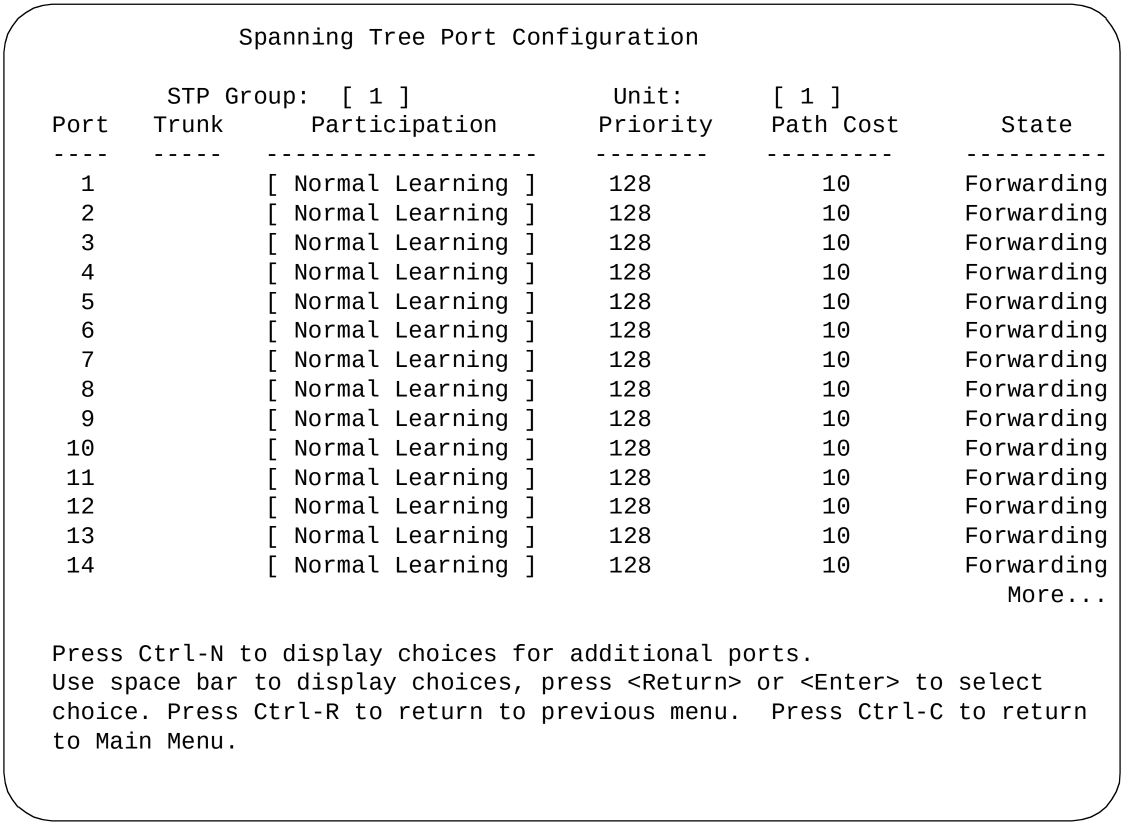
The Spanning Tree Port Configuration screen allows you to set the STG participation for each switch port or all ports and to display spanning tree settings for individual switch ports or all switch ports.

Note: If spanning tree participation of any trunk member is changed (enabled or disabled), the spanning tree participation of all members of that trunk is changed similarly.

Figure 96 shows sample port displays for the two Spanning Tree Port Configuration screens.

➨ Choose Spanning Tree Port Configuration (or press c) from the Spanning Tree Configuration Menu to open the Spanning Tree Port Configuration screen.

Figure 96 Spanning Tree Port Configuration



```
             Spanning Tree Port Configuration

        STP Group:  [ 1 ]              Unit:      [ 1 ]
Port   Trunk      Participation       Priority    Path Cost       State
----   -----   -------------------    --------    ---------    ----------
  1            [ Normal Learning ]     128           10        Forwarding
  2            [ Normal Learning ]     128           10        Forwarding
  3            [ Normal Learning ]     128           10        Forwarding
  4            [ Normal Learning ]     128           10        Forwarding
  5            [ Normal Learning ]     128           10        Forwarding
  6            [ Normal Learning ]     128           10        Forwarding
  7            [ Normal Learning ]     128           10        Forwarding
  8            [ Normal Learning ]     128           10        Forwarding
  9            [ Normal Learning ]     128           10        Forwarding
 10            [ Normal Learning ]     128           10        Forwarding
 11            [ Normal Learning ]     128           10        Forwarding
 12            [ Normal Learning ]     128           10        Forwarding
 13            [ Normal Learning ]     128           10        Forwarding
 14            [ Normal Learning ]     128           10        Forwarding
                                                                  More...

Press Ctrl-N to display choices for additional ports.
Use space bar to display choices, press <Return> or <Enter> to select
choice. Press Ctrl-R to return to previous menu.  Press Ctrl-C to return
to Main Menu.
```

Note: Because multiple STGs are available only in Pure BPS 2000 Stack mode, STP Group does not appear when you work in Hybrid Stack, or mixed stack, mode.

Table 46 describes the Spanning Tree Port Configuration screen fields.

Table 46 Spanning Tree Port Configuration screen fields

Field	Description
STP Group	The field allows you to select the number of the spanning tree group (STG) you want to view. To view another STG, type that STG ID number and press [Enter], or press the spacebar on your keyboard to to toggle the STP Group numbers. Default Value 1 Range 1 to 8; only created STP Groups display
Unit	This field only appears if the switch is participating in a stack configuration. The field allows you to select the number of the unit you want to view. To view another unit, type its unit number and press [Enter], or press the spacebar on your keyboard to toggle the unit numbers.
Port	Indicates the switch port numbers that correspond to the field values in that row of the screen (for example, the field values in row 2 apply to switch port 2). Note that the values in the *Switch* row affect all switch ports and, when the switch is part of a stack, the values in the *Stack* row affect all ports in the entire stack.
Trunk	The read-only data displayed in this column indicates the trunks that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen (see "MultiLink Trunk Configuration Menu screen" on page 225).
Participation	Allows you to configure any (or all) of the switch ports for spanning tree participation. When an individual port is a trunk member (see Trunk field), changing this setting for one of the trunk members changes the setting for all members of that trunk. You should consider how this can change your network topology before you change this setting (see Chapters 1 and 2). The Fast Learning parameter is the same as Normal Learning, except that the state transition timer is shortened to 2 seconds. Default Value Normal Learning Range Normal Learning, Fast Learning, Disabled
Priority	This read-only field is a bridge spanning tree parameter that prioritizes the lowest path cost to the root. When one or more ports have the same path cost, spanning tree selects the path with the highest priority (lowest numerical value). See also Path Cost. Default Value 128 Range 0 to 255

Table 46 Spanning Tree Port Configuration screen fields (continued)

Field	Description	
Path Cost	This read-only field is a bridge spanning tree parameter that determines the lowest path cost to the root.	
	Default Value	10 or 100 (1 for Gigabit port) Path Cost = 1000/LAN speed (in Mb/s) The higher the LAN speed, the lower the path cost. See also Priority.
	Range	1 to 65535
State	This read-only field indicates the current port state within the spanning tree network. Each port can transition to various states, as determined by the Participation field setting. For example, when the Participation field is set to disabled, the port does not participate in spanning tree and transitions to the Forwarding state (the default). When the Participation field is set to Normal Learning or Fast Learning, the port transitions from the Disabled state through the Blocking, Listening, and Learning states before entering the Forwarding state.	
	Default Value	Topology dependent
	Range	Disabled, Blocking, Listening, Learning, Forwarding

➡ **Note:** You can remove a port from the specified STP Group by toggling the Participation field to Disabled.

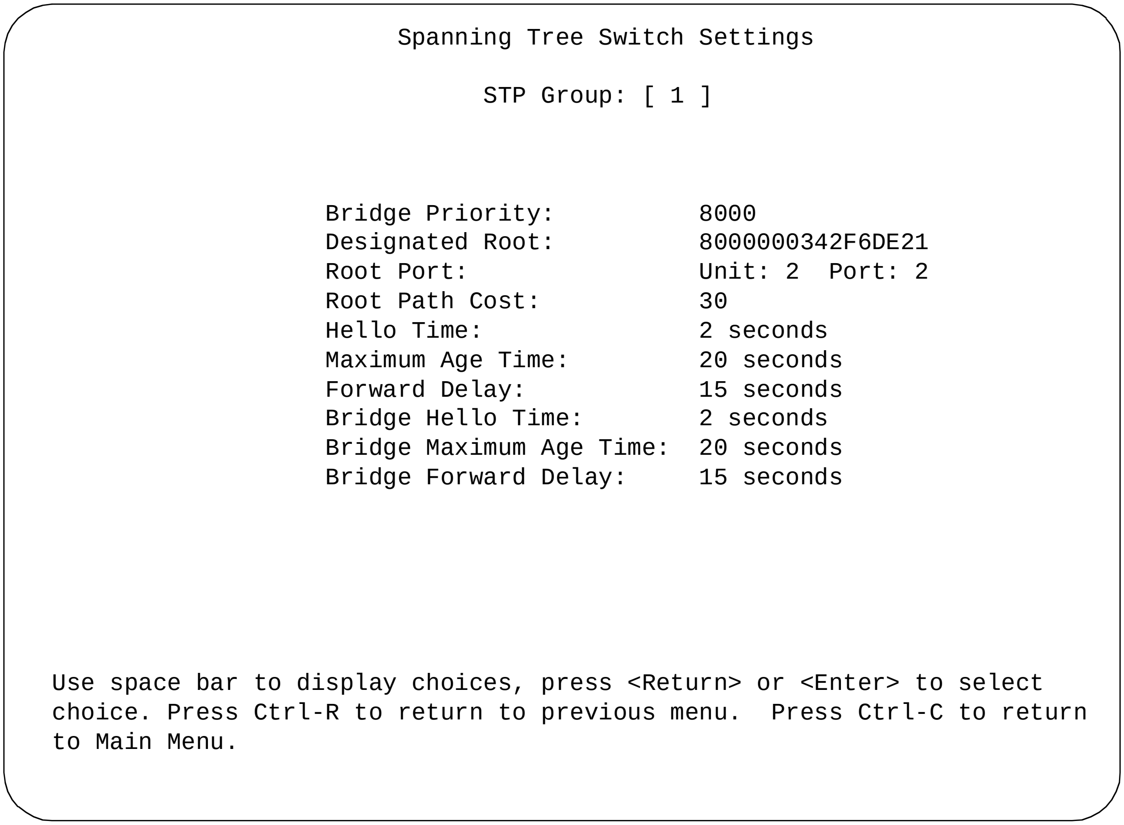
Spanning Tree Switch Settings screen

The Spanning Tree Switch Settings screen (Figure 97) allows you to view spanning tree parameter values for the selected STP Group. (STP Group 1 is the default STP group.)

To open the Spanning Tree Switch Settings screen:

➨ Choose Spanning Tree Switch Settings (or press d) from the Spanning Tree Configuration Menu screen.

Figure 97 Spanning Tree Switch Settings



```
                         Spanning Tree Switch Settings

                               STP Group: [ 1 ]



                   Bridge Priority:          8000
                   Designated Root:          8000000342F6DE21
                   Root Port:                Unit: 2  Port: 2
                   Root Path Cost:           30
                   Hello Time:               2 seconds
                   Maximum Age Time:         20 seconds
                   Forward Delay:            15 seconds
                   Bridge Hello Time:        2 seconds
                   Bridge Maximum Age Time:  20 seconds
                   Bridge Forward Delay:     15 seconds






Use space bar to display choices, press <Return> or <Enter> to select
choice. Press Ctrl-R to return to previous menu.  Press Ctrl-C to return
to Main Menu.
```

➡ **Note:** Because multiple STGs are available only in Pure BPS 2000 Stack mode, STP Group does not appear when you work in Hybrid Stack, or mixed stack, mode.

Table 47 describes the Spanning Tree Switch Settings parameters.

Table 47 Spanning Tree Switch Settings parameters

Parameter	Description
STP Group	The field allows you to select the number of the spanning tree group (STG) you want to view. To view another STG, type that STG ID number and press [Enter], or press the spacebar on your keyboard to to toggle the STP Group numbers. Default Value 1 Range 1 to 8; only created STP Groups display
Bridge Priority	For STP Group, indicates the management-assigned priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. Spanning tree 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.
Designated Root	For STP Group, indicates the bridge ID of the root bridge, as determined by spanning tree.
Root Port	For STP Group, indicates the switch port number that offers the lowest path cost to the root bridge.
Root Path Cost	For STP Group, indicates the path cost to the root bridge.
Hello Time	For STP Group, indicates 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 that all bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. See also Bridge Hello Time.

Table 47 Spanning Tree Switch Settings parameters (continued)

Parameter	Description
Maximum Age Time	For STP Group, indicates 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 that 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	For STP Group, indicates 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 that 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	For STP Group, indicates the Hello Interval (the amount of time between transmissions of BPDUs) specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge. Note that, although you can set the Hello Interval for a bridge using bridge management software, once the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge’s Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network. See also Hello Time.
Bridge Maximum Age Time	For STP Group, specifies the maximum age (in seconds) that a Hello message can attain before it is discarded. This parameter, specified by management for this bridge, takes effect only when the bridge becomes the root bridge. Note that, if this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. See also Maximum Age Time.
Bridge Forward Delay	For STP Group, indicates the Forward Delay parameter value specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge.

Table 47 Spanning Tree Switch Settings parameters (continued)

Parameter	Description
	The Forward Delay parameter value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. Note that all bridges participating in the spanning tree network use the root bridge's Forward Delay parameter value. See also Forward Delay.

Spanning Tree VLAN Membership screen

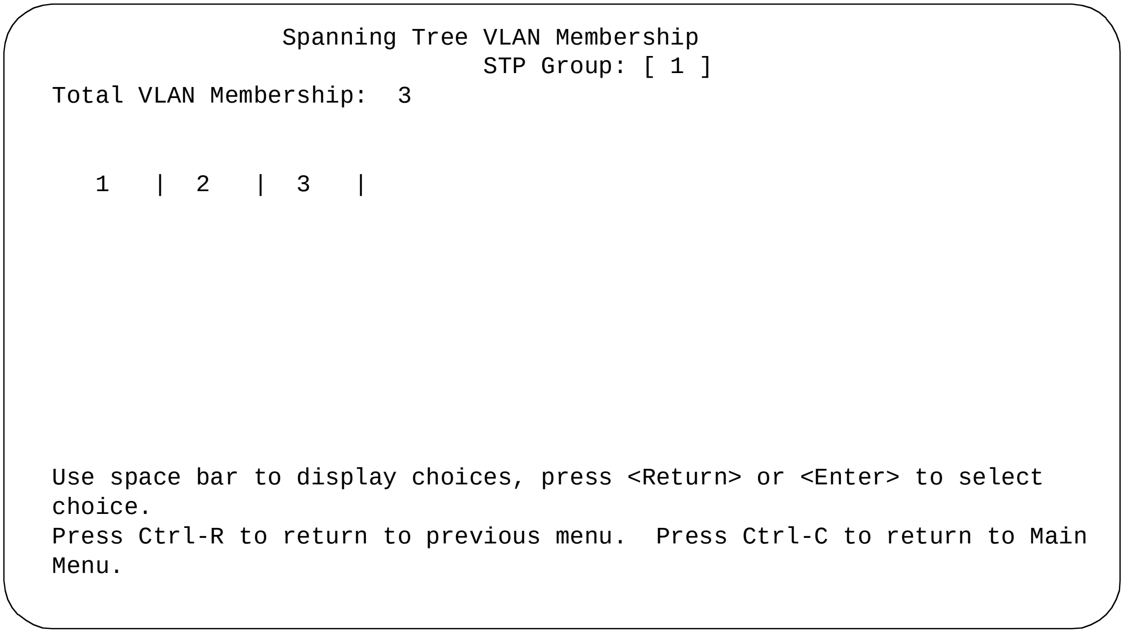
The Spanning Tree VLAN Membership screen (Figure 98) allows you to view which VLANs belong to the selected STP Group. (STP Group 1 is the default STP group.)

➡ **Note:** Because multiple STGs are available only in Pure BPS 2000 Stack mode, the Spanning Tree VLAN Membership screen does not appear when you work in Hybrid Stack, or mixed stack, mode.

To open the Spanning Tree VLAN Membership screen:

➨ Choose Spanning Tree VLAN Membership (or press v) from the Spanning Tree Configuration Menu screen.

Figure 98 Spanning Tree VLAN Membership screen



```
                Spanning Tree VLAN Membership
                              STP Group: [ 1 ]
Total VLAN Membership:  3


   1   |  2   |  3   |









Use space bar to display choices, press <Return> or <Enter> to select
choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main
Menu.
```

Table 48 describes the Spanning Tree VLAN Membership parameters.

Table 48 Spanning Tree VLAN Membership parameters

Parameter	Description
STP Group	The field allows you to select the number of the spanning tree group (STG) you want to view. To view another STG, type that STG ID number and press [Enter], or press the spacebar on your keyboard to to toggle the STP Group numbers. Default Value 1 Range 1 to 8; only created STP Groups display
VLAN Membership	Displays the total number of VLANs in the specified STP Group, as well as the VLAN IDs of the VLAN members.

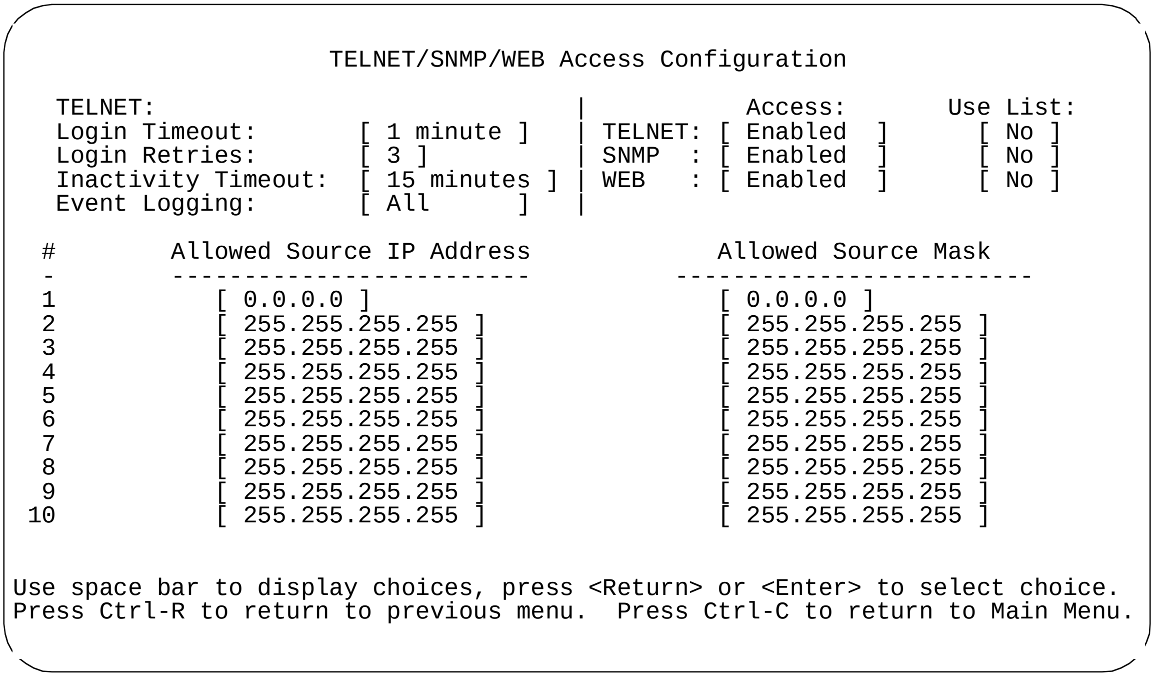
TELNET/SNMP/Web Access Configuration screen

The TELNET/SNMP/Web Access Configuration screen (Figure 99) allows a user at a remote console terminal to communicate with the Business Policy Switch as if the console terminal were directly connected to it. You can have up to four active Telnet sessions at one time.

To open the TELNET/SNMP/Web Access Configuration screen:

➨ Choose TELNET/SNMP/Web Access Configuration (or press t) from the main menu

Figure 99 TELNET/SNMP/Web Access Configuration screen



```
                      TELNET/SNMP/WEB Access Configuration

   TELNET:                             |           Access:       Use List:
   Login Timeout:       [ 1 minute ]   | TELNET: [ Enabled  ]      [ No ]
   Login Retries:       [ 3 ]          | SNMP  : [ Enabled  ]      [ No ]
   Inactivity Timeout:  [ 15 minutes ] | WEB   : [ Enabled  ]      [ No ]
   Event Logging:       [ All      ]   |

  #        Allowed Source IP Address             Allowed Source Mask
  -        -------------------------          -------------------------
  1           [ 0.0.0.0 ]                        [ 0.0.0.0 ]
  2           [ 255.255.255.255 ]                [ 255.255.255.255 ]
  3           [ 255.255.255.255 ]                [ 255.255.255.255 ]
  4           [ 255.255.255.255 ]                [ 255.255.255.255 ]
  5           [ 255.255.255.255 ]                [ 255.255.255.255 ]
  6           [ 255.255.255.255 ]                [ 255.255.255.255 ]
  7           [ 255.255.255.255 ]                [ 255.255.255.255 ]
  8           [ 255.255.255.255 ]                [ 255.255.255.255 ]
  9           [ 255.255.255.255 ]                [ 255.255.255.255 ]
 10           [ 255.255.255.255 ]                [ 255.255.255.255 ]


Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 49 describes the TELNET/SNMP/Web Access Configuration screen fields.

Table 49 TELNET/SNMP/Web Access Configuration screen fields

Field	Description
TELNET Access	Allows a user remote access to the management systems through a Telnet session. Default Value: Enabled Range: Enabled, Disabled
Login Timeout	Specifies the amount of time a user has to enter the correct password at the console-terminal prompt. Default Value: 1 minute Range: 0 to 10 minutes (0 indicates “no timeout”)
Login Retries	Specifies the number of times a user can enter an incorrect password at the console-terminal prompt before terminating the session. Default Value: 3 Range: 1 to 100
Inactivity Timeout	Specifies the amount of time the session can be inactive before it is terminated. Default Value: 15 minutes Range: 0 to 60 minutes (0 indicates “no timeout”)
Event Logging	Specifies the types of events that will be displayed in the Event Log screen (see “System Log screen” on page 292). Default Value: All Range: All, None, Accesses, Failures Description: *All:* Logs the following Telnet events to the Event Log screen: • TELNET connect: Indicates the IP address and access mode of a Telnet session. • TELNET disconnect: Indicates the IP address of the remote host and the access mode, due to either a logout or inactivity. • Failed TELNET connection attempts: Indicates the IP address of the remote host whose IP address is not on the list of allowed addresses, or indicates the IP address of the remote host that did not supply the correct password. *None:* Indicates that no Telnet events will be logged in the Event Log screen. *Accesses*: Logs only Telnet connect and disconnect events in the Event Log screen. *Failures:* Logs only failed Telnet connection attempts in the Event Log screen.

Table 49 TELNET/SNMP/Web Access Configuration screen fields (continued)

Field	Description	
TELNET Access	Specifies if Telnet access is allowed and only to those on the list.	
	Default Value:	Access: Enabled; Use List: Yes
	Range:	Access: Enabled, Disabled; Use List: Yes, No
SNMP Access	Specifies if SNMP access is allowed and only to those on the list. (SNMP access includes the DM system.)	
	Default Value:	Access: Enabled; Use List: Yes
	Range:	Access: Enabled, Disabled; Use List: Yes, No
WEB Access	Specifies if access to the Web-based management system is allowed and only to those on the list.	
	Default Value:	Access: Enabled; Use List: Yes
	Range:	Access: Enabled, Disabled; Use List: Yes, No
Allowed Source IP Address	Specifies up to 10 user-assigned host IP addresses that are allowed Telnet access to the management systems.	
	Default Value:	0.0.0.0 (no IP address assigned)
	Range:	Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
Allowed Source Mask	Specifies up to 10 user-assigned allowed source address masks. The remote IP address is masked with the Allowed Source Mask and, if the resulting value equals the Allowed Source IP address, the connection is allowed. For example, a connection would be allowed with the following settings: Remote IP address = 192.0.1.5 Allowed Source IP Address = 192.0.1.0 Allowed Source Mask = 255.255.255.0	
	Default Value:	0.0.0.0 (no IP mask assigned)
	Range:	Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point

Software Download screen

The Software Download screens (Figure 100 and Figure 101) allow you to revise the Business Policy Switch software image that is located in nonvolatile flash memory.

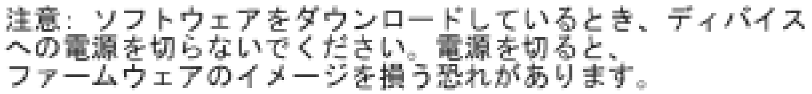
Caution: Do not interrupt power to the device during the software download process. If the power is interrupted, the firmware image can become corrupted.

Achtung: Unterbrechen Sie die Stromzufuhr zum Gerät nicht, während die Software heruntergeladen wird. Bei Unterbrechung der Stromzufuhr kann das Firmware-Image beschädigt werden.

Attention: Ne pas couper l'alimentation de l'appareil pendant le chargement du logiciel. En cas d'interruption, le programme résident peut être endommagé.

Precaución: No interrumpa la alimentación del dispositivo durante el proceso de descarga del software. Si lo hace, puede alterar la imagen de la programación (firmware).

Attenzione: Non interrompere l'alimentazione elettrica al dispositivo durante il processo di scaricamento del software. In caso di interruzione, l'immagine firmware potrebbe danneggiarsi.



注意：ソフトウェアをダウンロードしているとき、ディバイスへの電源を切らないでください。電源を切ると、ファームウェアのイメージを損う恐れがあります。

To download the software image, you need a properly configured Trivial File Transfer Protocol (TFTP) server in your network, and an IP address for the switch (or stack, if configured). To learn how to configure the switch or stack IP address, refer to "IP Configuration/Setup screen" on page 172.

This section covers the following topics:

- "Using the Software Download screen," next
- "LED Indications during the download process" on page 279
- "Upgrading software in a Pure BPS 2000 stack" on page 279
- "Upgrading software in a Hybrid stack" on page 280

Using the Software Download screen

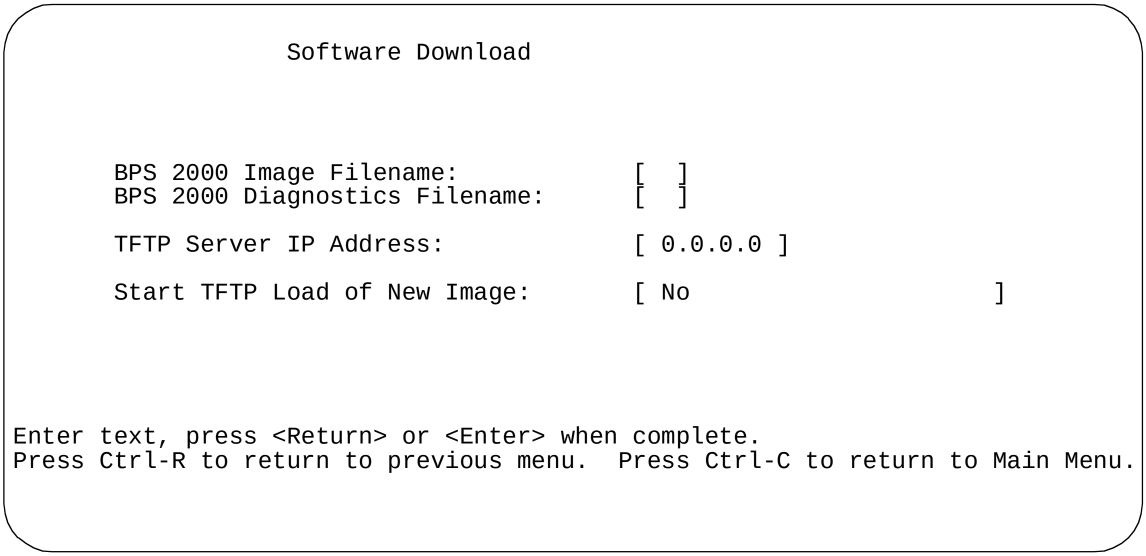
To open the Software Download screen:

➨ Choose Software Download (or press f) from the main menu.

The Software Download screen appears (Figure 100 and Figure 101).

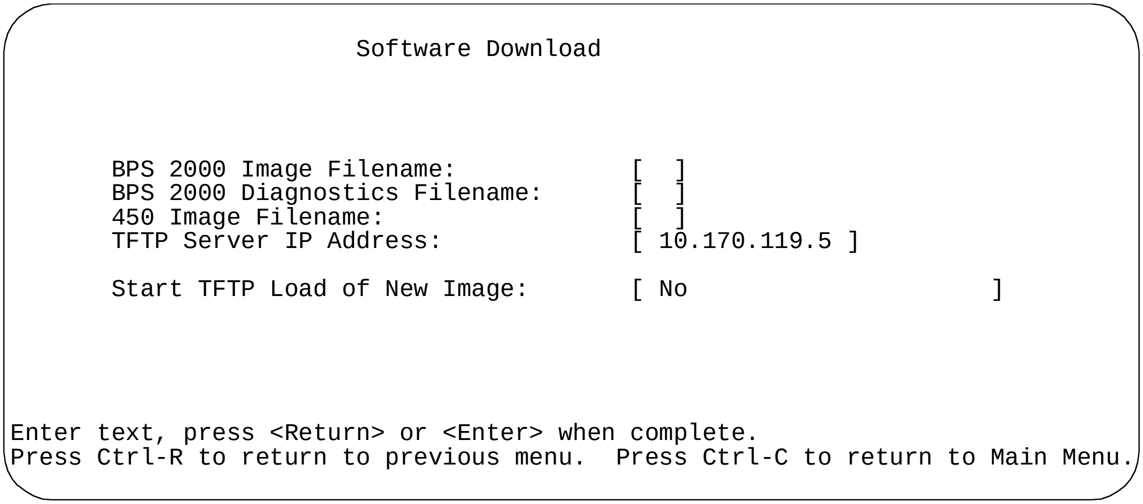
You can monitor the software download process by observing the LEDs (see "LED Indications during the download process" on page 279).

Figure 100 Software Download screen for Pure BPS 2000 Stack mode



```
                   Software Download



       BPS 2000 Image Filename:            [  ]
       BPS 2000 Diagnostics Filename:      [  ]

       TFTP Server IP Address:             [ 0.0.0.0 ]

       Start TFTP Load of New Image:       [ No                     ]




Enter text, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Figure 101 Software Download screen for Hybrid Stack mode



```
                        Software Download



       BPS 2000 Image Filename:            [  ]
       BPS 2000 Diagnostics Filename:      [  ]
       450 Image Filename:                 [  ]
       TFTP Server IP Address:             [ 10.170.119.5 ]

       Start TFTP Load of New Image:       [ No                     ]




Enter text, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 50 describes the Software Download screen fields.

Table 50 Software Download screen fields

Field	Description
BPS 2000 Image Filename	The Business Policy Switch software image load file name. Default Value Zero-length string Range An ASCII string of up to 30 printable characters
BPS 2000 Diagnostics Filename	The Business Policy Switch diagnostics file name. Default Value Zero-length string Range An ASCII string of up to 30 printable characters
450 Image Filename	The BayStack 450 software image load file name. Displays in a mixed stack environment. Default Value Zero-length string Range An ASCII string of up to 30 printable characters
TFTP Server IP Address	The IP address of your TFTP load host. Default Value 0.0.0.0 (no IP address assigned) Range Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
Start TFTP Load of New Image	Specifies whether to start the download of the switch software image (default is No). Use the spacebar to toggle the selection to the one you want. Press [Enter] to initiate the software download process.
	NOTE: The software download process can take up to 60 seconds to complete (or more if the load host path is congested or there is a high volume of network traffic).
	To ensure that the download process is not interrupted, do not power down the switch for approximately 10 minutes. Default Value No Range No, BPS 2000 Image, BPS 2000 Diagnostics, 450 Image, BPS 2000 and 450 Image

Note: If your station cannot ping the TFTP server during the downloading process, you may receive the following message:
`Image is Invalid`
Actually, the problem is that the TFTP server is not reachable, rather than any problems with the image.

LED Indications during the download process

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. Be careful not to interrupt the download process until after it runs to completion (the process can take up to 10 minutes, depending on network conditions).

Note: If problems occur during the software download process, refer to Chapter 6.

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.

Note: When you download new images to a mixed (Hybrid) stack, the LEDs may on the BPS 2000 units may not appear correctly. The BU (Base Unit) LEDs on all the BPS 2000 units may turn on or blink as if the stack has failed. However, the stack is operational and the upgrade should complete.

Upgrading software in a Pure BPS 2000 stack

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

1 Choose Software Download (or press f) from the main menu.

The Software Download screen appears (Figure 100).

2. In the BPS 2000 Image Filename field, enter the name of the BPS 2000 image file.
3. In the TFTP Server IP Address, enter the IP address of your TFTP load host.
4. Use the space bar to toggle to BPS 2000 Image in the Start TFTP Load of New Image field.
5. Press [Enter].

   The system resets and opens to the BPS2000 banner.

6. Press [Ctrl + Y] to access the main menu.
7. Choose Software Download (or press f) from the main menu.

   The Software Download screen appears (Figure 100).

8. In the BPS 2000 Diagnostics Filename field, enter the name of the BPS 2000 diags file.
9. In the TFTP Server IP Address, enter the IP address of your TFTP load host.
10. Use the space bar to toggle to BPS 2000 Diagnostics in the Start TFTP Load of New Image field.
11. Press [Enter].

    The system resets and opens to the BPS2000 banner.

12. Press [Ctrl + Y] to access the main menu.

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

Upgrading software in a Hybrid stack

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

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

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

This section describe the steps for the following software upgrades:

- "Upgrading software when ISVN is 2," next
- "Upgrading software when ISVN is 1" on page 282

Upgrading software when ISVN is 2

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

1. Choose Software Download (or press f) from the main menu.

   The Software Download screen appears (Figure 101).

2. In the BPS 2000 Image Filename field, enter the name of the BPS 2000 image file.
3. In the TFTP Server IP Address, enter the IP address of your TFTP load host.
4. Use the space bar to toggle to BPS 2000 Image in the Start TFTP Load of New Image field.
5. Press [Enter].

   The system resets and opens to the BPS2000 banner.

6. Press [Ctrl + Y] to access the main menu.

7. Choose Software Download (or press f) from the main menu.

   The Software Download screen appears (Figure 101).

8. In the BPS 2000 Diagnostics Filename field, enter the name of the BPS 2000 diags file.
9. In the TFTP Server IP Address, enter the IP address of your TFTP load host.
10. Use the space bar to toggle to BPS 2000 Diagnostics in the Start TFTP Load of New Image field.
11. Press [Enter].

    The system resets and opens to the BPS2000 banner.

12. Press [Ctrl + Y] to access the main menu.

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

Upgrading software when ISVN is 1

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

1. Choose Software Download (or press f) from the main menu.

   The Software Download screen appears (Figure 101).

2. In the BPS 2000 Image Filename field, enter the name of the BPS 2000 image file.
3. In the 450 Image Filename field, enter the name of the BayStack 450/410 image file.
4. In the TFTP Server IP Address, enter the IP address of your TFTP load host.
5. Use the space bar to toggle to Both BPS 2000 and 450 Image in the Start TFTP Load of New Image field.

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

6 Press [Enter].

The system resets and opens to the BPS2000 banner.

7 Press [Ctrl + Y] to access the main menu.

8 Choose Software Download (or press f) from the main menu.

The Software Download screen appears (Figure 101).

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

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

11 Use the space bar to toggle to 450 Image in the Start TFTP Load of New Image field.

12 Press [Enter].

The system resets and opens to the BPS2000 banner.

13 Press [Ctrl + Y] to access the main menu.

14 Choose Software Download (or press f) from the main menu.

The Software Download screen appears (Figure 101).

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

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

17 Use the space bar to toggle to BPS 2000 Diagnostics in the Start TFTP Load of New Image field.

18 Press [Enter].

The system resets and opens to the BPS2000 banner.

19 Press [Ctrl + Y] to access the main menu.

20 Choose System Characteristics (or press s) from the main menu.

The System Characteristics screen opens (Figure 59).

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

Configuration File Menu screen

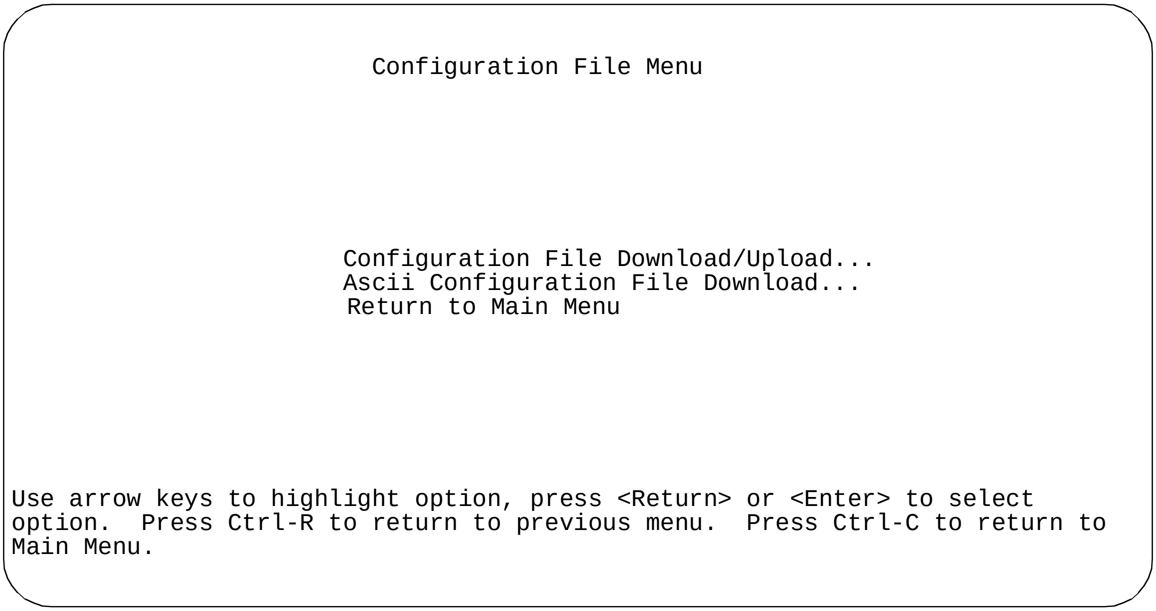
The Configuration File Menu screen (Figure 102) allows you to upload and download the configuration parameters of a BPS 2000 switch or stack to a TFTP server. With software version 1.2 or higher, you can also download an ASCII configuration file from a TFTP server.

These options allow you to store your switch/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. You must set up the file on your TFTP server and set the filename read/write permission to enabled before you can save the configuration parameters.

To open the Configuration File Menu screen:

➨ Choose Configuration File Menu from the main menu.

Figure 102 Configuration File Menu screen



```
                         Configuration File Menu




                       Configuration File Download/Upload...
                       Ascii Configuration File Download...
                       Return to Main Menu





Use arrow keys to highlight option, press <Return> or <Enter> to select
option.  Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to
Main Menu.
```

Table 51 describes the Configuration File Menu screen options.

Table 51 Configuration File Menu screen options

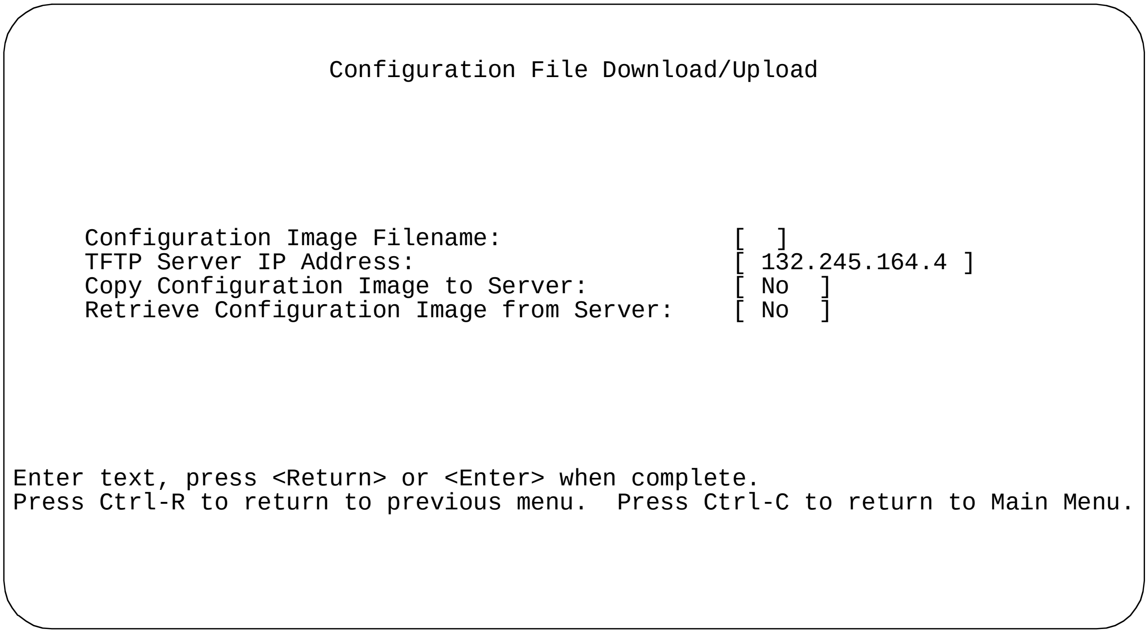
Option	Description
Configuration File Download/Upload...	Displays the Configuration File Download/Upload screen (see "Configuration File Download/Upload screen" on page 285).
Ascii Configuration File Download...	Displays the ASCII Configuration File Download screen (see "ASCII Configuration File Download screen" on page 289).

Configuration File Download/Upload screen

The Configuration File Download/Upload screen (Figure 103) allows you to store your switch/stack configuration parameters on a TFTP server. Certain requirements apply when automatically configuring a switch or stack using this feature (see "Requirements" on page 288). Although most configuration parameters are saved to the configuration file, certain parameters are not saved (see Table 53 on page 289).

Choose Configuration File Download/Upload from the Configuration File Menu to open the Configuration File Download/Upload screen.

Figure 103 Configuration File Download/Upload screen



```
                          Configuration File Download/Upload




     Configuration Image Filename:                   [  ]
     TFTP Server IP Address:                         [ 132.245.164.4 ]
     Copy Configuration Image to Server:             [ No   ]
     Retrieve Configuration Image from Server:       [ No   ]





Enter text, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 52 describes the Configuration File Download/Upload screen fields.

Table 52 Configuration File Download/Upload screen fields

Field	Description	
Configuration Image Filename	The file name you have chosen for the configuration file. Choose a meaningful file name that will allow you to identify the file for retrieval when required. The file must already exist on your TFTP server and must be read/write enabled.	
	Default Value	Zero-length string
	Range	An ASCII string of up to 30 printable characters
TFTP Server IP Address	The IP address of your TFTP load host.	
	Default Value	0.0.0.0 (no IP address assigned)
	Range	Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
Copy Configuration Image to Server	Specifies whether to copy the presently configured switch/stack parameters to the specified TFTP server (default is No). Use the spacebar to toggle the selection to Yes. Press [Enter] to initiate the process.	
	Default Value	No
	Range	Yes, No
Retrieve Configuration Image from Server	Specifies whether to retrieve the stored switch/stack configuration parameters from the specified TFTP server (default is No). If you choose Yes, the download process begins immediately and, when completed, causes the switch/stack to reset with the new configuration parameters. Use the spacebar to toggle the selection to Yes. Press [Enter] to initiate the process.	
	Default Value	No
	Range	Yes, No

Requirements

The following requirements apply to the Configuration File feature:

- 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 53 describes Configuration File parameter information.

Table 53 Parameters not saved to the Configuration File

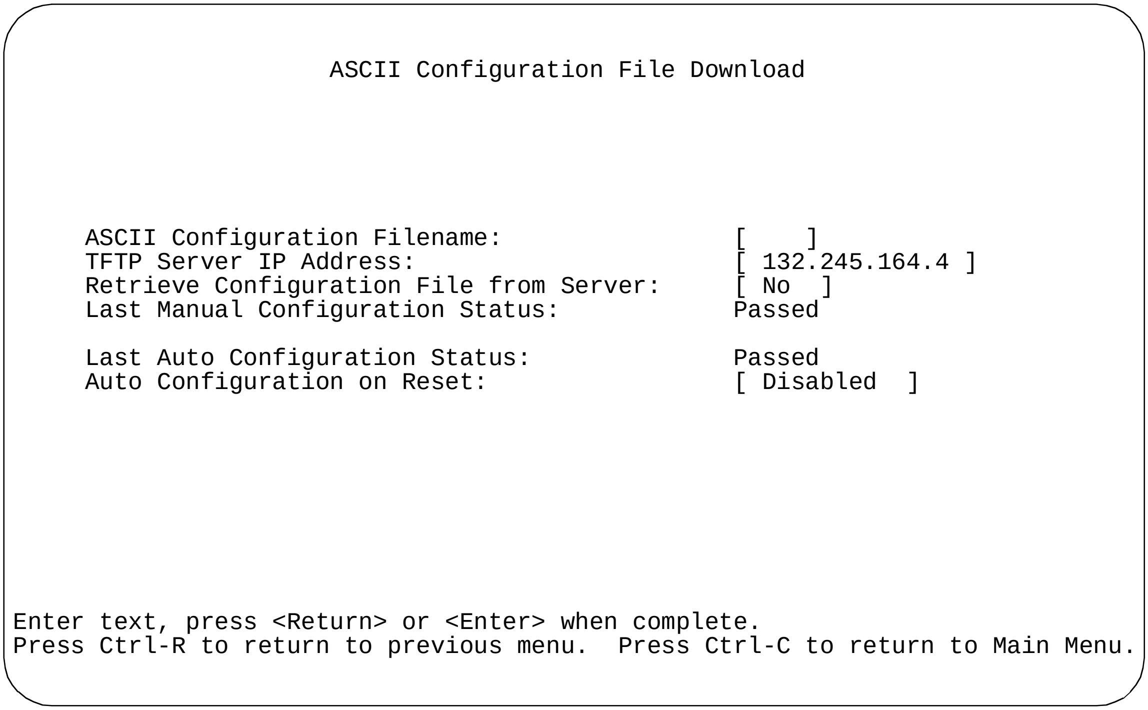
These parameters are not saved:	Used in this screen:	See page:
In-Band Stack IP Address	IP Configuration/Setup	172
In-Band Switch IP Address		
In-Band Subnet Mask		
Default Gateway		
Console Read-Only Switch Password	Console/Comm Port Configuration	249
Console Read-Write Switch Password		
Console Read-Only Stack Password		
Console Read-Write Stack Password		
Configuration Image Filename	Configuration File Download/Upload	285
TFTP Server IP Address		

ASCII Configuration File Download screen

The ASCII Configuration File Download screen (Figure 104) allows you to download an ASCII configuration file containing CLI commands from a TFTP server to configure the switch or stack.

➨ Choose ASCII Configuration File Download from the Configuration File Menu to open the ASCII Configuration File Download screen.

Figure 104 ASCII Configuration File Download screen



```
                      ASCII Configuration File Download




     ASCII Configuration Filename:                     [    ]
     TFTP Server IP Address:                           [ 132.245.164.4 ]
     Retrieve Configuration File from Server:          [ No  ]
     Last Manual Configuration Status:                 Passed

     Last Auto Configuration Status:                   Passed
     Auto Configuration on Reset:                      [ Disabled  ]







Enter text, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 54 describes the ASCII Configuration File Download screen fields.

Table 54 ASCII Configuration File Download screen fields

Field	Description
ASCII Configuration Filename	Enter the file name you have chosen for the ASCII configuration file. Choose a meaningful file name that will allow you to identify the file for retrieval when required. The file must already exist on your TFTP server and must be read/ write enabled. Default Value Zero-length string Range An ASCII string of up to 30 printable characters
TFTP Server IP Address	The IP address of your TFTP load host. Default Value 0.0.0.0 (no IP address assigned) Range Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
Retrieve Configuration File from Server	Specifies whether to retrieve the stored switch/stack ASCII configuration file from the specified TFTP server (default is No). If you choose Yes, the download process begins immediately and, when completed, causes the switch/stack to be configured according to the CLI commands in the file. Use the spacebar to toggle the selection to Yes. Press [Enter] to initiate the process. Default Value No Range Yes, No
Last Manual Configuration Status	The system displays if the last manual configuration passed or failed. Default Value Passed Range Passed, Failed
Last Auto Configuration Status	The system displays if the last automatic configuration passed or failed. Default Value Passed Range Passed, Failed
Auto Configuration on Reset	Allows you to choose to Disabled, Use Configured, or Use BootP: • Disabled—Auto configuration on reset is disabled. • Use Configured—Use manually configured ASCII configuration filename and TFTP server address for auto configuration on reset. • Use BootP—Retrieve ASCII configuration filename, and optionally server address, using BootP, when BootP is enabled, and perform auto configuration on reset using these parameters. Note: Refer to Appendix H for a sample BootP configuration file. Default Value Disabled Range Disabled, Use Configured, Use BootP

System Log screen

The System Log screen (Figure 105) displays or clears messages obtained from system nonvolatile random access memory (NVRAM) or dynamic random access memory (DRAM) and NVRAM. When the switch is part of a stack configuration, the System screen displays only the data for the Business Policy Switch you are connected to through the Console/Comm port.

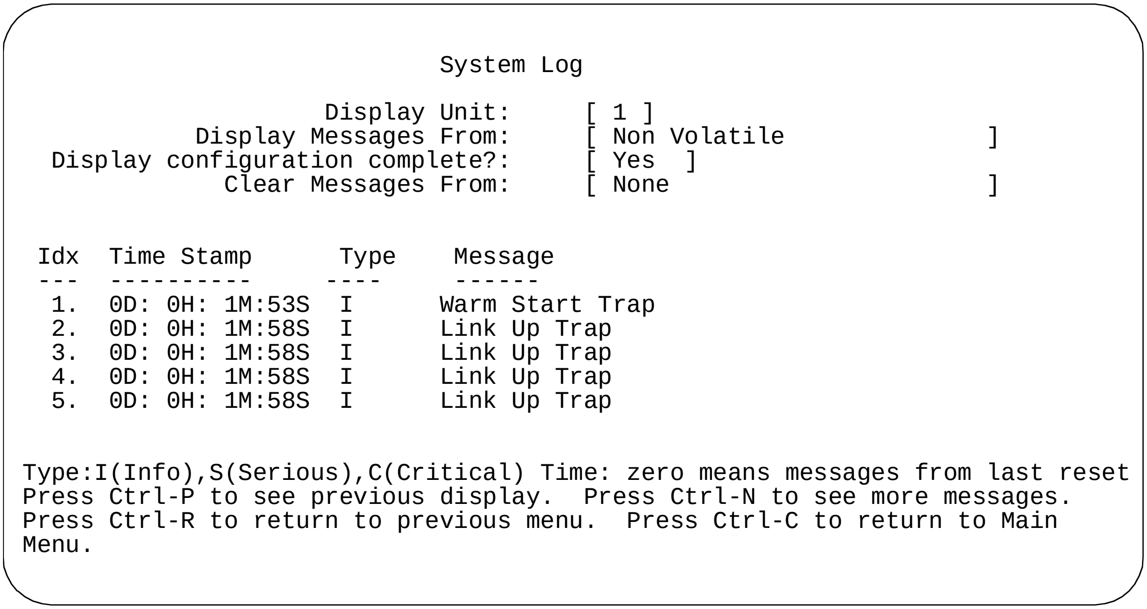
System Log messages operate as follows:

- NVRAM messages are retrievable after a system reset.
- DRAM messages can be viewed while the system is operational.
- All NVRAM and DRAM messages are time stamped.
- When you restart your system after a reset, the DRAM messages are deleted.
- After a reset, all messages stored in NVRAM are copied to DRAM (DRAM messages are not copied to NVRAM). The messages copied to DRAM are time stamped to zero (0).

To open the Event Log screen:

➨ Choose Display Event Log (or press y) from the main menu.

Figure 105 System Log screen



```
                              System Log

                      Display Unit:      [ 1 ]
             Display Messages From:      [ Non Volatile              ]
   Display configuration complete?:      [ Yes  ]
              Clear Messages From:       [ None                      ]


 Idx  Time Stamp      Type    Message
 ---  ----------     ----     ------
  1.  0D: 0H: 1M:53S  I      Warm Start Trap
  2.  0D: 0H: 1M:58S  I      Link Up Trap
  3.  0D: 0H: 1M:58S  I      Link Up Trap
  4.  0D: 0H: 1M:58S  I      Link Up Trap
  5.  0D: 0H: 1M:58S  I      Link Up Trap


Type:I(Info),S(Serious),C(Critical) Time: zero means messages from last reset
Press Ctrl-P to see previous display.  Press Ctrl-N to see more messages.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main
Menu.
```

Table 55 describes the System Log screen fields.

Table 55 System Log screen fields

Field	**Description**
Unit	This field only appears if the switch is participating in a stack configuration. The field allows you to select the unit number of the Business Policy Switch you want to view. To view the log messages of another Business Policy Switch, type its unit number and press [Enter], or press the spacebar on your keyboard to toggle the unit numbers.
Display Messages From	This field allows you to select the RAM source your messages are obtained from. Choose Non Volatile (NVRAM), or Volatile (DRAM) + Non Volatile. Use the spacebar to toggle between the options. Default Non Volatile Range Non Volatile, Volatile + Non Volatile
Display configuration complete?	This field allows you to determine whether the configuration information received from NVRAM/DRAM (depending on what is selected in the Display Messages From field) is complete. Use the spacebar to toggle between the options. Default No Range No, Yes
Clear Messages From	This field allows you to clear the information messages from DRAM, NVRAM or both. If you clear DRAM messages, existing NVRAM messages are copied into DRAM. After a system reset, all existing NVRAM messages are copied to DRAM. Use the spacebar to toggle between the options. Default None Range None, NVRAM, DRAM + NVRAM

Chapter 4
Policy-enabled networks

This chapter provides an overview of Differentiated Services Quality of Service (QoS) network architecture. The BPS 2000 provides a Web-based management interface, a Command Line Interface (CLI), and the graphical user interface Device Manager (DM) to configure QoS. Refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*, *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5*, and *Reference for the Business Policy Switch 2000 Management Software Version 2.5* for detailed information.

In addition to these management systems, policies can be configured using SNMP and Common Open Policy Services (COPS).

The complexities of QoS are discussed in the remainder of this chapter, which includes information about the following topics:

Summary

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

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

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

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

Summary of packet classifiers

The BPS 2000 classifies packets based on various parameters:

- IP packets
  - source address/mask
  - destination address/mask
  - IP protocol type (such as TCP/UDP)
  - DSCP value

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

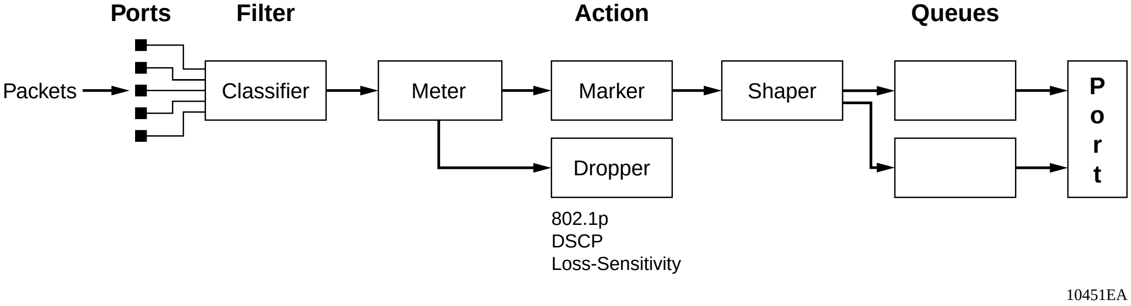
Summary of actions

The BPS 2000 filters collectively direct the system to initiate the following actions on a packet, depending on your configuration:

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

Figure 106 provides a schematic overview of QoS policies.

Figure 106 Schematic of QoS policy



Note: To use the QoS shaping feature with software version 2.5, you must use the BPS 2000-1GT, BPS 2000-2GT, or BPS 2000-2GE MDA in a Business Policy Switch.

Differentiated Services (DiffServ) overview

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

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

Within the DiffServ network, the marked packets are placed in a queue according to their marking, which in turn determines the per-hop-behavior (PHB) of that packet. For example, if a video stream is marked so that it receives the highest priority, then it is placed in a high-priority queue. As those packets traverse the DiffServ network, the video stream is forwarded before any other packets.

To ensure that the traffic stream conforms to the bandwidth assigned, policing within the network is necessary. Traffic shaping may also be used to temporarily delay traffic to ensure that the flows conform to downstream bandwidth limits.

DiffServ Concepts

DiffServ is described in IETF RFCs 2474 and 2475. This architecture is flexible and allows for either end-to-end QoS or intradomain QoS by implementing complex classification and mapping functions at the network boundary or access points. Within a DiffServ domain, the packet treatment is regulated by this classification and mapping.

The DiffServ basic elements are implemented within the network and include:

- Packet classification functions
- A small set of per-hop forwarding behaviors
- Traffic metering, marking, and shaping

Traffic is classified as it enters the DS network and is then assigned the appropriate PHB based on that classification. Within the IP packet, the 6 bits in the DSCP are marked to identify how the packet should be treated at each subsequent network node. This mapping of DS codepoints to per-hop behavior (PHB) is configurable, and the DSCP may be re-marked as it passes through a DiffServ network. Re-marking the DSCP allows for the treatment of packets to be reset based on new network specifications or desired levels of service.

DiffServ assumes the existence of a Service Level Agreement (SLA) between DS domains that share a border. The SLA defines the profile for the aggregate traffic flowing from one network to the other based on policy criteria. In a given traffic direction, the traffic is expected to be shaped at the egress point of the upstream network and metered at the ingress point of the downstream network.

As the traffic moves within the DiffServ network, policies ensure that traffic marked by the different DSCPs is treated according to that marking. Traffic metering and shaping ensures that the traffic flow conforms to an SLA to provide certain levels of service in terms of bandwidth for different types of network traffic.

QoS classes

The BPS 2000 supports the following Nortel Networks QoS classes:

- Critical and Network classes have the highest priority over all other traffic.
- Premium class is an end-to-end service functioning similarly to a virtual leased line. Traffic in this service class is normally guaranteed an agreed-upon peak bandwidth. Traffic requiring this service should be shaped at the network boundary in order to undergo a negligible delay and delay variance. This service class is suitable for real-time applications like video and voice over IP. The recommended PHB for this service is the Expedited Forwarding (EF) PHB.
- Platinum, Gold, Silver, and Bronze classes use the Assured Forwarding (AF) PHB. These classes are used for real-time, delay-tolerant traffic and non-real-time, mission-critical traffic.
- Standard class is the best-effort IP service with an additional, optional use of traffic classification that is used at the network boundary to request a better effort treatment for packets that are in-profile (packets that do not break the service agreements between the user and the service provider).

Table 56 describes the service classes and the required treatment.

Table 56 Service classes

Traffic category	**Service class**	**Application type**	**Required treatment**
Critical network control	Critical	Critical network control traffic	Highest priority over all other traffic. Guaranteed minimum bandwidth.
Standard network control	Network	Standard network control traffic	Priority over user traffic. Guaranteed minimum bandwidth.
Real time, delay intolerant, fixed bandwidth	Premium	Interhuman communications requiring interaction (such as VoIP).	Absolute bounded priority over user traffic. No packet loss for in-profile traffic. Virtual leased line with lowest amount of latency. Provisioned for peak rate.
Real time, delay tolerant, low variable bandwidth	Platinum	Interhuman communications requiring interaction with additional minimal delay (such as low-cost VoIP).	Higher-priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.

Table 56 Service classes (continued)

Traffic category	Service class	Application type	Required treatment
Real time, delay tolerant, high variable bandwidth	Gold	Single human communication with no interaction (such as Web site streaming video).	High-priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Non-real time, mission critical, interactive	Silver	Transaction processing (such as Telnet, Web browsing).	Medium priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Non-real time, mission critical, non-interactive	Bronze	For example, E-mail, FTP, SNMP.	Lower-priority scheduling providing guaranteed minimum provisioned bandwidth. Competes for additional bandwidth.
Non-real time, non-mission critical	Standard	Bulk transfer (such as large FTP transfers, after-hours tape backup).	Best effort delivery. Uses remaining available bandwidth.

Packet classifiers or filters

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

You can create the following two types of filter groups:

- Layer 2 filters
- IP filters

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

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

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

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

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

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

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

Layer 2 filters

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

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

Beginning with software version 2.5, there are up to 24 layer 2 filters available. The number of available layer 2 filters varies according to the category of interface class you have configured.

- If the supported interface class is untrusted, the default, there are 14 layer 2 filters available.
- If the supported interface class is trusted, there are 23 layer 2 filters available.
- If the supported interface class is unrestricted, there are 24 layer 2 filters available.

Refer to "Ports" on page 305 for information on configuring interface classes.

Beginning with software version 2.0, you can filter multiple VLANs with a single layer 2 filter. You can filter up to 32 VLANs with a single layer 2 filter.

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

Layer 2 classifiers can be associated with the following actions:

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

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

Refer to Table 57 and Table 58 for more information on layer 2 traffic, either IP or non-IP, and trusted, untrusted, or unrestricted ports.

IP filters

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

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

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

Refer to Table 57 and Table 58 for more information on layer 2 traffic, either IP or non-IP, and trusted, untrusted, or unrestricted ports.

Changing IEEE 802.1p priority and drop precedence

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

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

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

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

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

Refer to Table 57 and Table 58 for more information on layer 2 traffic, either IP or non-IP, and trusted, untrusted, or unrestricted ports.

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

Ports

BPS 2000 ports are classified into three categories: trusted, untrusted, and unrestricted ports. These three categories are also referred to as interface classes. In your network, trusted ports are usually connected to the core of the DiffServ network, and untrusted ports are typically access links that are connected to end stations. Unrestricted ports can be either access links or connected to the core network.

The classifications of trusted, untrusted, and unrestricted actually apply to *groups* of ports (interface groups). Because a port can belong to only one interface group, a port will be classified as trusted, untrusted, or unrestricted. These types are also referred to as interface classes. So, you have three classes of interface groups: Trusted, untrusted, and unrestricted. By default, all ports are untrusted.

Table 57 shows the configurations available to the user for each class of interface for IP traffic (including layer 2 traffic matching IP) and layer 2, non-IP traffic.

Table 57 Possible user re-marking of QoS fields by class of interface

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

Table 58 shows the default guidelines the switch uses to re-mark various fields of IP traffic (and layer 2 traffic matching IP) based on the class of the interface. These are the actions that occur if the user does not intervene at all; they are the default actions of the switch.

Table 58 Default with no user action re-marking of QoS fields by class of interface--IP only

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

Table 59 describes how to select the proper policy settings.

Table 59 Description of proper policy settings

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

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

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

If a packet is received from a trusted port and either it does not match any of the filters installed by the user on this port or it does match a filter but is not dropped, the BPS 2000 uses a default layer 2 filter to change the packet IEEE 802.1p and drop precedence based on the DSCP of the packet.

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

If an IP packet is received from an untrusted port and it does not match any one of the filters installed by the user on the port, the BPS 2000 uses default layer 2 filters to change the packet DSCP, IEEE 802.1p priority, and drop precedence as follows:

- If the packet is tagged, the BPS 2000 uses a layer 2 filter to change the DSCP, IEEE 802.1p to 0, and drop precedence to 1 so that the packet can get best effort treatment.
- If an IP packet is untagged, the BPS 2000 uses 8 default layer 2 filters to change the DSCP based on the default IEEE 802.1p priority of the ingress untrusted port. The BPS 2000 changes the packet DSCP using the 802.1p priority mapping table that matches each one of the eight IEEE 802.1p priorities to the corresponding DSCP. The values can be modified by a policy server or by the user.

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

Table 60 describes the default DSCP, QoS class, IEEE 802.1p, and egress queue assignment for packets in each traffic class.

Table 60 Default mapping of DSCP to QoS class and IEEE 802.1p

Incoming or re-marked DSCP (hex values)	QoS class	Number of queues			Outgoing IEEE 802.1p user priority
		2	4	8	
CS7 (0x38)	Critical	1	1	1	7
CS6 (0x30)	Network			1	
EF(0x2E), CS5(0x28)	Premium			2	6

Table 60 Default mapping of DSCP to QoS class and IEEE 802.1p (continued)

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

As displayed in Table 60, the traffic service class determines the IEEE 802.1p priority that determines the egress queue of the traffic. Non-IP traffic can be in the same IP service class if the non-IP packets are assigned the same IEEE 802.1p priority.

When the power is turned on, all ports are considered untrusted. You can change the power-up defaults using the Web-based management interface. See *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*.

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

Queue sets

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

The cascade port has a set of 2 queues that are serviced using an absolute priority discipline. Filters are installed only on cascade ports that are connected to BayStack 450 or BayStack 410 units in the stack.

BPS 2000 ports are associated with three types of queue sets:

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

There are 3 sets of external ports that correspond to the queue sets. The first set of external ports contains 24 10/100 Mb/s ports and the ports on the BPS2000-4TX MDA, BSP2000-4FX MDA, and BPS2000-2FX MDA; these interfaces are associated with queue set 1. Each port in this set has a set of 4 queues. The first queue holds the highest priority and is serviced in an absolute priority fashion, meaning that this queue is serviced first until all the queued packets are transmitted. The other three queues are serviced using a WRR scheduler.

The second set of external ports contains the ports for the BayStack 450-1GBIC, 1SR, 1SX, 1LR, and 1LX MDAs. These interfaces are associated with queue set 2, which has 2 queues that are serviced in an absolute priority fashion.

The third set of external ports contains the MDA front panel ports for the BPS2000-1GT, BPS2000-2GT, and BPS2000-2GE MDAs; these interfaces are associated with queue set 3. Each port in this set has a set of 8 queues. The first queue holds the highest priority and is serviced in an absolute priority fashion, meaning that this queue is serviced first until all the queued packets are transmitted. The other seven queues are serviced using a WRR scheduler.

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

Interface groups

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

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

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

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

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

Metering overview

QoS metering, which operates at ingress, provides different levels of service to data streams through user-configurable parameters. A meter is used to measure the traffic stream against a traffic profile, which you create. Thus, creating meters yields In-Profile and Out-of-Profile traffic.

Beginning with software version 2.0, you no longer need to configure a meter if you are not metering data.

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

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

An example of traffic policing is limiting traffic entering a port to a specified bandwidth, such as 25 Kb/s (Committed Rate). Instead of dropping all traffic that exceeds this threshold, you can configure a Maximum Burst Rate to exceed the threshold (Committed Rate), for a brief period of time (Duration), without being dropped.

Note: Burst rate and duration are used to determine burst size.

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

You can also configure policies without metering. In this case, using the Web-based management system, you choose No Meter Data in the Data Specification field of the Meter page. Refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5* for more information using the Web-based management system to configure QoS parameters on the BPS 2000.

Shaping overview

Shaping, or traffic shaping, which operates at egress, smooths the traffic on the uplink connection to the network core to provide efficient bandwidth utilization. Shaping is available only on the output ports of the BPS 2000-1GT, BPS 2000-2GT, or BPS 2000-2GE MDAs.

Note: You must install the BPS 2000-1GT, BPS 2000-2GT, or BPS 2000-2GE MDA in a Business Policy Switch in order to use shaping.

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

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

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

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

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

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

To define shaping criteria, you set a Shaping Rate in Kbps (1000 bits per second in each Kb/s) and a Shaping Burst Rate that specifies an allowed data burst larger than the Shaping Rate for a brief period. After you specify the Shaping Burst Rate, you choose among up to 6 possible Shaping Burst Rate Durations. Finally, you set the shaping queue size, which is used to configure the size of the shaping queue.

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

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

You can shape only those traffic flows that have an IEEE 802.1p value that is known at egress. Table 61 shows the type of traffic that can be shaped on trusted, untrusted, and unrestricted interface classes.

Table 61 Shaping possibilities by class of interface

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

Policy overview

When network traffic attributes match those specified in a traffic pattern, the policy instructs the network device to perform a specified action on each packet that passes through it.

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

A *policy* is a network traffic-controlling mechanism that monitors the characteristics of the traffic (for example, its source, destination, and protocol) and performs a controlling action on the traffic when certain user-defined characteristics are matched. A *policy action* is the effect a policy has on network traffic that matches the traffic profile of the policy.

The policies tie together:

- Actions
- Meters
- Shapers
- Filter groups
- Interface groups

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

Ports are assigned to interface groups that are linked to policies. Although a single policy can reference only one interface group, you can configure several policies that reference the same interface group. The policies determine the traffic treatment of the flows.

Beginning with software version 2.0, you can enable or disable policies; you do not have to delete a policy to disable it. However, you still have to delete a policy to modify it.

Packet flow using QoS

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

This section contains a very simplified introduction to the many ways to prioritize packets using QoS. In simple terms, the methods of prioritizing packets depend on the DSCP and the 802.1 priority level and drop precedence.

The QoS class basically directs which group of packets receives the best network throughput, which group of packets receives the next best throughput, and so on. The level of service for each packet is determined by the configurable DSCP.

The available levels of QoS classes are currently named Premium, Platinum, Gold, Silver, Bronze, and Standard. The level of service for each packet is determined by the configurable DSCP.

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

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

Meters, operating at ingress, keep the sorted packets within certain parameters. You configure a committed rate of traffic, allowing a certain size for a temporary burst, as In-Profile traffic. All other traffic is configured as Out-of-Profile traffic. If you choose not to meter the flow, you do not configure meters.

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

Actions determine how the traffic is treated.

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

Default QoS settings

The Business Policy Switch is shipped with limited default QoS information. Defaults include a default interface group, default user priority-to-queue mappings for each queue set, and default DSCP-to-user priority mappings.

QoS configuration guidelines

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

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

COPS overview

Common Open Policy Services (COPS) is important as a stateful protocol between a policy server and a network device such as the BPS 2000. COPS is implemented by using the Optivity Policy Services* (OPS), Version 1.2 or later, which is a comprehensive network management application. OPS provides a centralized management point for DiffServ policies. The policy server distributes policies to edge devices and border routers. These edge devices police traffic flows by marking packets and applying forwarding behaviors to the packets at the network node.

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

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

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

For information about OPS, and specific BPS 2000 implementation notes, go to the www.nortelnetworks.com/documentation URL. Then locate the specific software product (in this case, Optivity Policy Services).

Chapter 5
Sample QoS configuration

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

For more information on configuring QoS with the Web-based management system, refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*. For information on configuring QoS with other management systems, refer to *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5* and *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5*.

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

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

With software version 2.5, you can easily configure QoS parameters using the QoS Quick Config Web pages. QoS Quick Config allows you to configure multiple QoS components using only two Web pages. Although QoS Quick config does not provide the full range of options as the QoS Advanced Pages, Quick Config is suitable for many QoS applications.

Refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5* for sample QoS Wizard and QoS Quick Config configurations.

It is important that you refer to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5* for details to access the Web-based management interface, directory and page navigation information, and field descriptions

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

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

- "Creating interface groups," next
- "Accepting default mapping values" on page 327
- "Setting up filters and filter groups" on page 327
- "Configuring actions" on page 340
- "Configuring meters" on page 343
- "Configuring shapers" on page 346
- "Configuring policies" on page 348
- "Assigning mapping values" on page 353

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

Creating interface groups

To create an interface group:

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

The QoS Advanced menu option expands to display:

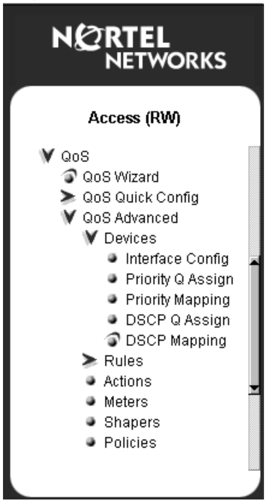
- Devices
- Rules
- Actions
- Meters
- Shapers
- Policies
- Agent

2 Click Devices.

The Devices menu option expands (Figure 107) to display:

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

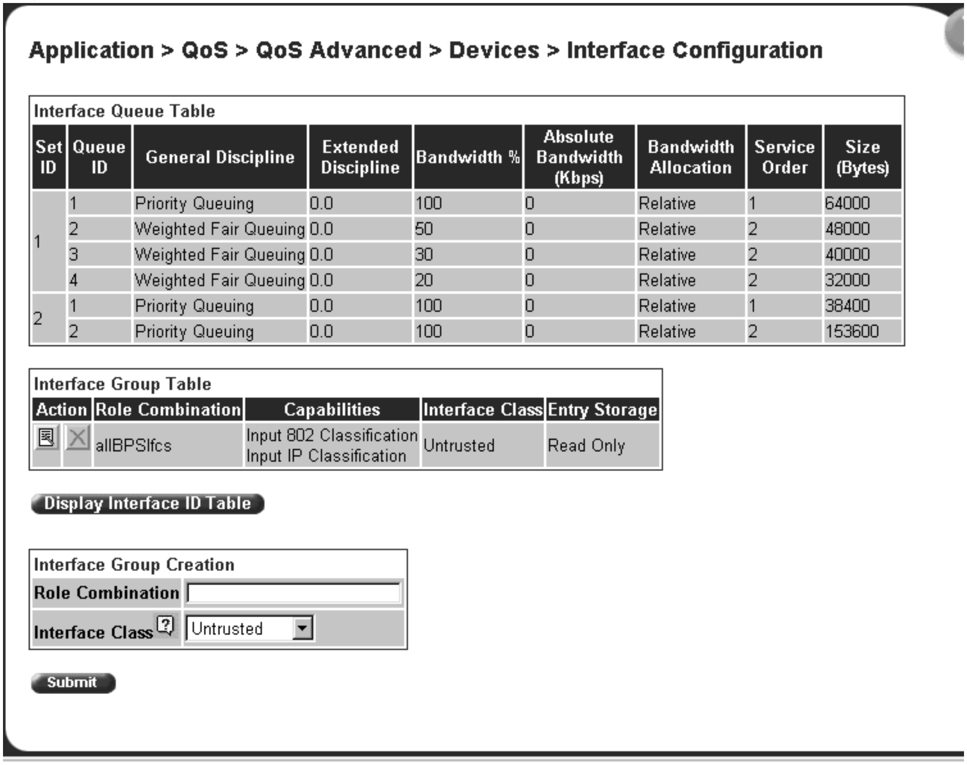
Figure 107 Web-based management menu page



3 Click Interface Config.

The Interface Configuration page opens (Figure 108).

Figure 108 Interface Configuration page



Application > QoS > QoS Advanced > Devices > Interface Configuration

Interface Queue Table

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

Interface Group Table

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

Display Interface ID Table

Interface Group Creation

Role Combination	
Interface Class ?	Untrusted ▾

Submit

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

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

Note: Do not use spaces in the naming field.

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

By selecting untrusted, incoming DSCP values will be changed. (Refer to Chapter 4 for more information on trusted, untrusted, and unrestricted interfaces classes.)

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

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

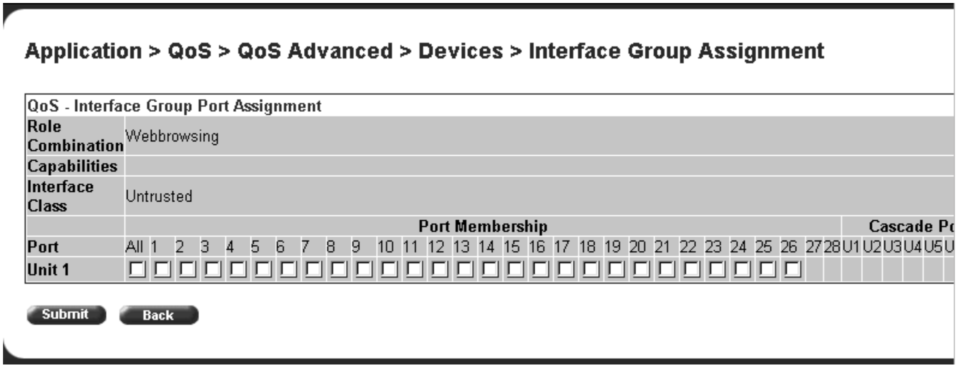
6 Click Submit.

The new entry appears in the Interface Group Table.

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

The Interface Group Assignment page opens (Figure 109).

Figure 109 Interface Group Assignment page



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

QoS - Interface Group Port Assignment

Role Combination	Webbrowsing
Capabilities	
Interface Class	Untrusted

	Port Membership																													Cascade Pc					
Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	U1	U2	U3	U4	U5	U
Unit 1	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□								

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

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

b Click Submit.

.

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

Accepting default mapping values

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

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

To manually configure mapping values, refer to "Assigning mapping values" on page 353.

Setting up filters and filter groups

Filters allow you to classify packets by various parameters. (For more information on these parameters, refer to Chapter 4.) Filters are combined into filter groups. Filter groups are then associated with an interface group.

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

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

Defining an IP filter

You create IP filters for IP packets that are to be forwarded through the BPS 2000 on specific ingress ports. In each IP packet, there is a differentiated services (DiffServ) field in the packet header that you can mark for specific treatment. This field is called the DiffServ code point (DSCP). The DSCP has a specific value that determines how the packet is treated as it travels through the network. As each packet is examined it will be forwarded or dropped, depending on whether or not the filter criteria is matched.

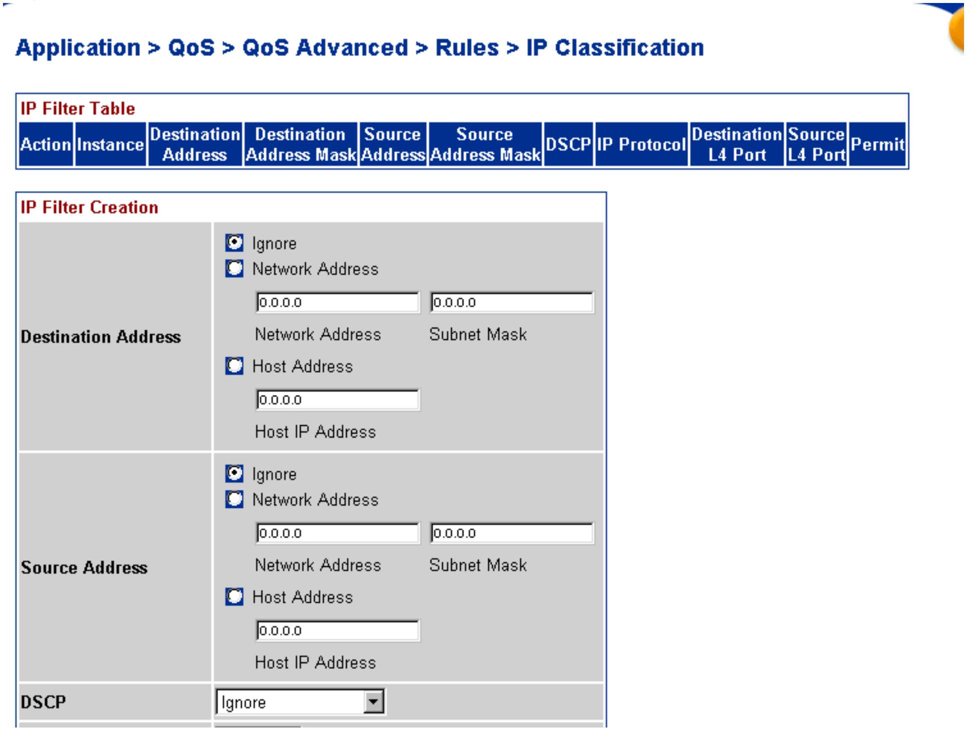
You use the IP Filter Creation section of the Rules > IP Classification page when defining your IP filters.

To define an IP filter:

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

The IP Classification page opens (Figure 110 and Figure 111).

Figure 110 IP Classification page (1 of 2)



Application > QoS > QoS Advanced > Rules > IP Classification

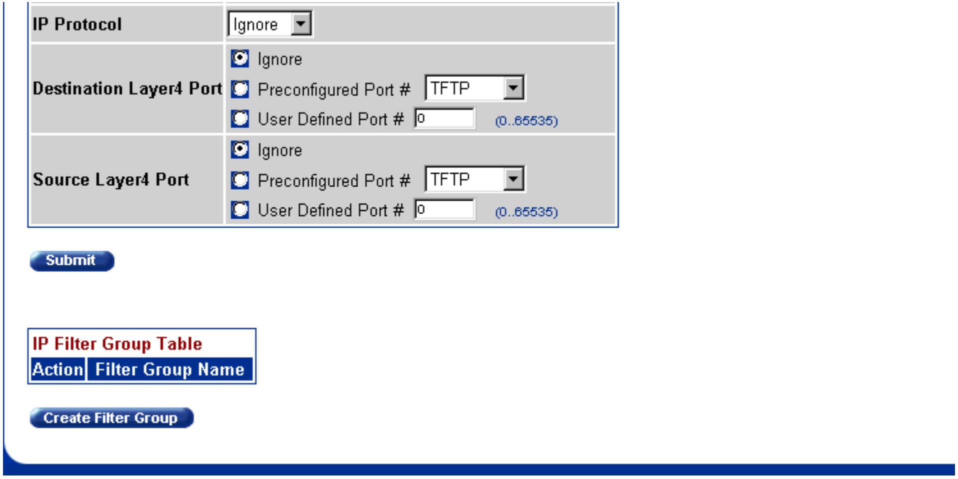
IP Filter Table

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

IP Filter Creation

Destination Address	● Ignore ○ Network Address 0.0.0.0 Network Address 0.0.0.0 Subnet Mask ○ Host Address 0.0.0.0 Host IP Address
Source Address	● Ignore ○ Network Address 0.0.0.0 Network Address 0.0.0.0 Subnet Mask ○ Host Address 0.0.0.0 Host IP Address
DSCP	Ignore

Figure 111 IP Classification page (2 0f 2)



IP Protocol	Ignore
Destination Layer4 Port	● Ignore ○ Preconfigured Port # TFTP ○ User Defined Port # 0 (0..65535)
Source Layer4 Port	● Ignore ○ Preconfigured Port # TFTP ○ User Defined Port # 0 (0..65535)

IP Filter Group Table

Action	Filter Group Name

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8 Click Submit.

The new entry appears in the IP Filter Table.

Creating an IP Filter Group Table entry

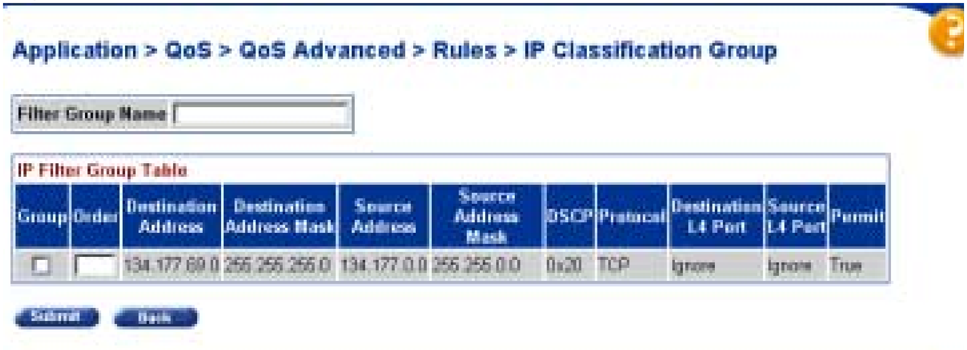
Now you can create an IP filter group in the IP Filter Group Table section of the IP Classification page.

To create an IP filter group entry:

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

The IP Classification Group page opens (Figure 112).

Figure 112 IP Classification Group page



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

Filter Group Name

IP Filter Group Table

Group	Order	Destination Address	Destination Address Mask	Source Address	Source Address Mask	DSCP	Protocol	Destination L4 Port	Source L4 Port	Permit
□		134.177.69.0	255.255.255.0	134.177.0.0	255.255.0.0	0x20	TCP	Ignore	Ignore	True

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

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

Note: Do not leave spaces in your naming entry.

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

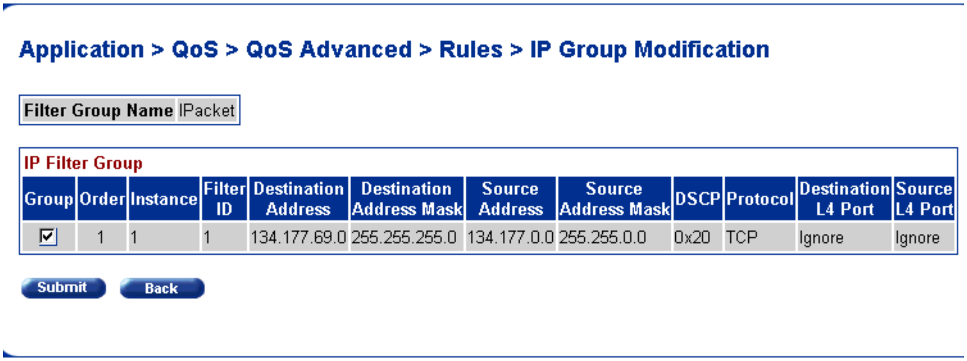
4 Enter the Order number **`1`**.

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

5 Click Submit.

The new entry is displayed on the IP Group Modification page (Figure 113).

Figure 113 IP Group Modification page



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

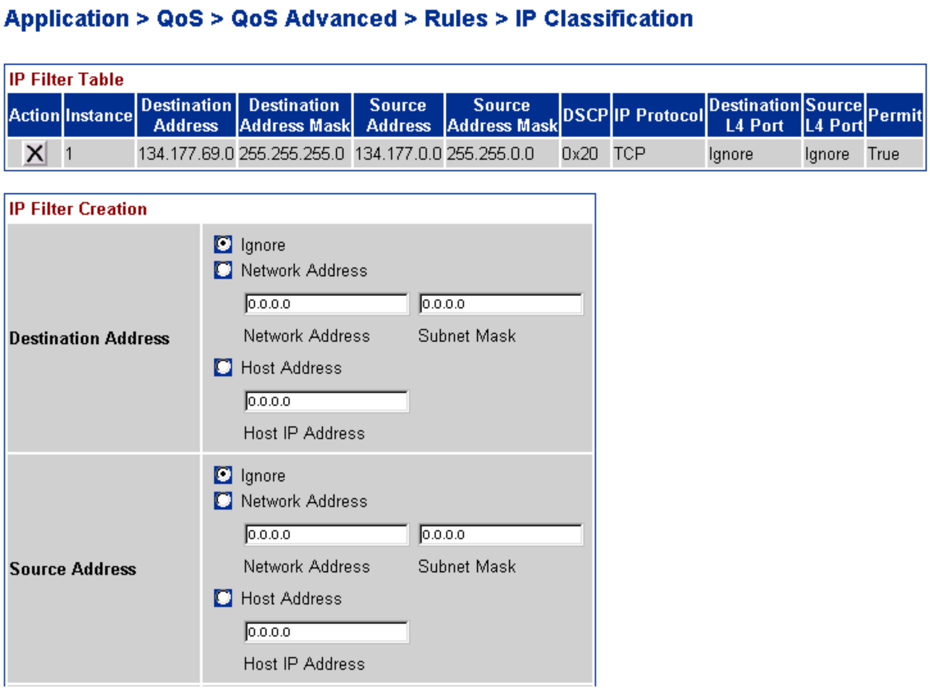
Filter Group Name IPacket

IP Filter Group

Group	Order	Instance	Filter ID	Destination Address	Destination Address Mask	Source Address	Source Address Mask	DSCP	Protocol	Destination L4 Port	Source L4 Port
☑	1	1	1	134.177.69.0	255.255.255.0	134.177.0.0	255.255.0.0	0x20	TCP	Ignore	Ignore

The system returns you to IP Classification page. The new filter appears in the IP Filter Table, and the new filter group appears in the IP Filter Group Table (Figure 114 and Figure 115).

Figure 114 IP Classification page (1 of 2)



Application > QoS > QoS Advanced > Rules > IP Classification

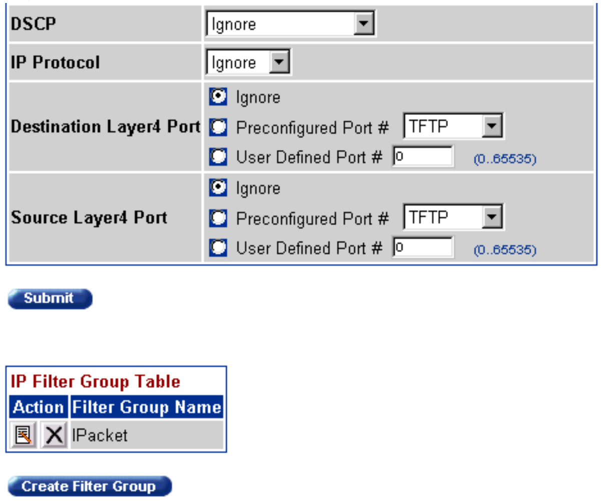
IP Filter Table

Action	Instance	Destination Address	Destination Address Mask	Source Address	Source Address Mask	DSCP	IP Protocol	Destination L4 Port	Source L4 Port	Permit
☒	1	134.177.69.0	255.255.255.0	134.177.0.0	255.255.0.0	0x20	TCP	Ignore	Ignore	True

IP Filter Creation

Destination Address	● Ignore ○ Network Address 0.0.0.0 0.0.0.0 Network Address Subnet Mask ○ Host Address 0.0.0.0 Host IP Address
Source Address	● Ignore ○ Network Address 0.0.0.0 0.0.0.0 Network Address Subnet Mask ○ Host Address 0.0.0.0 Host IP Address

Figure 115 IP Classification page (2 0f 2)



DSCP	Ignore
IP Protocol	Ignore
Destination Layer4 Port	● Ignore ○ Preconfigured Port # TFTP ○ User Defined Port # 0 (0..65535)
Source Layer4 Port	● Ignore ○ Preconfigured Port # TFTP ○ User Defined Port # 0 (0..65535)

IP Filter Group Table

Action	Filter Group Name
☒	IPacket

Defining a layer 2 filter

You 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.

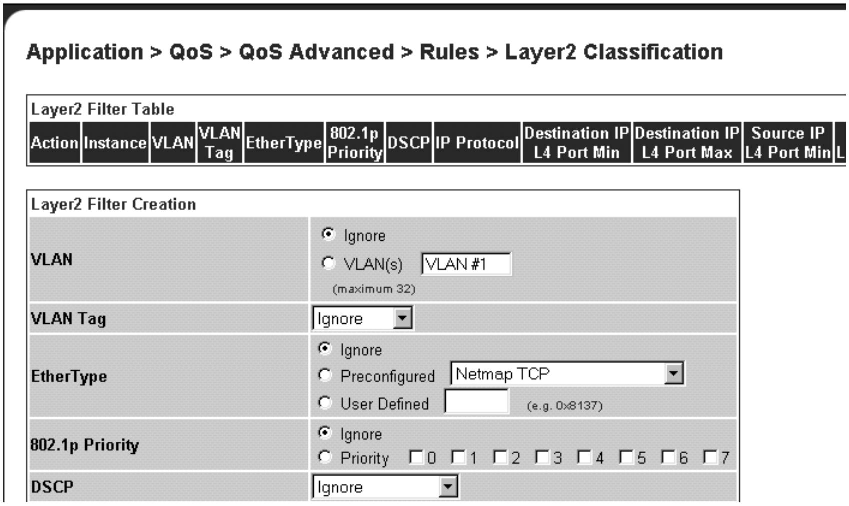
Note: Beginning with software version 2.0, you can reference up to 32 VLANs with a single layer 2 filter.

To configure a layer 2 filter:

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

The Layer2 Classification page opens (Figure 116 and Figure 117).

Figure 116 Layer 2 Classification page (1 of 2)



Application > QoS > QoS Advanced > Rules > Layer2 Classification

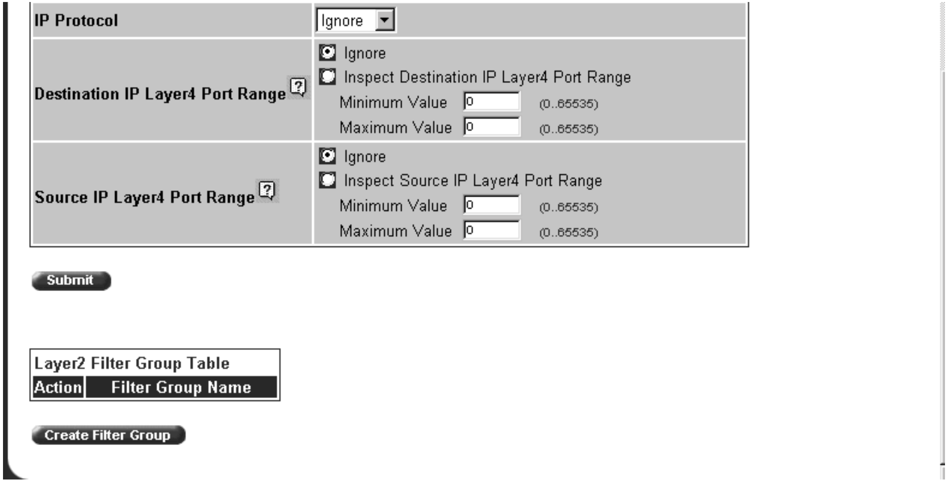
Layer2 Filter Table

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

Layer2 Filter Creation

VLAN	● Ignore ○ VLAN(s) VLAN #1 (maximum 32)
VLAN Tag	Ignore
EtherType	● Ignore ○ Preconfigured Netmap TCP ○ User Defined (e.g. 0x8137)
802.1p Priority	● Ignore ○ Priority □ 0 □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7
DSCP	Ignore

Figure 117 Layer 2 Classification page (2 of 2)



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

Layer2 Filter Group Table

Action	Filter Group Name

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

This filter matches packets in VLAN 1.

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

Only packets that have an IEEE 802.1p tag match this layer 2 filter.

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

All EtherTypes are ignored.

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

Only packets that have IEEE 802.1p user priority 0, 1, 2 will match this filter.

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

Any values that are in the DSCP field are ignored.

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

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

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

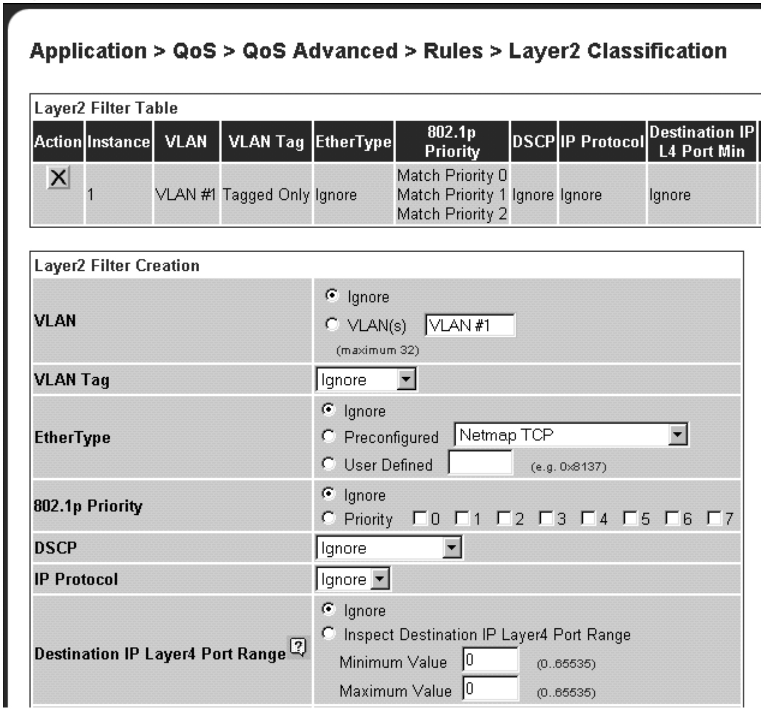
9 In the Source IP Layer4 Port Range field, click **`Ignore`**.

Any values for the packet’s layer 4 source port are ignored.

10 Click Submit.

The new entry is displayed in the Layer2 Filter Table (Figure 118 and Figure 119).

Figure 118 Layer 2 Classification page with new entry (1 of 2)



Application > QoS > QoS Advanced > Rules > Layer2 Classification

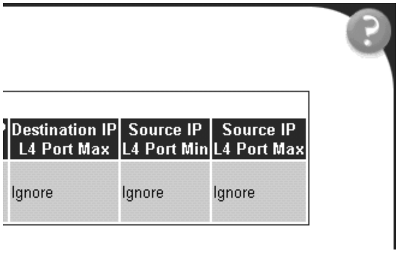
Layer2 Filter Table

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

Layer2 Filter Creation

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

Figure 119 Layer 2 Classification page with new entry (2 of 2)



Destination IP L4 Port Max	Source IP L4 Port Min	Source IP L4 Port Max
Ignore	Ignore	Ignore

Creating a Layer2 Filter Group Table entry

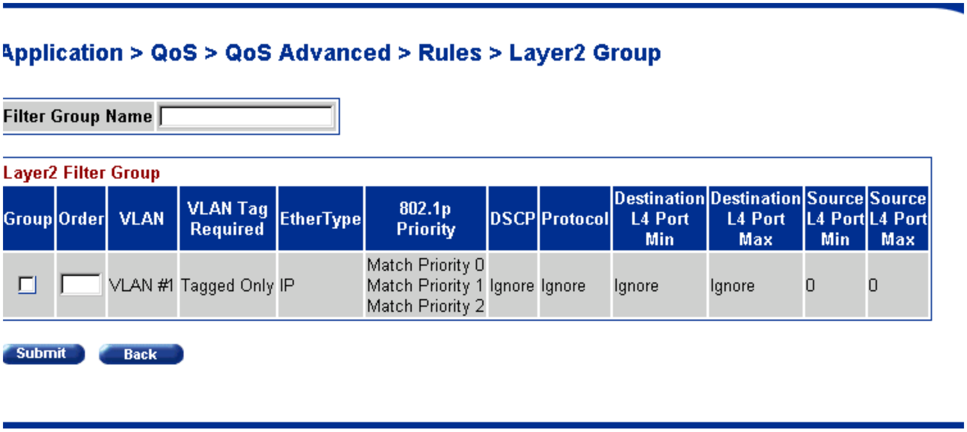
Now you can create a layer 2 filter group in the Layer2 Filter Group Table section of the Layer2 Classification page.

To create a layer 2 filter group entry:

1 Click Create Filter Group in the Layer2 Filter Group Table section of the Layer 2 Classification page (Figure 116 and Figure 117).

The Layer2 Group page opens (Figure 120).

Figure 120 Layer2 Group page



Application > QoS > QoS Advanced > Rules > Layer2 Group

Filter Group Name

Layer2 Filter Group

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

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

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

Note: Do not leave spaces in your naming entry.

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

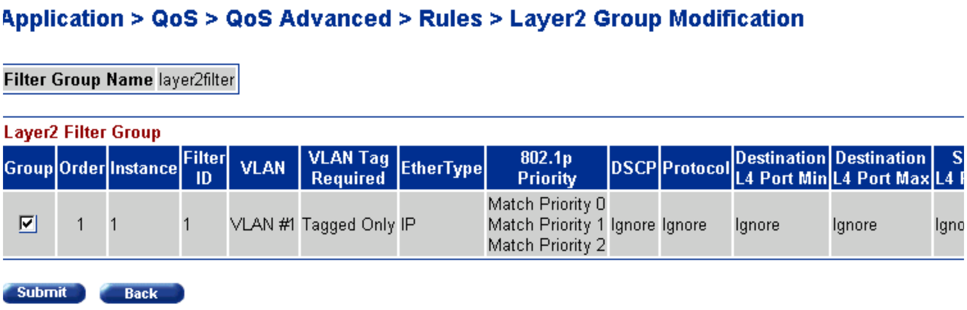
4 Enter the Order number **`1`**.

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

5 Click Submit.

The new entry is displayed on the Layer 2 Group Modification page (Figure 121).

Figure 121 Layer 2 Group Modification page



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

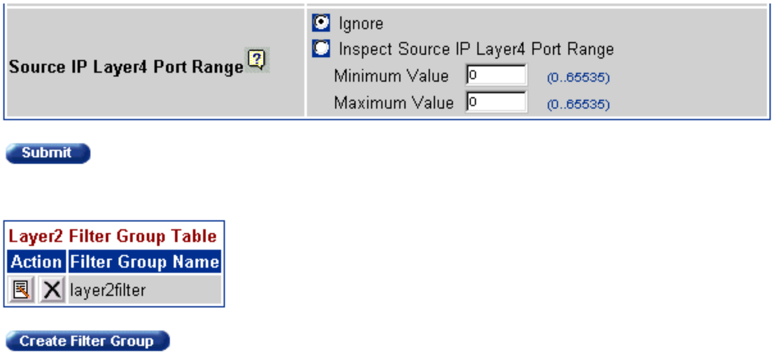
Filter Group Name layer2filter

Layer2 Filter Group

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

The system returns you to Layer 2 Classification page. The new filter group appears in the Layer2 Filter Group Table (Figure 122).

Figure 122 Layer 2 Classification page



Source IP Layer4 Port Range

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

Layer2 Filter Group Table

Action	Filter Group Name
	layer2filter

Configuring actions

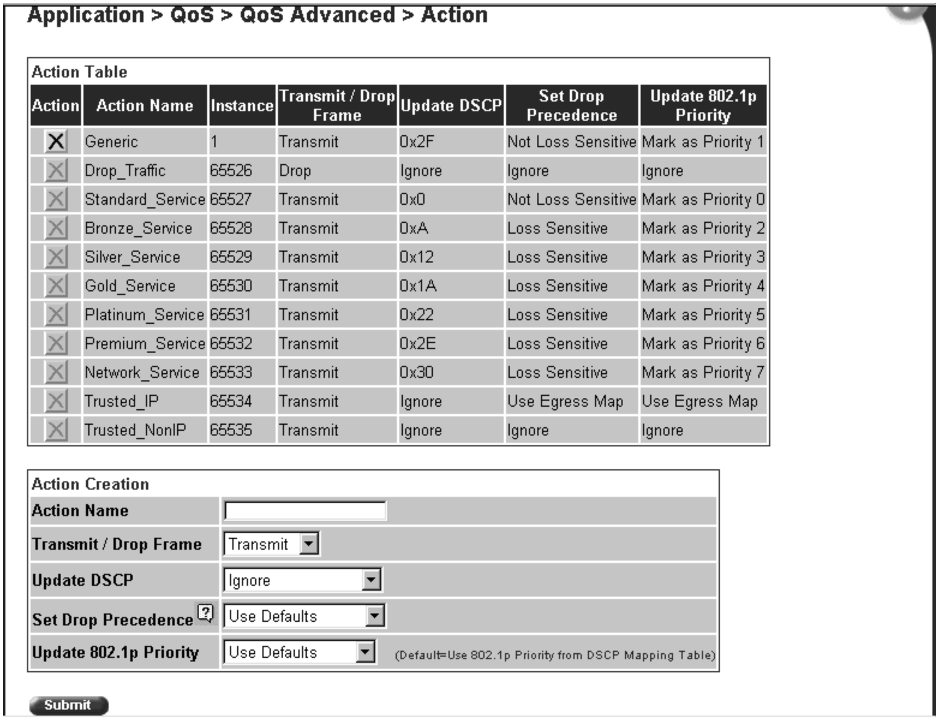
When you assign actions to filters, you specify the type of behavior you want a policy to apply to a flow of IP and IEEE 802 packets. Actions applied to filters establish packet-specific criteria that determine how a packet is to be processed. You specify the actions associated with specific IP and layer 2 filter groups. When filters match incoming packets, the actions are performed on those packets. Actions can be configured to re-mark packets, to change priorities and loss sensitivity (drop precedence), or to drop packets. In order to use a particular action, that action must be assigned to a meter (refer to "Configuring meters" on page 343).

To configure an action:

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

The Actions page opens (Figure 123).

Figure 123 Actions page



Application > QoS > QoS Advanced > Action

Action Table

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

Action Creation

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

Note: Beginning with software version 2.0, the Action page opens with configured actions for the classes of service as well as a few other typical actions.

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

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

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

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

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

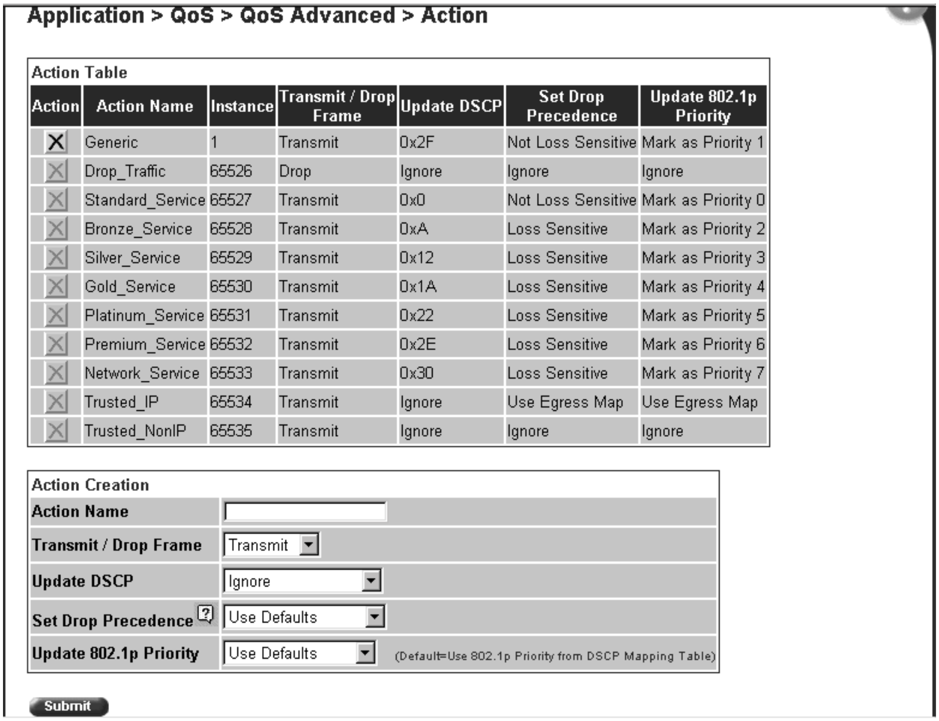
6 In the Update 802.1p Priority field, select **`Priority 1`**.

Priority 1 specifies a low priority.

7 Click Submit.

The entry is displayed in the Action Table (Figure 124).

Figure 124 Action page with entry in Action Table



Application > QoS > QoS Advanced > Action

Action Table

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

Action Creation

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

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

Configuring meters

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

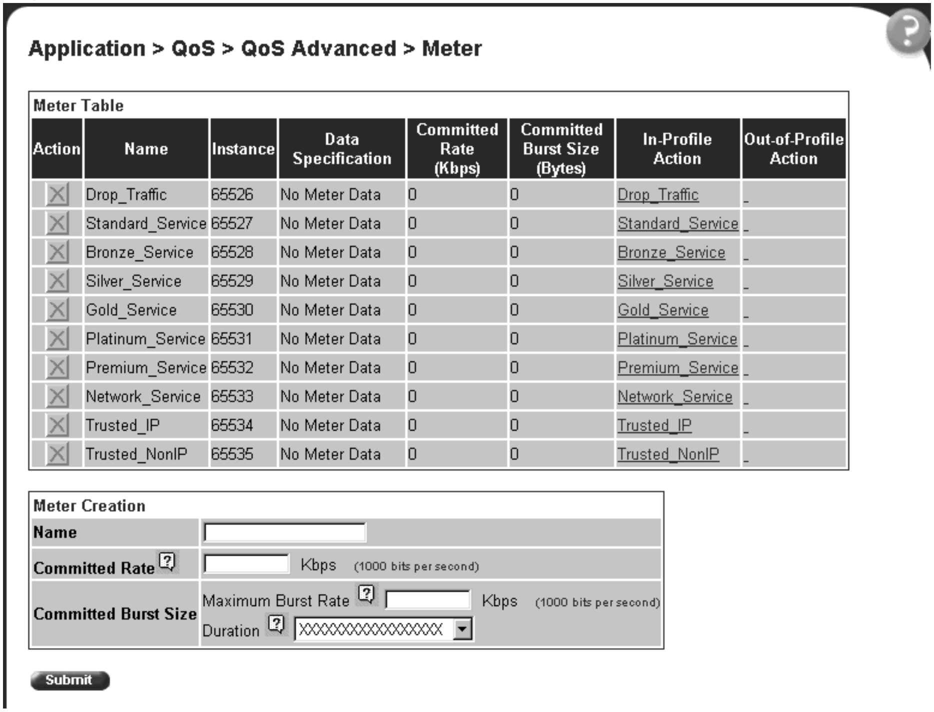
Note: If you not metering data, go to "Configuring shapers" on page 346.

To configure a meter:

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

The Meters page opens (Figure 123).

Figure 125 Meters page



Application > QoS > QoS Advanced > Meter

Meter Table

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

Meter Creation

Name	
Committed Rate ?	Kbps (1000 bits per second)
Committed Burst Size	Maximum Burst Rate ? Kbps (1000 bits per second) Duration ? XXXXXXXXXXXXXXXXX

Note: Beginning with software version 2.0, the Meter page opens with configured meters for the classes of service as well as a few other typical actions.

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

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

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

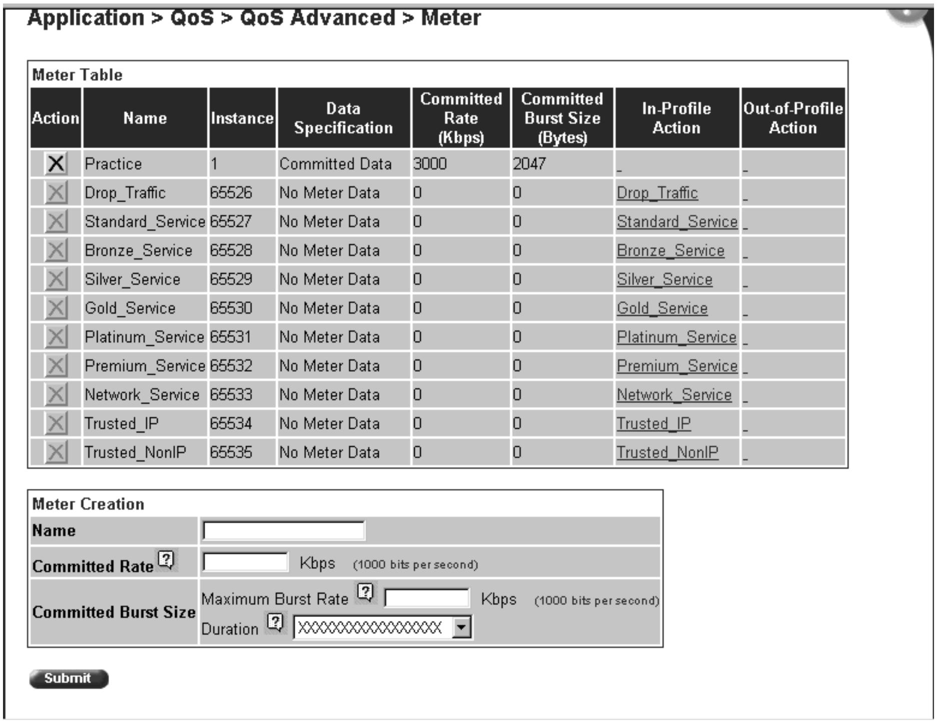
5 In the Duration field of the Committed Burst Size section, select **`33 milliseconds`** from the pull-down menu.

The switch calculates from 1 to 7 durations and presents the results to you in a pull-down menu. Choose the one you want.

6 Click Submit.

The new entry is displayed in the Meter Table (Figure 126).

Figure 126 Meter page with new entry in Meter Table



Application > QoS > QoS Advanced > Meter

Meter Table

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

Meter Creation

Name	
Committed Rate ?	Kbps (1000 bits per second)
Committed Burst Size	Maximum Burst Rate ? Kbps (1000 bits per second) Duration ? XXXXXXXXXXXXXXXXX

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

Configuring shapers

Note: To use the QoS shaping feature, you must install the BPS 2000-1GT, BPS 2000-2GT, or BPS 2000-2GE MDA in a Business Policy Switch.

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

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

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

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

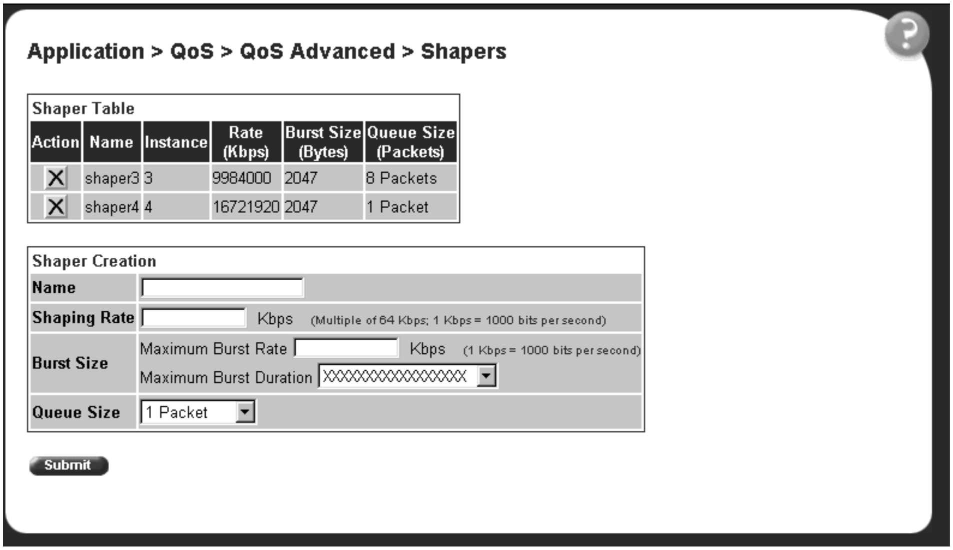
Note: If you do not want to shape the traffic, skip to "Configuring policies" on page 348.

To configure a shaper:

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

The Shapers page opens (Figure 127).

Figure 127 Shapers page



Application > QoS > QoS Advanced > Shapers

Shaper Table

Action	Name	Instance	Rate (Kbps)	Burst Size (Bytes)	Queue Size (Packets)
☒	shaper3	3	9984000	2047	8 Packets
☒	shaper4	4	16721920	2047	1 Packet

Shaper Creation

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

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

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

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

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

5 Choose **`2729 milliseconds`** from the pull-down menu for Maximum Burst Duration.

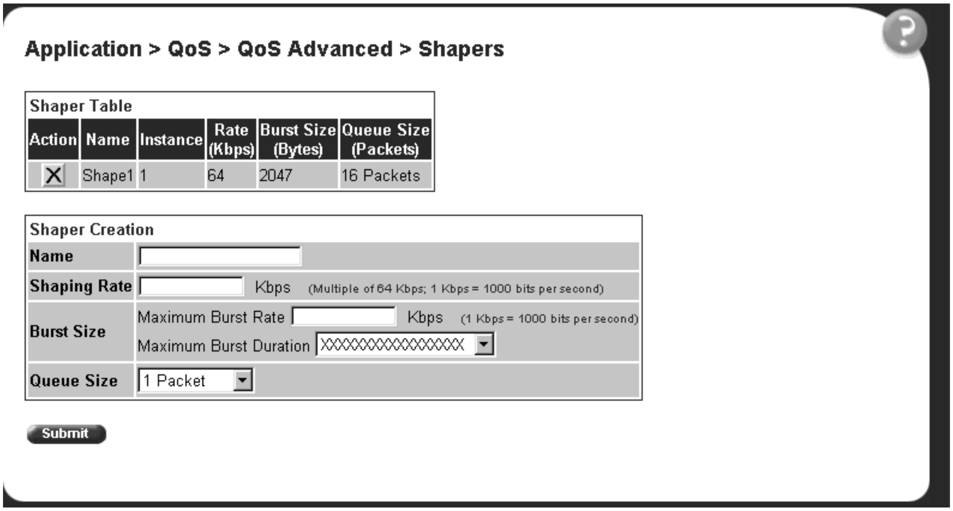
The switch calculates from 1 to 6 durations and presents the results to you in a pull-down menu. Choose the one you want.

6 Choose **16 Packets** from the pull-down menu for Queue Size.

7 Click Submit.

The new entry is displayed in the Shaper Table (Figure 128).

Figure 128 Shapers page with new entry in Shaper Table



Application > QoS > QoS Advanced > Shapers

Shaper Table

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

Shaper Creation

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

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

Configuring policies

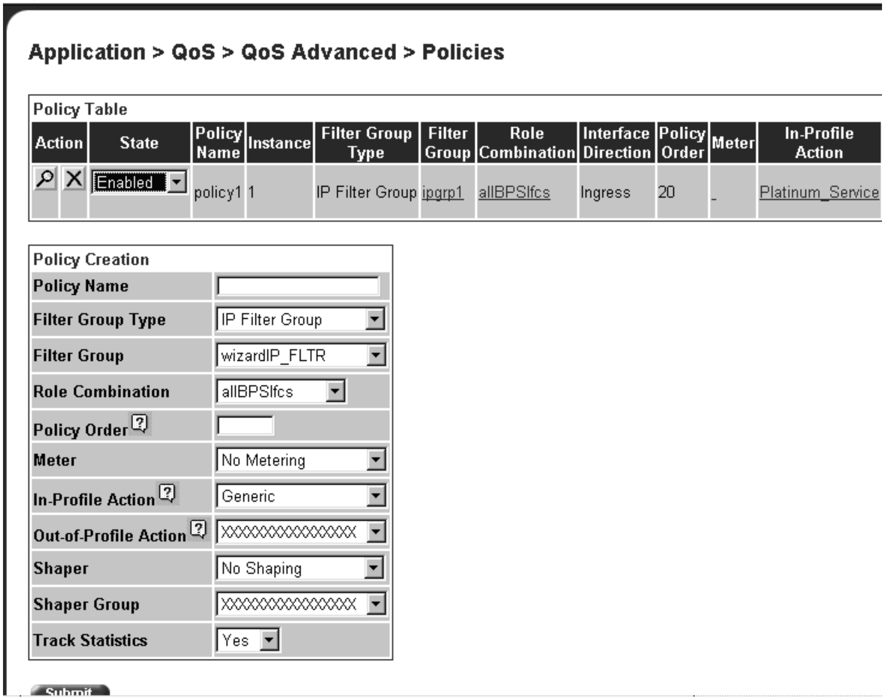
Now you are ready to configure a policy. A policy is an interface group, a group of filters (filter set) and the associated meter, shaper or shaper group, and action. Policies are applied according to the precedence order that you assign in the QoS Advanced > Policies page.

To configure a policy:

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

   The Policies page opens (Figure 129 and Figure 130).

Figure 129 Policies page (1 or 2)



Application > QoS > QoS Advanced > Policies

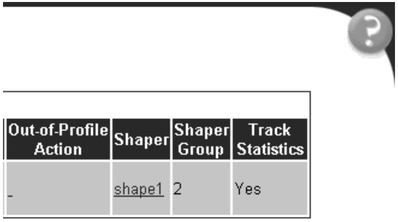
Policy Table

Action	State	Policy Name	Instance	Filter Group Type	Filter Group	Role Combination	Interface Direction	Policy Order	Meter	In-Profile Action
🔍 ✕	Enabled	policy1	1	IP Filter Group	ipgrp1	allBPSIfcs	Ingress	20	_	Platinum_Service

Policy Creation

Policy Name	
Filter Group Type	IP Filter Group
Filter Group	wizardIP_FLTR
Role Combination	allBPSIfcs
Policy Order ?	
Meter	No Metering
In-Profile Action ?	Generic
Out-of-Profile Action ?	XXXXXXXXXXXXXXXX
Shaper	No Shaping
Shaper Group	XXXXXXXXXXXXXXXX
Track Statistics	Yes

Figure 130 Policies page (2 of 2)



Out-of-Profile Action	Shaper	Shaper Group	Track Statistics
_	shape1	2	Yes

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

This entry is a unique name to identify this target.

Note: You cannot have spaces in the naming field.

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

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

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

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

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

This entry is the unique Role Combination that you created.

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

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

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

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

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

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

11 Leave the Shaper Group field as is.

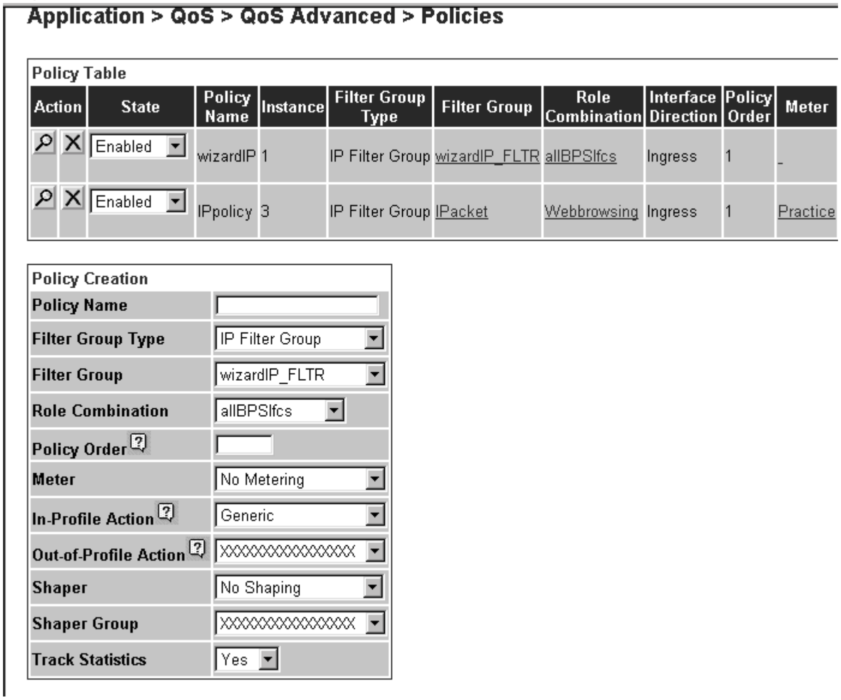
You may want to have the traffic associated with the policy you are now creating shaped as a group (or aggregate) with the traffic associated with other, installed policies. To do so, choose the Shaping Group identified in the Policy Table with the policy or policies you want to group with this traffic,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

12 In the Track Statistics field, choose **`Yes`**.

13 Click Submit.

The new entry is displayed in the Policy Table (Figure 131 and Figure 132).

Figure 131 Policies page with new entry (1 of 2)



Application > QoS > QoS Advanced > Policies

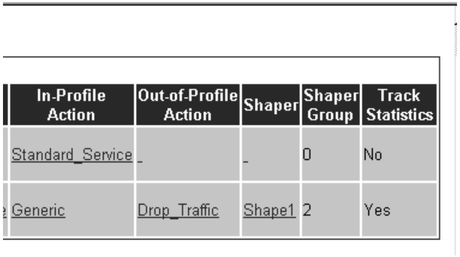
Policy Table

Action	State	Policy Name	Instance	Filter Group Type	Filter Group	Role Combination	Interface Direction	Policy Order	Meter
🔍 ✕	Enabled	wizardIP	1	IP Filter Group	wizardIP_FLTR	allBPSIfcs	Ingress	1	_
🔍 ✕	Enabled	IPpolicy	3	IP Filter Group	IPacket	Webbrowsing	Ingress	1	Practice

Policy Creation

Policy Name	
Filter Group Type	IP Filter Group
Filter Group	wizardIP_FLTR
Role Combination	allBPSIfcs
Policy Order ?	
Meter	No Metering
In-Profile Action ?	Generic
Out-of-Profile Action ?	XXXXXXXXXXXXXXXX
Shaper	No Shaping
Shaper Group	XXXXXXXXXXXXXXXX
Track Statistics	Yes

Figure 132 Policies page with new entry (2 of 2)



In-Profile Action	Out-of-Profile Action	Shaper	Shaper Group	Track Statistics
Standard_Service	_	_	0	No
Generic	Drop_Traffic	Shape1	2	Yes

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

You enable or disable each policy using the pull-down menu under the Status heading. The default value is Enabled.

Assigning mapping values

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

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

- "Assigning 802.1p priority queue assignment" on page 353
- "Verifying DSCP mapping" on page 354
- "Assigning 802.1p user priority mapping" on page 357
- "Verifying DSCP queue assignments" on page 358

Assigning 802.1p priority queue assignment

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

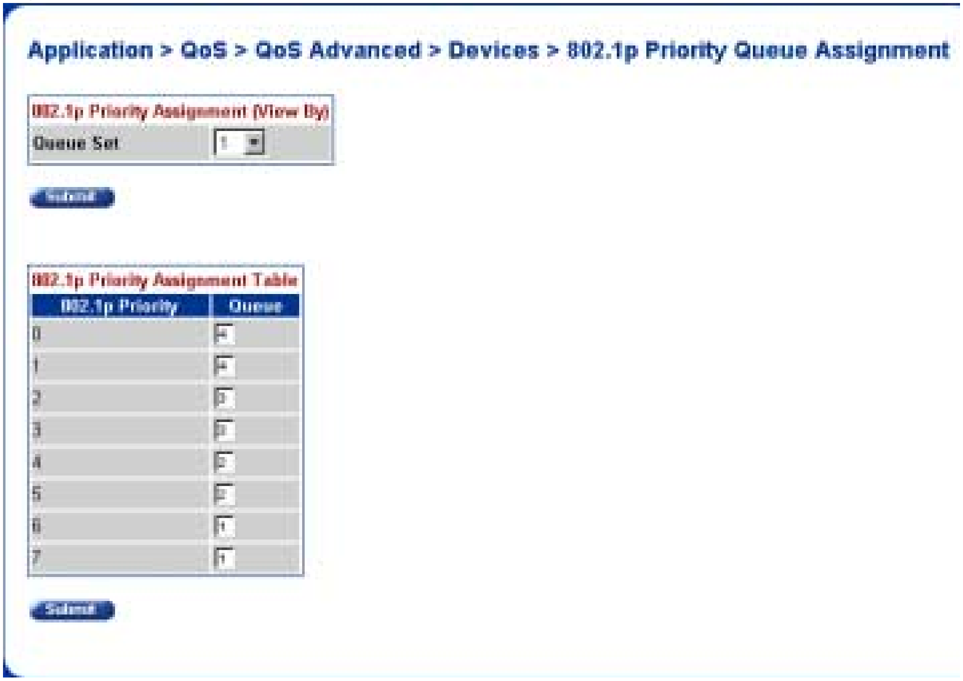
Note: If you want to change the traffic class prioritization on a BayStack 450 switch in a mixed stack configuration, use the 802.1p Priority Queue Assignment page for queue set 2.

To configure 802.1p priority:

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

The 802.1p Priority Queue Assignment page opens (Figure 133).

Figure 133 802.1p Priority Queue Assignment page



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

802.1p Priority Assignment (View By)

Queue Set: 1

802.1p Priority Assignment Table

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

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

This value is the queue set you want to modify.

3 Click Submit.

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

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

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

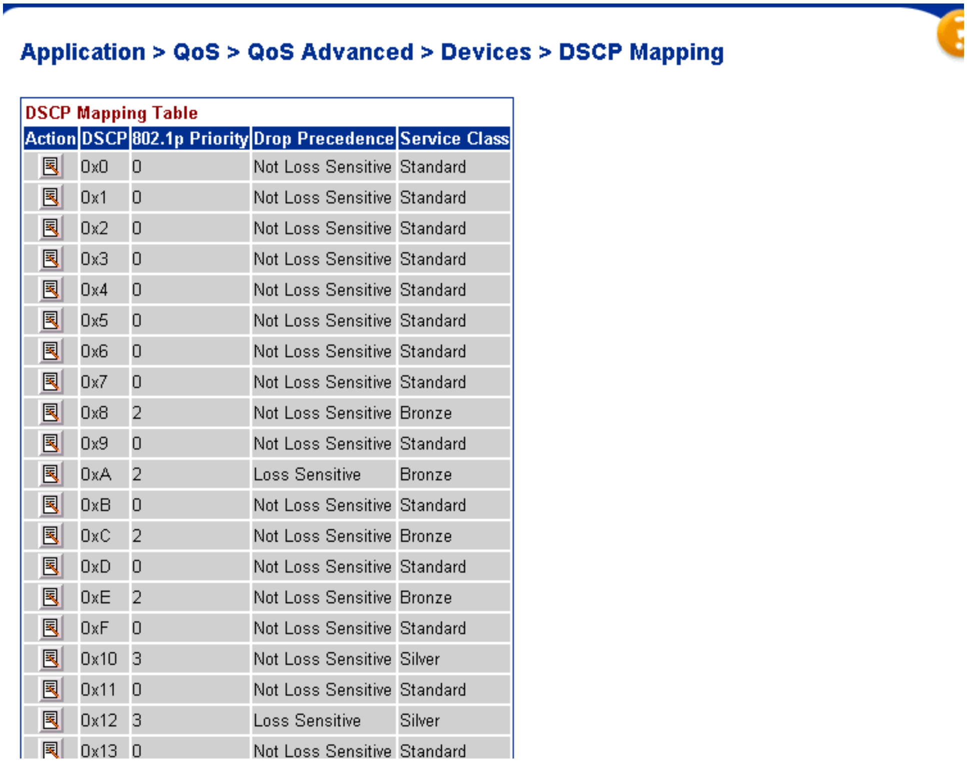
Verifying DSCP mapping

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

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

The DSCP Mapping page opens (Figure 134).

Figure 134 DSCP Mapping page



Application > QoS > QoS Advanced > Devices > DSCP Mapping

DSCP Mapping Table

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

To change the DSCP to an 802.1p priority:

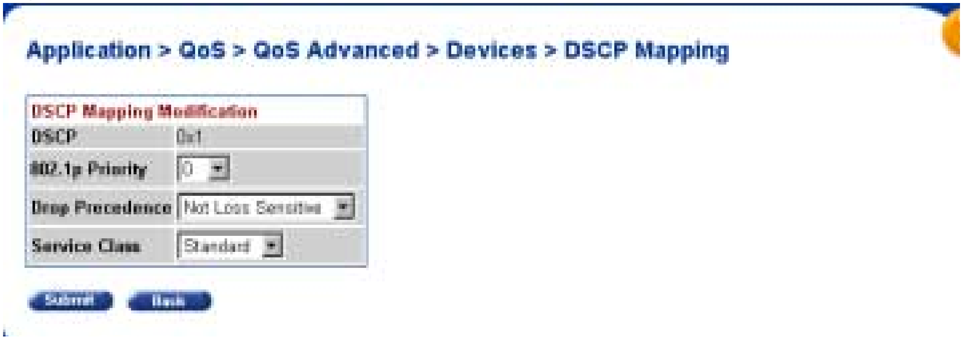
1. Click the Application > QoS > QoS Advanced > Devices > DSCP Mapping menu option.

   The DSCP Mapping page opens (Figure 134).

2. Click the Modify icon of DSCP 0x1.

   The DSCP Mapping page opens (Figure 135) for DSCP 0x1.

Figure 135 DSCP Mapping page



Application > QoS > QoS Advanced > Devices > DSCP Mapping

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

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

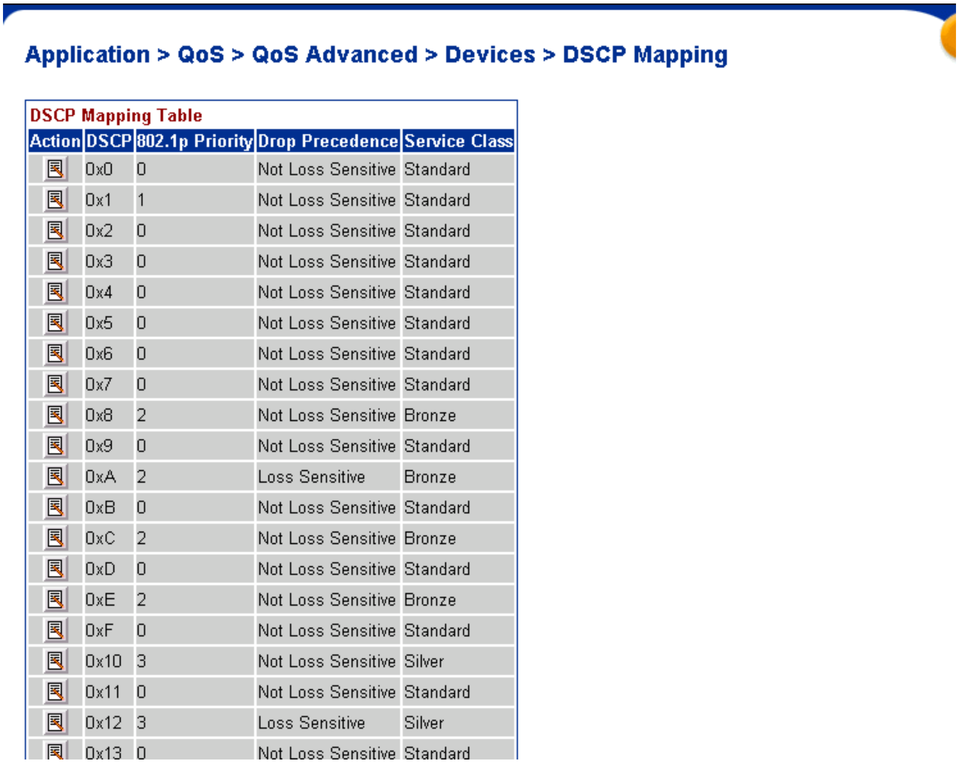
4 In the Drop Precedence field, choose **`Not Loss Sensitive`**.

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

6 Click Submit.

The DSCP Mapping page opens with the updated information (Figure 136).

Figure 136 DSCP Mapping page



Application > QoS > QoS Advanced > Devices > DSCP Mapping

DSCP Mapping Table

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

Assigning 802.1p user priority mapping

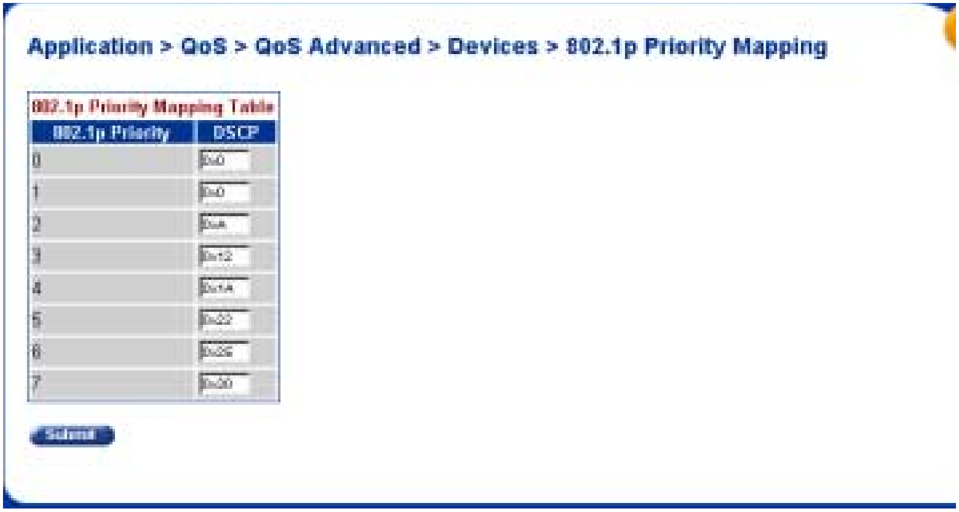
Now, you want to map the 802.1p priority to a specific DSCP.

To configure IEEE 802.1p user priority to DSCP mapping:

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

The 802.1p Priority Mapping page opens (Figure 137).

Figure 137 802.1p Priority Mapping page



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

802.1p Priority Mapping Table

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

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

3 Click Submit.

Verifying DSCP queue assignments

Next, view the DSCP queue assignments.

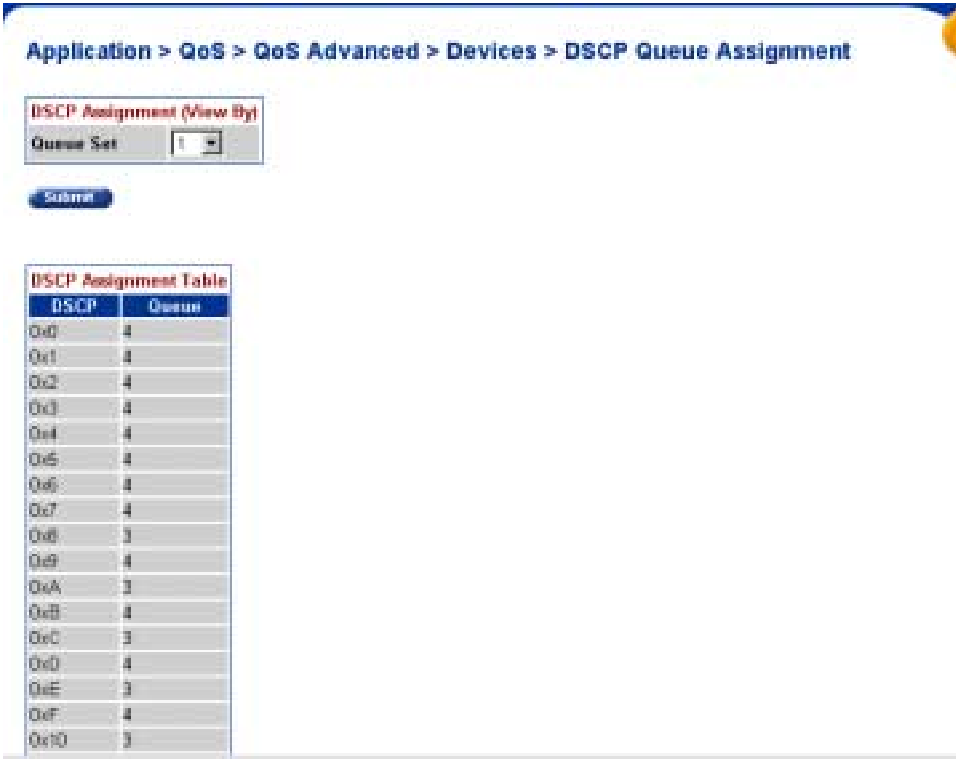
Note: When you want to map DSCP to a queue, you must map DSCP to 802.1p, and then map 802.1p to a queue.

To view DSCP queue assignments:

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

The DSCP Queue Assignment page opens (Figure 138).

Figure 138 DSCP Queue Assignment page



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

DSCP Assignment (View By)

Queue Set: 1

DSCP Assignment Table

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

2 Choose Queue Set `1`.

3 Click Submit.

4 View the queue assignment.

Chapter 6
Troubleshooting

This chapter describes how to isolate and diagnose problems with your Business Policy Switch and covers the following topics:

- "Interpreting the LEDs," next
- "Diagnosing and correcting problems" on page 365

The chapter topics lead you through a logical process for troubleshooting the Business Policy Switch. For example, because LEDs provide visual indications of certain problems, see Chapter 1 to understand the various states (Table 62) that your switch LEDs can exhibit during normal operation.

For more help in determining the problem, "Diagnosing and correcting problems" describes symptoms and corrective actions (Table 63) you can perform to resolve specific problems. Subsequent sections give step-by-step procedures to correct the problems.

Interpreting the LEDs

Figure 139 shows the Business Policy Switch LED display panel. Table 62 describes the LEDs.

Figure 139 LED display panel

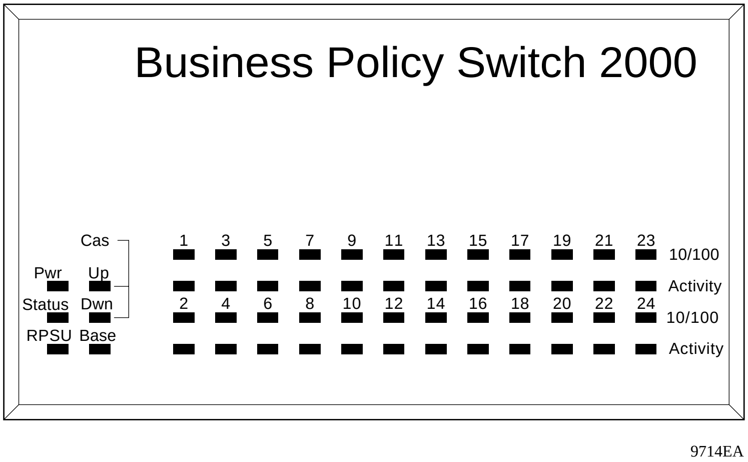


Table 62 Business Policy Switch LED descriptions

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. (This includes nonworking fans.)
			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.

Table 62 Business Policy Switch LED descriptions (continued)

Label	Type	Color	State	Meaning
		Green	On	The switch is connected to the *upstream* unit's Cascade A In connector.
		Amber	On	This unit has detected a problem with the switch connected to the cascade up connector. In order to maintain the integrity of the stack, this unit has bypassed its upstream neighbor and has wrapped the stack backplane onto an alternate path.
		Amber or Green	Blinking	Incompatible software revision or unable to obtain a unit ID (Renumber Stack Unit table full). The unit is on the ring but cannot participate in the stack configuration.
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	This unit has detected a problem with the switch connected to the cascade down connector. In order to maintain the integrity of the stack, this unit has bypassed its downstream neighbor and has wrapped the stack backplane onto an alternate path.
		Amber or Green	Blinking	Incompatible software revision or unable to obtain a unit ID (Renumber Stack Unit table full). The unit is on the ring but cannot participate in the stack configuration.

Table 62 Business Policy Switch LED descriptions (continued)

Label	Type	Color	State	Meaning
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).
			Blinking	Stack configuration error: indicates that *multiple* base units or *no* base units are configured in the stack.
		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.
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.
			Blinking	The corresponding port has been disabled by software.
		Amber	On	The corresponding port is set to operate at 10 Mb/s and the link is good.
			Blinking	The corresponding port has been disabled by software.
			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.
			Blinking	The corresponding port is management disabled.
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.

Diagnosing and correcting problems

This section discusses some common problems in using the BPS 2000, such as joining stacks and upgrading software in mixed stacks. This sections discusses the following topics:

- "Normal power-up sequence," next
- "Port connection problems" on page 366
- "Upgrading software" on page 369
- "Joining stacks" on page 372

Before you perform the problem-solving steps in this section, cycle the power to the Business Policy Switch (disconnect and then reconnect the AC power cord); then verify that the switch follows the normal power-up sequence.

⚠ **Warning:** To avoid bodily injury from hazardous electrical current, never remove the top cover of the device. There are no user-serviceable components inside.

⚠ **Vorsicht:** Um Verletzungsgefahr durch einen elektrischen Stromschlag auszuschließen, nehmen Sie niemals die obere Abdeckung vom Gerät ab. Im Geräteinnern befinden sich keine Komponenten, die vom Benutzer gewartet werden können.

⚠ **Avertissement:** Pour éviter tout risque d'électrocution, ne jamais retirer le capot de l'appareil. Cet appareil ne contient aucune pièce accessible par l'utilisateur.

⚠ **Advertencia:** A fin de evitar daños personales por corrientes eléctricas peligrosas, no desmonte nunca la cubierta superior de este dispositivo. Los componentes internos no son reparables por el usuario.

Avvertenza: Per evitare lesioni fisiche dovute a scariche pericolose di corrente, non rimuovere mai il coperchio superiore del dispositivo. I componenti interni non possono essere manipolati dall'utente.

警告：危険な電流から身体を保護するために、ディバイスの上部カバーを決して取り外さないでください。内部には、ユーザが扱うコンポーネントはありません。

Normal power-up sequence

In a normal power-up sequence, the LEDs appear as follows:

1. After power is applied to the switch, the Pwr (Power) LED turns on within 5 seconds.
2. The switch initiates a self-test, during which the port LEDs display various patterns to indicate the progress of the self-test.
3. Upon successful completion of the self-test (within 10 seconds after power is applied), the Status LED turns on.
4. The remaining port LEDs indicate their operational status, as described in Table 63.

Port connection problems

You can usually trace port connection problems to either a poor cable connection or an improper connection of the port cables at either end of the link. To remedy these types of problems, make sure that the cable connections are secure and that the cables connect to the correct ports at both ends of the link.

Port connection problems are also traceable to the autonegotiation mode or the port interface.

Table 63 Corrective actions

Symptom	Probable cause	Corrective action
All LEDs are off.	The switch is not receiving AC power.	Verify that the AC power cord is fastened securely at both ends and that power is available at the AC power outlet.
	The fans are not operating or the airflow is blocked, causing the unit to overheat.	Verify that there is sufficient space for adequate airflow on both sides of the switch. **Note:** Operating temperature for the switch must not exceed 40°C (104°F). Do not place the switch in areas where it can be exposed to direct sunlight or near warm air exhausts or heaters.
The Activity LED for a connected port is off or does not blink (and you have reason to believe that traffic is present).	The switch is experiencing a port connection problem. The switch's link partner is not autonegotiating properly.	See "Port connection problems" next.
The Status LED is off.	A fatal error was detected by the self-test.	Cycle the power to the switch (disconnect and then reconnect the AC power cord). If the problem persists, replace the switch.
The Status LED is blinking.	A nonfatal error occurred during the self-test.	Cycle the power to the switch (disconnect and then reconnect the AC power cord). If the problem persists, contact the Nortel Networks Technical Solutions Center.

Autonegotiation modes

Port connection problems can occur when a port (or station) is connected to another port (or station) that is not operating in a compatible mode (for example, connecting a full-duplex port on one station to a half-duplex port on another station).

Note: Autonegotiation can be enabled on *every* supported gigabit fiber optic MDA except the BPS2000-2GE MDA.

The Business Policy Switch negotiates port speeds according to the IEEE 802.3u autonegotiating standard. The switch adjusts (autonegotiates) its port speed and duplex mode to match the best service provided by the connected station, up to 100 Mb/s in full-duplex mode as follows:

- If the connected station uses a form of autonegotiation that is not compatible with the IEEE 802.3u autonegotiating standard, the Business Policy Switch cannot negotiate a compatible mode for correct operation.
- If the autonegotiation feature is not present or not enabled at the connected station, the Business Policy Switch may not be able to determine the correct duplex modes.

In both situations, the Business Policy Switch "autosenses" the speed of the connected station and, by default, reverts to half-duplex mode. If the connected station is operating in full-duplex mode, it cannot communicate with the switch.

To correct this mode mismatch problem:

1. Use the Port Configuration screen to disable autonegotiation for the suspect port (see Chapter 3).
2. Manually set the Speed/Duplex field to match the speed/duplex mode of the connected station (see Chapter 3).

   You may have to try several settings before you find the correct speed/duplex mode of the connected station.

If the problem persists:

1. Disable the autonegotiation feature at the connected station.
2. Manually set the speed/duplex mode of the connected station to the same speed/duplex mode you have manually set for the Business Policy Switch port.

Note: Nortel Networks recommends that you manually set the Business Policy Switch port to the desired speed/duplex mode when you connect to any of the following Nortel Networks products:

- BayStack 450 product family
- BayStack 410 product family

Port interface

Ensure that the devices are connected using the appropriate crossover or straight-through cable (see Appendix).

Upgrading software

Note: Use the Command Line Interface (CLI), console interface (CI) menus, or the Web-based management system to upgrade to software version 2.5. For detailed instructions, refer to Chapter 3, *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5*, and *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*.

You use one of the management systems to upgrade or downgrade software. You follow a different procedure depending on whether you are using a Pure BPS 2000 stack or a Hybrid stack.

The stacking software compatibility requirements are as follows:

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

This section discusses the following topics:

- "Upgrading software in a Pure BPS 2000 stack," next
- "Upgrading software in a Hybrid stack" on page 370

Upgrading software in a Pure BPS 2000 stack

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

1. Download the operational software, or agent, image.
2. Download the diagnostics image.

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

➡ **Note:** Once you begin the upgrading process, do not interrupt the process at all. Interrupting the downloading (or upgrading) process may cause loss of connectivity.

Upgrading software in a Hybrid stack

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

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

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

This section describe the steps for the following software upgrades:

- "Upgrading software when ISVN is 2," next
- "Upgrading software when ISVN is 1" on page 371

Upgrading software when ISVN is 2

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

1 Download the BPS 2000 image file.

The system resets.

2 Download the BPS 2000 diags file.

The system resets.

➡ **Note:** Once you begin the upgrading process, do not interrupt the process at all. Interrupting the downloading (or upgrading) process may cause loss of connectivity.

Upgrading software when ISVN is 1

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

1 Download the BPS 2000 image file and the BayStack 450/410 file *simultaneously*.

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

The system resets.

2 Download the other BayStack 450 image file.

The system resets.

3 Download the BPS 2000 diags file.

The system resets.

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

➡ **Note:** Once you begin the upgrading process, do not interrupt the process at all. Interrupting the downloading (or upgrading) process may cause loss of connectivity.

Joining stacks

You can join two stacks, whether entirely BPS 2000 units, or mixed units. You do not have to renumber the units in either stack.

To join two existing stacks:

1 Designate one stack as the one to join the other stack.

2 Reset the stack that will join the other stack to factory defaults.

3 Turn off the power to the all units in the stack that will join the other stack by unplugging the power cords from each unit.

   a On the unit that was the Base Unit of this stack, use the Unit Select switch to deselect it as the Base Unit.

   b Redo all the cabling so that all units will work as one stack.

4 Power-up the newly joined units by plugging in the power cords.

It may take a few minutes for the entire stack to display on the console. All units will show as their new numbers within the newly joined stack.

Appendix A
Technical specifications

This appendix provides technical specifications for the Business Policy Switch 2000.

Environmental

Table 64 lists environmental specifications.

Table 64 Environmental specifications

Parameter	**Operating specification**	**Storage specification**
Temperature	0° to 40°C (32° to 104°F)	-25° to 70°C (-13° to 158°F)
Humidity	85% maximum relative humidity, noncondensing	95% maximum relative humidity, noncondensing
Altitude	3024 m (10,000 ft)	3024 m (10,000 ft)

Electrical

Table 65 lists power electrical parameters for the Business Policy Switch.

Table 65 Electrical parameters

Parameter	**Electrical specification**
Input Voltage	100 to 240 VAC @ 47 to 63 Hz
Input Power Consumption	150 W maximum
Input Volt Amperes Rating	200 VA maximum

Table 65 Electrical parameters (continued)

Input current	1.5 A @ 100 VAC .6 A @ 240 VAC
Maximum thermal output	500 BTU/hr

Physical dimensions

Table 66 lists physical dimensions.

Table 66 Physical dimensions

Parameter	**Specifications**
Height	7.04 cm (2.77 in.)
Width	43.82 cm (17.25 in.)
Depth	38.35 cm (15.1 in)
Weight	4.8 kg (10.60 lb)

Performance specifications

Table 67 lists performance specifications.

Table 67 Performance specifications

Parameter	**Specifications**
Frame Forward Rate (64-byte packets)	Up to 3.2 million packets per second (pps) maximum, learned unicast traffic
Port Forwarding/Filtering Performance (64-byte packets)	• For 10 Mb/s: 14,880 pps maximum • For 100 Mb/s: 148,810 pps maximum
Address Database Size	16,000 entries at line rate (32,000 entries without flooding)
Addressing	48-bit MAC address
Frame Length	64 to 1518 bytes (IEEE 802.1Q Untagged) 64 to 1522 bytes (IEEE 802.1Q Tagged)

Data rate

The data rate is 10 Mb/s Manchester encoded or 100 Mb/s 4B/5B encoded.

Interface options

The BPS2000 has 10BASE-T/100BASE-TX switch ports with RJ-45 (8-pin modular) connectors for MDA-X interfaces.

Refer to *Installing Media Dependent Adapters (MDAs)* and *Installing Gigabit Interface Converters and Small Form Factor Pluggable Interface Converters* for information on the interface connectors on available uplink modules.

Safety agency certification

The safety certifications follow:

- UL Listed (UL 1950)
- IEC 950/EN60950
- C22.2 No. 950 (CUL) with all national deviations
- UL-94-V1 flammability requirements for PC board
- NOM (NOM-019)

Electromagnetic emissions

The module meets the following standards:

- US. CFR47, Part 15, Subpart B, Class A
- Canada. ICES-003, Issue 2, Class A
- Australia/New Zealand. AS/NZS 3548:1995, Class A
- Japan. V-3/97.04:1997, Class A
- Taiwan. CNS 13438, Class A

- EN55022:1995, Class A
- EN61000-3-2:1995
- EN61000-3-3:1994

Electromagnetic immunity

The module meets the EN50082-1:1997 standard.

Declaration of Conformity

The Declaration of Conformity for the BPS 2000 complies with ISO/IEC Guide 22 and EN45014. The declaration identifies the product models, the Nortel Networks name and address, and the specifications recognized by the European community.

As stated in the Declaration of Conformity, the Business Policy Switch 2000 complies with the provisions of Council Directives 89/336/EEC and 73/23/EEC.

Appendix B
Interoperability in a mixed stack configuration

This appendix presents important interoperability guidelines when you implement a mixed stack configuration. A mixed stack consists of a combination of Business Policy Switches *and* BayStack 450 and/or BayStack 410 switches.

This appendix covers the following topics:

- "Compatibility with BayStack 450 switches," next
- "Setting up your mixed stack configuration" on page 378
- "Upgrading software in a mixed stack" on page 383
- "Joining stacks" on page 385
- "Troubleshooting problems" on page 386

Compatibility with BayStack 450 switches

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

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

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

- CI menus—From the main menu of the console, choose Systems Characteristics menu. The software currently running is displayed in sysDescr.

- Web-based management system—Open the System Information page, which is under Administration on the main menu. The software currently running is displayed in the sysDescription field.

You can use 256 port-, protocol-, and MAC SA-based VLANs for the stack with a Pure BPS 2000 stack running software version 2.5. (The maximum number available of MAC SA-based is 48). If you are working with a mixed, or hybrid, stack, you can use 64 VLANs for the entire stack. When you change from a Pure BPS 2000 Stack mode to a Hybrid Stack mode:

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

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

Setting up your mixed stack configuration

To set up a mixed stack configuration, follow the basic instructions regarding Business Policy Switch configuration detailed in Chapters 1 and 2, *Installing the Business Policy Switch 2000*, and *Installing the BayStack 400-ST1 Cascade Module*.

In the following sections you will find *specific* information about implementing a mixed stack configuration:

- "Configuration requirements," next
- "Automatic failover" on page 380
- "Troubleshooting problems" on page 386

Configuration requirements

The configuration requirements described here can help you to implement your mixed stack configuration.

Base unit

In a mixed stack configuration, a Business Policy Switch *must* be configured as the base unit (Unit Select switch set to On on the cascade module). All other units in the stack *must* have their Unit Select switch set to Off. The base unit switch is the unique stack switch that you configure with the Unit Select switch on the front panel of the BayStack 400-ST1 Cascade Module. If you do not designate a Business Policy Switch as the base unit, the stack will not operate.

Merging the Business Policy Switch into a mixed stack

Nortel Networks recommends that you start up your Business Policy Switch initially in a standalone mode and perform preliminary IP configuration tasks before you add it to an existing stack.

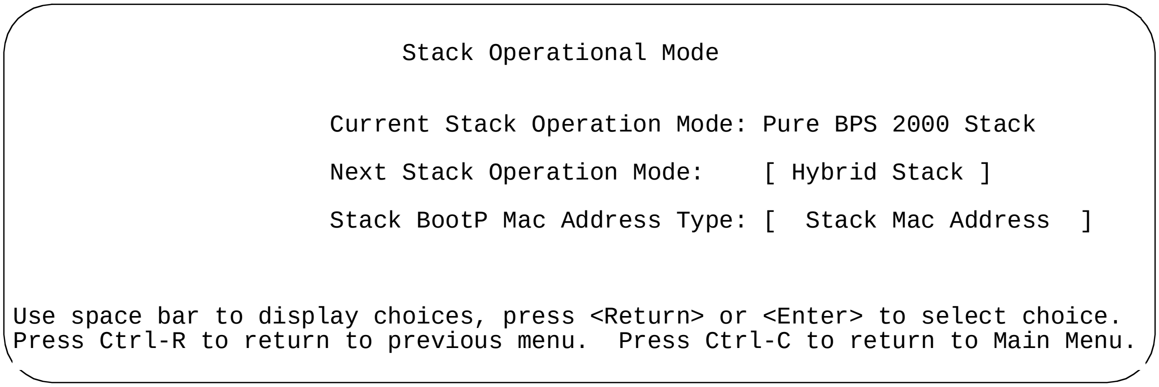
Note: When you add a new (factory direct) unconfigured Business Policy Switch 2000 to your stack, the Business Policy Switch acts as the dominant unit (base unit) and *overwrites* certain configuration settings. You cannot reset the switch to its previous configurations. To recover previous configurations, you must reconfigure parameters such as MLT, VLAN, and conversation steering.

To add a Business Policy Switch to your stack:

1. Change the new Business Policy Switch base unit setting on the BayStack 400-ST1 Cascade Module to Base.
2. Ensure that no other unit in the existing stack is selected as the base unit.
3. Power up the switch.
4. Change the Stack Operational Mode field on the Business Policy Switch to **`Hybrid Stack`** (Figure 140).
5. Perform configuration tasks for:
   - IP address
   - Subnet mask
   - Gateway address
6. Reset the switch to save your changes.

7 Add the newly configured Business Policy Switch to your existing stack.

Figure 140 Stack Operational Mode screen



```
                          Stack Operational Mode

                     Current Stack Operation Mode: Pure BPS 2000 Stack

                     Next Stack Operation Mode:    [ Hybrid Stack ]

                     Stack BootP Mac Address Type: [  Stack Mac Address  ]


Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Automatic failover

The automatic failover is a temporary safeguard only. If the stack loses power or is reset, 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 (assign another Business Policy Switch, if available) as the base unit (set the Unit Select switch to Base) until the failed unit is repaired or replaced. When a failure of the base unit is discovered, the Unit Select switch on the temporary base unit should be set to Base.

Note: If you do not reassign the temporary base unit as the new base unit, and 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.

For detailed information about temporary base units, see *Installing the BayStack 400-ST1 Cascade Module*.

Temporary base unit

In a mixed stack containing only one Business Policy Switch

If there is only one Business Policy Switch in your mixed stack configuration and it fails, the next upstream BayStack 410 *or* BayStack 450 switch from the failed base unit will become the temporary base unit and will continue stack operation. The base unit change is indicated by the base LED on the temporary base unit's LED display panel turning on (amber).

If the stack's base unit reverts to a BayStack 410 *or* BayStack 450 switch, the stack does not maintain Business Policy Switch features and will continue operation as a BayStack 410 or BayStack 450 stack.

In a mixed stack containing more than one Business Policy Switch

If the assigned Business Policy Switch base unit fails, the next *Business Policy Switch* unit in the stack order automatically becomes the new temporary base unit. All Business Policy Switch units in the stack will be exhausted as base units, successively, before assigning a BayStack 410 *or* BayStack 450 as base unit. The base unit change is indicated by the base LED on the temporary base unit's LED display panel turning on (amber).

If the stack's base unit reverts to a BayStack 410 *or* BayStack 450 switch, the stack does not maintain Business Policy Switch features and will continue operation as a BayStack 410 or BayStack 450 stack.

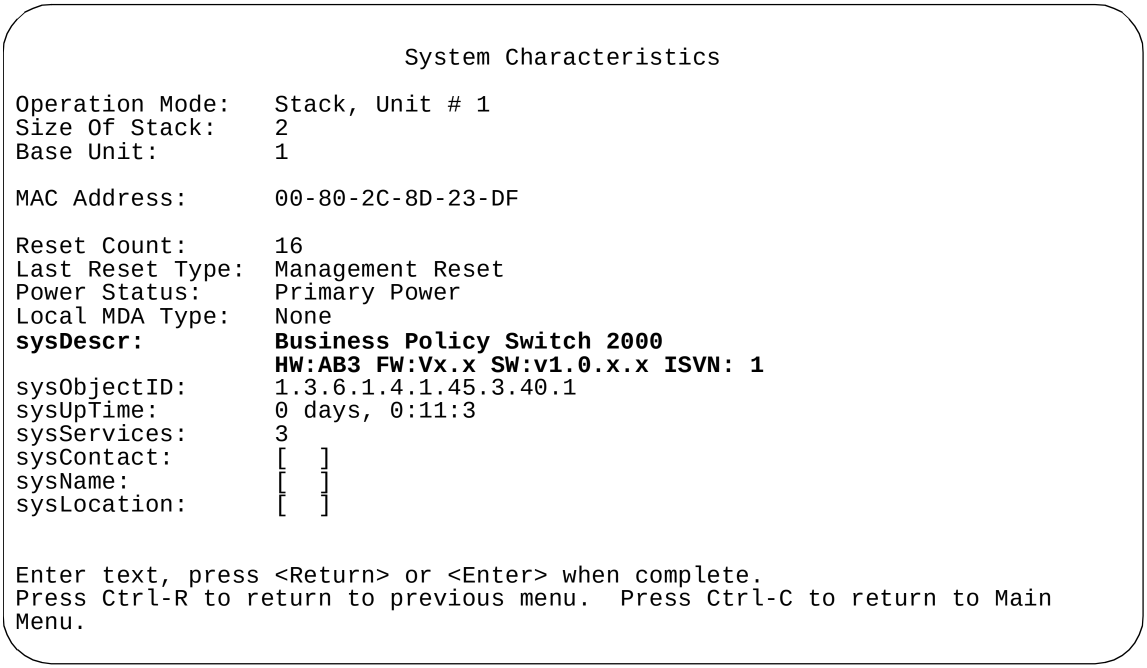
Compatible software versions

Be sure to follow the instructions for the initial setup according to the *Installing the Business Policy Switch 2000* guide.

In a mixed stack, the BayStack 450 and BayStack 410 switches must use compatible, but device specific, software versions to operate with the Business Policy Switch. You *must* ensure that the Interoperability Software Version Numbers (ISVN) are identical. That is, the ISVN number for the BayStack 450 switch and BayStack 410 switch must have the same ISVN as the Business Policy Switch. If they are not the same, the stack does not operate.

You can verify the software version and the ISVN in the sysDescr field (see Figure 141) in the System Characteristics screen.

Figure 141 System Characteristics screen



```
                              System Characteristics

Operation Mode:   Stack, Unit # 1
Size Of Stack:    2
Base Unit:        1

MAC Address:      00-80-2C-8D-23-DF

Reset Count:      16
Last Reset Type:  Management Reset
Power Status:     Primary Power
Local MDA Type:   None
sysDescr:         Business Policy Switch 2000
                  HW:AB3 FW:Vx.x SW:v1.0.x.x ISVN: 1
sysObjectID:      1.3.6.1.4.1.45.3.40.1
sysUpTime:        0 days, 0:11:3
sysServices:      3
sysContact:       [  ]
sysName:          [  ]
sysLocation:      [  ]


Enter text, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main
Menu.
```

Refer to “Software Download screen” on page 275 for software downloading information.

Using cascade modules

Installation instructions are provided with each BayStack 400-ST1 Cascade Module (see *Installing the BayStack 400-ST1 Cascade Module*). The BayStack 400-ST1 Cascade Module *does not operate* with BayStack 450 or BayStack 410 switches that are configured with BayStack 450 software versions *earlier than* version V1.1.0.

For information about using MDAs, refer to *Installing Media Dependent Adapters (MDA)s* and *Installing Gigabit Interface Converters and Small Form Factor Pluggable Interface Converters*.

Using the console interface

Console/Comm port

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.

For more information about the console/comm port, see Chapter 1.

Upgrading software in a mixed stack

Note: Use the Command Line Interface (CLI), console interface (CI) menus, or the Web-based management system to upgrade to software version 2.5. For detailed instructions, refer to Chapter 3, *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.5,* and *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.5*.

You use one of the management systems to upgrade or downgrade software.

The stacking software compatibility requirements are as follows in a mixed, or Hybrid, stack:

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

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

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

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

Upgrading software when ISVN is 2

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

1. Download the BPS 2000 image file.

   The system resets.

2. Download the BPS 2000 diags file.

   The system resets.

Note: Once you begin the upgrading process, do not interrupt the process at all. Interrupting the downloading (or upgrading) process may cause loss of connectivity.

Upgrading software when ISVN is 1

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

1 Download the BPS 2000 image file and the BayStack 450/410 file *simultaneously*.

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

The system resets.

2 Download the other BayStack 450 image file.

The system resets.

3 Download the BPS 2000 diags file.

The system resets.

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

Note: Once you begin the upgrading process, do not interrupt the process at all. Interrupting the downloading (or upgrading) process may cause loss of connectivity.

Joining stacks

You can join two stacks, whether entirely BPS 2000 units, or mixed units. You do not have to renumber the units in either stack.

To join two existing stacks:

1 Designate one stack as the one to join the other stack.

2 Reset the stack that will join the other stack to factory defaults.

3 Turn off the power to the all units in the stack that will join the other stack by unplugging the power cords from each unit.

a On the unit that was the Base Unit of this stack, use the Unit Select switch to deselect it as the Base Unit.

b Redo all the cabling so that all units will work as one stack.

4 Power-up the newly joined units by plugging in the power cords.

It may take a few minutes for the entire stack to display on the console. All units will show as their new numbers within the newly joined stack.

Troubleshooting problems

If you suspect problems with a newly installed mixed stack configuration, start troubleshooting by verifying the following items:

- A Business Policy Switch is designated as the base unit.
- All other units in the stack have the base unit select switch set to Off.
- The Business Policy Switch's operational mode is set to Hybrid Stack, and the unit has been reset after changing the operational mode (Figure 140).
- All units in the stack exhibit the same ISVN.
- All units must be reset when you add a Business Policy Switch to an existing BayStack 450 and 410 switch stack.
- All Business Policy Switches have the same software version. Similarly, all BayStack 450 and BayStack 410 switches are operating with updated and compatible software.
- When the stack is powered up, ensure that the Cas Up and Cas Dwn (cascade) and Base LEDs are green (steady, not blinking).

Appendix C
Quick steps to features

If you are a system administrator with experience configuring Business Policy Switch 2000 VLANs, MultiLink Trunking, Port Mirroring, IGMP Snooping, and EAPOL authentication processes, use the flowcharts on the following pages as quick configuration guides. The flowcharts refer you to the “configuration rules” appropriate for each feature.

The flowcharts cover the following features:

- 802.1Q VLANs (page 387)
- MultiLink Trunking (page 391)
- Port Mirroring (page 392)
- IGMP Snooping (page 393)
- EAPOL Authentication (page 396)

Configuring 802.1Q VLANs

To create or modify an 802.1Q VLAN, follow the flowcharts in Figure 142, Figure 143, and Figure 144.

To open the VLAN Configuration screen:

➨ Choose VLAN Configuration (or press v) from the VLAN Configuration Menu screen.

Figure 142 Configuring 802.1Q VLANs (1 of 3)

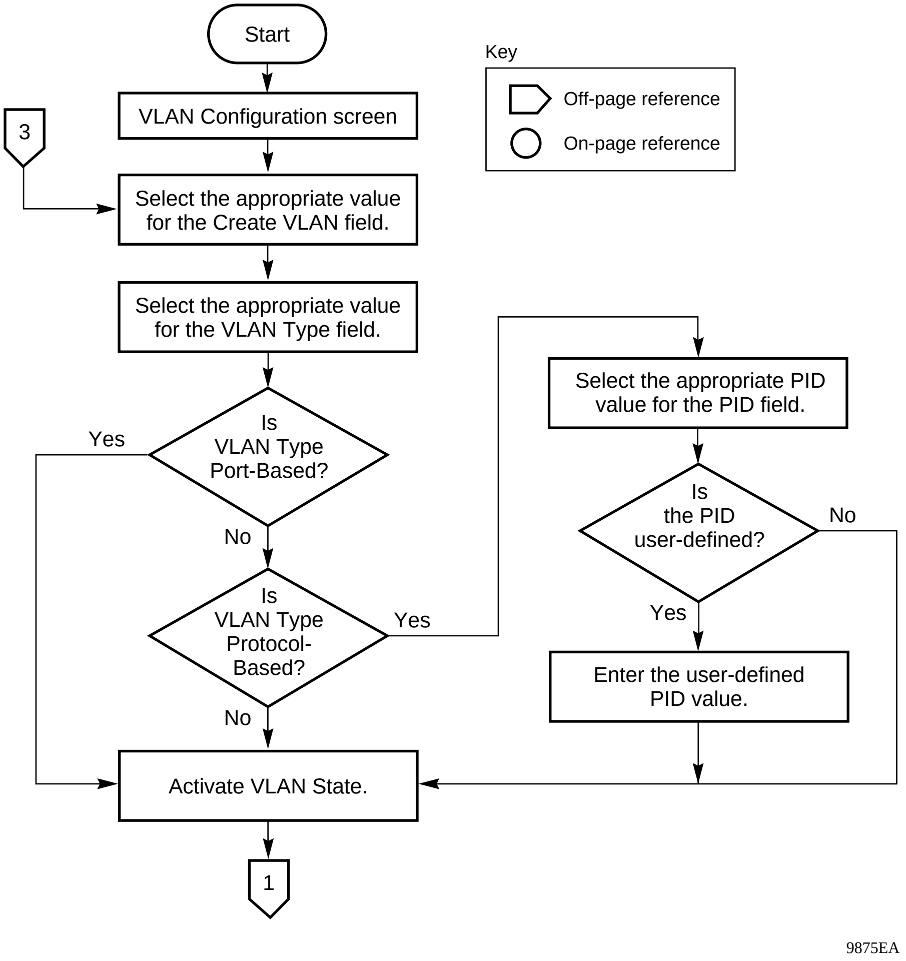

Start
VLAN Configuration screen
3
Select the appropriate value for the Create VLAN field.
Select the appropriate value for the VLAN Type field.
Is VLAN Type Port-Based?
Yes
No
Is VLAN Type Protocol-Based?
Yes
No
Select the appropriate PID value for the PID field.
Is the PID user-defined?
No
Yes
Enter the user-defined PID value.
Activate VLAN State.
1
Key
Off-page reference
On-page reference
9875EA

Figure 143 Configuring 802.1Q VLANs (2 of 3)

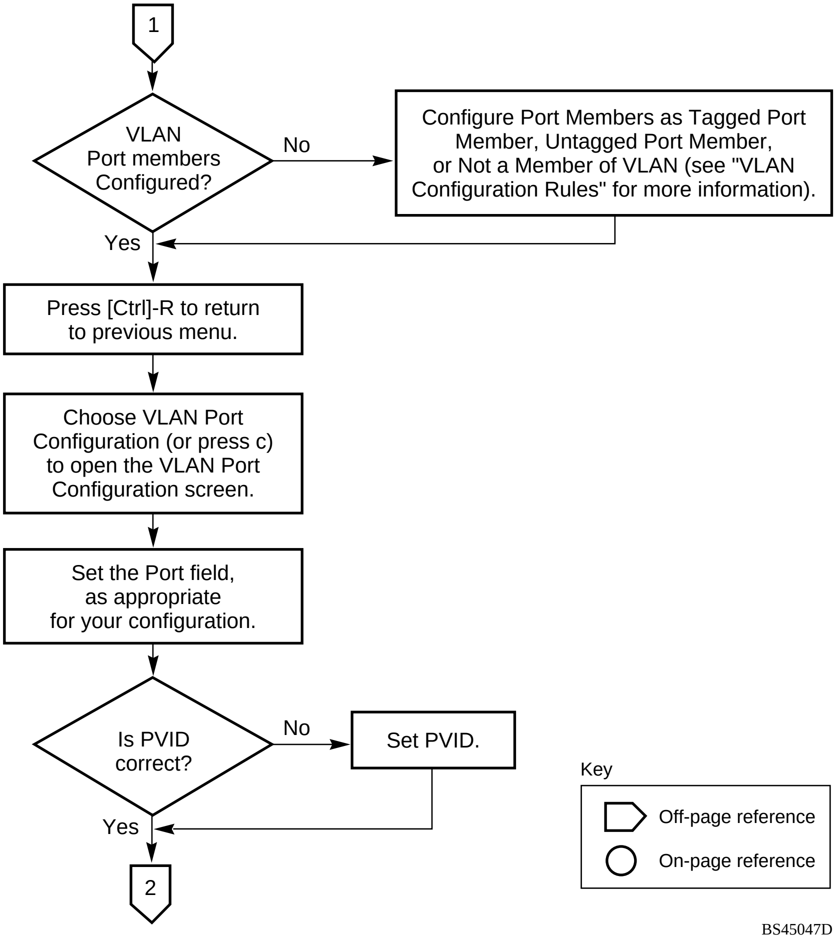
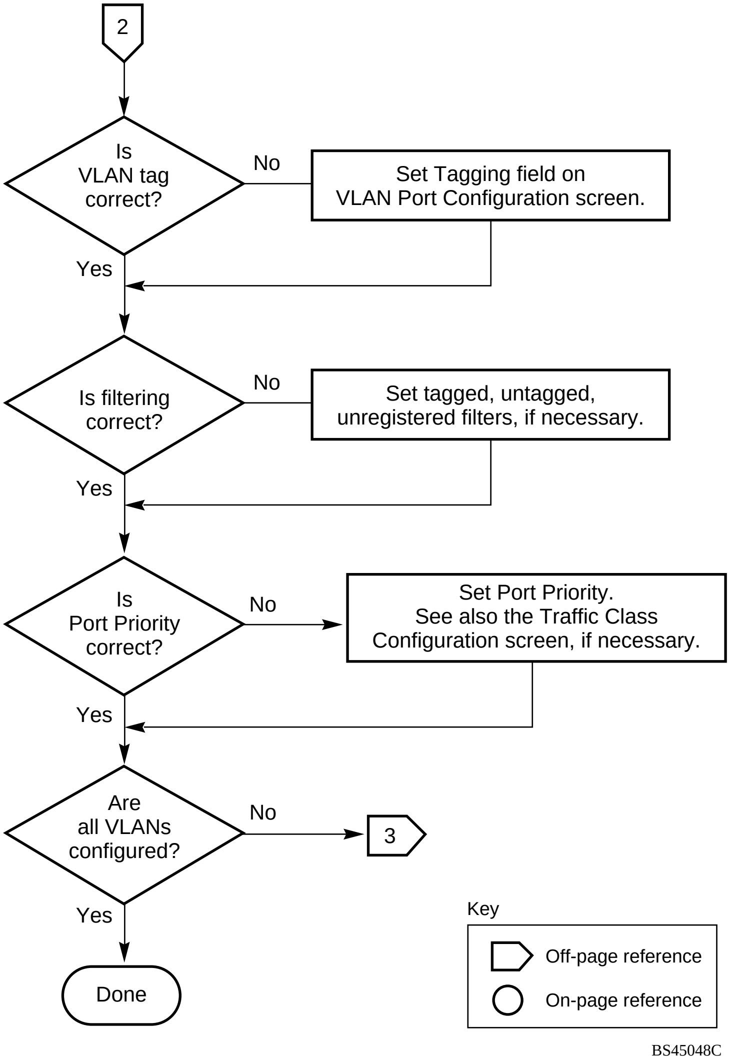

1
VLAN Port members Configured?
No
Configure Port Members as Tagged Port Member, Untagged Port Member, or Not a Member of VLAN (see "VLAN Configuration Rules" for more information).
Yes
Press [Ctrl]-R to return to previous menu.
Choose VLAN Port Configuration (or press c) to open the VLAN Port Configuration screen.
Set the Port field, as appropriate for your configuration.
Is PVID correct?
No
Set PVID.
Yes
2
Key
Off-page reference
On-page reference
BS45047D

Figure 144 Configuring 802.1Q VLANs (3 of 3)


2
Is VLAN tag correct?
No
Set Tagging field on VLAN Port Configuration screen.
Yes
Is filtering correct?
No
Set tagged, untagged, unregistered filters, if necessary.
Yes
Is Port Priority correct?
No
Set Port Priority. See also the Traffic Class Configuration screen, if necessary.
Yes
Are all VLANs configured?
No
3
Yes
Done
Key
Off-page reference
On-page reference
BS45048C

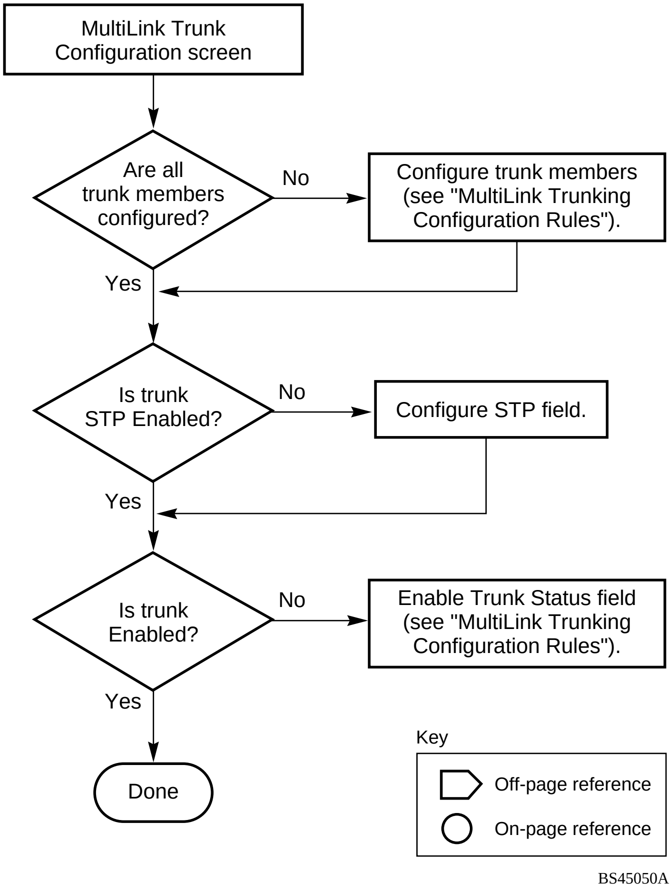
Configuring MultiLink Trunks

To create or modify a MultiLink Trunk, follow the flowchart in Figure 145.

To open the MultiLink Trunk Configuration screen:

➨ Choose MultiLink Trunk Configuration (or press t) from the MultiLink Trunk Configuration Menu screen

Figure 145 Configuring MultiLink Trunks


MultiLink Trunk Configuration screen
Are all trunk members configured?
No
Configure trunk members (see "MultiLink Trunking Configuration Rules").
Yes
Is trunk STP Enabled?
No
Configure STP field.
Yes
Is trunk Enabled?
No
Enable Trunk Status field (see "MultiLink Trunking Configuration Rules").
Yes
Done
Key
Off-page reference
On-page reference
BS45050A

Configuring Port Mirroring

To create or modify port-mirroring ports, follow the flowcharts in Figure 146 and Figure 147).

To open the Port Mirroring Configuration screen:

➨ Choose Port Mirroring Configuration (or press i) from the Switch Configuration Menu screen

Figure 146 Configuring Port Mirroring (1 of 2)

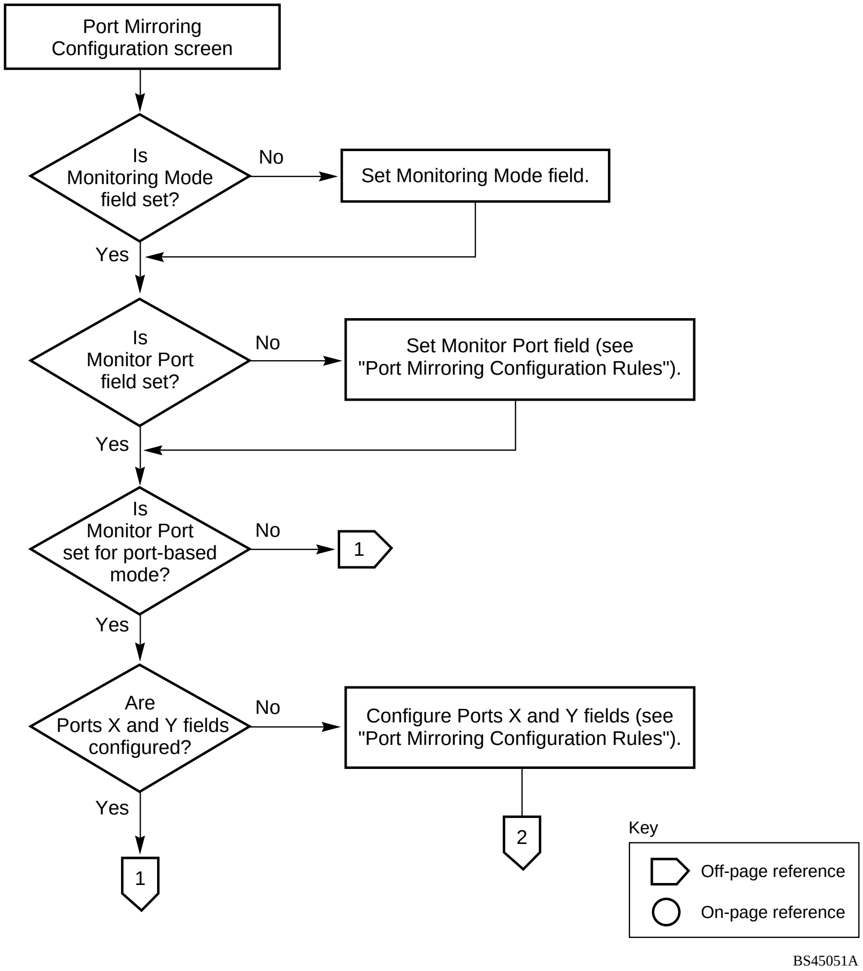
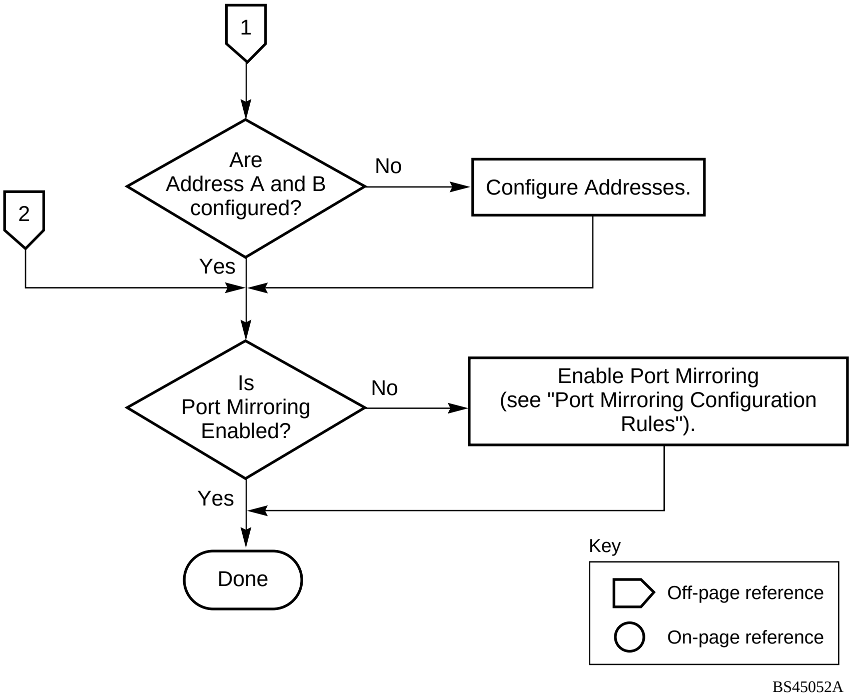

Port Mirroring Configuration screen
Is Monitoring Mode field set?
No
Set Monitoring Mode field.
Yes
Is Monitor Port field set?
No
Set Monitor Port field (see "Port Mirroring Configuration Rules").
Yes
Is Monitor Port set for port-based mode?
No
1
Yes
Are Ports X and Y fields configured?
No
Configure Ports X and Y fields (see "Port Mirroring Configuration Rules").
Yes
1
2
Key
Off-page reference
On-page reference
BS45051A

Figure 147 Configuring Port Mirroring (2 of 2)


1
Are Address A and B configured?
No
Configure Addresses.
2
Yes
Is Port Mirroring Enabled?
No
Enable Port Mirroring (see "Port Mirroring Configuration Rules").
Yes
Done
Key
Off-page reference
On-page reference
BS45052A

Configuring IGMP Snooping

To create or modify IGMP Snooping ports, follow the flowcharts in Figures Figure 148 to Figure 150.

To open the IGMP Configuration screen:

➨ Choose IGMP Configuration (or press g) from the Switch Configuration Menu screen.

Figure 148 Configuring IGMP Snooping (1 of 3)

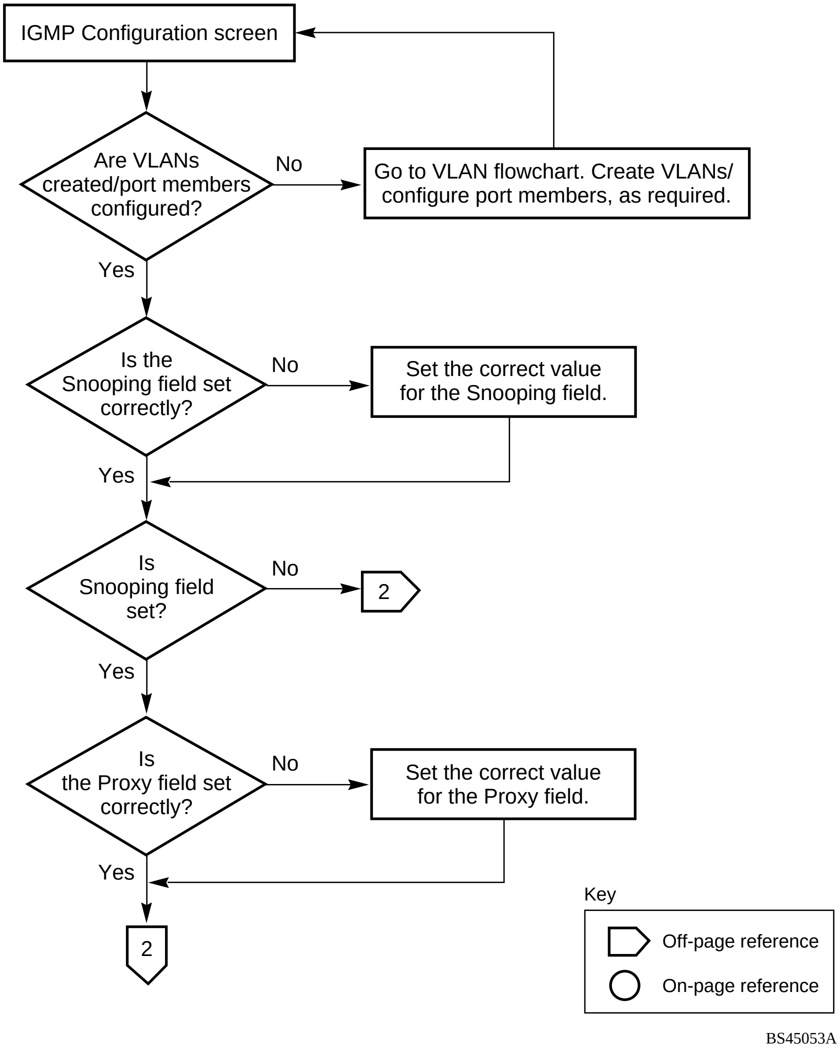

IGMP Configuration screen
Are VLANs created/port members configured?
No
Go to VLAN flowchart. Create VLANs/ configure port members, as required.
Yes
Is the Snooping field set correctly?
No
Set the correct value for the Snooping field.
Yes
Is Snooping field set?
No
2
Yes
Is the Proxy field set correctly?
No
Set the correct value for the Proxy field.
Yes
2
Key
Off-page reference
On-page reference
BS45053A

Figure 149 Configuring IGMP Snooping (2 of 3)

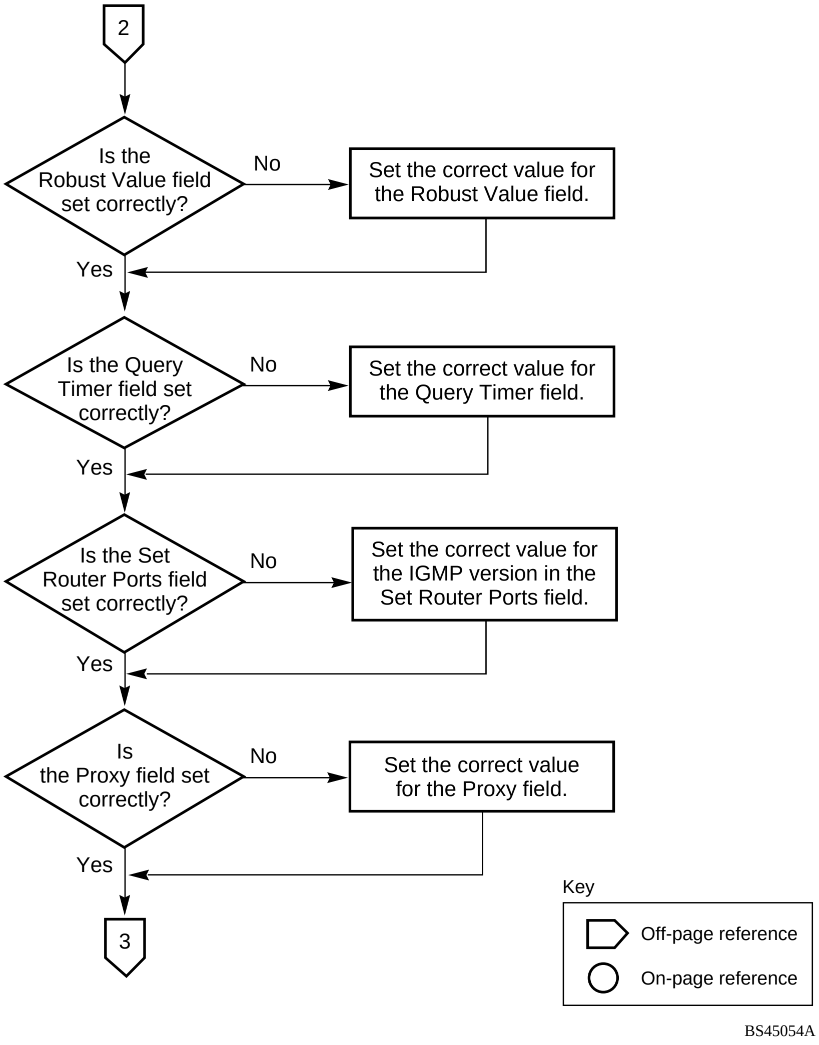
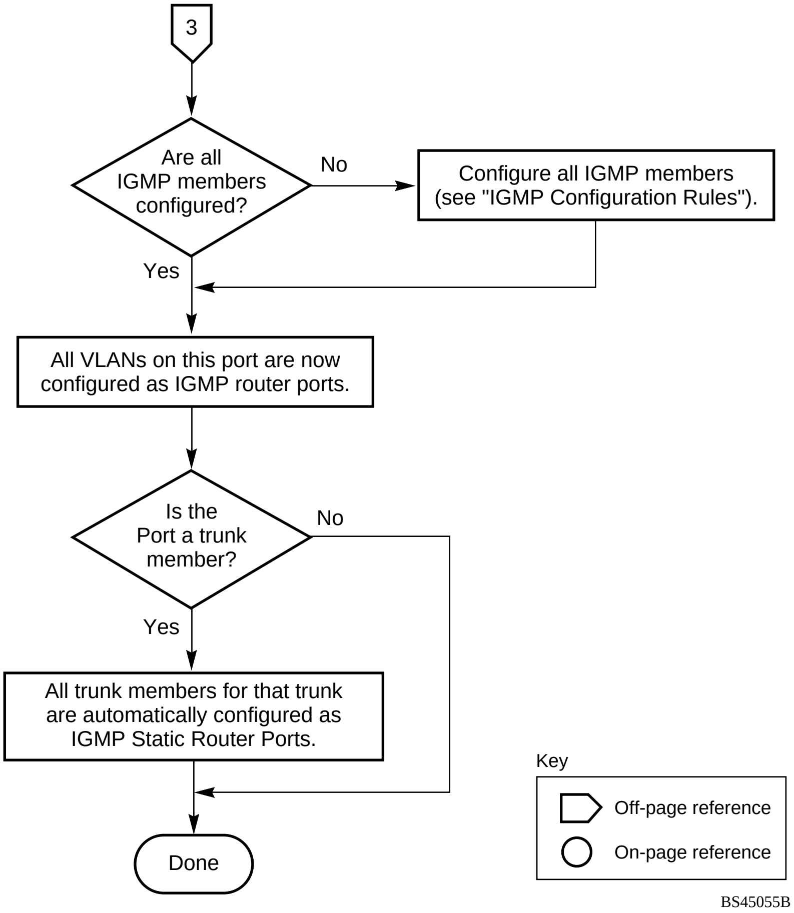

2
Is the Robust Value field set correctly?
No
Set the correct value for the Robust Value field.
Yes
Is the Query Timer field set correctly?
No
Set the correct value for the Query Timer field.
Yes
Is the Set Router Ports field set correctly?
No
Set the correct value for the IGMP version in the Set Router Ports field.
Yes
Is the Proxy field set correctly?
No
Set the correct value for the Proxy field.
Yes
3
Key
Off-page reference
On-page reference
BS45054A

Figure 150 Configuring IGMP Snooping (3 of 3)


3
Are all IGMP members configured?
No
Configure all IGMP members (see "IGMP Configuration Rules").
Yes
All VLANs on this port are now configured as IGMP router ports.
Is the Port a trunk member?
No
Yes
All trunk members for that trunk are automatically configured as IGMP Static Router Ports.
Done
Key
Off-page reference
On-page reference
BS45055B

Configuring authentication process for EAPOL-based security

To create or modify EAPOL-based security parameters, follow the flowcharts in Figure 151 and Figure 152.

To open the EAPOL Security Configuration screen:

➨ Choose EAPOL Security Configuration from the Switch Configuration Menu screen.

Figure 151 Authenticaton process flowchart (1 of 2)

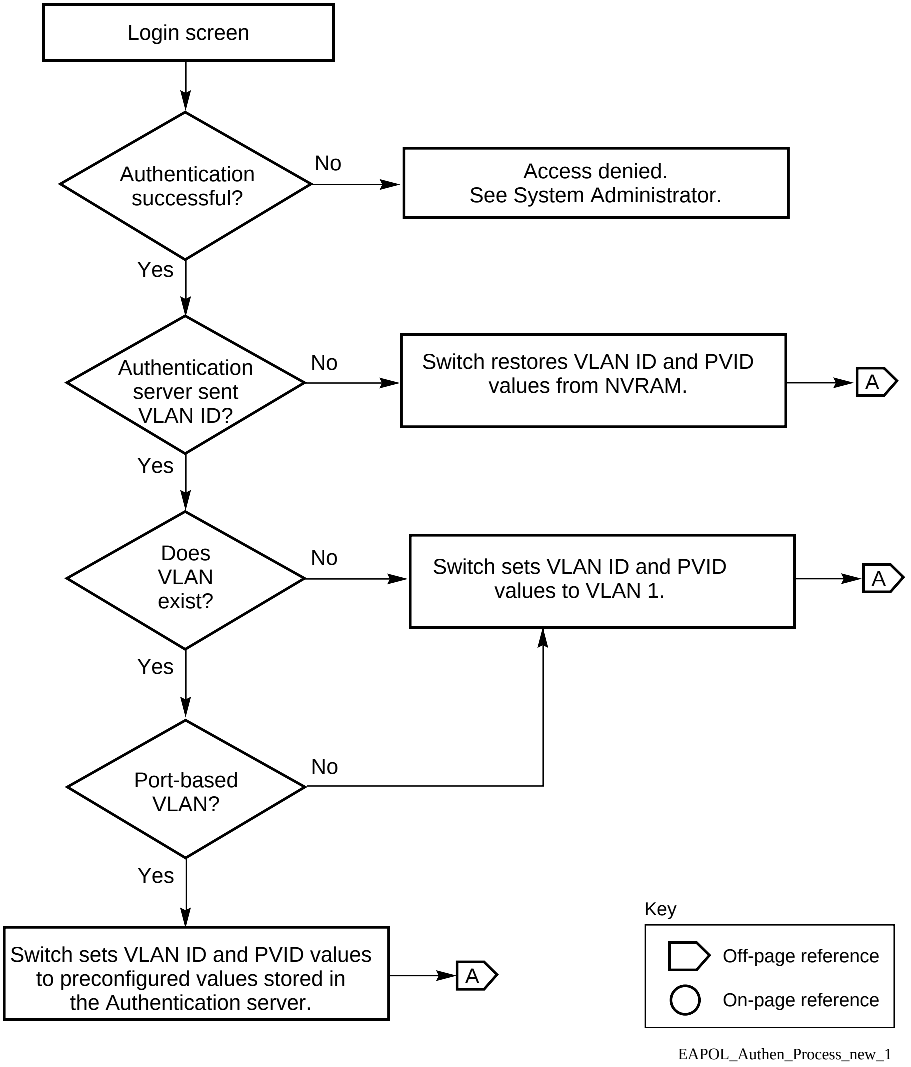
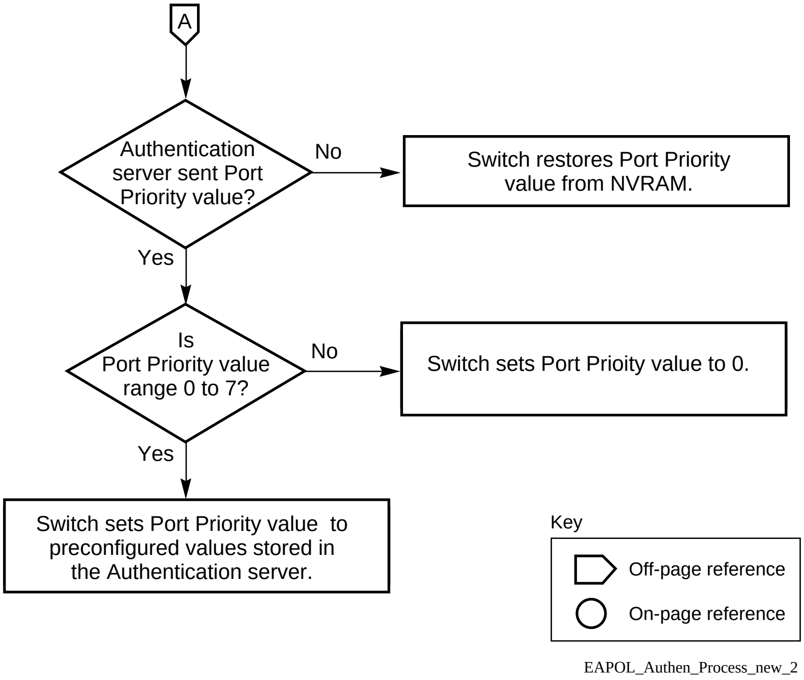

Login screen
Authentication successful?
No
Access denied.
See System Administrator.
Yes
Authentication server sent VLAN ID?
No
Switch restores VLAN ID and PVID values from NVRAM.
A
Yes
Does VLAN exist?
No
Switch sets VLAN ID and PVID values to VLAN 1.
A
Yes
Port-based VLAN?
No
Yes
Switch sets VLAN ID and PVID values to preconfigured values stored in the Authentication server.
A
Key
Off-page reference
On-page reference
EAPOL_Authen_Process_new_1

Figure 152 Authenticaton process flowchart (2 of 2)


A
Authentication server sent Port Priority value?
No
Switch restores Port Priority value from NVRAM.
Yes
Is Port Priority value range 0 to 7?
No
Switch sets Port Prioity value to 0.
Yes
Switch sets Port Priority value to preconfigured values stored in the Authentication server.
Key
Off-page reference
On-page reference
EAPOL_Authen_Process_new_2

Appendix D
Connectors and pin assignments

This appendix describes the Business Policy Switch 2000 port connectors and pin assignments.

RJ-45 (10BASE-T/100BASE-TX) port connectors

The RJ-45 port connectors (Figure 153) are wired as MDI-X ports to connect end stations without using crossover cables. (See “MDI and MDI-X devices” on page 400 for information about MDI-X ports.) For 10BASE-T connections, use Category 3 (or higher) UTP cable. For 100BASE-TX connections, use only Category 5 UTP cable.

Figure 153 RJ-45 (8-Pin Modular) port connector

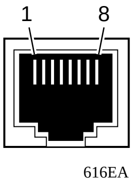


Table 68 lists the RJ-45 (8-pin modular) port connector pin assignments.

Table 68 RJ-45 port connector pin assignments

Pin	Signal	Description
1	RX+	Receive Data +
2	RX-	Receive Data -
3	TX+	Transmit Data +
4	Not applicable	Not applicable
5	Not applicable	Not applicable
6	TX-	Transmit Data -
7	Not applicable	Not applicable
8	Not applicable	Not applicable

MDI and MDI-X devices

Media dependent interface (MDI) is the IEEE standard for the interface to unshielded twisted pair (UTP) cable.

For two devices to communicate, the transmitter of one device must connect to the receiver of the other device. The connection is established through a crossover function, which can be a crossover cable or a port that implements the crossover function internally.

Ports that implement the crossover function internally are known as MDI-X ports, where X refers to the crossover function.

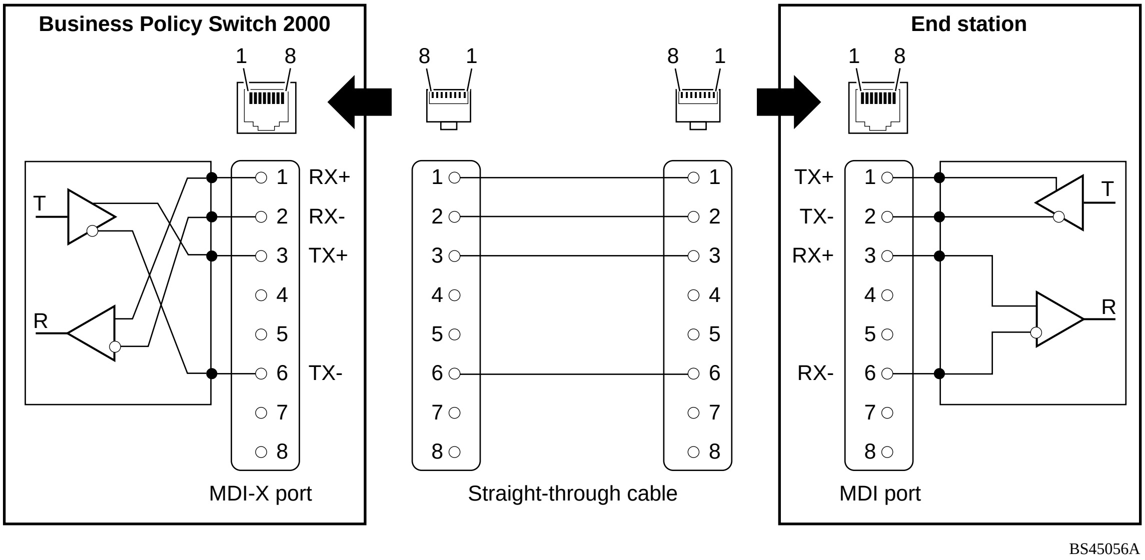
➡ **Note:** For the transmitter of one device to connect to the receiver of another device, the total number of crossovers must always be an odd number.

The following sections describe the use of straight-through and crossover cables for connecting MDI and MDI-X devices.

MDI-X to MDI cable connections

Business Policy Switch switches use MDI-X ports that allow you to connect directly to end stations without using crossover cables (Figure 154).

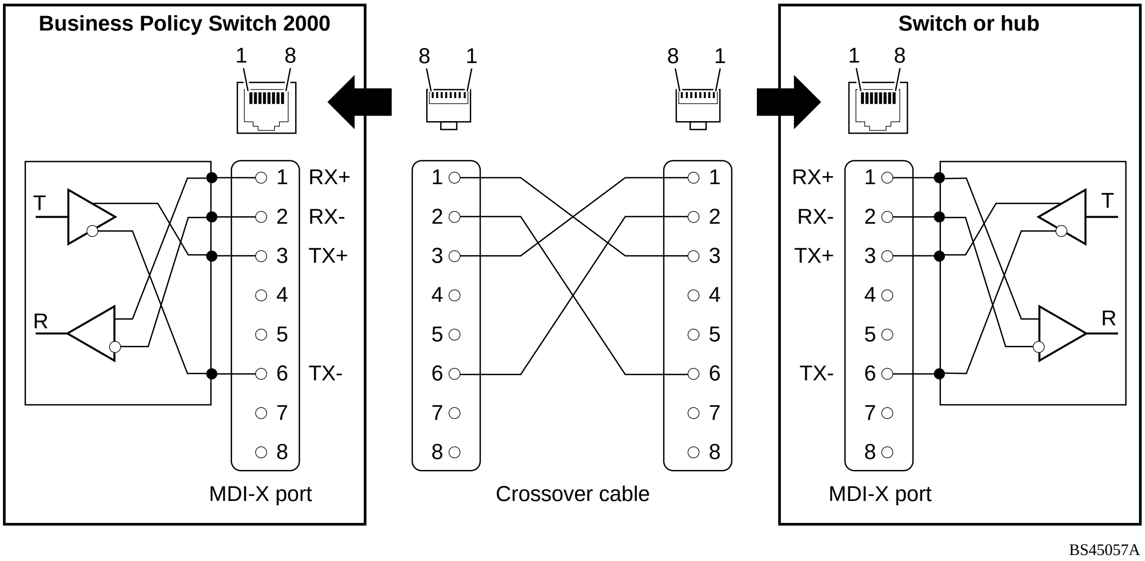
Figure 154 MDI-X to MDI cable connections



MDI-X to MDI-X cable connections

If you are connecting the Business Policy Switch to a device that also implements MDI-X ports, use a crossover cable (Figure 155).

Figure 155 MDI-X to MDI-X cable connections



DB-9 (RS-232-D) Console/Comm Port connector

The DB-9 Console/Comm Port connector (Figure 156) is configured as a data communications equipment (DCE) connector. The DSR and CTS signal outputs are always asserted; the CD, DTR, RTS, and RI signal inputs are not used. This configuration enables a management station (a PC or console terminal) to connect directly to the switch using a straight-through cable.

Figure 156 DB-9 Console port connector

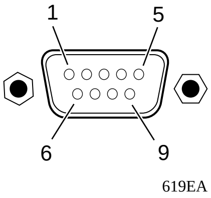


Table 69 lists the DB-9 Console connector pin assignments.

Table 69 DB-9 Console port connector pin assignments

Pin	Signal	Description
1	CD	Carrier detect (not used)
2	TXD	Transmit data (output)
3	RXD	Receive data (input)
4	DTR	Data terminal ready (not used)
5	GND	Signal ground
6	DSR	Not used
7	RTS	Request to send (not used)
8	CTS	Not used
9	RI	Ring indicator (not used)
Shell		Chassis ground

Appendix E
Default Settings

Table 70 lists the factory default settings for the Business Policy Switch 2000 according to the console interface (CI) screens and fields for the settings.

Table 70 Factory default settings

Field	Default setting	Appears in this CI screen
Unit	1	"IP Configuration/Setup screen" on page 172
BootP Request Mode	BootP Disabled	
In-Band Stack IP Address	0.0.0.0 (no IP address assigned)	
In-Band Switch IP Address	0.0.0.0 (no IP address assigned)	
In-Band Subnet Mask	0.0.0.0 (no subnet mask assigned)	
Default Gateway	0.0.0.0 (no IP address assigned)	
Read-Only Community String	public	"SNMP Configuration screen" on page 177
Read-Write Community String	private	
Trap IP Address	0.0.0.0 (no IP address assigned)	
Community String	Zero-length string	
Authentication Trap	Enabled	
Link Up/Down Trap	Enabled	
sysContact	Zero-length string	"System Characteristics screen" on page 179
sysName	Zero-length string	
sysLocation	Zero-length string	

Table 70 Factory default settings (continued)

Field	Default setting	Appears in this CI screen
Aging Time	300 seconds	"MAC Address Table screen" on page 184
Find an Address	00-00-00-00-00-00 (no MAC address assigned)	
Port Mirroring Address A:	00-00-00-00-00-00 (no MAC address assigned)	
Port Mirroring Address B:	00-00-00-00-00-00 (no MAC address assigned)	
MAC Address Security	Disabled	"MAC Address Security Configuration Menu screen" on page 186
MAC Address Security SNMP-Locked	Disabled	
Partition Port on Intrusion Detected:	Disabled	
Partition Time	0 seconds (the value 0 indicates forever)	
DA Filtering on Intrusion Detected:	Disabled	
Generate SNMP Trap on Intrusion	Disabled	
Clear by Ports	NONE	
Learn by Ports	NONE	
Current Learning Mode	Not Learning	
Trunk	blank field	"MAC Address Security Port Configuration screen" on page 191
Security	Disabled	
Port List	blank field	"MAC Address Security Port Lists screens" on page 194
Find an Address	blank field	"MAC Address Security Table screens" on page 199
MAC Address	- - - - - - (no address assigned)	
Allowed Source	- (blank field)	
MAC-SA based VLAN	The least active MAC-SA based VLAN will be displayed.	"MAC Address Configuration for MAC-SA-Based VLAN screen" on page 214
Display/Create MAC Address	00-00-00-00-00-00	

Table 70 Factory default settings (continued)

Field	Default setting	Appears in this CI screen
Create VLAN	1	"VLAN Configuration screen" on page 207
Delete VLAN	blank field	
VLAN Name	VLAN # (*VLAN number*)	
Management VLAN	Yes, VLAN #1	
IVL/SVL	IVL	
VLAN Type	Port-based	
Protocol ID (PID)	None	
User-Defined PID	0x0000	
VLAN State	Inactive	
Subnet Addr	0.0.0.0.	
Subnet Mask	0.0.0.0.	
Port Membership	U (all ports assigned as untagged members of VLAN 1)	
Unit	1	"VLAN Port Configuration screen" on page 215
Port	1	
Filter Tagged Frames	No	
Filter Untagged Frames	No	
Filter Unregistered Frames	No	
Port Name	Unit 1, Port 1	
PVID	1	
Port Priority	0	
Tagging	Untagged Access	
AutoPVID	Disabled	
BootP Mac Address Type	Stack Mac Address	"Stack Operational Mode screen" on page 248

Table 70 Factory default settings (continued)

Field	**Default setting**	**Appears in this CI screen**
Unit	1	"VLAN Display by Port screen" on page 218
Port	1	
PVID	1 (read only)	
Port Name	Unit 1, Port 1 (read only)	
Unit	1	"Port Configuration screen" on page 219
Status	Enabled (for all ports)	
Autonegotiation	Enabled (for all ports)	
Speed/Duplex	100Mbs/Half (when Autonegotiation is Disabled)	
Trunk	1 to 6 (depending on configuration status)	"MultiLink Trunk Configuration Menu screen" on page 225
Trunk Members (Unit/Port)	Blank field	
STP Learning	Normal	
Trunk Mode	Basic	
Trunk Status	Disabled	
Trunk Name	Trunk #1 to Trunk #6	
Traffic Type	Rx and Tx	"MultiLink Trunk Utilization screen" on page 229

Table 70 Factory default settings (continued)

Field	Default setting	Appears in this CI screen
Monitoring Mode	Disabled	"Port Mirroring Configuration screen" on page 231
Monitor/Unit Port	Zero-length string	
Unit/Port X	Zero-length string	
Unit/Port Y	Zero-length string	
Address A	00-00-00-00-00-00 (no MAC address assigned)	
Address B	00-00-00-00-00-00 (no MAC address assigned)	
Packet Type	Both	"Rate Limiting Configuration screen" on page 234
Limit	None	
VLAN	1	"IGMP Configuration screen" on page 239
Snooping	Enabled	
Proxy	Enabled	
Robust Value	2	
Query Time	125 seconds	
Set Router Ports	Version 1	
Static Router Ports	- (for all ports)	
Unit	1	"Port Statistics screen" on page 244
Port	1	
Console Port Speed	9600 Baud	"Console/Comm Port Configuration screen" on page 249
Console Switch Password	Not Required	
Console Stack Password	Not Required	
Console Read-Only Switch Password	user	
Console Read-Write Switch Password	secure	
Console Read-Only Stack Password	user	
Console Read-Write Stack Password	secure	

Table 70 Factory default settings (continued)

Field	Default setting	Appears in this CI screen
Note: The following two fields only appear when the switch is a participant in a stack configuration.		
New Unit Number	Current stack order	"Renumber Stack Units screen" on page 256
Renumber units with new setting?	No	
Group	1	"Spanning Tree Group Configuration screen" on page 260
Bridge Priority	8000	
Bridge Hello Time	2 seconds	
Bridge Maximum Age Time	20 seconds	
Bridge Forward Delay	15 seconds	
Add VLAN Membership	1	
Tagged BPDU on tagged port	• STP Group 1—No • Other STP Groups—Yes	
STP Group State	• STP Group 1—Active • Other STP Groups—InActive	
VID used for tagged BPDU	4001-4008 for STGs 1-8, respectively	
STP Group	1	"Spanning Tree Port Configuration screen" on page 263
Participation	Normal Learning	
Priority	128	
Path Cost	10 or 100	
STP Group	1	"Spanning Tree Switch Settings screen" on page 266
STP Group	1	"Spanning Tree VLAN Membership screen" on page 270
TELNET Access	Enabled	"TELNET/SNMP/Web Access Configuration screen" on page 272
Login Timeout	1 minute	
Login Retries	3	
Inactivity Timeout	15 minutes	

Table 70 Factory default settings (continued)

Field	Default setting	Appears in this CI screen
Event Logging	All	
Allowed Source IP Address (10 user-configurable fields)	First field: 0.0.0.0 (no IP address assigned)	
	Remaining nine fields: 255.255.255.255 (any address is allowed)	

Table 70 Factory default settings (continued)

Field	Default setting	Appears in this CI screen
Allowed Source Mask (10 user-configurable fields)	First field: 0.0.0.0 (no IP address assigned)	
	Remaining nine fields: 255.255.255.255 (any address is allowed)	
Image Filename	Zero-length string	"Software Download screen" on page 275
TFTP Server IP Address	0.0.0.0 (no IP address assigned)	
Start TFTP Load of New Image	No	
Configuration Image Filename	Zero-length string	"Configuration File Download/Upload screen" on page 285
TFTP Server IP Address	0.0.0.0 (no IP address assigned)	
Copy Configuration Image to Server	No	
Retrieve Configuration Image from Server	No	
ASCII Configuration Filename	Zero-length string	"ASCII Configuration File Download screen" on page 289
TFTP Server IP Address	0.0.0.0 (no IP address assigned)	
Retrieve Configuration file from Server	No	
Last Manual Configuration Status	Passed	
Last Auto Configuration Status	Passed	
Auto Configuration on Reset	Disabled	

Appendix F
Sample BootP Configuration File

This appendix provides a sample BootP configuration file. The BootP server searches for this file, called bootptab (or BOOTPTAB.TXT, depending on your operating system), which contains the site-specific information (including IP addresses) needed to perform the software download and configuration. You can modify this sample BootP configuration file or create one of your own.

A sample BootP configuration file follows:

```
# The following is a sample of a BootP configuration file that was extracted
# from a Nortel Networks EZ LAN network management application.  Note that
other BootP daemons can use a configuration file with a different format.
#
# Before using your switch BootP facility, you must customize your BootP
# configuration file with the appropriate data.
#
# Blank lines and lines beginning with ’#’ are ignored.
#
# Legend:
#
#       first field -- hostname
#                ht -- hardware type
#                ha -- host hardware address
#                tc -- template host (points to similar host entry)
#                ip -- host IP address
#                hd -- bootfile home directory
#                bf -- bootfile
# EZ             dt -- device type
# EZ             fv -- firmware version
# EZ             av -- agent version
#                cs – TFTP server address for ASCII config file (optional)
#
# Fields are separated with a pipe (|) symbol. Forward slashes (/) are
# required to indicate that an entry is continued to the next line.
#
```

```
# Caution
#
#     Omitting a Forward slash (/) when the entry is continued to the next
#     line, can cause the interruption of the booting process or the
#     incorrect image file to download.  Always include forward slashes
#     where needed.
#
# Important Note:
#
#     If a leading zero (0) is used in the IP address it is calculated as an
#     octal number.  If the leading character is "x" (upper or lower case),
#     it is calculated as a hexadecimal number. For example, if an IP address
#     with a base 10 number of 45 is written as .045 in the BOOTPTAB.TXT file,
#     the Bootp protocol assigns .037 to the client.
#
# Global entries are defined that specify the parameters used by every device.
# Note that hardware type (ht) is specified first in the global entry.
#
# The following global entry is defined for an Ethernet device. Note that this
# is where a client’s subnet mask (sm) and default gateway (gw) are defined.
#
global1|/
      |ht=ethernet|/
      |hd=c:\opt\images|/
      |sm=255.255.255.0|/
      |gw=192.0.1.0|
#
# The following sample entry describes a BootP client:

bay1|ht=ethernet|ha=0060fd000000|ip=192.0.0.1|hd=c:\ezlan\images|bf=bps2000.txt

# Where:
#    host name:                    bay1
#    hardware type:                Ethernet
#    MAC address:                  00-60-FD-00-00-00
#    IP address:                   192.0.0.0
#    home directory of boot file:  c:\ezlan\images
#    ASCII config file:            bps2000.txt
# When ASCII configuration download is configured to perform auto configuration
# on reset using BootP, the filename must be specified using the ‘bf’ keyword.
# If the ASCII configuration file is not resident on the BootP server, the
# server address can be specified using the ‘cs’ keyword.
```

Index