Part No. 212859-A
September 2002

4655 Great America Parkway
Santa Clara, CA 95054

Using the BayStack 380 10/100/1000 Switch

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 Inc.

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, and BayStack 380 are trademarks of Nortel Networks.

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

SPARC is a trademark of Sparc International, Inc.

Sun and Solaris are trademarks of Sun Microsystems, Inc.

HP is a trademark of Hewlett-Packard Corporation.

UNIX is a trademark of X/Open Company Limited.

IBM and AIX are trademarks of International Business Machines Corporation (IBM).

Netscape Navigator is a trademark of Netscape Communications Corporation.

Ethernet is a trademark of Xerox Corporation.

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.

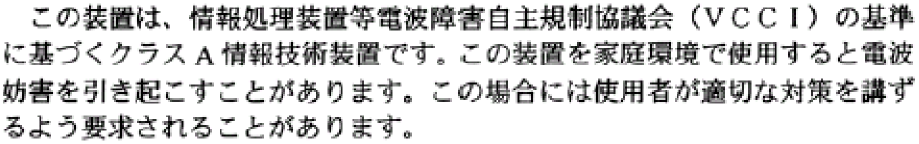
Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such 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).

Japan/Nippon Requirements Only

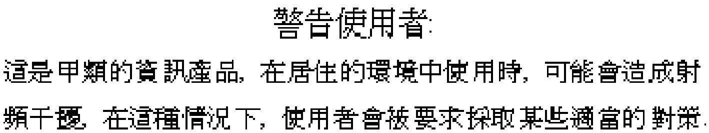
Voluntary Control Council for Interference (VCCI) Statement



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, 可能會造成射頻千擾, 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 (Baystack 380 Switch) 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 (Baystack 380 Switch) 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

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

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

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

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee’s intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee’s requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor’s product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

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

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

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

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

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

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

Should you have any questions concerning this Agreement, contact Nortel Networks Inc., 2375 N. Glenville Dr., Richardson, TX 75082.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Chapter 4

Appendix A

Appendix B

Figures

Tables

Preface

This guide describes the Nortel Networks* BayStack* 380 10/100/1000 Switch features and uses. The terms “BayStack 380 10/100/1000 Switch” and “BayStack 380 Switch” are both used in this document.

Before you begin

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

- Basic knowledge of networks, Ethernet* bridging, and IP
- 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

Text conventions

This guide uses the following text conventions:

angle brackets (< >)

Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command.

Example: If the command syntax is:

`ping` <*`ip_address`*>, you enter:

`ping 192.32.10.12`

`bold text`

Indicates command names and options and text that you need to enter.

Example: Enter **`show ip`** {**`alerts`** | **`routes`**}.

Example: Use the **`dinfo`** command.

braces ({})

Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command.

Example: If the command syntax is:

`show ip {alerts | routes}`, you must enter either:

`show ip alerts or show ip routes`, but not both.

brackets ([ ])

Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.

Example: If the command syntax is:

`show ip interfaces` [**`-alerts`**], you can enter either:

`show ip interfaces or show ip interfaces -alerts`.

ellipsis points (. . .)

Indicate that you repeat the last element of the command as needed.

Example: If the command syntax is:

`ethernet/2/1` [*<parameter> <value>*] `. . .` , you enter

`ethernet/2/1` and as many parameter-value pairs as needed.

italic text

Indicates file and directory names, new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore.

Example: If the command syntax is:

`show at` *<valid_route>*

valid_route is one variable and you substitute one value for it.

`screen text`

Indicates system output, for example, prompts and system messages.

Example: `Set Trap Monitor Filters`

separator (>)

Shows menu paths.

Example: Protocols > IP identifies the IP option on the Protocols menu.

vertical line (|)

Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command.

Example: If the command syntax is:

`show ip` {**`alerts`** | **`routes`**}, you enter either:

`show ip alerts` or **`show ip routes`**, but not both.

Related publications

For more information about using the BayStack 380 Switch, refer to the following publications:

- *Using the BayStack 380 10/100/1000 Switch* (part number 212859-A)

  Describes how to use the BayStack 380 10/100/1000 Switch for network configuration.

- *Using Web-Based Management for the BayStack 380 10/100/1000 Switch* (part number 212863-A)

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

- *Installing the BayStack 380 10/100/1000 Switch* (part number 212860-A)

  Describes how to install the BayStack 380 Switch.

- *Release Notes for the BayStack 380 10/100/1000 Switch* (part number 212864-A)

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

- *Getting Started with the BayStack 380 Management Software* (part number 212861-A)

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

- *Reference for the BayStack 380 Management Software* (part number 212862)

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

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

You can purchase printed books and documentation sets from Vervante. To order printed documentation, go to Vervante at the www.vervante.com/nortel URL.

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

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the www12.nortelnetworks.com/ URL and click ERC at the bottom of the page.

Chapter 1
BayStack 380 Switch

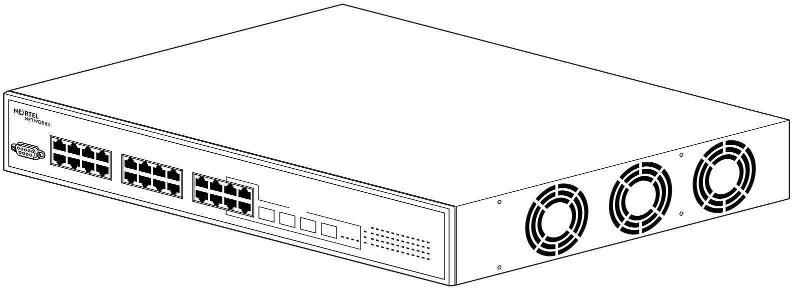
This chapter introduces the BayStack 380 Switch and covers the following topics:

- "Physical description," next
- "Features" on page 36

Physical description

Figure 1 depicts the front and side views of the BayStack 380 Switch.

Figure 1 BayStack 380 Switch



Front panel

Figure 2 shows the configuration of the front panel on the BayStack 380 Switch. Table 1 describes the components on the front panel.

For descriptions of the back panel BayStack 380 Switch components, see “Back panel” on page 32.

Figure 2 BayStack 380 Switch front panel

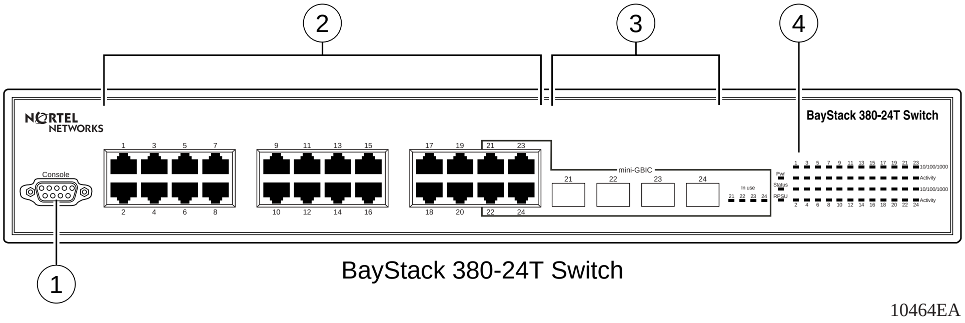


Table 1 Components on the BayStack 380 Switch front panel

Item	Description
1	Console port
2	10/100/1000BASE-TX RJ-45 Port connectors
3	Small Form Factor Pluggable (SFP) Gigabit Interface Converter (mini-GBIC)
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, “Using the console interface,” on page 93).

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 BayStack 380 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 BayStack 380 10/100/1000 Switch* 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 Appendix D, "Connectors and pin assignments," on page 201).

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 enabled.

Small Form Factor Pluggable (SFP) Gigabit Interface Converter

Small Form Factor Pluggable Gigabit Interface Converters are hot-swappable input/output enhancement components designed for use with Nortel Networks products to allow Gigabit Ethernet ports to link with Short Wavelength (SX), Long Wave length (LX), and Coarse Wavelength Division Multiplexed (CWDM) fiber optic networks.

Port connectors

The BayStack 380 Switch uses 10/100/1000BASE-TX RJ-45 (8-pin modular) port connectors.

The 10/100/1000BASE-TX port connectors feature auto-MDI-X (media-dependent interface-crossover). These ports connect over straight-through cables to the network interface card (NIC) in a node or server, similar to a conventional Ethernet repeater hub. However, with this feature and auto-negotiation enabled, you can still use straight-through cables while connecting to an Ethernet hub or switch.

For details on pin assignments and for directions on how to make your own cross-over cables, see "Appendix D, "Connectors and pin assignments," on page 201).

The BayStack 380 Switch uses autosensing ports designed to operate at 10 Mb/s (megabits per second), 100 Mb/s, OR 1000 Mb/s (1 gigabit) depending on the connecting device. These ports support the IEEE 802.3u, 802.3z for 1000SS, or 802.3ab for 1000TX autonegotiation standard, which means that when a port is connected to another device that also supports the IEEE 802.3u, 802.3z for 1000SS, or 802.3ab for 1000TX standard, the two devices negotiate the best speed and duplex mode.

The BayStack 380 Switch features auto-polarity. With autonegotiation enabled, auto-polarity automatically reverses the polarity of a pair of pins from positive to negative or negative to positive. This corrects the polarity of the received data if the port detects that the polarity of the data has been reversed due to a wiring error.

The 10/100/1000BASE-TX switch ports also support half- and full-duplex mode operation at 10 Mb/s and 100 Mb/s (refer to *Installing the BayStack 380 10/100/1000 Switch*).

The 10/100/1000BASE-TX RJ-45 ports can connect to 10 Mb/s or 100 Mb/s or 1000 Mb/s (1 gigabit) Ethernet segments or nodes.

➡ **Note:** Use only Category 5 copper unshielded twisted pair (UTP) cable connections when connecting 10/100/1000BASE-TX ports.

➡ **Note:** IEEE 1000BASE-TX requires operating in full-duplex mode with auto-negotiation enabled.

See Appendix D, “Connectors and pin assignments,” on page 201 for more information about the RJ-45 port connectors.

LED display panel

Figure 3 shows the BayStack 380 Switch LED display panel. See Table 2 for a description of the LEDs.

Figure 3 BayStack 380 Switch LED display panel

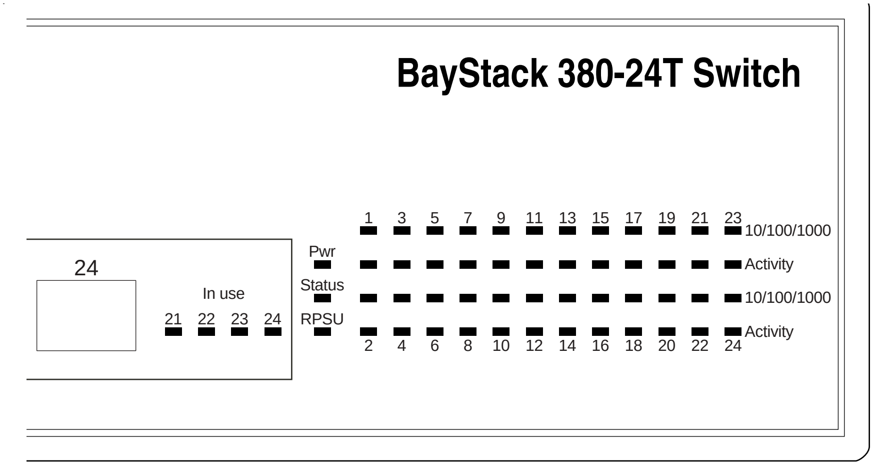


Table 2 BayStack 380 switch LED descriptions

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.
10/100/ 1000	Speed/Link Status indicator	Alternating Green/ Amber (10)	On	The corresponding port is set to operate at 10 Mb/s, and the link is good.
			Blinking	The corresponding 10 Mb/s port has been disabled by software.
			Off	The link connection is bad, or there is no connection to this port.
		Solid Amber (100)	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.
			Off	The link connection is bad, or there is no connection to this port.
		Solid Green (1000)	On	The corresponding port is set to operate at 1000 Mb/s and the link is good.
			Blinking	The corresponding 1000 Mb/s port has been disabled by software.
			Off	The link connection is bad, or there is no connection to this port.
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.

Note: The speed indicator LED for a port operating at 10 Mb/s is solid amber for 5 seconds, then switches to green for 1 second. It alternates in this way while the switch is on.

Multi-mode LEDs are used per port to display 10/100/1000BaseTX speed and port status:

- 1000Mbps - solid green
- 100Mbps - solid amber
- 10Mbps - solid amber for 5 seconds, solid green for 1 second, repeat
- If the port is disabled, the port speed LED blinks at a rate of once per second:
- disabled 1000Mbps - blink green
- disabled 100Mbps - blink amber
- disabled 10Mbps - blink amber 5 times, blink green 1 time, repeat
- System ready LED
- Redundant power LED

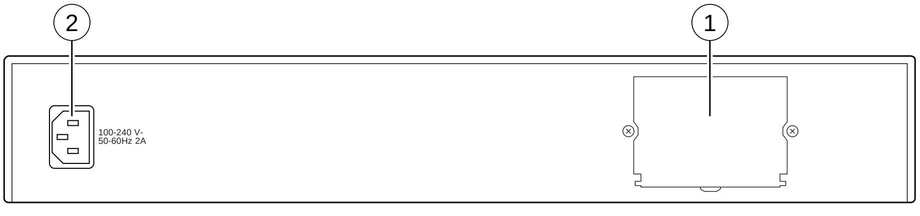
Activity LED: to be driven directly by PHYs Mini-GBICs and the corresponding copper ports are sharing the same activity LEDs

Mini-GBIC “In Use” LEDs: “In Use” is indicated by a green LED. If the “In Use” LED is lit, then the 10/100/1000 LED for the corresponding RJ-45 port will be off.

Back panel

The switch back panel is shown in Figure 4. Table 3 describes the components on the back panel.

Figure 4 BayStack 380 Switch back panel



10474EA

Table 3 Components on the BayStack 380 Switch back panel

Item	Description
1	DC-DC module for the Redundant power supply unit (RPSU)
2	AC power receptacle

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 BayStack 380 Switch. Nortel Networks provides an optional redundant power supply unit (RPSU) for this purpose. The BayStack 10 Power Supply Unit (Order number AA0005005) is a hot-swappable power supply unit that provides uninterrupted operation to as many as four BayStack 380 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.

DC-DC module

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 (Order number AA0005010) provides a plug-and-play redundant power supply unit for the BayStack 380 Switch, 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.

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

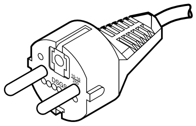
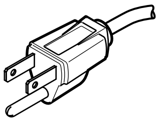
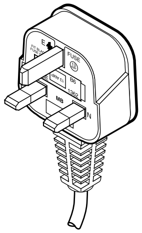
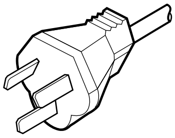
Country/Plug description	Specifications	Typical plug
Continental Europe: • CEE7 standard VII male plug • Harmonized cord (HAR marking on the outside of the cord jacket to comply with the CENELEC Harmonized Document HD-21)	220 or 230 VAC 50 Hz Single phase	 228FA
U.S./Canada/Japan: • NEMA5-15P male plug • UL recognized (UL stamped on cord jacket) • CSA certified (CSA label secured to the cord)	100 or 120 VAC 50–60 Hz Single phase	 227FA

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

Caution: Please read immediately.

Inspect this power cord and determine if it provides the proper plug and is appropriately certified for use with your electrical system. Immediately discard this cord if it is inappropriate for your country's electrical system and obtain the proper cord as required by your national electrical codes or ordinances.

Refer to this product's technical documentation for detailed installation procedures to be followed by qualified service personnel.

Vorsicht: Bitte sofort lesen.

Sehen Sie nach, ob dieses Netzkabel über den richtigen Stecker verfügt und für die Verwendung in Ihrem Stromversogungsnetz zertifiziert ist. Falls dieses Kabel nicht für das Stromversorgungsnetz in Ihrem Land geeignet ist, darf es nicht verwendet werden. Besorgen Sie sich ein Kabel, das die Vorschriften der Zulassungsbehörden in Ihrem Land erfüllt.

Die technische Dokumentation dieses Produkts enthält ausführliche Installationsanweisungen, die nur von qualifiziertem Kundendienstpersonal ausgeführt werden dürfen.

Attention: Lisez ceci immédiatement.

Examinez ce cordon d'alimentation pour déterminer s'il dispose de la fiche appropriée et s'il est bien agréé pour utilisation sur votre installation électrique. Débarrassez-vous en immédiatement s'il ne convient pas à l'utilisation sur le secteur électrique en usage dans votre pays et procurez-vous un cordon conforme à la réglementation nationale en vigueur.

Reportez-vous à la documentation technique de ce produit pour obtenir des instructions détaillées d'installation, destinées à un technicien qualifié.

Attenzione: Leggere attentamente.

Controllare questo cavo di alimentazione, verificarne il collegamento con la presa appropriata nonché la certificazione per l'uso nell'impianto elettrico posseduto. Non utilizzare assolutamente in caso tale cavo non sia adatto al sistema elettrico del paese in cui viene utilizzato e richiederne un altro certificato dall'ente nazionale di fornitura elettrica.

Per le procedure di installazione che devono essere seguite dal personale di servizio, consultare questa documentazione tecnica del prodotto.

Advertencia: Sírvase leer inmediatamente.

Inspeccione este cable de alimentación eléctrica y determine si viene con el enchufe apropiado y está debidamente certificado para el uso con su sistema eléctrico. Si no cumple con los reglamentos del sistema eléctrico de su país, despójese de este cable de alimentación inmediatamente y obtenga el cable requerido, según las ordenanzas y códigos eléctricos nacionales.

Refiérase a la documentación técnica de este producto para recibir información detallada sobre los procedimientos que el personal calificado de reparaciones deberá seguir.

Caution:

注意：最初にお読み下さい。

本電源コードが、ご使用になる電力規格に適したプラグ部で、且つ適正な規格証明がついているかどうかをお確かめ下さい。

もし本電源コードがご使用の電力規格に不適格な場合はただちに使用を中止し、ご使用の国家規格・法令に定められた適切な電源コードをご使用下さい。

本製品の取付方法につきましては、取扱技術説明書をご覧のうえ資格認定を受けたサービス・スタッフの指示に従って下さい。

Warning: Removal of the power cord is the only way to turn off power to this device. The power cord must always be connected in a location that can be accessed quickly and safely in case of an emergency.

Vorsicht: Die Stromzufuhr zu diesem Gerät kann nur durch Ziehen des Netzstromkabels unterbrochen werden. Die Netzsteckdose, an die das Netzstromkabel angeschlossen ist, muß sich stets an einem Ort befinden, der bei einem Notfall schnell und einfach zugänglich ist.

Avertissement: Le débranchement du cordon d'alimentation constitue le seul moyen de mettre cet appareil hors tension. Le cordon d'alimentation doit donc toujours être branché dans une prise accessible pour faciliter la mise hors tension en cas d'urgence.

Advertencia: La única forma de desconectar la alimentación de este dispositivo es desenchufar el cable de alimentación. El cable de alimentación siempre debe estar conectado en una ubicación que permita acceder al cable de forma rápida y segura en caso de emergencia.

Avvertenza: Estrarre il cavo di alimentazione è l'unico sistema per spegnere il dispositivo. Il cavo di alimentazione deve essere sempre collegato in una posizione che permetta l'accesso facile e sicuro in caso di emergenza.

警告: 電源コードを取り外すことが、このディバイスへの電源を切る唯一の方法です。電源コードは緊急の場合、迅速かつ安全に近づける場所に接続してください。

Features

The BayStack 380 Switch 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 BayStack 380 Switch provides the following features.

Virtual Local Area Networks (VLANs)

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 provides a mechanism to fine-tune broadcast domains.

Your BayStack 380 Switch allows you to create port-based 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.

- Auto PVID

  When Auto PVID is active, a port that is assigned to a numbered VLAN has the same number for its PVID. For example, if the VLAN is 2, the PVID is 2.

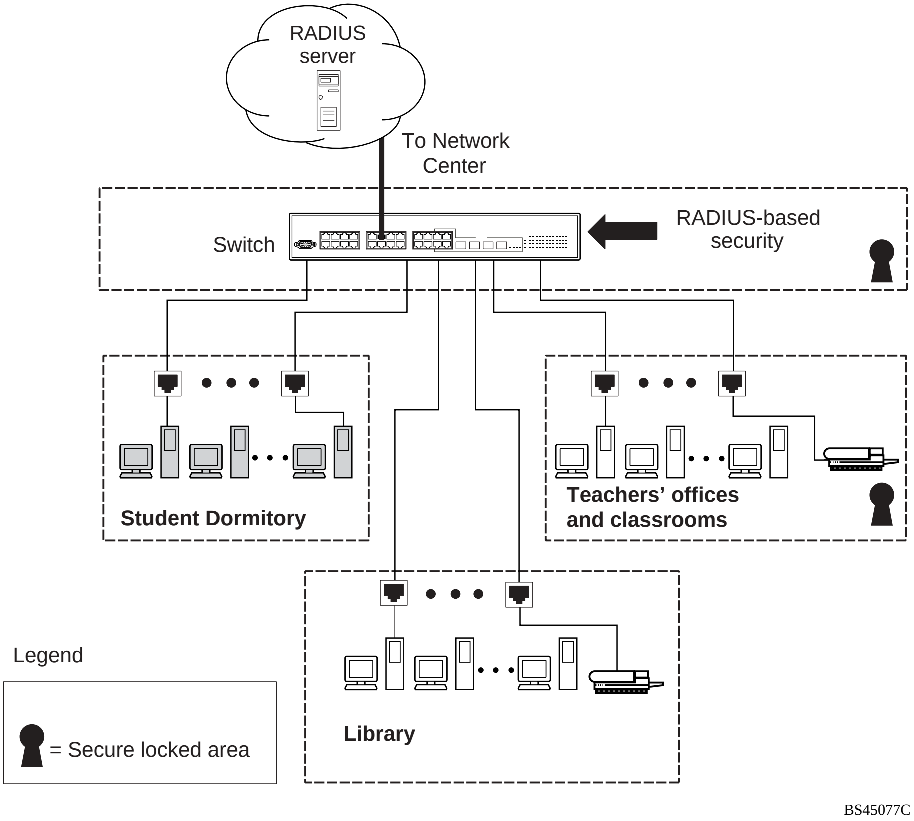
Security

The BayStack 380 Switch security features provide two 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

Figure 5 shows a typical campus configuration using the BayStack 380 Switch security features. 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 5 BayStack 380 Switch 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 40).
  - 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 40).
  - 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 RADIUS (Remote Authentication Dial-In User Services) 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.

For instructions to use the console interface (CI) to set up the RADIUS-based security feature, see Chapter 3, "Using the console interface," on page 93.

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 448 MAC addresses and specify which addresses are authorized to connect to your switch configuration. The 448 MAC addresses can be configured within a single standalone switch.
- Specify which of your switch ports each MAC address is allowed to access.

  The options for allowed port access include: NONE, ALL, and a single port.

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.

For instructions to use the console interface (CI) to set up the RADIUS-based security feature, see Chapter 3, “Using the console interface,” on page 93.

Flash memory storage

Switch software image storage

The BayStack 380 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 “Software Download screen” on page 164). 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.

Warning: Do not power off the switch within 10 seconds of changing any configuration parameters. Powering down the switch within 10 seconds of changing configuration parameters can cause the changed configuration parameters to be lost.

MultiLink Trunking

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 8 Gb/s in full-duplex mode. The BayStack 380 Switch can be configured with up to six MultiLink Trunks.

For more information about the MultiLink Trunking feature, see “MultiLink Trunk Configuration Menu screen” on page 136.

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 a specified port. You can specify *port-based* monitoring for ingress and egress at a specific port. You can also 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, see "Port Mirroring Configuration screen" on page 142.

Autosensing, autonegotiation, auto-MDI/X, and autopolarity

The BayStack 380 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 or 802.3z or 802.3ab) that exists between two IEEE -capable devices. Autonegotiation allows the switch to select the best of both speed and duplex modes.
- The term *autopolarity* refers to automatic detection of transmit and receive twisted pairs.

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 802.3z autonegotiation standard. In this case, because it is not possible to sense the duplex mode of the attached device, the BayStack 380 Switch reverts to half-duplex mode.

When autonegotiation-capable devices are attached to the BayStack 380 Switch, the ports negotiate down from 1000 Mb/s speed and full-duplex mode until the attached device acknowledges a supported speed and duplex mode.

Auto-MDI-X detects receive and transmit twisted pairs automatically. When auto-MDI-X is active, any straight or crossover category 5 cable can be used to provide connection to a port. If autonegotiation is disabled, then auto-polarity is not active.

The BayStack 380 Switch features auto-polarity. With autonegotiation enabled, auto-polarity automatically reverses the polarity of a pair of pins from positive to negative or negative to positive. This corrects the polarity of the received data if the port detects that the polarity of the data has been reversed due to a wiring error.

For more information about autosensing and autonegotiation modes, see Chapter 4, “Troubleshooting,” on page 171.

RFCs

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

- RFC 1213 (MIB-II)
- RFC 1493 (Bridge MIB)
- RFC 1573 (Interface MIB)
- RFC 1643 (Ethernet MIB)
- RFC 1757 (RMON)
- RFC 1271 (RMON)
- RFC 1157 (SNMP)

Standards

The following IEEE Standards also contain information germane to the BayStack 380 Switch:

- IEEE 802.3 10BASE-T (ISO/IEC 8802-3, Clause 14)
- IEEE 802.3u 100BASE-TX (ISO/IEC 8802-3, Clause 25)
- IEEE 802.3ab 1000BASE-T
- IEEE 802.3z (gigabit ethernet)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.3x (Flow Control with 802.1D compliant device)
- IEEE 802.1D (Spanning tree protocol)
- IEEE 802.1p (Prioritization)

SNMP MIB support

The BayStack 380 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
RMON	rfc1757.mib	
MLT		rcMLT
SNMPv3 MIBs	RFCs 2571, 2572, 2573, 2574, 2575, 2576	
MIB2	rfc1213.mib	
IF-MIB	rfc2233.mib	
Etherlike MIB	rfc1643.mib	
Interface Extension MIB		s5ifx100.mib
Switch Bay Secure		s5sbs102.mib
System Log MIB		bnlog.mib
S5 Autotopology MIB		s5emt104.mib
VLAN		rcVlan
Entity MIB	RFC 2037	
Spanning Tree	RFC1493 Bridge MIB	

SNMP trap support

The BayStack 380 Switch supports an SNMP agent with industry standard SNMPv1 traps, as well as private SNMPv1 trap extensions (Table 6).

Table 6 Support 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.
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 a configuration.
s5CtrUnitDown	Always on	A unit is removed from a configuration.
s5CtrHotSwap	Always on	A unit is hot-swapped in a configuration.
s5CtrProblem	Always on	An assigned unit fails.
s5EtrSbsMacAccessViolation	Always on	A MAC address violation is detected.

BootP automatic IP configuration/MAC address

The BayStack 380 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 BayStack 380 Switch BootP requests. A properly configured BootP server enables the switch to automatically learn its assigned IP address, subnet mask, IP address of the default router (default gateway), and software image file name.

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.

For more information and an example of a BootP configuration file, see Appendix F, “Sample BootP configuration file,” on page 211.

Configuration and switch management

The BayStack 380 Switch is shipped directly from the factory ready to operate in any 10BASE-T, 100BASE-TX, or 1000BASE-TX standard network.

You must assign an IP address to the switch, 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 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 BayStack 380 Switch, remotely through a dial-up modem connection, or in-band through a Telnet session.

  For information about the console interface, see Chapter 3, “Using the console interface,” on page 93.

- Web-based management

  You can manage the network from the World Wide Web. Access the Web-based graphical user interface (GUI) through the Embedded Web Server (EWS), 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 BayStack 380 10/100/1000 Switch*.

- Java-based Device Manager

  Device Manager is a Java-based set of graphical network management applications used to configure and manage a BayStack 380 Switch. See *Reference for the BayStack 380 10/100/1000 Switch Management Software* for more information.

- Any generic SNMP-based network management software.

  You can use any generic SNMP-based network management software to configure and manage a BayStack 380 Switch.

- Nortel Networks Optivity* network management software

  Optivity network management software consists of views, most of which are maps that illustrate the interconnections between the segments, rings, and nodes of your network. The views allow you to analyze network performance and fault conditions on the individual segments and specific areas in your network. They can also alert you when a problem has occurred in a specific location. For further information about Optivity, contact your Nortel Networks sales representative.

Chapter 2
Network configuration

Use BayStack 380 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 describes the following topics:

- "Network configuration examples," next
- "IEEE 802.1Q VLAN workgroups" on page 55
- "IEEE 802.1p Prioritizing" on page 71
- "MultiLink Trunks" on page 74
- "Port mirroring" on page 91

Network configuration examples

This section provides four network configuration examples using BayStack 380 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. The examples are:

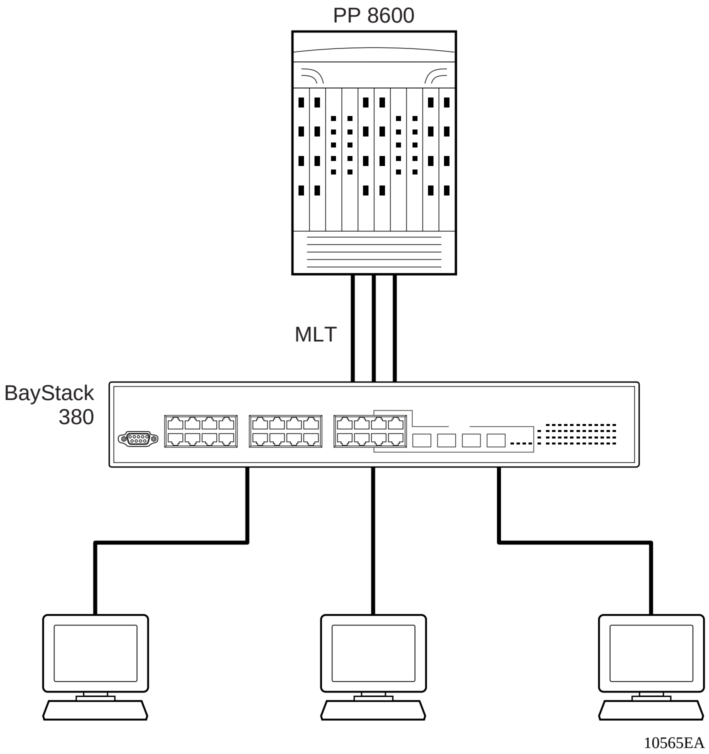
- High-bandwidth Desktop switch configuration (next)
- High-bandwidth server configuration
- OEL2 Aggregation
- Layer 2 Aggregator

High-bandwidth Desktop switch configuration

Figure 6 shows a BayStack 380 Switch used as a desktop switch, where desktop workstations are connected directly to BayStack 380 switch ports. A Passport 8600 provides high-capacity and low latency connections to the rest of the network. Users can transfer files to and from the network with much greater speed. Configuring a high bandwidth desktop configuration requires only three major steps:

1. Configure the multi-link transfer (MLT) ports that link to the Passport 8600
2. Configure the MLT ports on the Passport 8600 that attach to the BayStack 380 switch.
3. Attach one or more high-speed workstations to the BayStack 380 switch.

Figure 6 BayStack 380 Switch used as a desktop switch



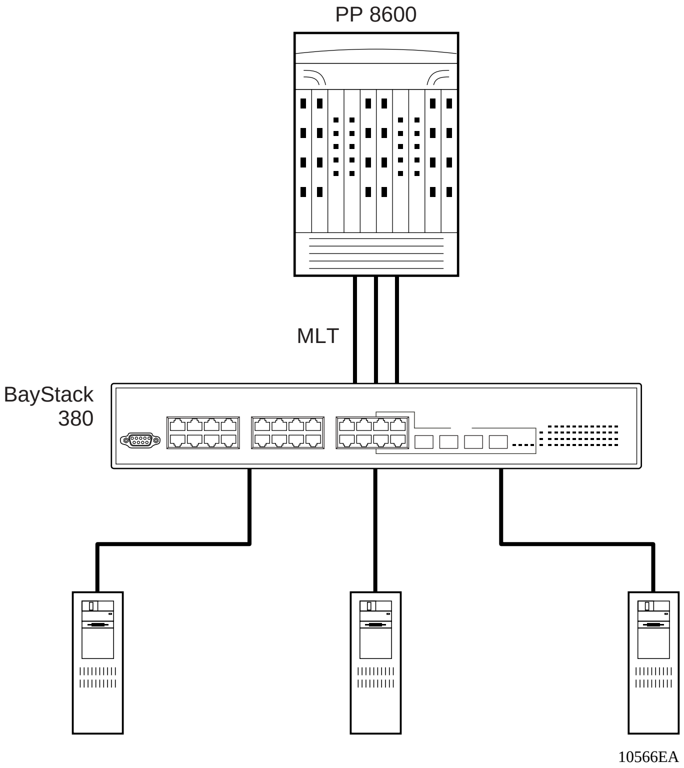
High-bandwidth server configuration

Figure 7 shows an example of a BayStack 380 Switch used to service a group of servers, where the servers are connected directly to BayStack 380 switch ports. A Passport 8600 provides high-capacity and low latency connections to the rest of the network. The BayStack 380 provides up to four gigabit links for each server, and can balance the high speed server connections with multi-gigabit links back to the network. The BayStack 380 also provides configuration of multiple 10/100/1000 Mbps link. This allows for the evolution of connections from a single 10 Mbps connection to a multi-gigabit connection without requiring another switch.

Configuring a high-bandwidth server configuration requires only four major steps:

1. Configure the network servers.
2. Configure the multi-link transfer (MLT) ports on the BayStack 380 that link to the network servers.
3. Configure the MLT ports that link to the Passport 8600.
4. Configure the MLT ports on the Passport 8600 that attach to the BayStack 380.

Figure 7 BayStack 380 used in a high-bandwidth server configuration



OEL2 Aggregation

Figure 8 shows an example of the BayStack 380 used to aggregate the uplink connection from OPTera Metro 1200 Ethernet Service modules (OM 1200 ESM) at one site to a Passport 8600 at another site. Inexpensive copper connections can be used to connect the OM 1200 OSM units to the BayStack 380 at one site, while small form factor pluggable gigabit interface connectors (SFP GBICs) connect the BayStack 380 to the Passport 8600 at the other site.

Configuring the OEL2 aggregation requires four major steps:

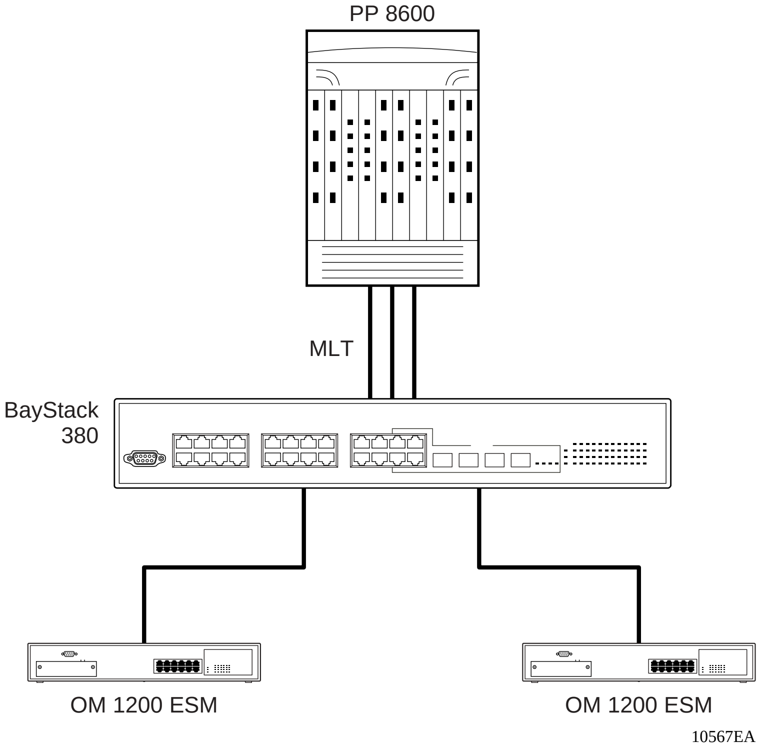
1 Configure the OM 1200 ESM units

2 Configure the multi-link transfer (MLT) ports that link the OM 1200 ESM units to the BayStack 380.

3 Configure the MLT ports on the BayStack 380 that link to the Passport 8600.

4 Configure the MLT ports on the Passport 8600 that link to the BayStack 380.

Figure 8 BayStack 380 used in an OEL2 Aggregation



Layer 2 Aggregator

Figure 9 shows an example of the BayStack 380 used to aggregate the uplink connection from several Business Policy Switch 2000 (BPS 2000) switches to a Passport 8600.

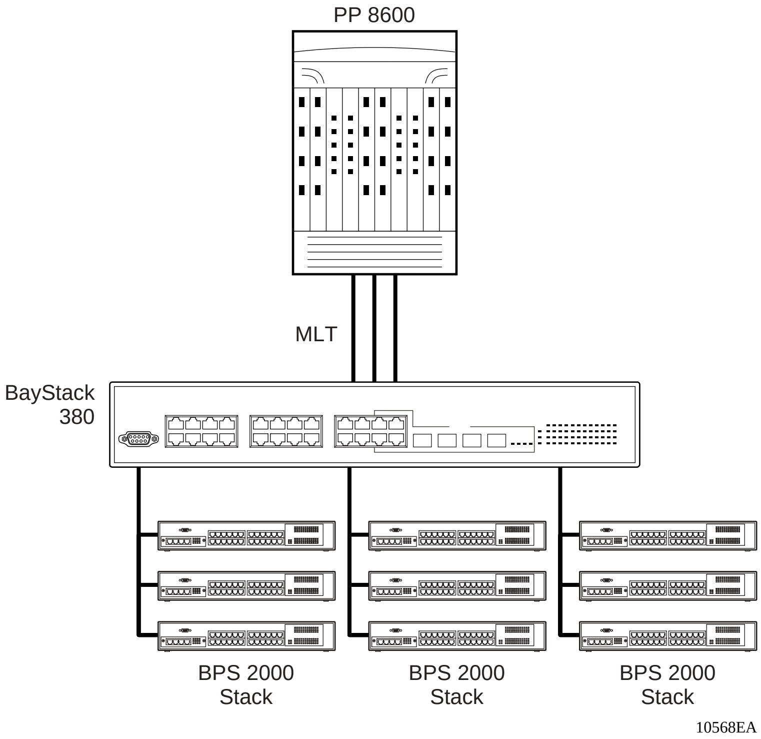
Configuring the BayStack 380 as a layer 2 aggregator requires three major steps:

1 Attach the BPS 2000 switches to tagged VLAN ports on the BayStack 380

2 Configure the multi-link transfer (MLT) ports on the BayStack that connect to the Passport 8600.

3. Configure the MLT ports on the Passport 8600 that connect to the BayStack 380.

Figure 9 Layer 2 Aggregator



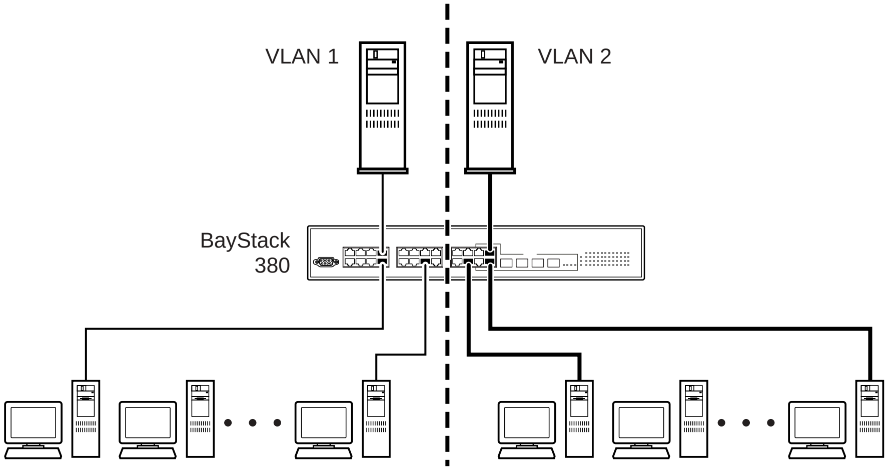
IEEE 802.1Q VLAN workgroups

BayStack 380 switches support up to 64 port-based VLANs with IEEE 802.1Q tagging available per port. 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 10). 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 BayStack 380 Switch allows you to assign ports to VLANs using the console, Telnet, Web-based management, or an appropriate SNMP-based application. 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 10 Port-based VLAN example



10004EB

IEEE 802.1Q tagging

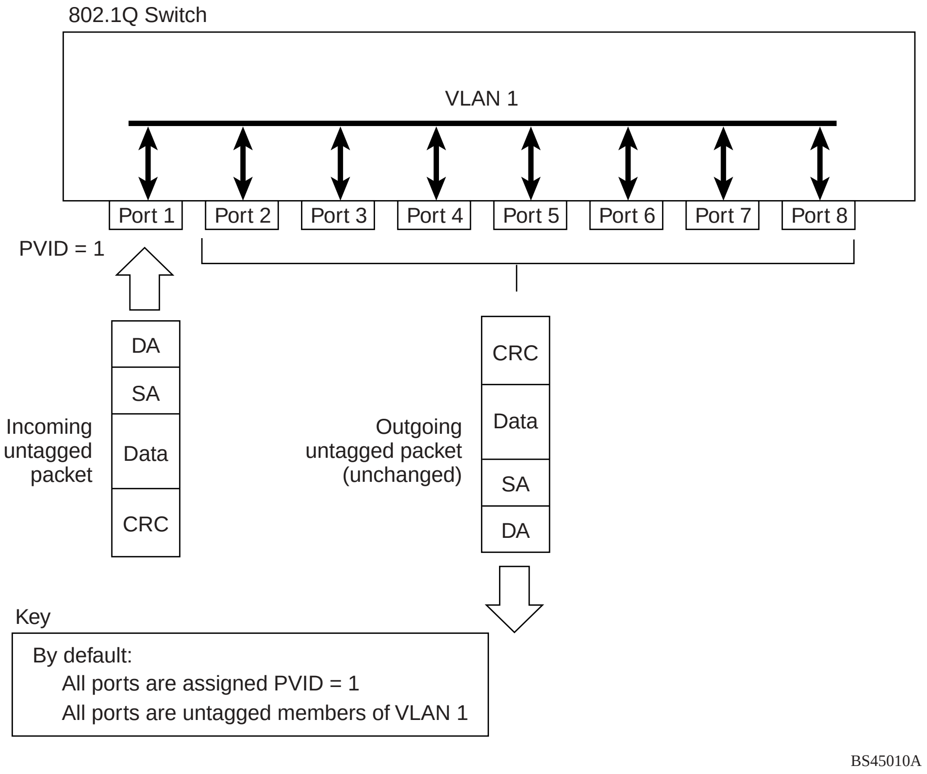
BayStack 380 switches operate in accordance with the IEEE 802.1Q tagging rules. Important terms used with the 802.1Q tagging feature are:

- 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 Web-based management interface. Refer to *Using Web-Based Management for the BayStack 380 10/100/1000 Switch*.
- 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.
- 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.

The default configuration settings for BayStack 380 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 11, all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID =1). Untagged packets enter and leave the switch unchanged.

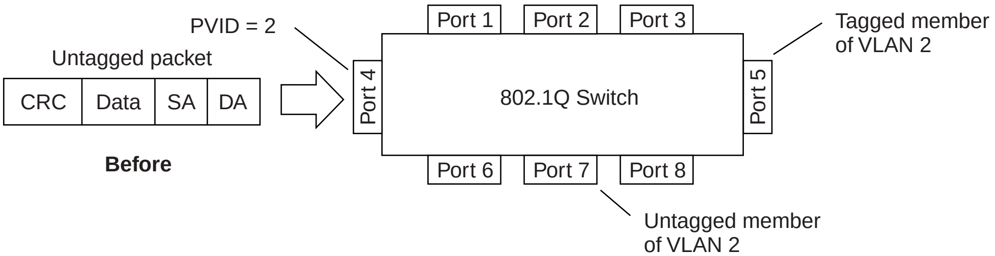
Figure 11 Default VLAN settings



When you configure VLANs, you configure the switch ports as *tagged* or *untagged* members of specific VLANs (see Figure 12 through Figure 20).

In Figure 12, 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.

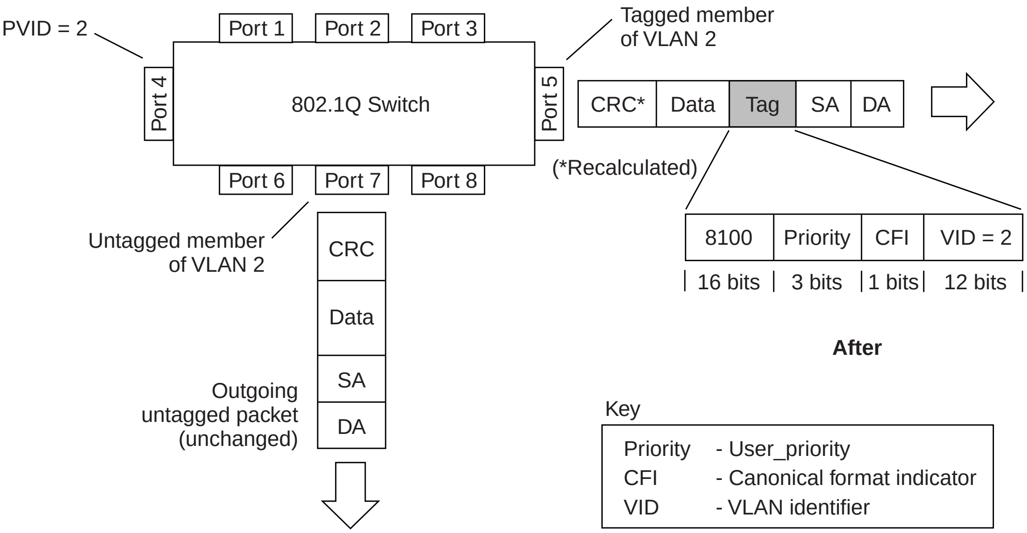
Figure 12 Port-based VLAN assignment



BS45011A

As shown in Figure 13, 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.

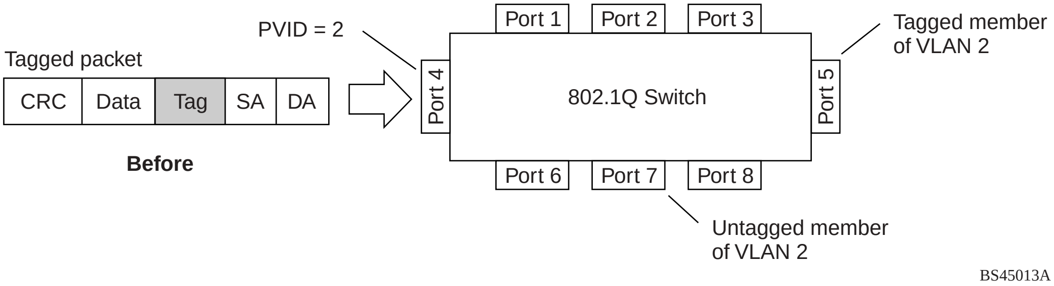
Figure 13 802.1Q tagging (after port-based VLAN assignment)



BS45012A

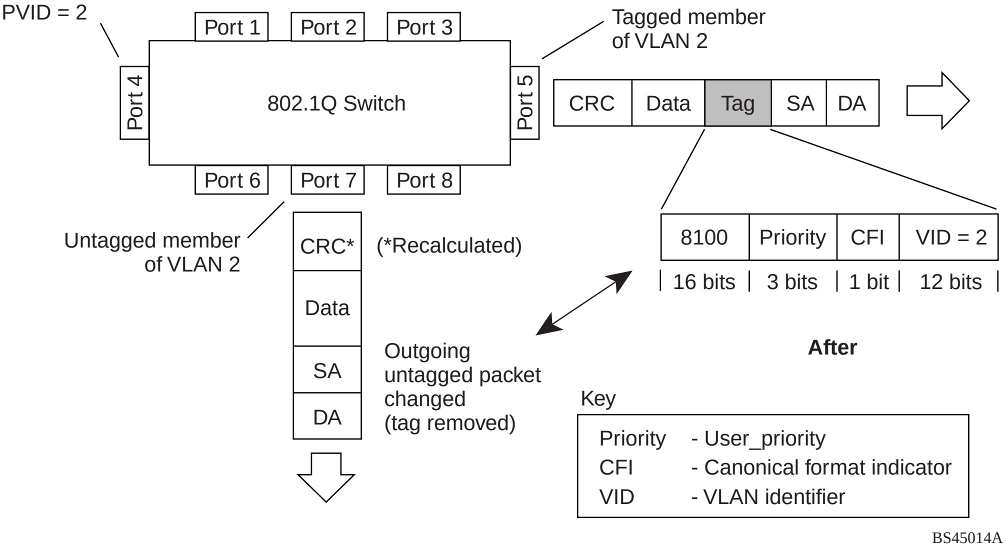
In Figure 14, tagged incoming packets are assigned directly to VLAN 2 because of the tag assignment in the packet. Port 5 is configured as a *tagged* member of VLAN 2, and port 7 is configured as an *untagged* member of VLAN 2.

Figure 14 802.1Q tag assignment



As shown in Figure 15, 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 15 802.1Q tagging (after 802.1Q tag assignment)



VLANs spanning multiple switches

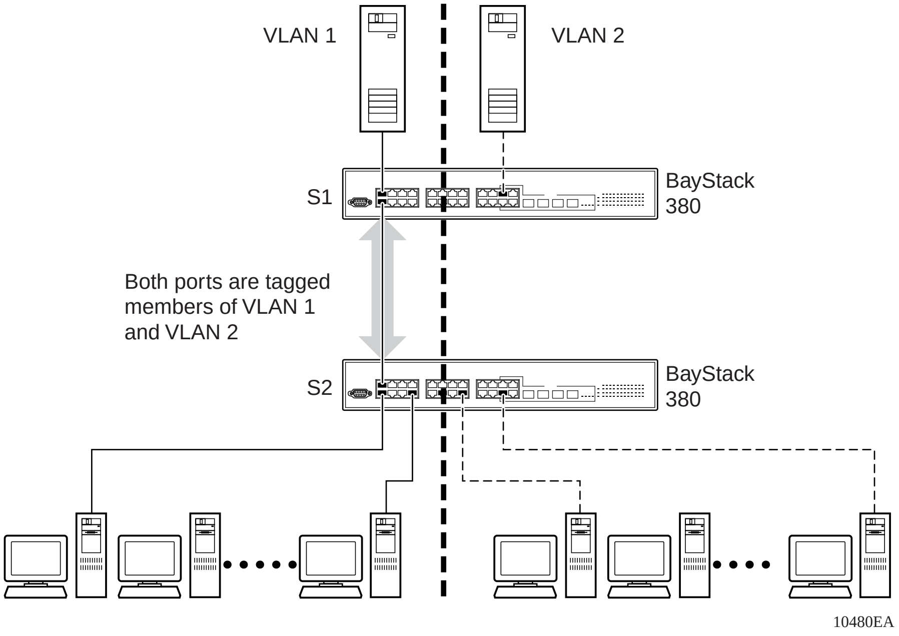
You can use VLANs to segment a network within a switch. When you connect multiple switches, it is possible to connect users of one VLAN with users of that same VLAN in another switch. However, the configuration guidelines depend on whether both switches support 802.1Q tagging.

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.

VLANs spanning multiple 802.1Q tagged switches

Figure 16 shows VLANs spanning two BayStack 380 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 16 VLANs spanning multiple 802.1Q tagged switches



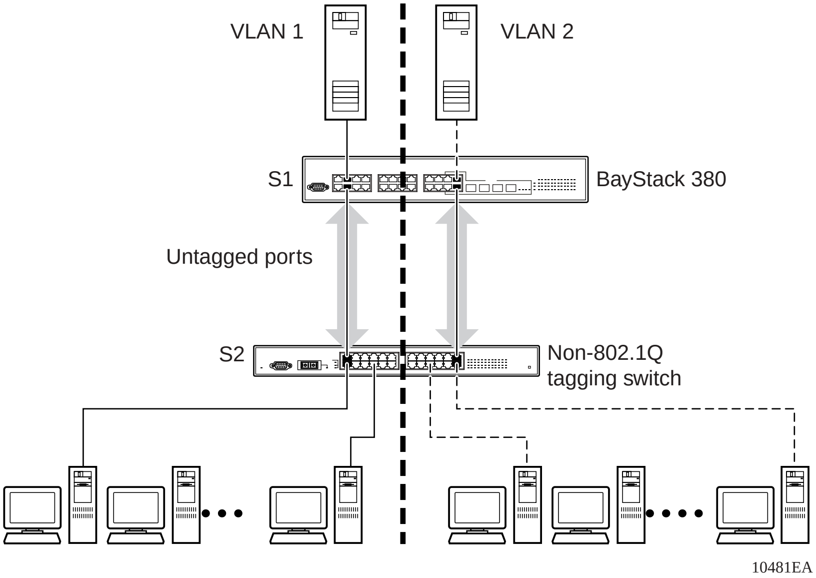
Because there is only one link between the two switches, the Spanning Tree Protocol (STP) treats this configuration as any other switch-to-switch connection. For this configuration to work properly, both switches must support the 802.1Q tagging protocol.

VLANS spanning multiple untagged switches

Figure 17 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).

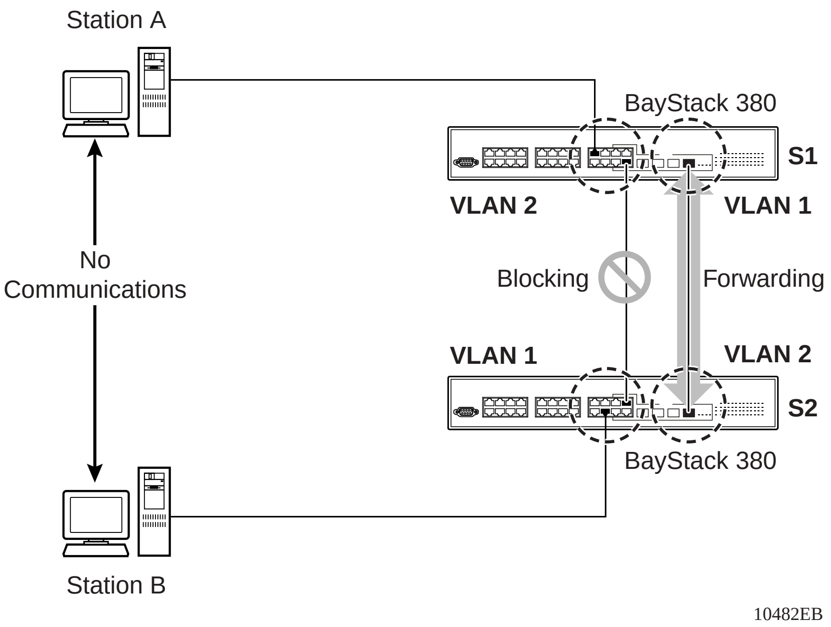
Figure 17 VLANs spanning multiple untagged switches



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 18 shows possible consequences of enabling the STP when using VLANs between untagged (non-802.1Q tagged) switches.

Figure 18 Possible problems with VLANs and Spanning Tree Protocol



As shown in Figure 18, 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.

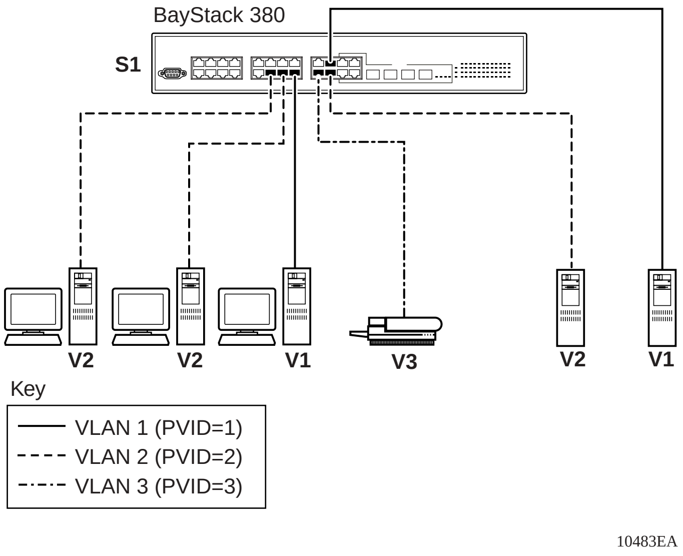
The STP selects the link connecting VLAN 1 on Switches S1 and S2 as the forwarding link based on port speed, duplex-mode, and port priority. Because the other link connecting VLAN 2 is in Blocking mode, stations on VLAN 2 in Switch S1 cannot communicate with stations in VLAN 2 on Switch S2. With multiple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

Shared servers

BayStack 380 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 19.

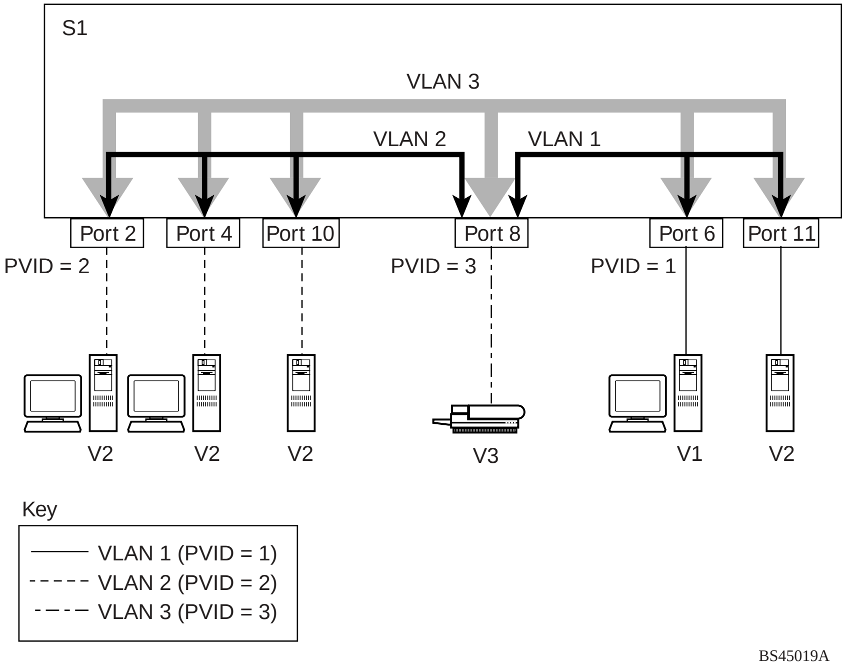
In this example, clients on different broadcast domains share resources. The broadcasts from ports configured in VLAN 3 can be seen by all VLAN port members of VLAN 3.

Figure 19 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 20).

Figure 20 VLAN broadcast domains within the switch



For example, to create a broadcast domain for each VLAN shown in Figure 20, 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.

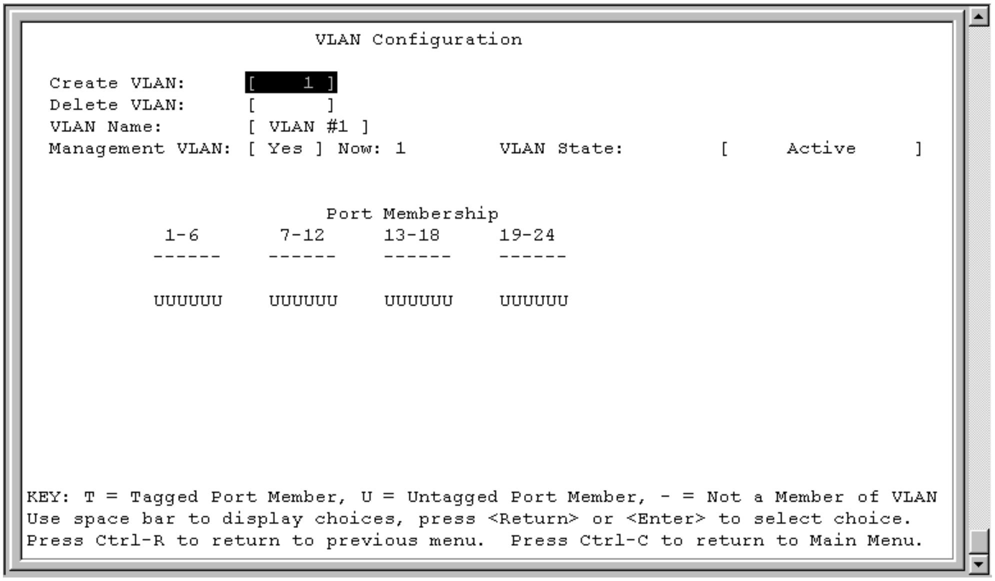
The following steps show how to use the VLAN configuration screens to configure the VLAN 3 broadcast domain shown in Figure 20.

To configure the VLAN port membership for VLAN 1:

1. Select Switch Configuration from the BayStack 380 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 21).

Figure 21 Default VLAN Configuration screen example



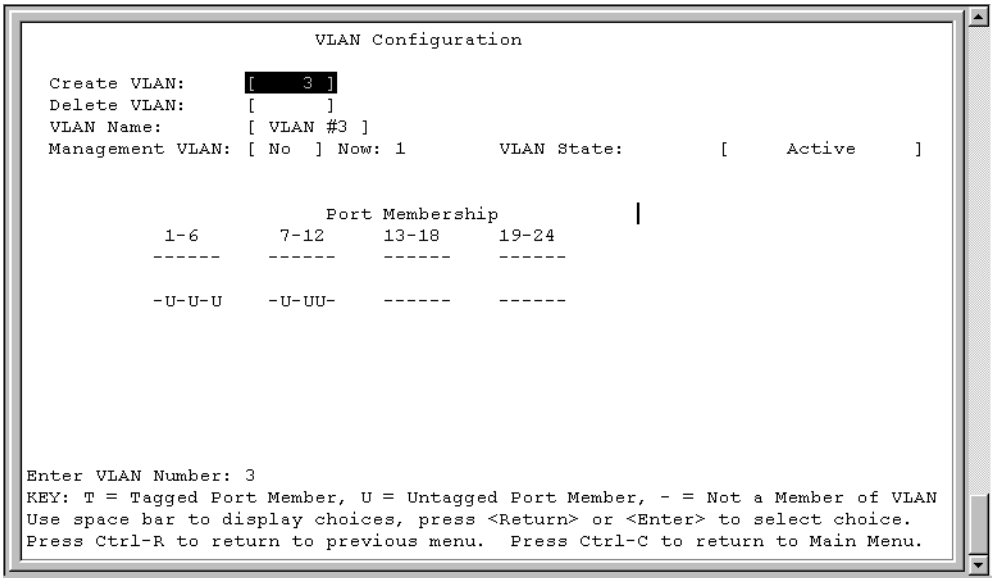
```
                          VLAN Configuration

  Create VLAN:        [      1 ]
  Delete VLAN:        [        ]
  VLAN Name:          [ VLAN #1 ]
  Management VLAN:    [ Yes ] Now: 1        VLAN State:        [     Active     ]


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

          UUUUUU     UUUUUU     UUUUUU     UUUUUU









KEY: T = Tagged Port Member, U = Untagged Port Member, - = Not a Member of 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.
```

The VLAN Configuration screen settings shown in Figure 21 are default settings with all switch ports classified as *untagged* members of VLAN 1.

Figure 22 shows the VLAN Configuration screen after it is configured to support the VLAN 3 broadcast domain shown in Figure 20 on page 64 (VLAN Name is optional).

Ports 2, 4, 6, 8, 10, and 11 are now untagged members of VLAN 3 as shown in Figure 20 on page 64.

Figure 22 VLAN Configuration screen example



```
                              VLAN Configuration

  Create VLAN:       [     3 ]
  Delete VLAN:       [       ]
  VLAN Name:         [ VLAN #3 ]
  Management VLAN:   [ No  ] Now: 1        VLAN State:         [     Active     ]


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


          -U-U-U    -U-UU-    ------    ------








Enter VLAN Number: 3
KEY: T = Tagged Port Member, U = Untagged Port Member, - = Not a Member of 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.
```

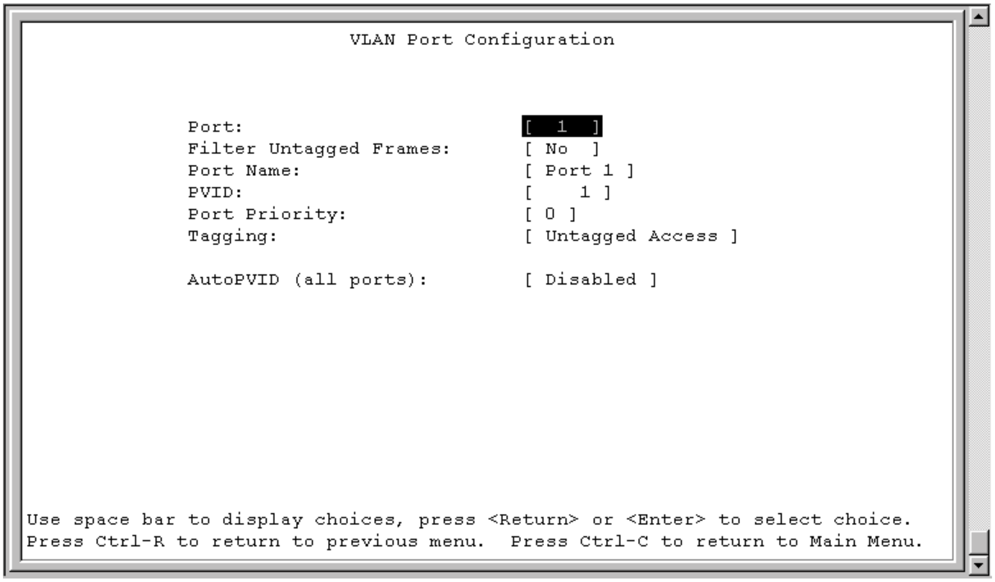
To configure the PVID (port VLAN identifier) for port 8:

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 23).

   The VLAN Port Configuration screen settings shown in Figure 23 are default settings.

Figure 23 Default VLAN Port Configuration screen example

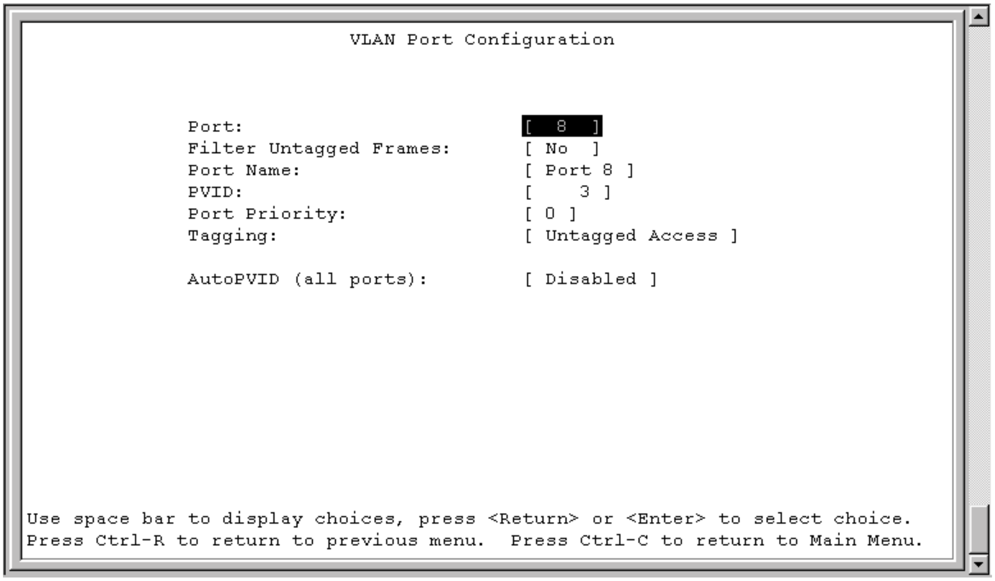


```
                          VLAN Port Configuration


       Port:                               [  1  ]
       Filter Untagged Frames:             [ No   ]
       Port Name:                          [ Port 1 ]
       PVID:                               [     1 ]
       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.
```

Figure 24 shows the VLAN Port Configuration screen after it is configured to support the PVID assignment for port 8, as shown in Figure 20 on page 64 (Port Name is optional).

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

Figure 24 VLAN Port Configuration screen example



```
                         VLAN Port Configuration


             Port:                            [  8  ]
             Filter Untagged Frames:          [ No   ]
             Port Name:                       [ Port 8 ]
             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.

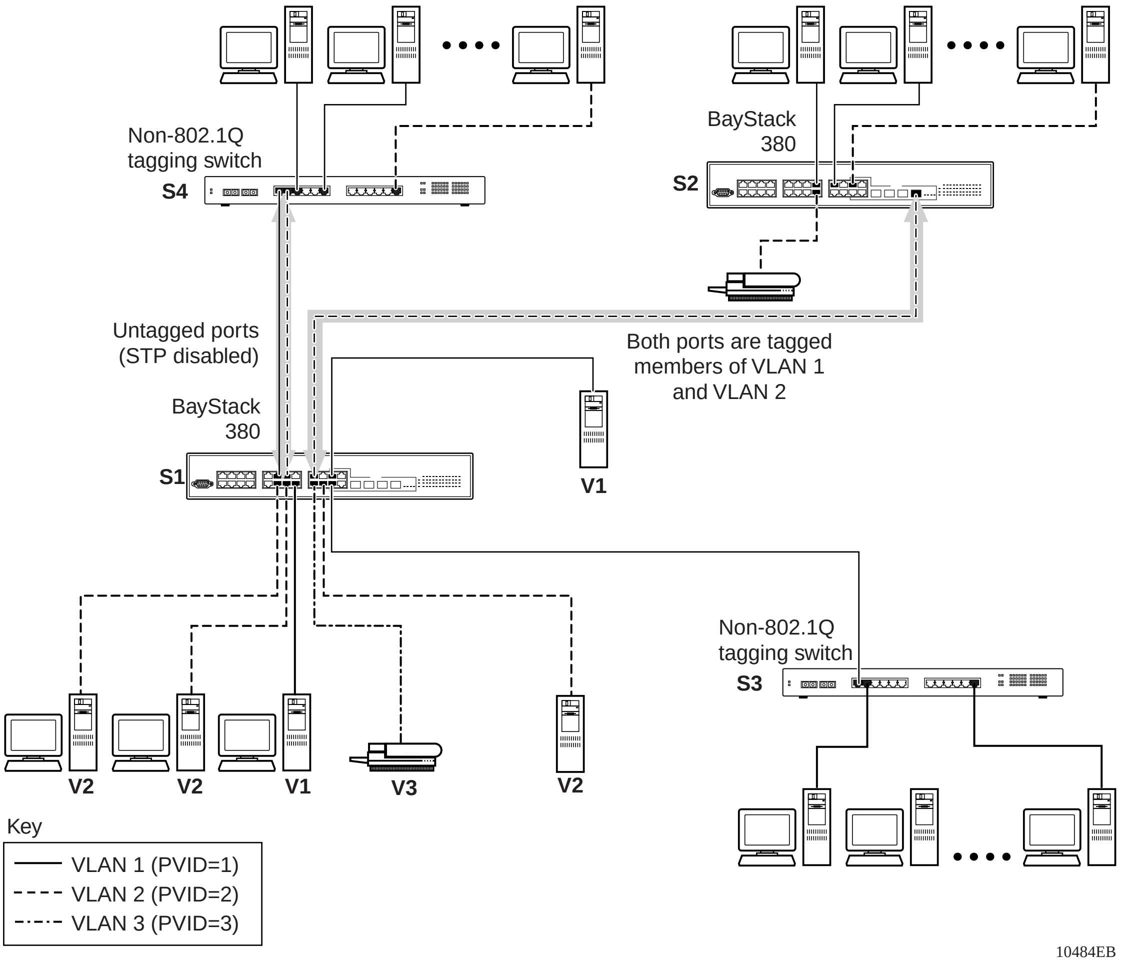
As shown in Figure 25, Switch S1 (BayStack 380 Switch) is configured with multiple VLANs:

- 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” on page 61).

The connection to S2 requires only one link between the switches because S1 and S2 are both BayStack 380 switches that support 802.1Q tagging (see “VLANs spanning multiple 802.1Q tagged switches” on page 60).

Figure 25 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:

- 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.
- Auto PVID can be activated by creating a VLAN and enabling Auto PVID for it.

Independent VLANs (IVL)

You can configure a VLAN as an Independent VLAN (IVL). Each independent VLAN maintains its own MAC Address table.

Independent VLANs can have duplicate MAC Addresses on different VLANs. In Table 7, both VLANs use the duplicate MAC Address “A”.

Table 7 Independent VLAN (IVL) Forwarding Database Table Example

Port	MAC Address	VLAN
1	00081XXXA	1
2	00081XXXA	2

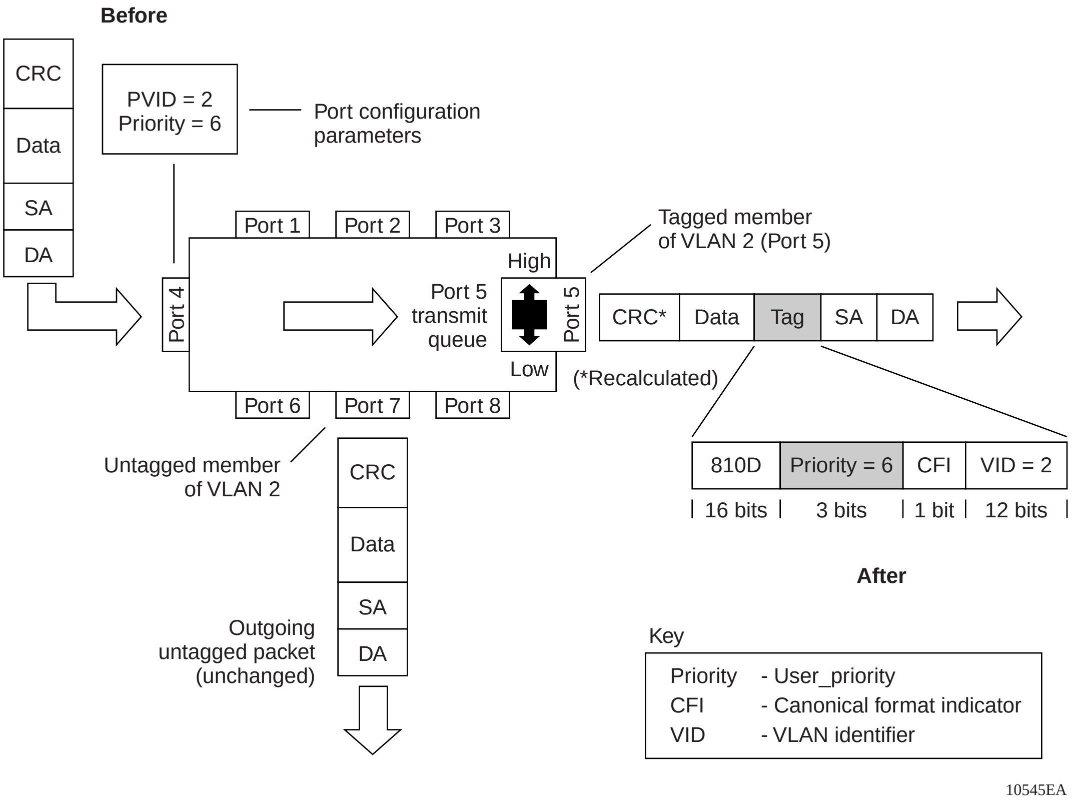
For more information about configuring VLANs, see “VLAN Configuration Menu screen” on page 120.

See also Appendix C, “Quick configuration for MultiLink Trunking,” on page 199 for configuration flowcharts that can help you use this feature.

IEEE 802.1p Prioritizing

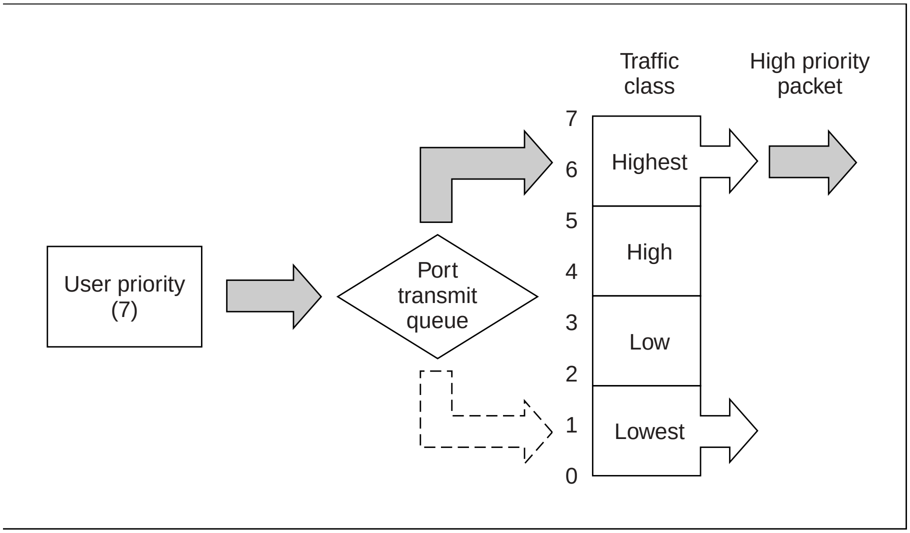
You can use the VLAN Configuration screens to prioritize the order in which the switch forwards packets, on a per-port basis. For example, if messages from a specific segment are crucial to your operation, you can set the switch port connected to that segment to a higher priority level (by default, all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

Figure 26 Prioritizing packets



The newly tagged frame is read within the switch and sent to the port's high or low transmit queue for disposition. The port transmit queue example shown in Figure 27 applies to all ports in the BayStack 380 switch.

Figure 27 Port Transmit Queue



As shown in Figure 27, the switch provides four transmission queues, *Highest, High*, *Low*, and *Lowest* for any given port. Frames are assigned to one of these queues on the basis of the user_priority value, using a *traffic class table*. This table is managed by using the Traffic Class Configuration screen. The table indicates the traffic class assigned to the frame for each user_priority value. If the frame leaves the switch formatted as a tagged packet, the traffic class assigned to the frame is carried forward to the next 802.1p-capable switch. This allows the packet to carry the assigned traffic class priority through the network until it reaches its destination.

The following steps show how to use the Traffic Class Configuration screen to configure the port priority level.

To configure the priority level, follow these steps:

1 Determine the priority level you want to assign to the switch port.

User priority levels are assigned default settings in all BayStack 380 switches. The range is from 0 to 7. The traffic class table can be modified. You can view the settings shown in the Traffic Class configuration screen, and then set the port priority in the VLAN Port Configuration screen.

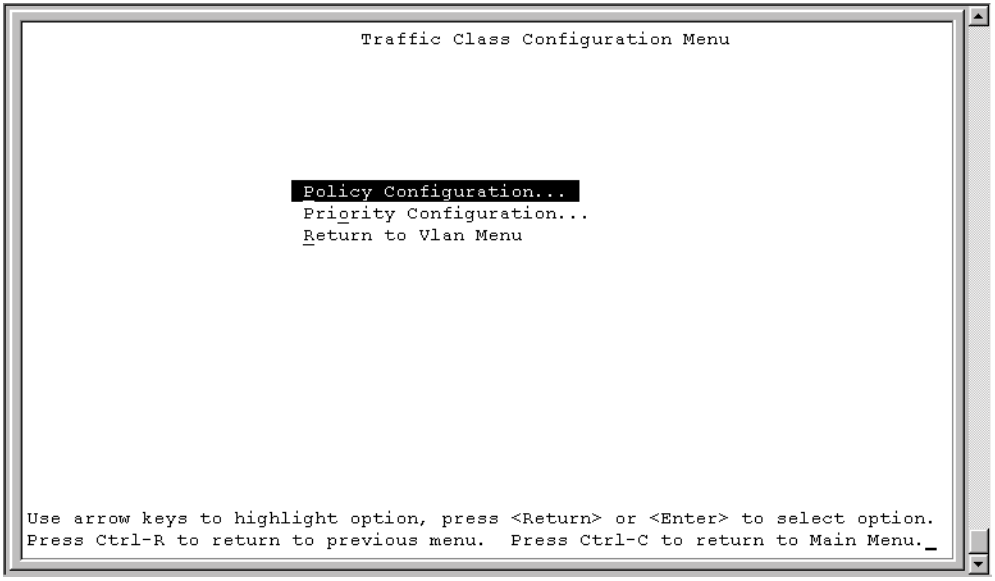
2 Select Switch Configuration from the BayStack 380 Main Menu (or press w).

3 From the Switch Configuration Menu, select VLAN Configuration (or press w).

4 From the VLAN Configuration Menu, select Traffic Class Configuration (or press t).

The Traffic Class Configuration screen opens.

Figure 28 Default Traffic Class Configuration Screen Example



```
                        Traffic Class Configuration Menu




                   Policy Configuration...
                   Priority Configuration...
                   Return to Vlan 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._
```

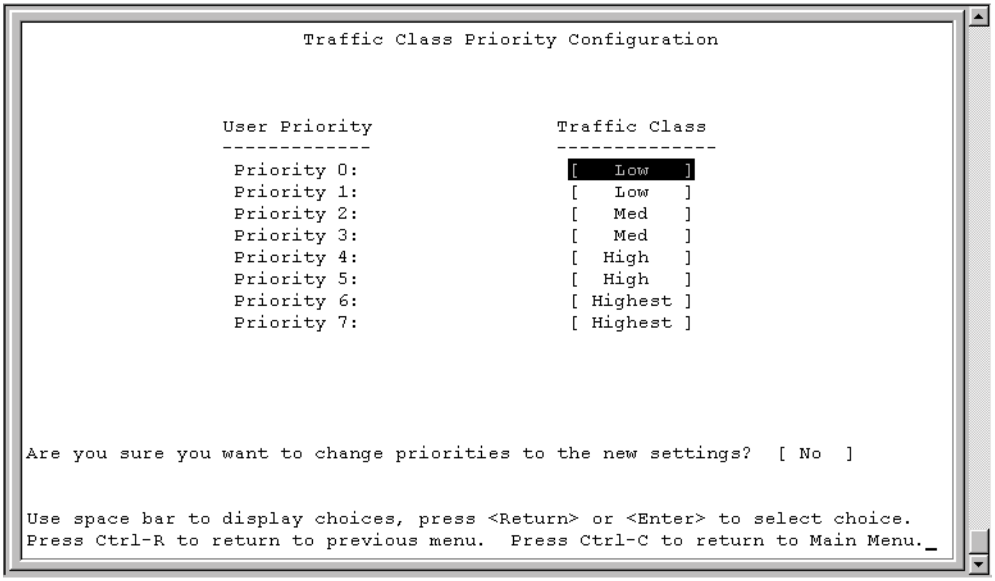
5 Select a priority level from the range shown in the Traffic Class Configuration screen (or modify the Traffic Class parameters to suit your needs).

6 Assign the priority level to ports using the VLAN Port Configuration screen:

a Press [Ctrl]-R to return to the VLAN Configuration Menu.

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

Figure 29 Traffic Class Priority Configuration screen example



```
                      Traffic Class Priority Configuration


                 User Priority                Traffic Class
                 -------------                --------------
                  Priority 0:                  [   Low    ]
                  Priority 1:                  [   Low    ]
                  Priority 2:                  [   Med    ]
                  Priority 3:                  [   Med    ]
                  Priority 4:                  [  High    ]
                  Priority 5:                  [  High    ]
                  Priority 6:                  [ Highest ]
                  Priority 7:                  [ Highest ]






Are you sure you want to change priorities to 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._
```

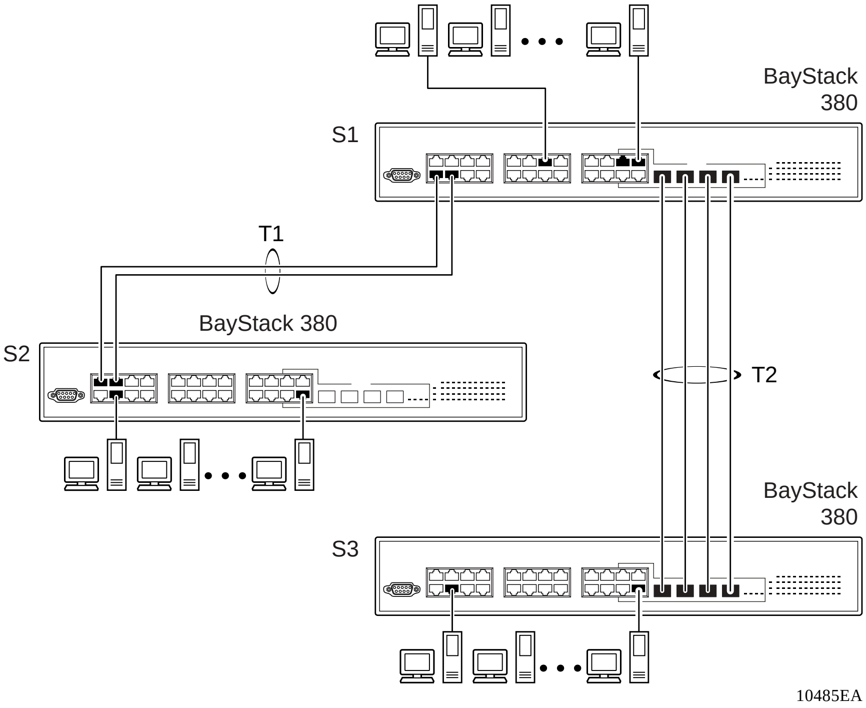
MultiLink Trunks

MultiLink Trunks allow you to group from two 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 8 Gb/s in full-duplex mode). You can configure up to six MultiLink Trunks. The trunk members can only reside on a single unit. 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. If there is only a single trunk, the trunk can be blocked and no traffic will get through.

You can use the Trunk Configuration screen to create switch-to-switch and switch-to-server MultiLink Trunk links (Figure 30 and Figure 31).

Figure 30 shows two trunks (T1 and T2) connecting Switch S1 to switches S2 and S3.

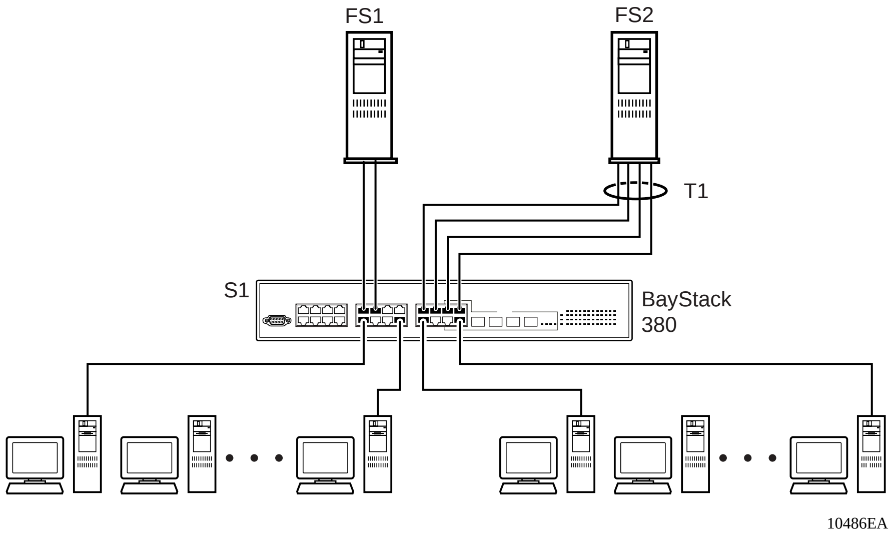
Figure 30 Switch-to-switch trunk configuration example



You can configure each of the trunks shown in Figure 30 with up to four switch ports to provide up to 8 Gb/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 31 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 31 Switch-to-server trunk configuration example



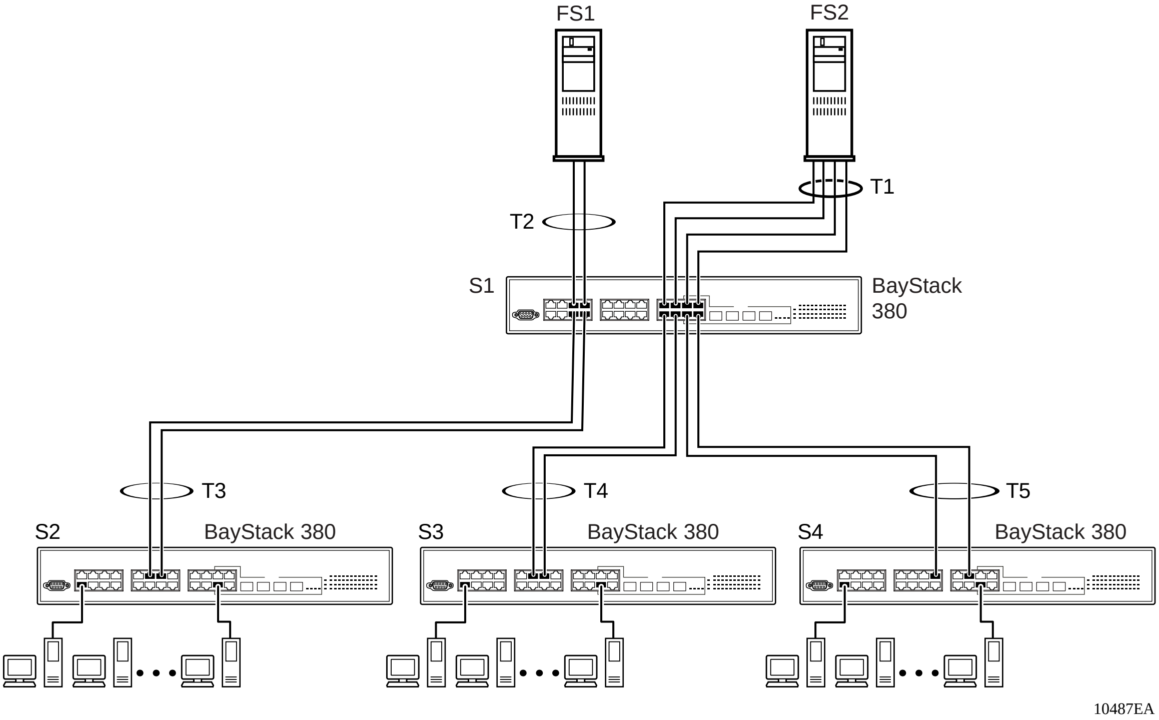
Client/server configuration using MultiLink Trunks

Figure 32 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 Refer to “IEEE 802.1Q VLAN workgroups” on page 55 for more information.

Figure 32 Client/server configuration example



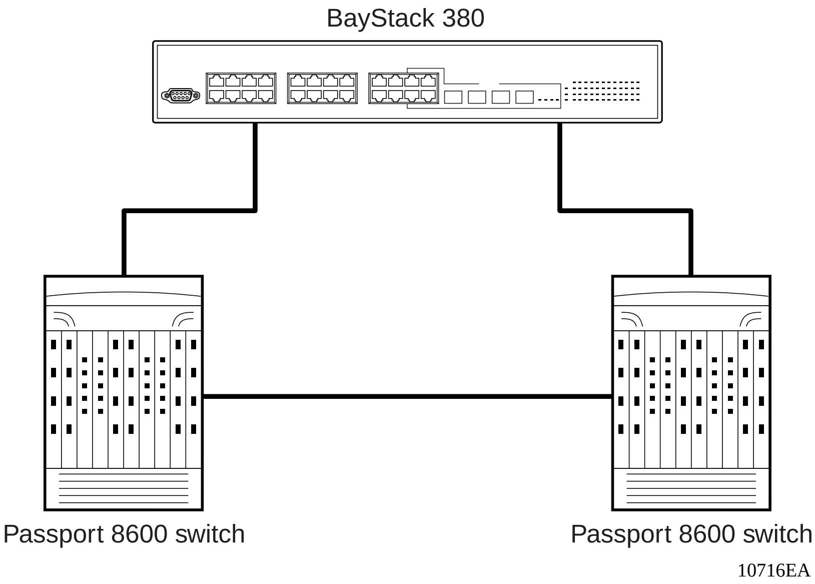
The trunk configuration screens for switches S1 to S4 are shown in "Trunk configuration screen examples" following this section. For detailed information about configuring trunks, see "MultiLink Trunk Configuration screen" on page 138.

Split MultiLink Trunks

This section provides an example of a split MultiLink Trunk. To use split MLT, you must disable spanning tree on the BayStack 380 switch.

Figure 33 shows an example of a split MultiLink Trunk:

Figure 33 Split MultiLink Trunk



Trunk configuration screen examples

This section shows examples of the MultiLink Trunk configuration screens for the client/server configuration example shown in Figure 32. The screens show how you could set up the trunk configuration screens for switches S1 to S4. See “Spanning tree considerations for MultiLink Trunks” on page 87, and “MultiLink Trunk Configuration screen” on page 138 for more information.

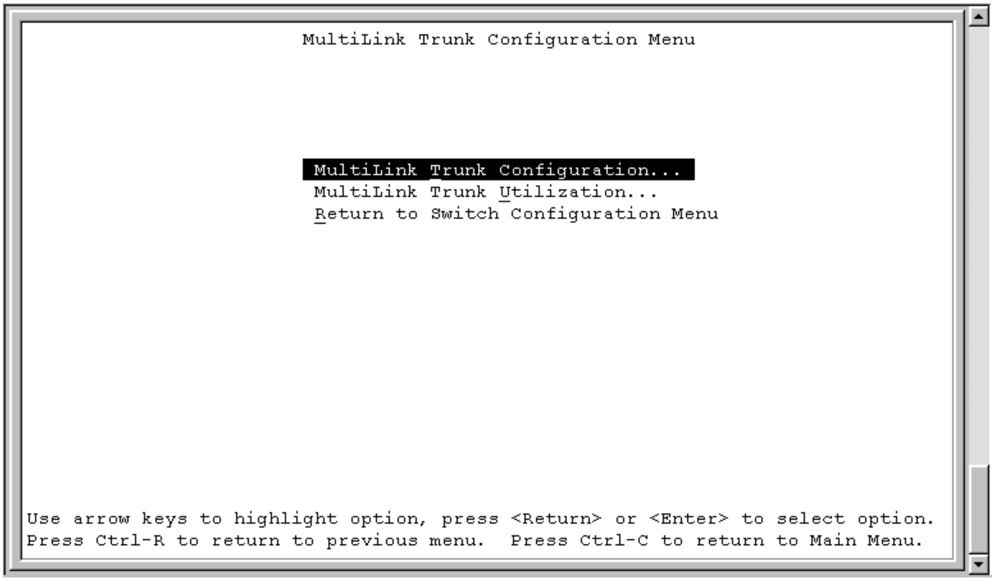
Trunk configuration screen for Switch S1

Switch S1 is set up with five trunk configurations: T1, T2, T3, T4, and T5.

To set up the S1 trunk configuration:

➔ Choose MultiLink Trunk Configuration (or press t) from the MultiLink Trunk Configuration Menu screen (Figure 34).

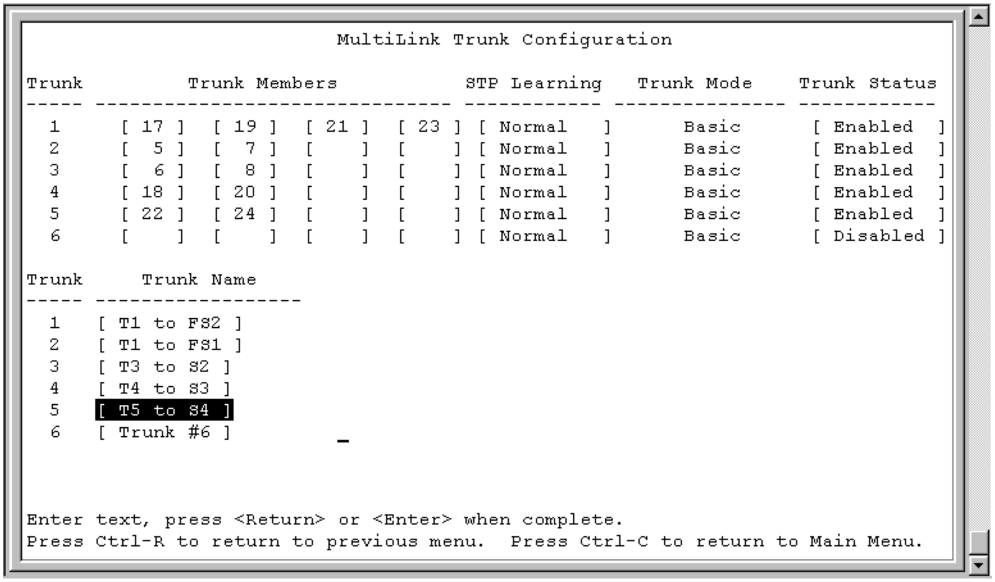
Figure 34 Choosing the MultiLink Trunk Configuration Menu screen



```
                  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.
```

The MultiLink Trunk Configuration Menu screen opens (Figure 35).

Figure 35 MultiLink Trunk Configuration screen



```
                           MultiLink Trunk Configuration

Trunk         Trunk Members           STP Learning   Trunk Mode    Trunk Status
----- ------------------------------- ------------ --------------- ------------
  1     [ 17 ]  [ 19 ]  [ 21 ]  [ 23 ] [ Normal    ]      Basic      [ Enabled  ]
  2     [  5 ]  [  7 ]  [    ]  [    ] [ Normal    ]      Basic      [ Enabled  ]
  3     [  6 ]  [  8 ]  [    ]  [    ] [ Normal    ]      Basic      [ Enabled  ]
  4     [ 18 ]  [ 20 ]  [    ]  [    ] [ Normal    ]      Basic      [ Enabled  ]
  5     [ 22 ]  [ 24 ]  [    ]  [    ] [ Normal    ]      Basic      [ Enabled  ]
  6     [    ]  [    ]  [    ]  [    ] [ Normal    ]      Basic      [ Disabled ]

Trunk     Trunk Name
----- ------------------
  1   [ T1 to FS2 ]
  2   [ T1 to FS1 ]
  3   [ T3 to S2 ]
  4   [ T4 to S3 ]
  5   [ T5 to S4 ]
  6   [ Trunk #6 ]         _



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

Switch S1 is configured as follows:

- **Trunk** (read only) indicates the trunks (1 to 6) that correspond to the switch ports specified in the Trunk Members fields.
- **Trunk Members** indicates the ports that can be configured, in each row, to create the corresponding trunk:
  - — Ports 17, 19, 21, and 23 are assigned as trunk members of trunk 1.
  - — Ports 5 and 7 are assigned as trunk members of trunk 2.
  - — Ports 6 and 8 are assigned as trunk members of trunk 3.
  - — Ports 18 and 20 are assigned as trunk members of trunk 4.
  - — Ports 22 and 24 are assigned as trunk members of trunk 5.

Note: Assigning ports across the 12 port groups is not recommended. For example, do not assign ports 11 and 14 as members of trunk 6.

- **STP Learning** indicates the spanning tree participation setting for each of the trunks:
  - — Trunks 1 through 4 are enabled for Normal STP Learning.
  - — Trunk 5 is enabled for Fast STP Learning.
- **Trunk Mode** (read only) indicates the Trunk Mode for each of the trunks.

  The Trunk Mode field values for trunks 1 to 6are set to Basic. Source MAC addresses are statically 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** indicates the Trunk Status for each of the trunks. When set to Enabled, the configuration settings for that specific trunk are activated.
- **Trunk Name** indicates optional fields for assigning names to the corresponding configured trunks.

  The names chosen for this example provide meaningful information to the user of this switch (for example, S1:T1 to FS2 indicates that Trunk 1, in Switch S1, connects to File Server 2).

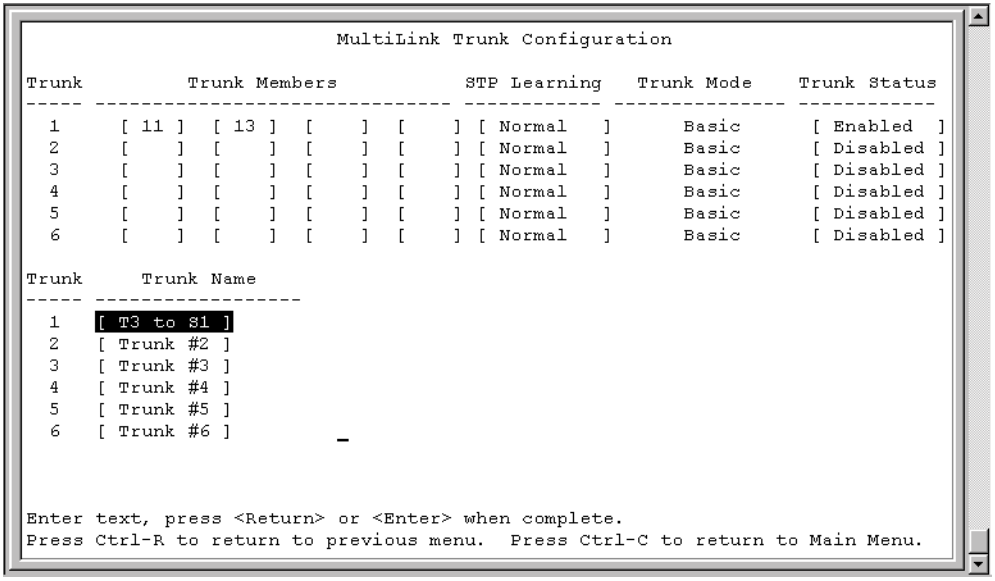
Trunk configuration screen for Switch S2

As shown in Figure 32 on page 77, Switch S2 is set up with two trunk configurations (T2 and T3). Both trunks connect directly to Switch S1.

As in the previous screen examples, to set up a trunk configuration, choose MultiLink Trunk Configuration from the MultiLink Trunk Configuration Menu screen.

Figure 36 shows the MultiLink Trunk Configuration screen for Switch S2.

Figure 36 MultiLink Trunk Configuration screen for Switch S2



```
                          MultiLink Trunk Configuration

Trunk          Trunk Members               STP Learning   Trunk Mode     Trunk Status
----- ------------------------------- ------------ --------------- ------------
  1      [ 11 ]  [ 13 ]  [    ]  [    ]  [ Normal    ]      Basic       [ Enabled  ]
  2      [    ]  [    ]  [    ]  [    ]  [ Normal    ]      Basic       [ Disabled ]
  3      [    ]  [    ]  [    ]  [    ]  [ Normal    ]      Basic       [ Disabled ]
  4      [    ]  [    ]  [    ]  [    ]  [ Normal    ]      Basic       [ Disabled ]
  5      [    ]  [    ]  [    ]  [    ]  [ Normal    ]      Basic       [ Disabled ]
  6      [    ]  [    ]  [    ]  [    ]  [ Normal    ]      Basic       [ Disabled ]

Trunk      Trunk Name
----- ------------------
  1    [ T3 to S1 ]
  2    [ Trunk #2 ]
  3    [ Trunk #3 ]
  4    [ Trunk #4 ]
  5    [ Trunk #5 ]
  6    [ Trunk #6 ]          _



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

Switch S2 is configured as follows:

- **Trunk** (read only) indicates the trunks (1 to 6) that correspond to the switch ports specified in the Trunk Members fields.
- **Trunk Members** indicates the ports that can be configured, in each row, to create the corresponding trunk:
  - — Ports 11 and 13 are assigned as trunk members of trunk 1.
- **STP Learning** indicates the spanning tree participation setting for each of the trunks. Trunks 1 and 2 are enabled for Normal STP Learning.
- **Trunk Mode** (read only) indicates the Trunk Mode for each of the trunks. The Trunk Mode field values for trunks 1 and 2 are set to Basic. Source MAC addresses are statically 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** indicates the Trunk Status for each of the trunks. When set to Enabled, the configuration settings for that specific trunk are activated.

- **Trunk Name** indicates optional fields for assigning names to the corresponding configured trunks.

  The names chosen for this example provide meaningful information to the user of this switch (for example, S2:T2 to S1 indicates that Trunk 1, in Switch S2, connects to Switch 1).

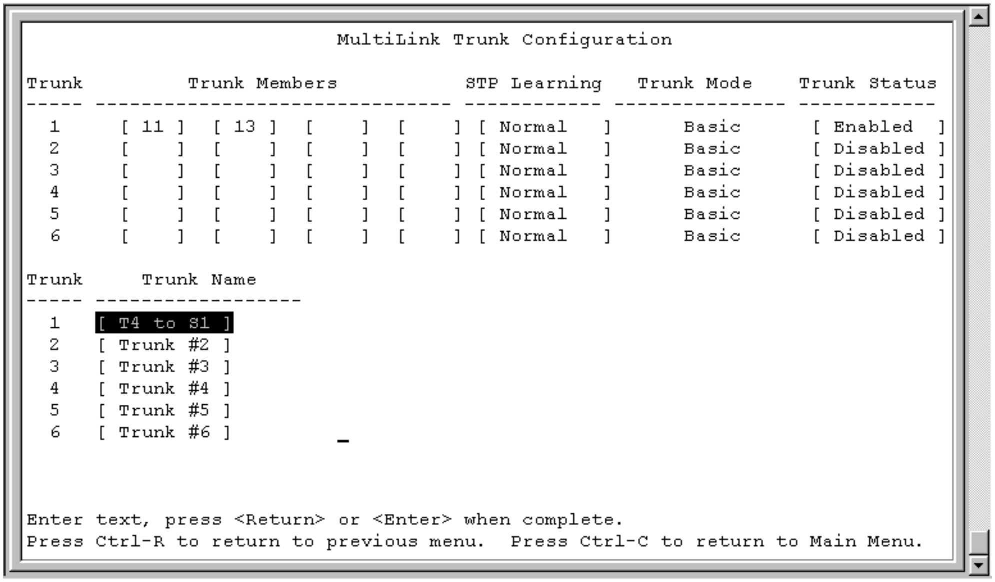
Trunk Configuration screen for Switch S3

As shown in Figure 32 on page 77, Switch S3 is set up with one trunk configuration (T4). This trunk connects directly to Switch S1.

As in the previous screen examples, to set up an interswitch trunk configuration, choose MultiLink Trunk Configuration from the MultiLink Trunk Configuration Menu screen.

Figure 37 shows the MultiLink Trunk Configuration screen for Switch S3.

Figure 37 MultiLink Trunk Configuration screen for Switch S3



```
                          MultiLink Trunk Configuration

Trunk           Trunk Members              STP Learning   Trunk Mode     Trunk Status
----- ------------------------------- ------------ --------------- ------------
  1      [ 11 ]  [ 13 ]  [    ]  [    ] [ Normal    ]      Basic      [ Enabled  ]
  2      [    ]  [    ]  [    ]  [    ] [ Normal    ]      Basic      [ Disabled ]
  3      [    ]  [    ]  [    ]  [    ] [ Normal    ]      Basic      [ Disabled ]
  4      [    ]  [    ]  [    ]  [    ] [ Normal    ]      Basic      [ Disabled ]
  5      [    ]  [    ]  [    ]  [    ] [ Normal    ]      Basic      [ Disabled ]
  6      [    ]  [    ]  [    ]  [    ] [ Normal    ]      Basic      [ Disabled ]

Trunk      Trunk Name
----- ------------------
  1    [ T4 to S1 ]
  2    [ Trunk #2 ]
  3    [ Trunk #3 ]
  4    [ Trunk #4 ]
  5    [ Trunk #5 ]
  6    [ Trunk #6 ]          _


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

Switch S3 is configured as follows:

- **Trunk** (read only) indicates the trunk (1 to 6) that corresponds to the switch ports specified in the Trunk Members fields.
- **Trunk Members** indicates the ports that can be configured, in each row, to create the corresponding trunk.
  - — Ports 11 and 13 are assigned as trunk members of trunk 1.
- **STP Learning** indicates the spanning tree participation setting for each of the trunks. Trunk 1 is enabled for Normal STP Learning.
- **Trunk Mode** (read only) indicates the Trunk Mode for each of the trunks. The Trunk Mode field value for trunk 1 is set to Basic. Source MAC addresses are statically 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** indicates the Trunk Status for each of the trunks. When set to Enabled, the configuration settings for that specific trunk are activated.
- **Trunk Name** indicates optional fields for assigning names to the corresponding configured trunks.

Trunk Configuration screen for Switch S4

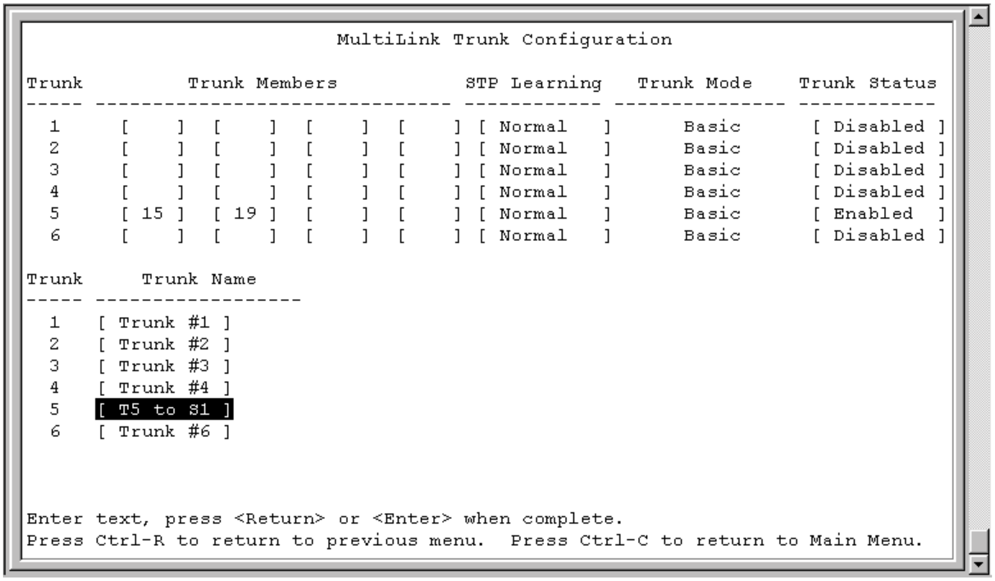
The names chosen for this example provide meaningful information to the user of this switch (for example, S3:T4 to S1 indicates that Trunk 1, in Switch S3, connects to Switch 1).

As shown in Figure 38, Switch S4 is set up with one trunk configuration (T5). This trunk connects directly to Switch S1.

As in the previous screen examples, to set up a trunk configuration, choose MultiLink Trunk Configuration from the MultiLink Trunk Configuration Menu screen.

Figure 38 shows the MultiLink Trunk Configuration screen for Switch S4.

Figure 38 MultiLink Trunk Configuration screen for Switch S4



```
                          MultiLink Trunk Configuration

Trunk          Trunk Members             STP Learning   Trunk Mode     Trunk Status
----- ------------------------------- ------------ --------------- ------------
  1     [    ]  [    ]  [    ]  [    ] [ Normal   ]      Basic       [ Disabled ]
  2     [    ]  [    ]  [    ]  [    ] [ Normal   ]      Basic       [ Disabled ]
  3     [    ]  [    ]  [    ]  [    ] [ Normal   ]      Basic       [ Disabled ]
  4     [    ]  [    ]  [    ]  [    ] [ Normal   ]      Basic       [ Disabled ]
  5     [ 15 ]  [ 19 ]  [    ]  [    ] [ Normal   ]      Basic       [ Enabled  ]
  6     [    ]  [    ]  [    ]  [    ] [ Normal   ]      Basic       [ Disabled ]

Trunk     Trunk Name
----- ------------------
  1   [ Trunk #1 ]
  2   [ Trunk #2 ]
  3   [ Trunk #3 ]
  4   [ Trunk #4 ]
  5   [ T5 to S1 ]
  6   [ Trunk #6 ]



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

Switch S4 is configured as follows:

- **Trunk** (read only) indicates the trunk (1 to 6) that corresponds to the switch ports specified in the Trunk Members fields.
- **Trunk Members** indicates the ports that can be configured, in each row, to create the corresponding trunk.
  - — Ports 15 and 19 are assigned as trunk members of trunk T5.
- **STP Learning** indicates the spanning tree participation setting for each of the trunks. Trunk 1 is enabled for Normal STP Learning.
- **Trunk Mode** (read only) indicates the Trunk Mode for each of the trunks. The Trunk Mode field value for trunk 1 is set to Basic. Source MAC addresses are statically 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** indicates the Trunk Status for each of the trunks. When it is set to Enabled, the configuration settings for that specific trunk are activated.
- **Trunk Name** indicates optional fields for assigning names to the corresponding configured trunks.

The names chosen for this example provide meaningful information to the user (for example, S4:T5 to S1 indicates that Trunk 1, in Switch S4, connects to Switch 1).

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, "Spanning tree considerations for MultiLink Trunks" on page 87.
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.

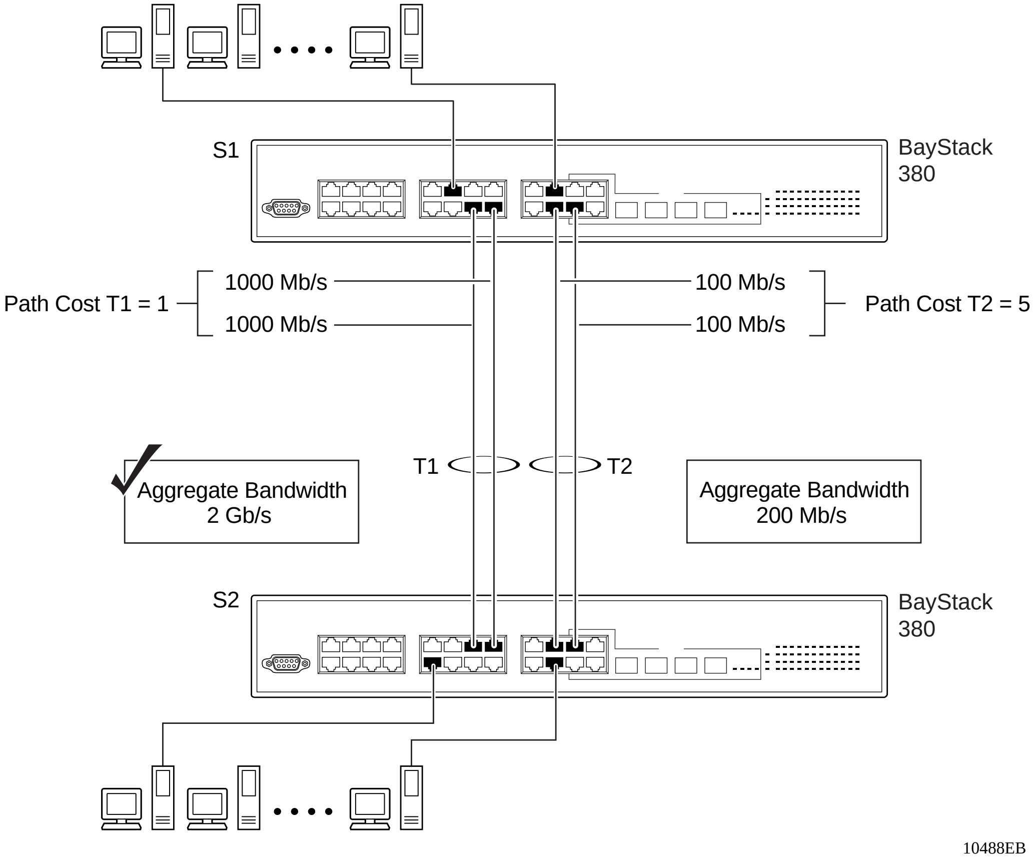
   Ensure that the chosen switch ports are set to Enabled, using either the Port Configuration screen (see "Port Configuration screen" on page 131) or network management.

   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" on page 87).
5. Consider how existing VLANs will be affected by the addition of a trunk.
6. After completing the above steps, see "MultiLink Trunk Configuration screen" on page 138 for screen examples and field descriptions that will help you configure your MultiLink Trunks.

Spanning tree considerations for MultiLink Trunks

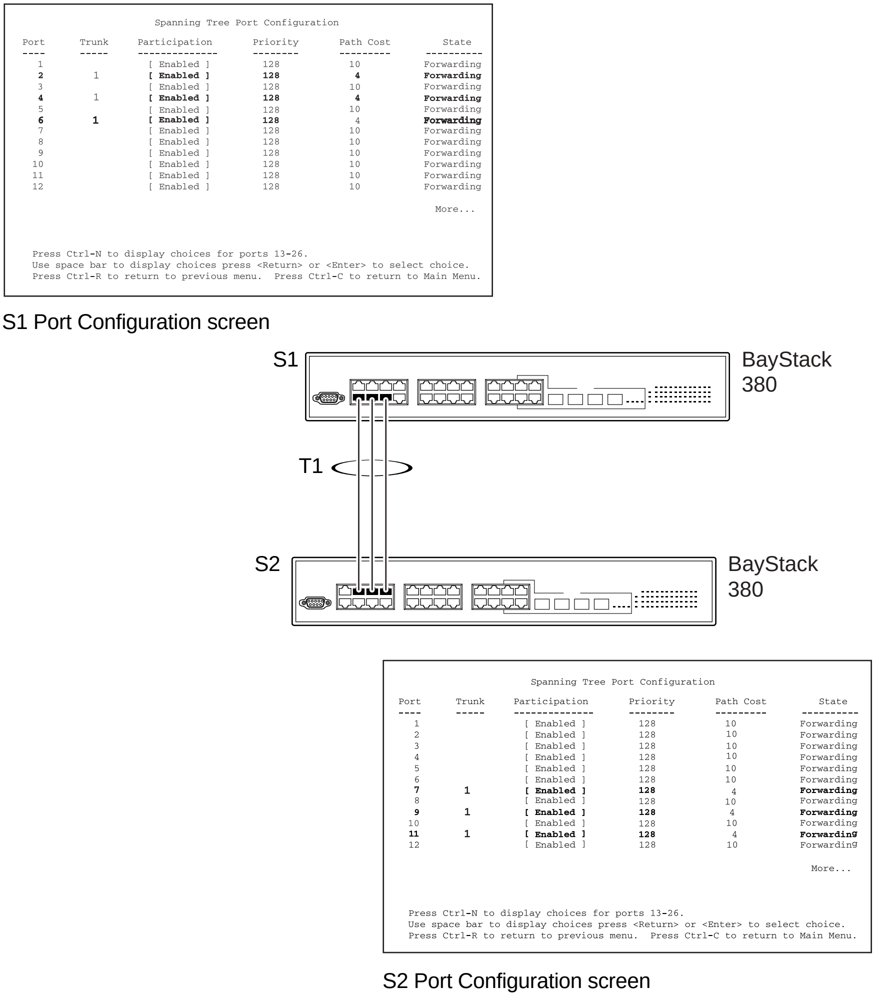
The spanning tree Path Cost parameter is recalculated based on the aggregate bandwidth of the trunk. For example, Figure 39 shows a four-port trunk (T1) with two port members operating at an aggregate bandwidth of 2.2 Gb/s, with a comparable Path Cost of 4. When the Path Cost calculations for both trunks are equal, the software chooses the trunk with the larger aggregate bandwidth (T1) to determine the most efficient path.

Figure 39 Path Cost arbitration example



The switch can also detect trunk member ports that are physically misconfigured. For example, in Figure 40, 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 40 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

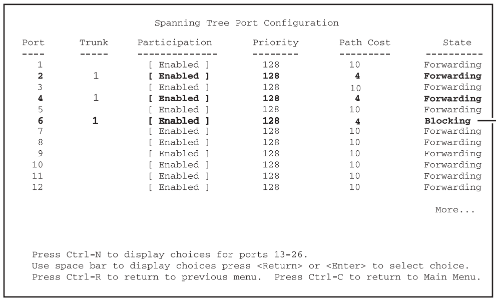
```
                         Spanning Tree Port Configuration

 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

10489EA

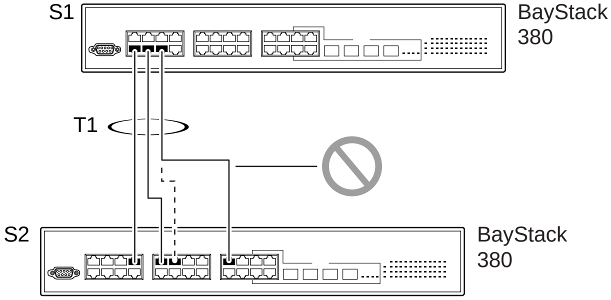
If Switch S2’s trunk member port 7 is physically disconnected and then reconnected to port 9, the Spanning Tree Port Configuration screen for Switch S1 changes to show port 6 in the Blocking state (Figure 41).

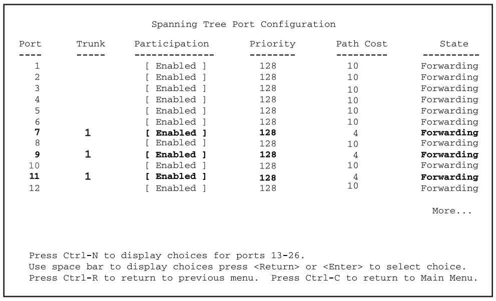
Figure 41 Example 2: detecting a misconfigured port



```
                    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

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 about using the MultiLink Trunking feature, see “MultiLink Trunk Configuration Menu screen” on page 136.

See also Appendix C, “Quick configuration for MultiLink Trunking,” on page 199 for a configuration flowchart that can help you use this feature.

Port mirroring

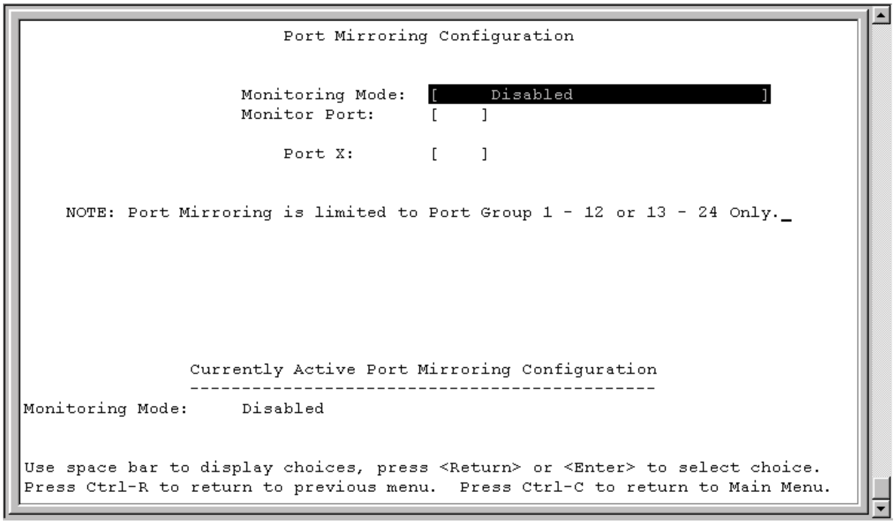
You can designate one of your switch ports to monitor ingress traffic on a single specified switch port (port-based).

Figure 38 provides a sample Port Mirroring Configuration screen. Note that the displayed screens do not show all of the screen prompts that precede some actions.

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 ]
```

Figure 42 Port Mirroring Configuration port-based screen example



```
                              Port Mirroring Configuration


                      Monitoring Mode:   [     Disabled                ]
                      Monitor Port:      [    ]

                          Port X:        [    ]


     NOTE: Port Mirroring is limited to Port Group 1 - 12 or 13 - 24 Only._






                     Currently Active Port Mirroring Configuration
                     ---------------------------------------------
Monitoring 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.
```

Chapter 3
Using the console interface

This chapter describes how to configure and manage the BayStack 380 Switch using the menu-driven console interface (CI).

This chapter covers the following topics:

- "Accessing the CI menus and screens," next
- "Using the CI menus and screens" on page 94
- "Main menu" on page 96

Accessing the CI menus and screens

You can access the CI menus and screens locally through a console terminal attached to your BayStack 380 Switch, remotely through a dial-up modem connection, or in-band through a Telnet session (see "Console port" on page 26). You can connect your console cable into any BayStack 380 Switch.

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.

Using the CI menus and screens

The CI menus and screens provide options that allow you to configure and manage BayStack 380 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 options allow you to toggle among several possible values; other options allow you to set or modify a parameter.

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.

To toggle between values in a form:

1 Use the spacebar to highlight the value.

2 Press [Enter].

To clear a string field:

1 Position the cursor in the string field.

2 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.

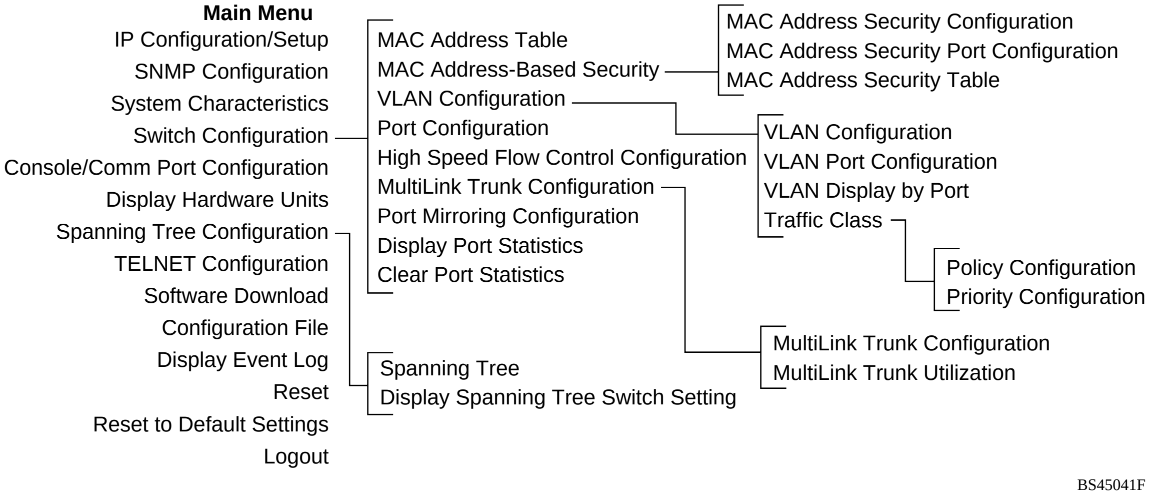
Press [Backspace] to delete entered text.

Options that appear in brackets (for example, [Enabled]) are user-settable options.

Screen fields and descriptions

Figure 43 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 43 Map of console interface screens



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.

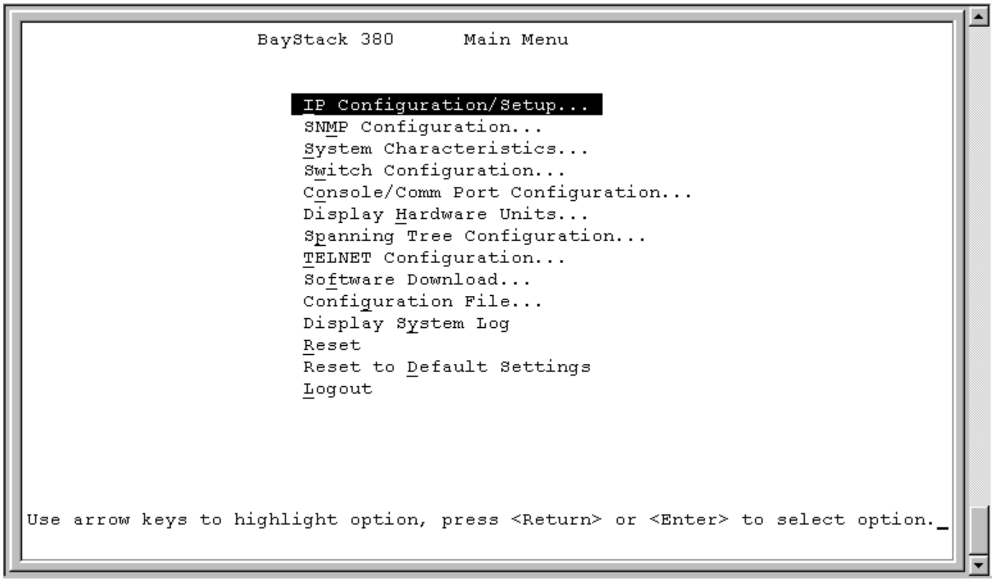
Note: The field values shown in the CI screens in this section are provided as examples only.

Main menu

This section describes the options available from the CI main menu (Figure 44). 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 44 Console interface main menu



```
                    BayStack 380       Main Menu


                      IP Configuration/Setup...
                      SNMP Configuration...
                      System Characteristics...
                      Switch Configuration...
                      Console/Comm Port Configuration...
                      Display Hardware Units...
                      Spanning Tree Configuration...
                      TELNET Configuration...
                      Software Download...
                      Configuration File...
                      Display System Log
                      Reset
                      Reset to Default Settings
                      Logout




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

Table 8 describes the CI main menu options.

Table 8 Console interface main menu options

Option	Description
IP Configuration/ Setup...	Displays the IP Configuration/Setup screen (see "IP Configuration/Setup screen" on page 99). This screen allows you to set or modify IP configuration parameters.
SNMP Configuration...	Displays the SNMP Configuration screen (see "SNMP Configuration screen" on page 104). 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 106). This screen allows you to view switch characteristics, including number of resets, power status, hardware and firmware version, and MAC address. This screen also contains three user-configurable fields: sysContact, sysName, and sysLocation.
Switch Configuration...	Displays the Switch Configuration Menu screen (see "Switch Configuration Menu screen" on page 108). This menu provides the following configuration options: MAC Address Table, MAC Address-Based Security, VLAN Configuration, Port Configuration, MultiLink Trunk Configuration, Port Mirroring Configuration, Display Port Statistics, Clear All Port Statistics, and Display System Log.
Console/Comm Port Configuration...	Displays the Console/Comm Port Configuration screen (see "Console/Comm Port Configuration screen" on page 149). This screen allows you to configure and modify the console/Comm port parameters, including the console port speed and password settings for the switch operation.
Spanning Tree Configuration...	Displays the Spanning Tree Configuration Menu (see "Spanning Tree Configuration Menu screen" on page 155). This menu provides the following options: Spanning Tree Port Configuration, Display Spanning Tree Switch Settings.
TELNET Configuration...	Displays the TELNET Configuration screen (see "TELNET Configuration screen" on page 162). This screen allows you to set your switch to enable a user at a remote console terminal to communicate with the BayStack 380 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 a standalone switch.
Software Download...	Displays the Software Download screen (see "Software Download screen" on page 164). This screen allows you to revise the BayStack 380 Switch software image that is located in nonvolatile flash memory.
Configuration File	Displays the Configuration File Download/Upload screen (see "Configuration File Download/Upload screen" on page 168). This screen allows you to store your switch configuration parameters on a TFTP server. You can retrieve the configuration parameters for automatically configuring a replacement switch with the same configuration when required.

Table 8 Console interface main menu options (continued)

Option	**Description**
Display System Log	Displays the System Log screen (see "System Log screen" on page 147).
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: • 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 BayStack 380 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: • 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 BayStack 380 Switch main menu.
	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].
	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。
Logout	Allows a user in a Telnet session or a user working at a password-protected console terminal to terminate the session.

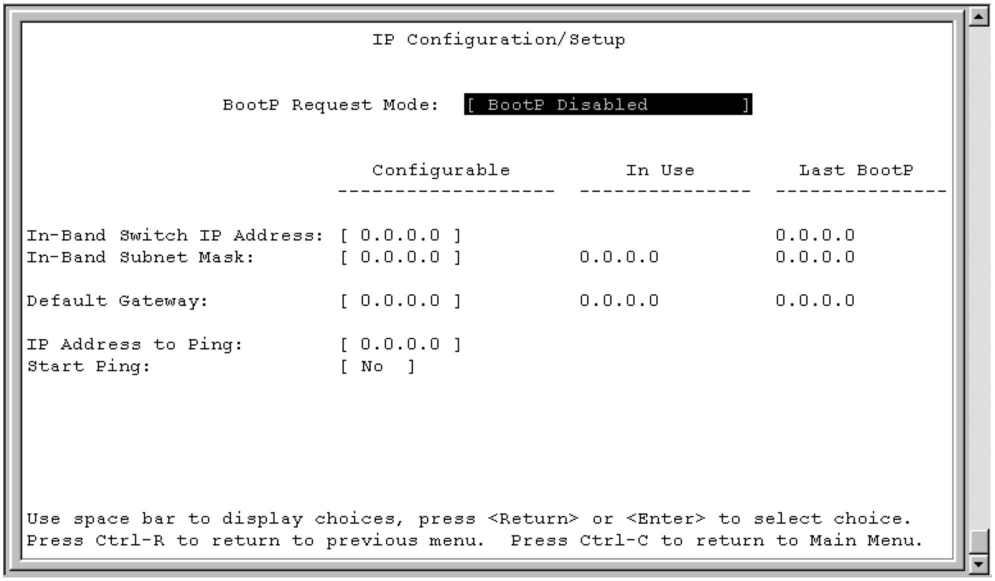
IP Configuration/Setup screen

The IP Configuration/Setup screen (Figure 45) allows you to set or modify the BayStack 380 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 45 IP Configuration/Setup screen



```
                                   IP Configuration/Setup


                BootP Request Mode:   [ BootP Disabled          ]


                                   Configurable          In Use         Last BootP
                                ------------------    --------------   --------------

In-Band Switch IP Address:   [ 0.0.0.0 ]                               0.0.0.0
In-Band Subnet Mask:         [ 0.0.0.0 ]              0.0.0.0          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 9 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 102 for more information.)

Table 9 IP Configuration/Setup screen fields

Field	Description
BootP Request Mode	One of four modes of operation for BootP. (See "Choosing a BootP request mode" on page 102 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 Switch IP Address	The in-band IP address of the 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 **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 9 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.	
	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.

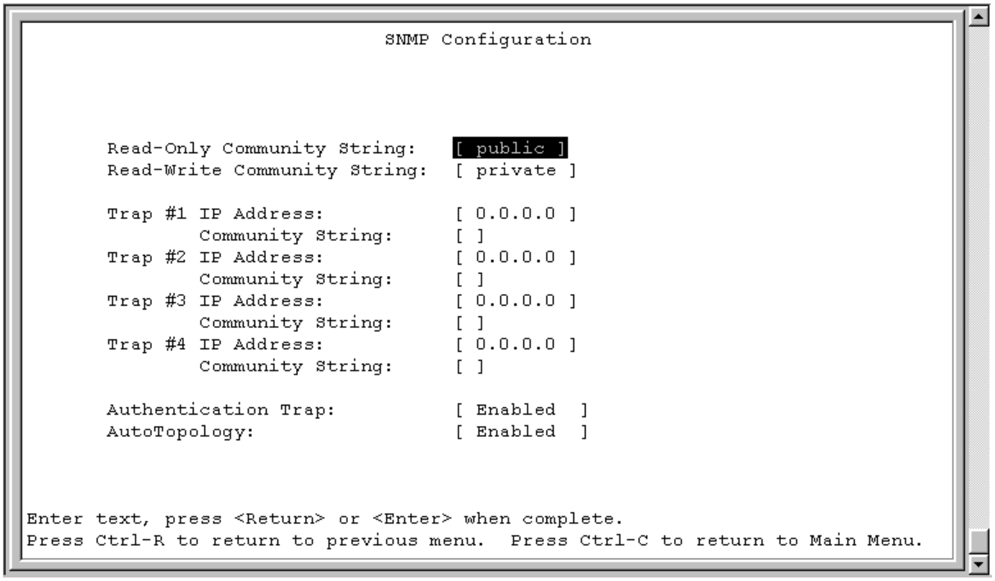
SNMP Configuration screen

The SNMP Configuration screen (Figure 46) 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 46 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 10 describes the SNMP Configuration screen fields.

Table 10 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[1]	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

[1] **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.**

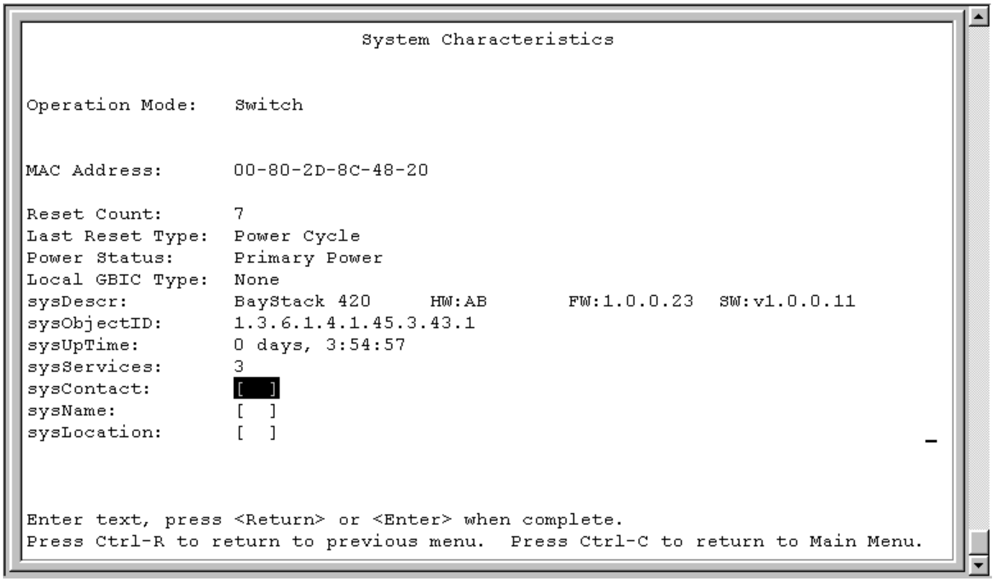
System Characteristics screen

The System Characteristics screen (Figure 47) 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 47 System Characteristics screen



```
                              System Characteristics


Operation Mode:    Switch


MAC Address:       00-80-2D-8C-48-20

Reset Count:       7
Last Reset Type:   Power Cycle
Power Status:      Primary Power
Local GBIC Type:   None
sysDescr:          BayStack 420     HW:AB       FW:1.0.0.23   SW:v1.0.0.11
sysObjectID:       1.3.6.1.4.1.45.3.43.1
sysUpTime:         0 days, 3:54:57
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 11 describes the System Characteristics screen fields.

Table 11 System Characteristics screen fields

Field	Description
Operation Mode	Read-only field that indicates the operation mode of the switch.
MAC Address	The MAC address of the switch
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
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.
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[1]
sysName	A name that uniquely identifies the switch. Default Value Zero-length string Range Any ASCII string of up to 56 printable characters[1]
sysLocation	The physical location of the switch. Default Value Zero-length string Range Any ASCII string of up to 56 printable characters

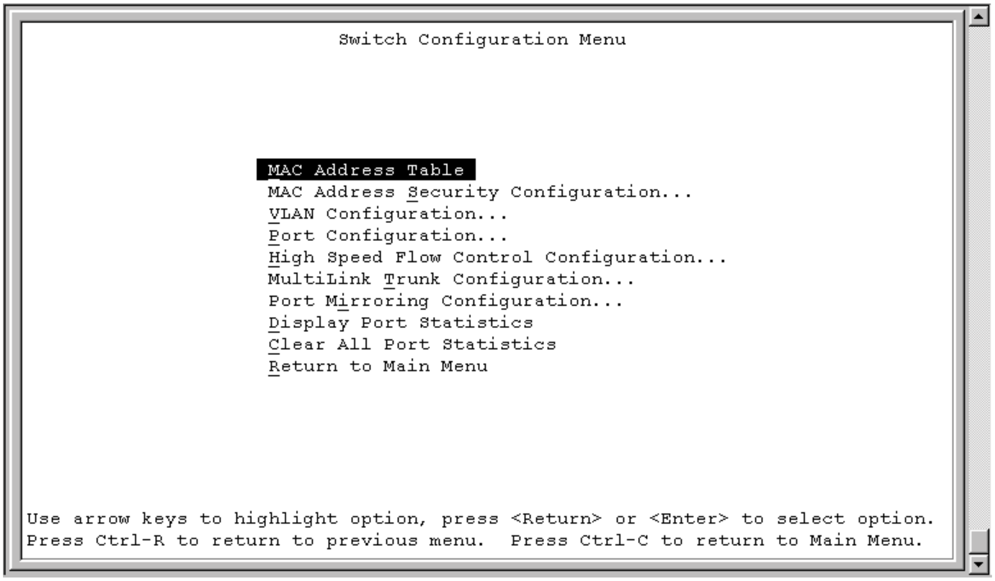
[1] Although this field can be set to up to 255 characters from a Network Management Station (NMS), only 56 characters are displayed on the console terminal.

Switch Configuration Menu screen

The Switch Configuration Menu screen (Figure 48) allows you to set or modify your switch configuration.

Choose Switch Configuration (or press w) from the main menu to open the Switch Configuration Menu screen (Table 12).

Figure 48 Switch Configuration Menu screen



```
                    Switch Configuration Menu



              MAC Address Table
              MAC Address Security Configuration...
              VLAN Configuration...
              Port Configuration...
              High Speed Flow Control Configuration...
              MultiLink Trunk Configuration...
              Port Mirroring Configuration...
              Display Port Statistics
              Clear All Port Statistics
              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 12 describes the Switch Configuration Menu options.

Table 12 Switch Configuration Menu options

Option	Description
MAC Address Table	Displays the MAC Address Table screen (see "MAC Address Table screen" on page 110). 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 111). 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, and MAC Address Security Table. This menu allows you to enable and disable security features on the port and trunk levels.
VLAN Configuration...	Displays the VLAN Configuration Menu (see "VLAN Configuration Menu screen" on page 120). This menu provides the following options: VLAN Configuration, VLAN Port Configuration, VLAN Display by Port, MAC-SA, and Return to Switch Configuration Menu screen. This menu allows you to create and modify VLANs.
Port Configuration...	Displays the Port Configuration screen (see "Port Configuration screen" on page 131). This screen allows you to configure a specific switch port, or all switch ports.
High Speed Flow Control Configuration...	Displays the High Speed Flow Control Configuration screen.
MultiLink Trunk Configuration...	Displays the MultiLink Trunk Configuration Menu (see "MultiLink Trunk Configuration Menu screen" on page 136). This menu provides the following options: MultiLink Trunk Configuration, MultiLink Trunk Utilization, and Return to Switch Configuration Menu screen. 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 142). This screen allows you to designate a single switch port as a traffic monitor for one specific port.
Display Port Statistics	Displays the Port Statistics screen (see "Port Statistics screen" on page 144). This screen allows you to view detailed information about any switch port.
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: • Choose one of the following: • Yes, to clear all port statistics for all switch ports • No, to abort the option

MAC Address Table screen

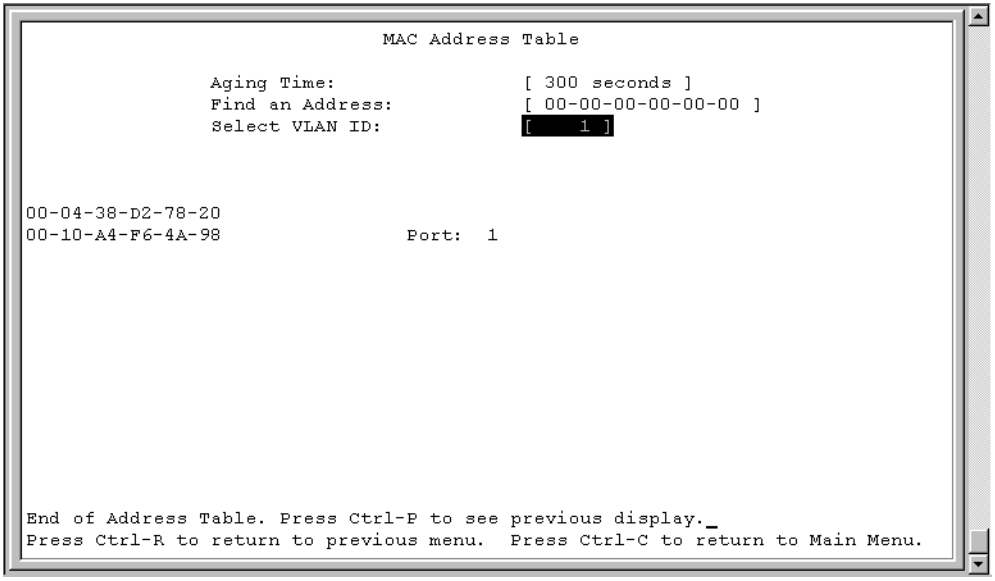
The MAC Address Table screen (Figure 49) allows you to view MAC addresses that the switch has discovered or to search for a specific MAC address.

The MAC Address Table screen also operates in conjunction with the Port Mirroring Configuration screen. When you configure a switch for MAC address-based port mirroring, you can use the MAC Address Table screen to find an address and enter the address directly from this screen. You can enter addresses from either screen, but you must return to the Port Mirroring Configuration screen to activate the feature (see "Port Mirroring Configuration screen" on page 142). When you add a security MAC Address, it is added to the MAC Address Table screen (Figure 49).

Choose MAC Address Table (or press m) from the Switch Configuration Menu screen to open the MAC Address Table screen (Figure 49).

Note: This screen does not refresh dynamically to show new entries. To refresh the screen, press [Ctrl]-R to return to the previous menu.

Figure 49 MAC Address Table screen



```
                              MAC Address Table

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


00-04-38-D2-78-20
00-10-A4-F6-4A-98                Port:   1











End of Address Table. Press Ctrl-P to see previous display._
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 13 describes the MAC Address Table screen fields.

Table 13 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
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

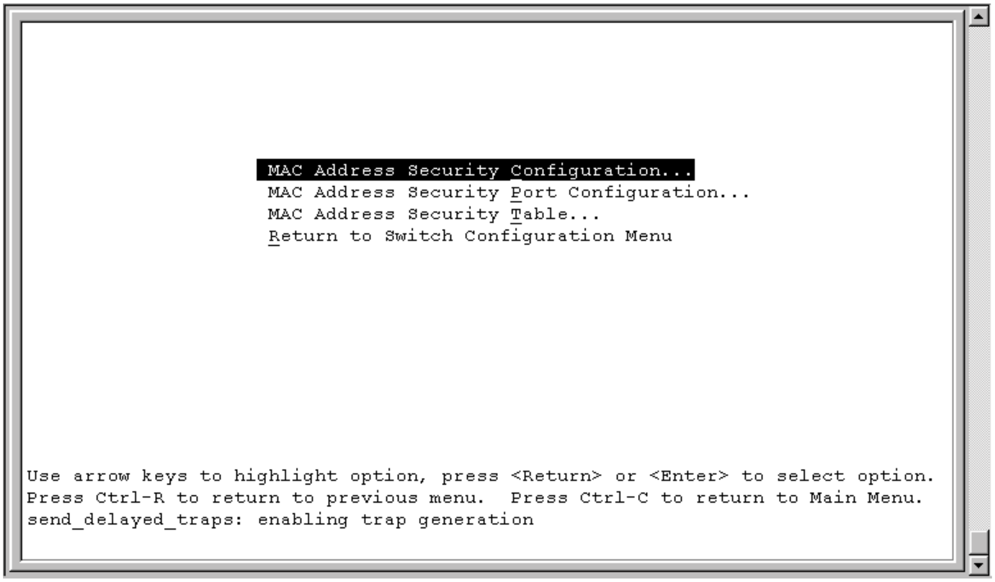
MAC Address Security Configuration Menu screen

The MAC Address Security Configuration Menu screen (Figure 50) allows you to specify a range of system responses to unauthorized network access to your switch. 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 or a single port that is specified in a list, for example, 1, 6, 9, etc. You must also include the MAC address of any router connected to any secure ports.

To open the MAC Address Security Configuration screen:

➔ Choose MAC Address Security Configuration from the Switch Configuration Menu.

Figure 50 MAC Address Security Configuration Menu screen



```
                    MAC Address Security Configuration...
                    MAC Address Security Port Configuration...
                    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.
send_delayed_traps: enabling trap generation
```

Table 14 describes the MAC Address Security Configuration Menu options.

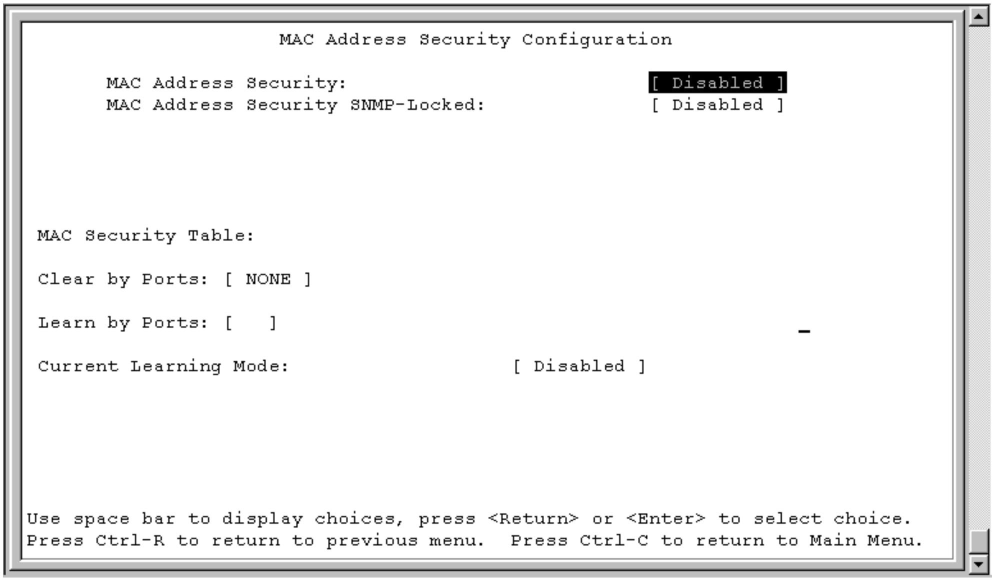
Table 14 MAC Address Security Configuration Menu options

Option	Description
MAC Address Security Configuration...	Displays the MAC Address Security Configuration screen (see “Table 14 describes the MAC Address Security Configuration Menu options.” on page 112). 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 115”). This screen allows you to Enable or Disable MAC Security for each port.
MAC Address Security Table...	Displays the MAC Address Security Table screen (see “MAC Address Security Table screens” on page 117). This screen allows you to specify the MAC addresses that are allowed to access the switch.
Return to Switch Configuration Menu...	Exits the MAC Address Security Configuration Menu screen and displays the Switch Configuration Menu screen.

The MAC Address Security Configuration screen (Figure 51) allows you to enable or disable the MAC address security feature.

Choose MAC Address Security Configuration from the MAC Address Security Configuration Menu to open the MAC Address Security Configuration screen.

Figure 51 MAC Address Security Configuration screen



```
                    MAC Address Security Configuration

      MAC Address Security:                           [ Disabled ]
      MAC Address Security SNMP-Locked:               [ Disabled ]




 MAC Security Table:

 Clear by Ports: [ NONE ]

 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 15 describes the MAC Address Security Configuration screen fields.

Table 15 MAC Address Security Configuration screen fields

Field	Description
MAC Address Security	When this field is set to enabled, the switch 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 switch detects a source MAC address that is not an allowed member, the switch drops the packets. 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. 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 117). 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, 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 Learning in Progress. You cannot include any of the port values whose security is enabled. You must disable port security for that port. Default NONE Range NONE, ALL, a port number list (for example, 1, 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 Disabled, Enabled

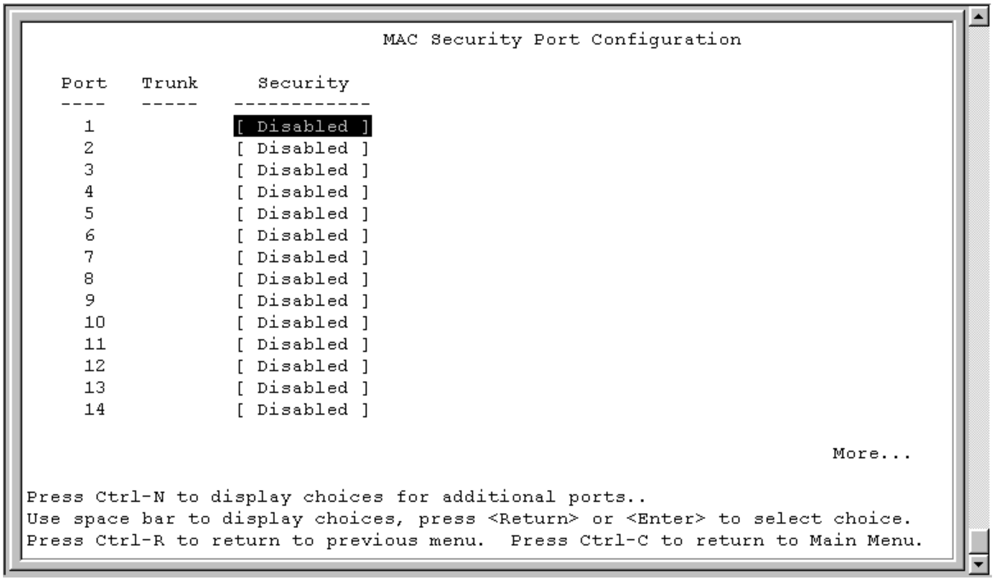
MAC Address Security Port Configuration screen

The MAC Address Security Port Configuration screens (Figure 52 and Figure 53) 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:

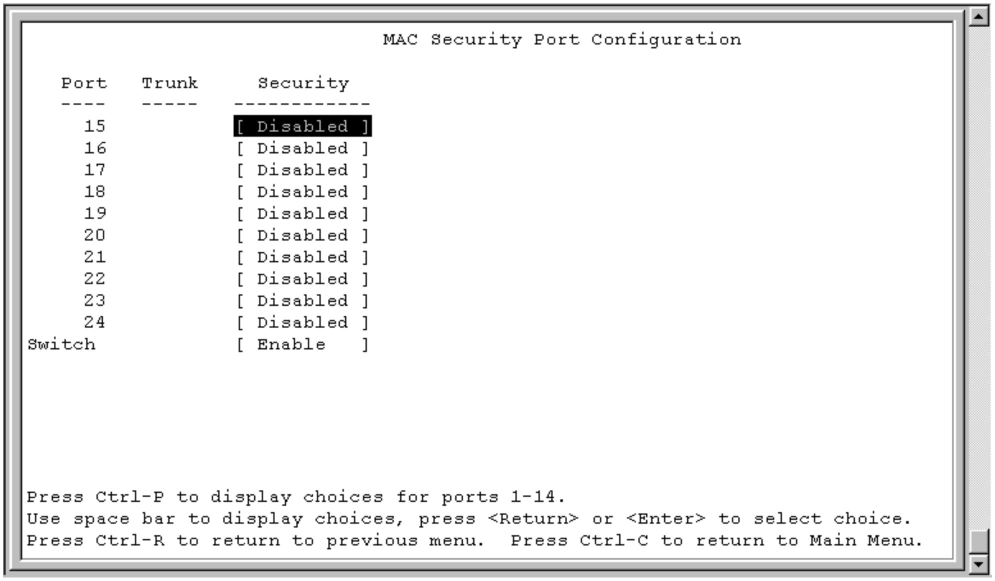
➔ Choose MAC Address Security Port Configuration from the MAC Address Security Configuration Menu.

Figure 52 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 53 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   ]






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 16 describes the MAC Security Port Configuration screen fields.

Table 16 MAC Security Port Configuration screen fields

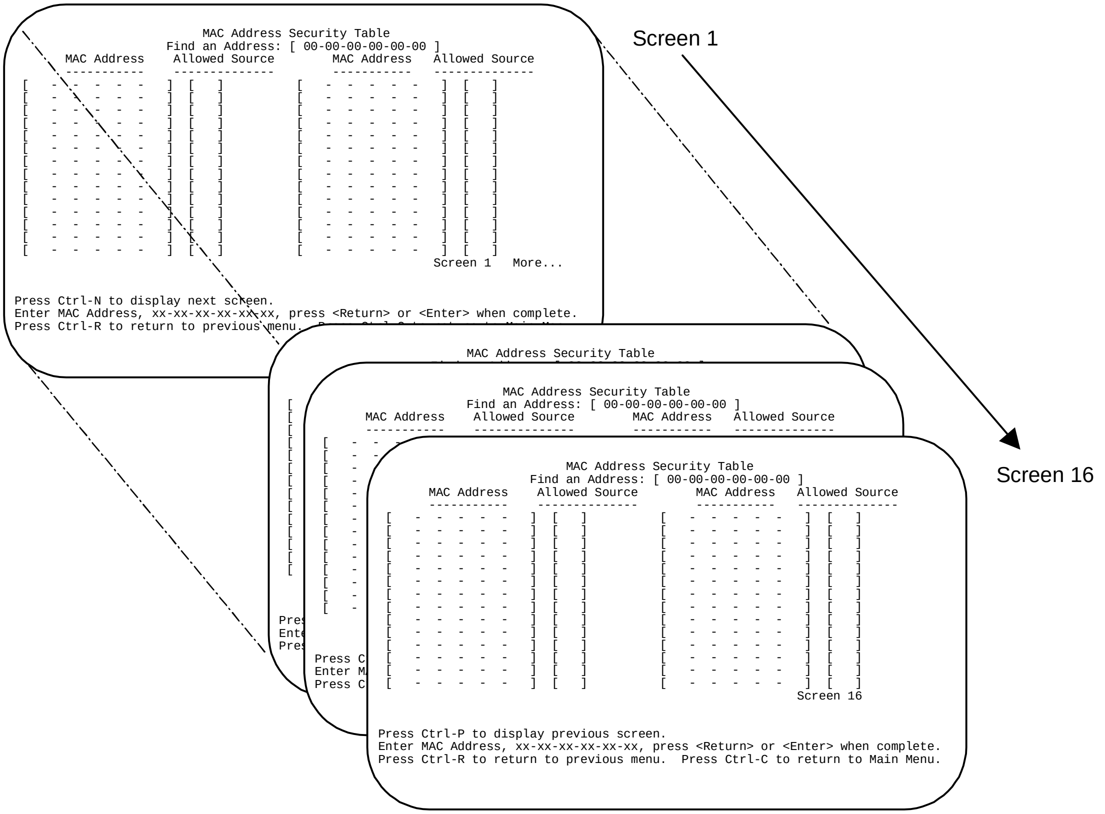
Field	Description
Port	Displays a numbered port list.
Trunk	Displays the trunk number if the port is a member of that trunk. Default blank field
Security	This field value determines whether or not security is enabled or disabled on the port level. This field must be enabled for a port to be a member of MAC Security. Default Disabled Range Disabled, Enabled

MAC Address Security Table screens

The MAC Address Security Table screens allow you specify one port for each MAC address. 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 54) that you can use to create up to 448 MAC address entries (28 per screen).

Figure 54 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.
```

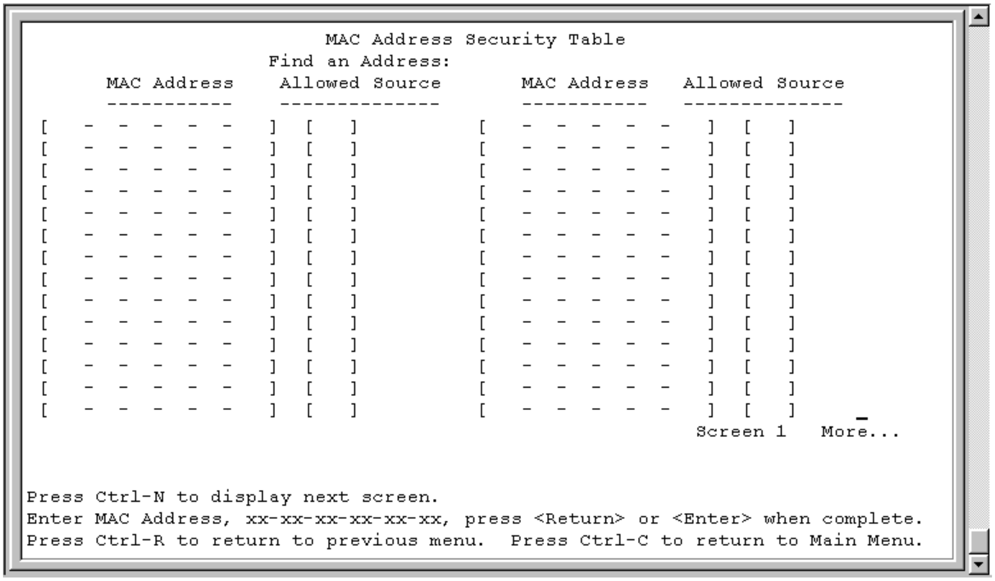
```
                    MAC Address Security Table
```

```
                    MAC Address Security Table
               Find an Address: [ 00-00-00-00-00-00 ]
     MAC Address    Allowed Source        MAC Address    Allowed Source
     -----------    --------------        -----------    --------------
```

```
                    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 55).

Figure 55 MAC Address Security Table screen



```
                          MAC Address Security Table
                     Find an Address:
       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.  Press Ctrl-C to return to Main Menu.
```

Table 17 describes the MAC Address Security Table screen fields.

Table 17 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 port 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. 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[1] and broadcast addresses are not allowed).
Allowed Source	Allows you to specify a port that each MAC address is allowed to access. The options for the Allowed Source field include a single port number or a port list value. The port security for the allowed sources should be enabled for the security to be effective.	
	Default	- (Blank field)
	Range	A single unit/port or a port list value (for example, 1, 6, etc.).

[1] Multicast address -- Note that the first octet of any Multicast address will always be an odd number.

VLAN Configuration Menu screen

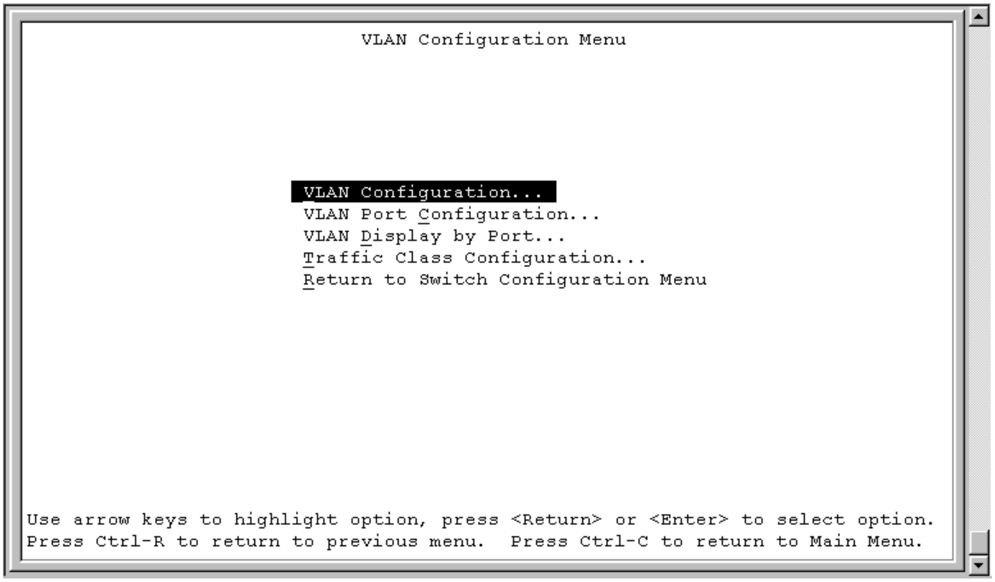
The VLAN Configuration Menu screen (Figure 56) allows you to select the appropriate screen to configure up to 64 VLANs.

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.

To open the VLAN Configuration Menu:

➔ Choose VLAN Configuration (or press v) from the Switch Configuration Menu screen.

Figure 56 VLAN Configuration Menu screen



```
                          VLAN Configuration Menu




                      VLAN Configuration...
                      VLAN Port Configuration...
                      VLAN Display by Port...
                      Traffic Class Configuration...
                      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 18 describes the VLAN Configuration Menu options.

Table 18 VLAN Configuration Menu options

Option	Description
VLAN Configuration...	Displays the VLAN Configuration screen (see "VLAN Configuration screen" on page 121). This screen allows you to set up VLAN workgroups.
VLAN Port Configuration...	Displays the VLAN Port Configuration screen (see "VLAN Port Configuration screen" on page 124). 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 126).
Return to Switch Configuration Menu	Exits the VLAN Configuration Menu screen and displays the Switch Configuration Menu screen.
Traffic Class	Specifies the traffic class, either policy or priority.

VLAN Configuration screen

The VLAN Configuration screen (Figure 57) allows you to create and assign VLAN port memberships to 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) manually, or use Auto PVID to assign it automatically.

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 as VLAN port members of one or more VLANs.

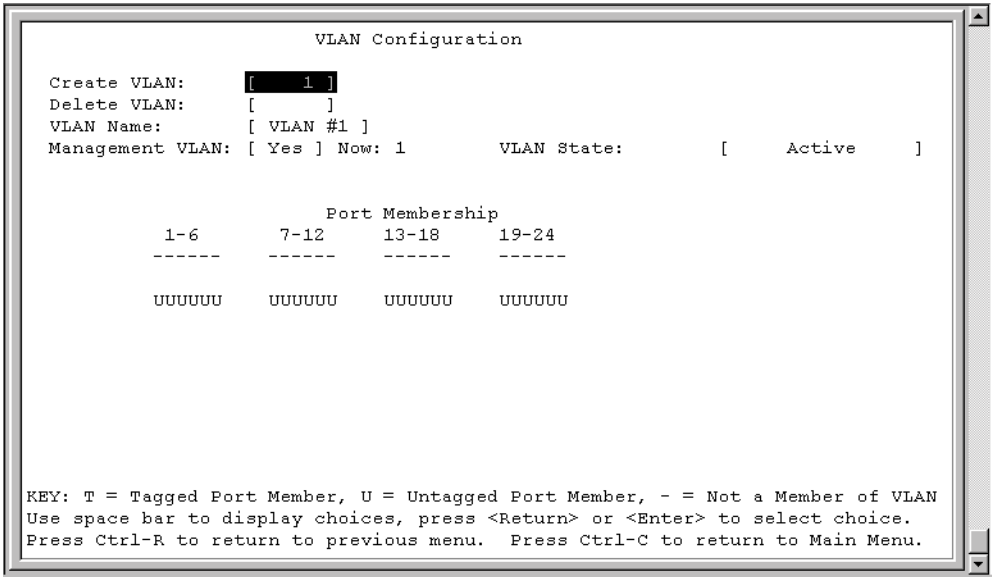
You can add or remove port members from a VLAN in accordance with the IEEE 802.1Q tagging rules. See "IEEE 802.1Q VLAN workgroups" on page 55 for a description of important terms used with 802.1Q VLANs.

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 57 VLAN Configuration screen



```
                         VLAN Configuration

 Create VLAN:       [      1 ]
 Delete VLAN:       [        ]
 VLAN Name:         [ VLAN #1 ]
 Management VLAN:   [ Yes ] Now: 1        VLAN State:        [     Active     ]


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

          UUUUUU    UUUUUU    UUUUUU    UUUUUU






KEY: T = Tagged Port Member, U = Untagged Port Member, - = Not a Member of 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 19 describes the VLAN Configuration screen fields.

Table 19 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 64 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 19 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 “IEEE 802.1Q VLAN workgroups” on page 55 for more information.
	Default blank field 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
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 port memberships to VLANs. The ports can be configured in one or more VLANs. To set this field, you must set the VLAN State field to Active. 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 125). 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 (-).

Table 19 VLAN Configuration screen fields (continued)

Field	Description
	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 GBIC installed in the Uplink Module slot. Default U (All ports are assigned as untagged members of VLAN 1.) Range U, T, and -

VLAN Port Configuration screen

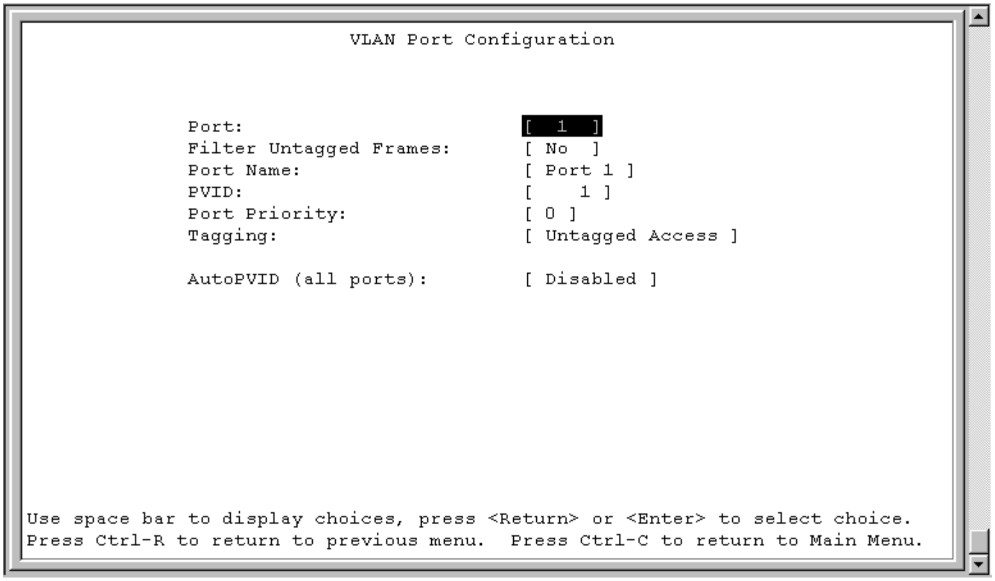
The VLAN Port Configuration screen (Figure 58) allows you to configure specified switch ports with the appropriate PVID/VLAN association that enables the creation of VLAN broadcast domains (see "Shared servers" on page 63 for more information about setting up VLAN broadcast domains).

You can configure specified switch ports to filter (discard) all received untagged frames (see "IEEE 802.1Q VLAN workgroups" on page 55).

To open the VLAN Port Configuration screen.

➔ Choose VLAN Port Configuration (or press c) from the VLAN Configuration Menu screen.

Figure 58 VLAN Port Configuration screen



```
                         VLAN Port Configuration


              Port:                          [   1   ]
              Filter Untagged Frames:        [ No   ]
              Port Name:                     [ Port 1 ]
              PVID:                          [     1 ]
              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.
```

Table 20 describes the VLAN Port Configuration screen fields.

Table 20 VLAN Port Configuration screen fields

Field	Description
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 Untagged Frames	Sets this port to filter (discard) all received untagged frames. Default No Range No, Yes
Port Name	The default port name assigned to this port. You can change this field to any name that is up to 16 characters long. Default 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

Table 20 VLAN Port Configuration screen fields (continued)

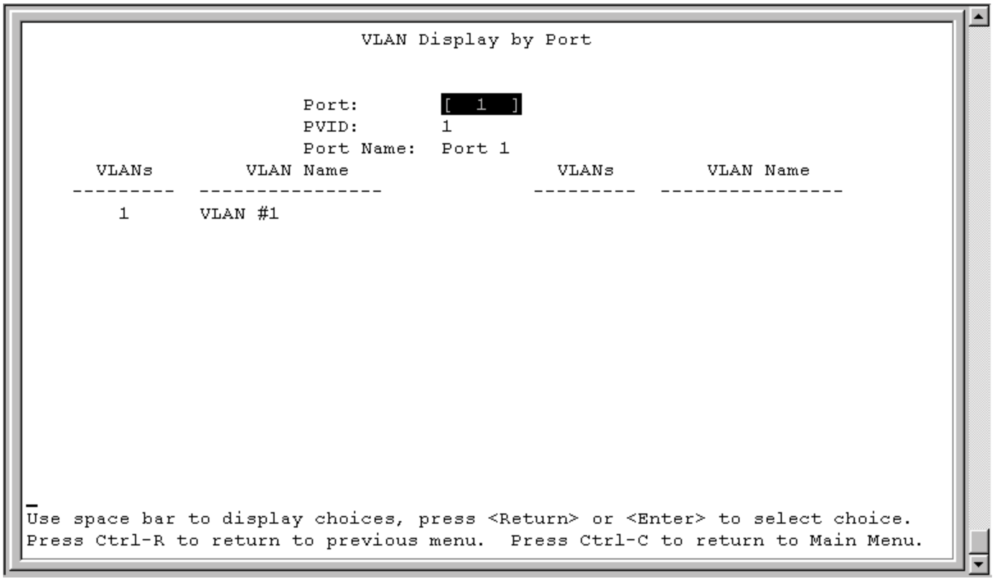
Field	Description
Tagging	Allows you to assign VLAN Port Membership tagging options to this port, as follows: • Untagged Access: Any VLAN that this port is a member of *will not* be 802.1Q tagged. Default Untagged Access Range Untagged Access, Tagged Trunk
Auto PVID	Specifies the port VLAN identifier (PVID) automatically

VLAN Display by Port screen

The VLAN Display by Port screen (Figure 59) 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 59 VLAN Display by Port screen



```
                          VLAN Display by Port


                    Port:           [  1  ]
                    PVID:           1
                    Port Name:      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 21 describes the VLAN Display by Port screen fields.

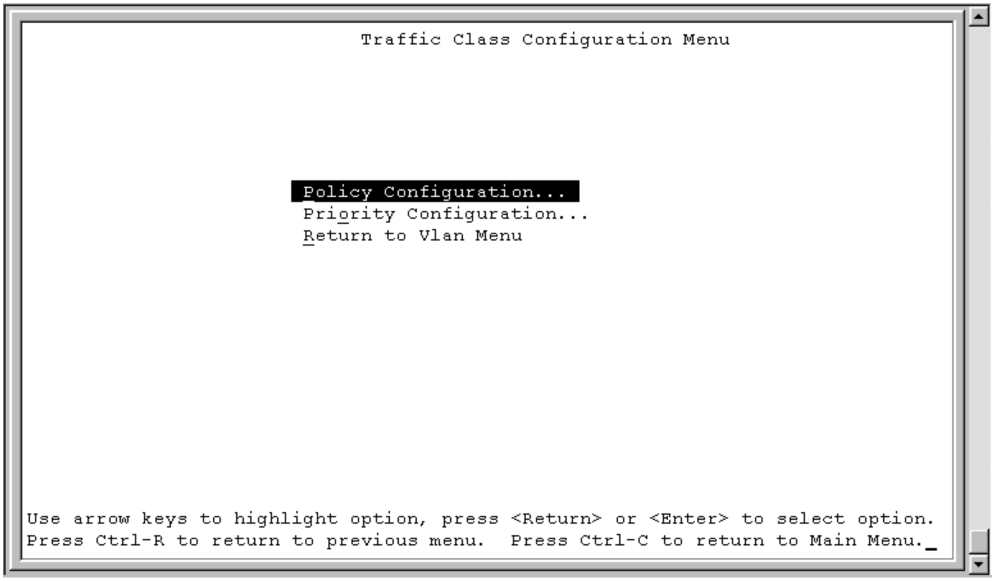
Table 21 VLAN Display by Port screen fields

Field	Description
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.

VLAN Traffic Class Configuration screen

The VLAN Traffic Class Configuration screen allows you to specify policy or priority configuration.

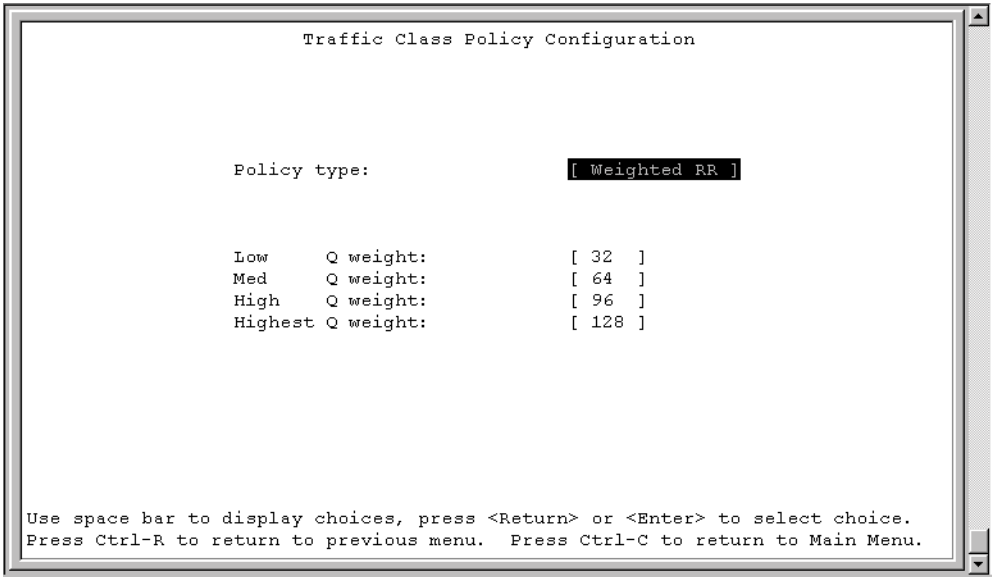
Figure 60 VLAN Traffic Class Configuration screen



```
                    Traffic Class Configuration Menu



                Policy Configuration...
                Priority Configuration...
                Return to Vlan 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._
```

The Policy Configuration screen prioritizes the order in which a switch forwards packets, on a per-port basis. BayStack 380 provides 4 transmission queues. Frames are assigned to one of these queues on the basis of the user-priority using a traffic class table. The table indicates the traffic class that is assigned to the frame for each possible user-priority value.

Figure 61 Traffic Class Policy Configuration

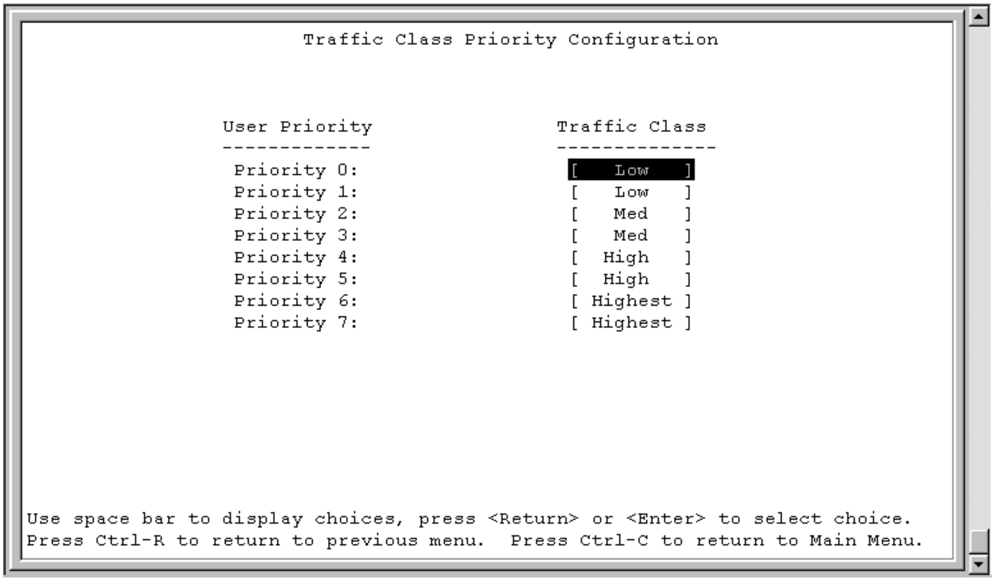


```
                         Traffic Class Policy Configuration




                  Policy type:                  [ Weighted RR ]



                  Low     Q weight:             [ 32  ]
                  Med     Q weight:             [ 64  ]
                  High    Q weight:             [ 96  ]
                  Highest Q weight:             [ 128 ]








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 22 Policy Configuration screen fields

Field	**Description**
Policy Type	Specifies the type of policy. There are 2 types: weighted round robin, and strict.
Weighted RR	Each queue is assigned a weight. This value indicates how many packets may be transmitted out of the queue before the next highest queue is serviced. Control may transfer to the next highest queue even though the higher priority queues have not emptied To determine the percentage of bandwidth allocated to each queue, add the total weight and then divide each queue weight by that value. This formula works only when all queues are fully utilized.
Strict	The strict dequeuing algorithm empties the higher priority queues first Once the higher priority queue is empty, then the next priority queue is serviced. If a packet comes out of a higher priority queue transmission out of the lower priority queue is suspended until transmission from the higher priority queues finish transmitting.
Q Weight	.This value indicates how many packets may be transmitted out of the queue before the next highest queue is serviced.

Figure 62 Traffic Class Priority Configuration



```
                         Traffic Class Priority Configuration



                User Priority                   Traffic Class
                -------------                   --------------
                 Priority 0:                     [   Low    ]
                 Priority 1:                     [   Low    ]
                 Priority 2:                     [   Med    ]
                 Priority 3:                     [   Med    ]
                 Priority 4:                     [  High    ]
                 Priority 5:                     [  High    ]
                 Priority 6:                     [ Highest  ]
                 Priority 7:                     [ Highest  ]









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 Priority Configuration screen fields

Field	**Description**
User Priority	Specifies the user priority.
Traffic Class	Specifies the associated traffic class from low to highest

Port Configuration screen

The Port Configuration screen (Figures 63 and 64) 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).

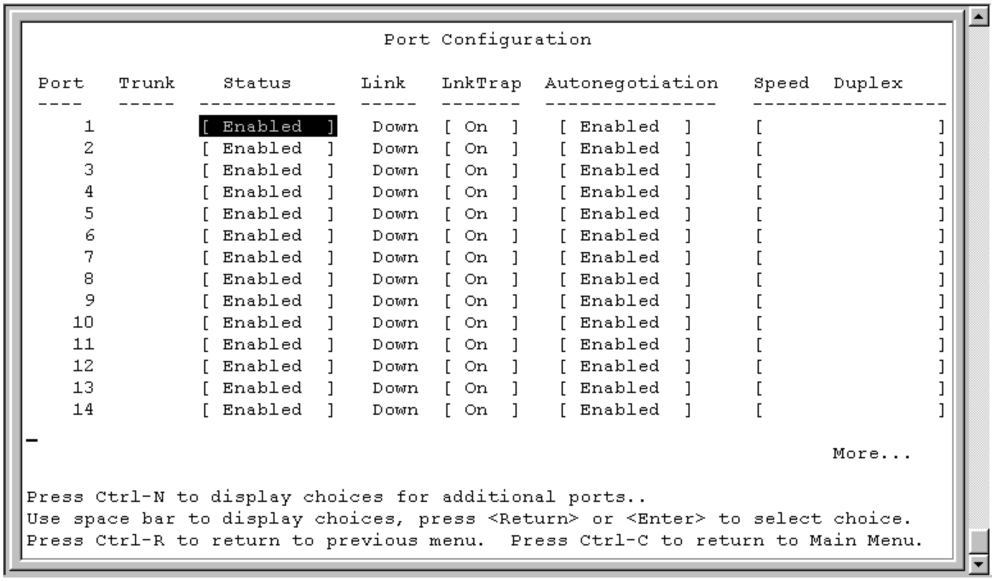
You can disable switch ports that are trunk members; however, the screen prompts for verification of the request before completing the action. Choosing [Yes] disables the port and removes it from the trunk.

Note: The Autonegotiation fields, the Speed fields, and the Duplex fields are independent of MultiLink Trunking, VLANs, and the STP.

To open the Port Configuration screen:

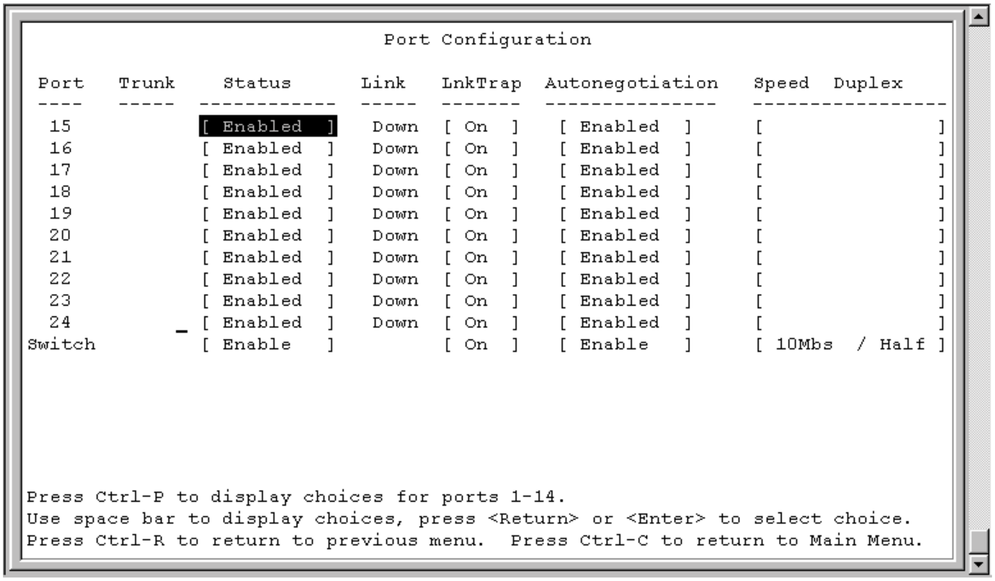
➔ Choose Port Configuration (or press p) from the Switch Configuration Menu screen.

Figure 63 Port Configuration screen (1 of 2)



```
                                Port Configuration

 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  ]      Down   [ On  ]    [ Enabled   ]      [                ]
    6            [ Enabled  ]      Down   [ On  ]    [ Enabled   ]      [                ]
    7            [ Enabled  ]      Down   [ On  ]    [ Enabled   ]      [                ]
    8            [ Enabled  ]      Down   [ On  ]    [ Enabled   ]      [                ]
    9            [ Enabled  ]      Down   [ On  ]    [ Enabled   ]      [                ]
   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 64 Port Configuration screen (2 of 2)



```
                               Port Configuration

 Port    Trunk     Status      Link    LnkTrap  Autonegotiation    Speed  Duplex
 ----    -----  ------------   -----   -------  ---------------    ----------------
  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  ]    Down   [ On  ]   [ Enabled  ]      [                ]
  23            [ Enabled  ]    Down   [ On  ]   [ Enabled  ]      [                ]
  24          _ [ Enabled  ]    Down   [ On  ]   [ Enabled  ]      [                ]
Switch          [ 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.
```

Table 24 describes the Port Configuration screen fields.

Table 24 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.
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 136).
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.

Table 24 Port Configuration screen fields (continued)

Field	**Description**
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 1000 Mb/s in full-duplex mode. This field is disabled for all fiber optic ports. Default Value Enabled Range Enabled, Disabled
Speed/Duplex[1]	Allows you to manually configure any port to support an Ethernet speed of 10 Mb/s 100 Mb/s, in half- or full-duplex mode, or 1000 Mb/s in full-duplex mode. This field is set (by default) to 1000 Mb/s, full-duplex for Gigabit ports only. Default Value 1000Mbs/Full (when Autonegotiation is Disabled) Range 10Mbs/Half, 10Mbs/Full, 100Mbs/Half, 100Mbs/Full, and 1000 Mb/s in full-duplex mode.

[1] Fiber optic ports can only be set to 100 Mb/s/Half or 100 Mb/s Full.

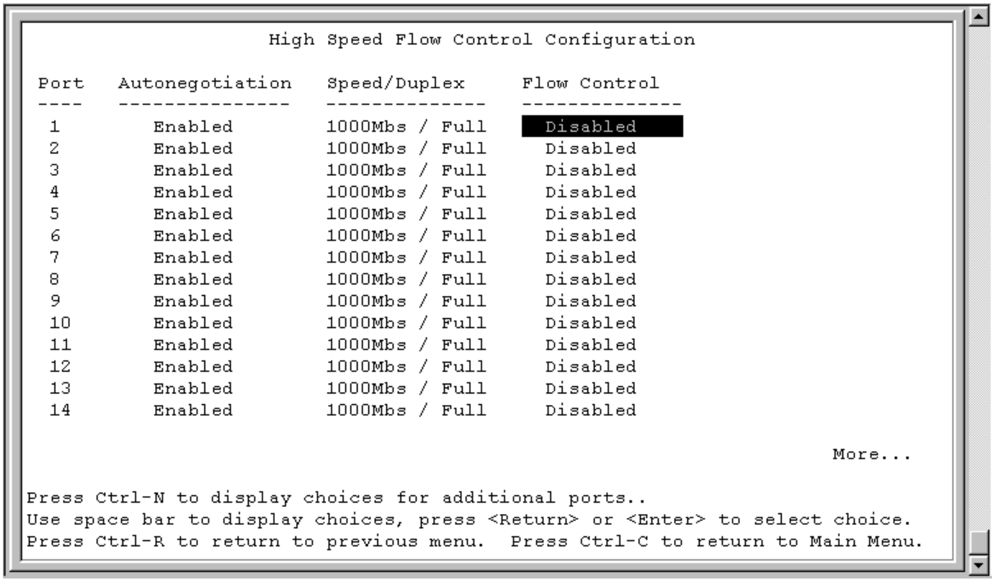
High Speed Flow Control Configuration screen

The High Speed Flow Control Configuration screen (Figure 65) allows you to set the port parameters for the Gigabit Ethernet Interface.

Note: The GBIC module does not need to be installed to configure the port.

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 65 High Speed Flow Control Configuration



```
                   High Speed Flow Control Configuration

 Port    Autonegotiation    Speed/Duplex      Flow Control
 ----    ---------------    --------------    --------------
  1         Enabled         1000Mbs / Full      Disabled
  2         Enabled         1000Mbs / Full      Disabled
  3         Enabled         1000Mbs / Full      Disabled
  4         Enabled         1000Mbs / Full      Disabled
  5         Enabled         1000Mbs / Full      Disabled
  6         Enabled         1000Mbs / Full      Disabled
  7         Enabled         1000Mbs / Full      Disabled
  8         Enabled         1000Mbs / Full      Disabled
  9         Enabled         1000Mbs / Full      Disabled
  10        Enabled         1000Mbs / Full      Disabled
  11        Enabled         1000Mbs / Full      Disabled
  12        Enabled         1000Mbs / Full      Disabled
  13        Enabled         1000Mbs / Full      Disabled
  14        Enabled         1000Mbs / Full      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.
```

Table 25 describes the High Speed Flow Control Configuration screen fields.

Table 25 High Speed Flow Control Configuration screen fields

Field	Description
Port	Allows you to select the port number to view or configure. To view or configure another port, type its unit number and press [Enter], or press the spacebar to toggle the port numbers.
Autonegotiation	When enabled, the port only advertises support for 1000 Mb/s operation, in full-duplex mode. Note: Autonegotiation can be changed only in the Port Configuration screen. Default Value Enabled Range Enabled, Disabled
Speed/Duplex	Specifies the speed and duplexity mode (read only) and whether full or not. Note: The speed can be changed in the Port Configuration screen.
Flow Control	Allows you to control traffic and avoid congestion on the Gigabit port. Two modes are available (see "Choosing a high speed flow control mode," next, for details about the two modes). The Flow Control field can be configured only when you set the Autonegotiation field value to Disabled and the speed to 1000M/bs/full duplex. Default Value Disabled Range Disabled, Symmetric, Asymmetric

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 BayStack 380 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.

Note: For high speed flow control, the BayStack 380 must be connected to a device that is IEEE802.3x compliant.

Symmetric mode

This mode allows the ports and their link partner to send flow control *pause* frames to each other.

When a pause frame is received (by either the 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 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 port is disabled from transmitting pause frames to its link partner. Use this mode when the port is connected to a buffered repeater device.

MultiLink Trunk Configuration Menu screen

The MultiLink Trunk Configuration Menu screen (Figure 66) 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).

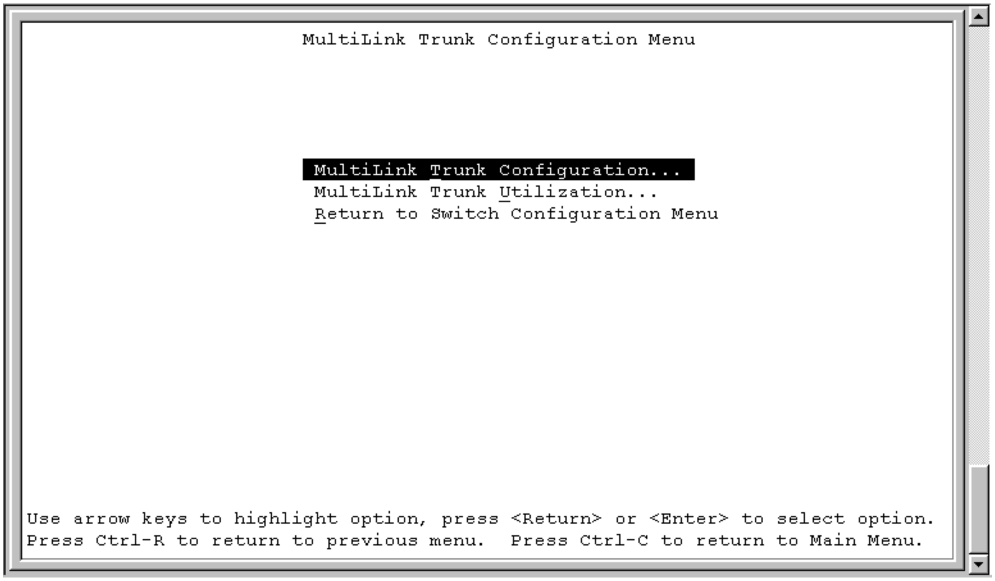
You can monitor the bandwidth usage for the trunk member ports within each trunk. For more information about configuring MultiLink Trunks, see “MultiLink Trunks” on page 74.

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 66 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 26 describes the MultiLink Trunk Configuration Menu options.

Table 26 MultiLink Trunk Configuration Menu options

Option	Description
MultiLink Trunk Configuration...	Displays the MultiLink Trunk Configuration screen (Figure 67). This screen allows you to configure up to six MultiLink Trunks within a switch configuration. You can group up to four switch ports together to form each trunk.
MultiLink Trunk Utilization...	Displays the MultiLink Trunk Utilization screen (Figure 68 and Figure 69). This screen allows you to monitor the bandwidth utilization of the configured trunks.
Return to Switch Configuration Menu	Exits the MultiLink Trunk Configuration Menu screen and displays the Switch Configuration Menu screen.

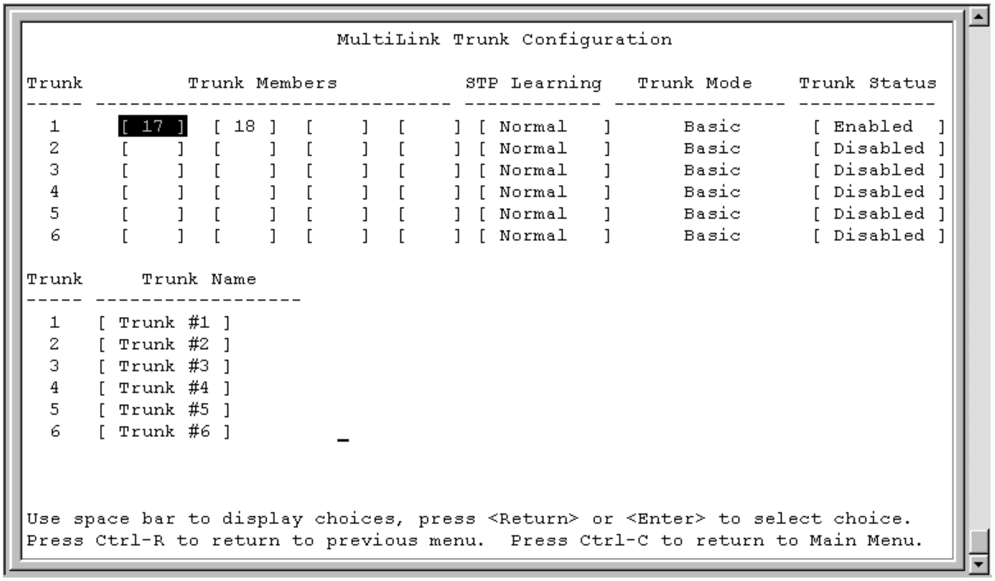
MultiLink Trunk Configuration screen

The MultiLink Trunk Configuration screen (Figure 67) allows you to configure up to six trunks in a switch.

To open the MultiLink Trunk Configuration screen:

➔ Choose Trunk Configuration (or press t) from the MultiLink Trunk Configuration Menu screen.

Figure 67 MultiLink Trunk Configuration screen



```
                           MultiLink Trunk Configuration

Trunk         Trunk Members           STP Learning   Trunk Mode     Trunk Status
----- ------------------------------- ------------ --------------- ------------
  1     [ 17 ]  [ 18 ]  [    ]  [    ] [ Normal   ]      Basic      [ Enabled  ]
  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 27 describes the MultiLink Trunk Configuration screen fields.

Table 27 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 (Port)	The Trunk Members column contains fields in each row that can be configured to create the corresponding trunk. Each switch port can only be a member of a single trunk. The appropriate trunk number for each trunk member configured within this field is shown adjacent to the corresponding switch port in the following screens: Port Configuration screen, and Spanning Tree Configuration screen. Default Value blank field 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).

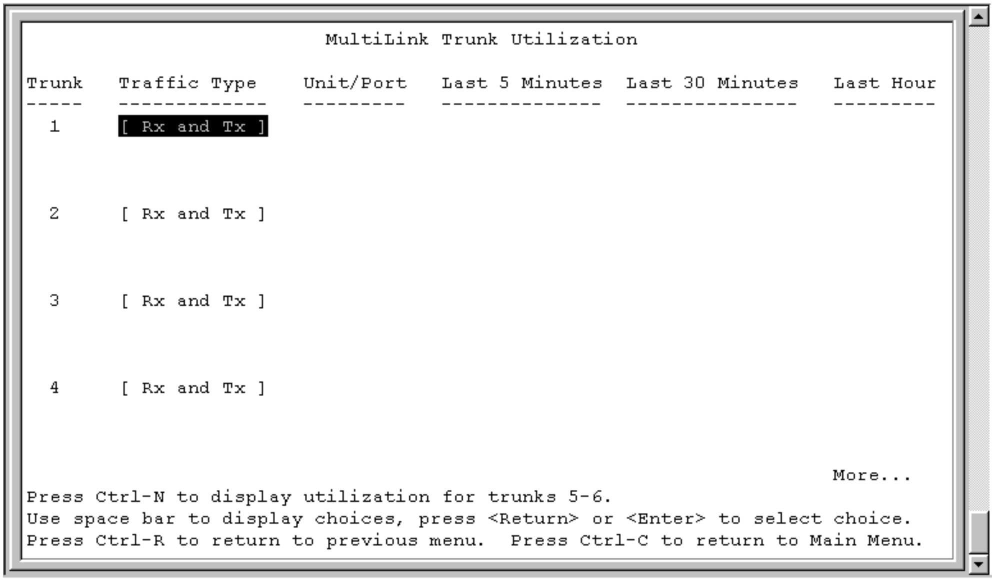
MultiLink Trunk Utilization screen

The MultiLink Trunk Utilization screen (Figure 68 and Figure 69) allows you to monitor the percentage of bandwidth used by configured trunk members. You can choose the type of traffic to monitor.

Figure 68 shows an *example* of bandwidth utilization rates for the trunk member ports configured in Figure 67. 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.

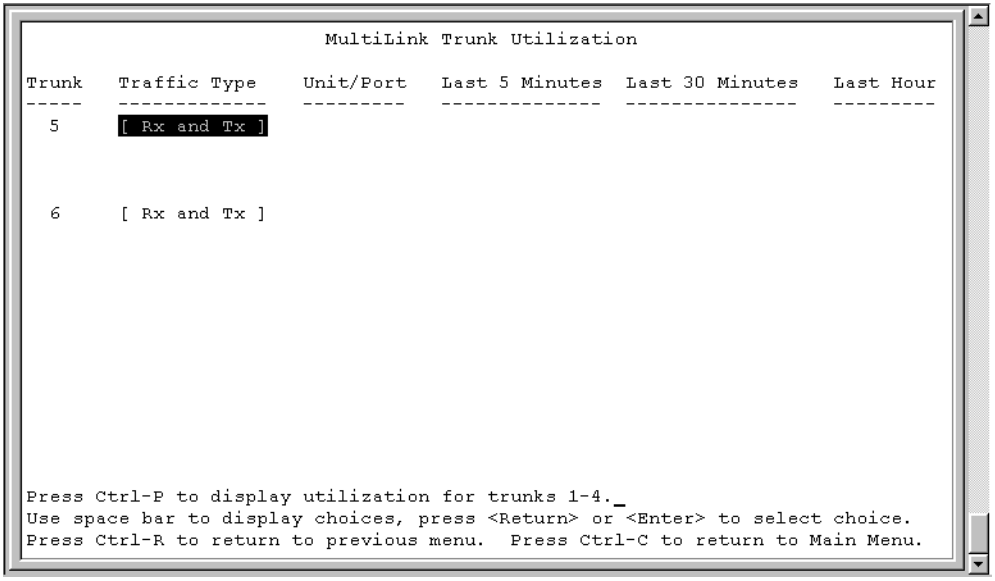
Choose MultiLink Trunk Utilization (or press u) from the MultiLink Trunk Configuration Menu screen to open the MultiLink Trunk Utilization screen.

Figure 68 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 ]



  2      [ Rx and Tx ]



  3      [ Rx and Tx ]



  4      [ Rx and Tx ]



                                                                      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 69 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 ]



  6      [ Rx and Tx ]











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 28 describes the MultiLink Trunk Utilization screen fields.

Table 28 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
Port	Lists the trunk member ports that correspond to the trunk specified in the Trunk column.
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 28 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 one specific port. You can specify ingress and egress port-based monitoring.

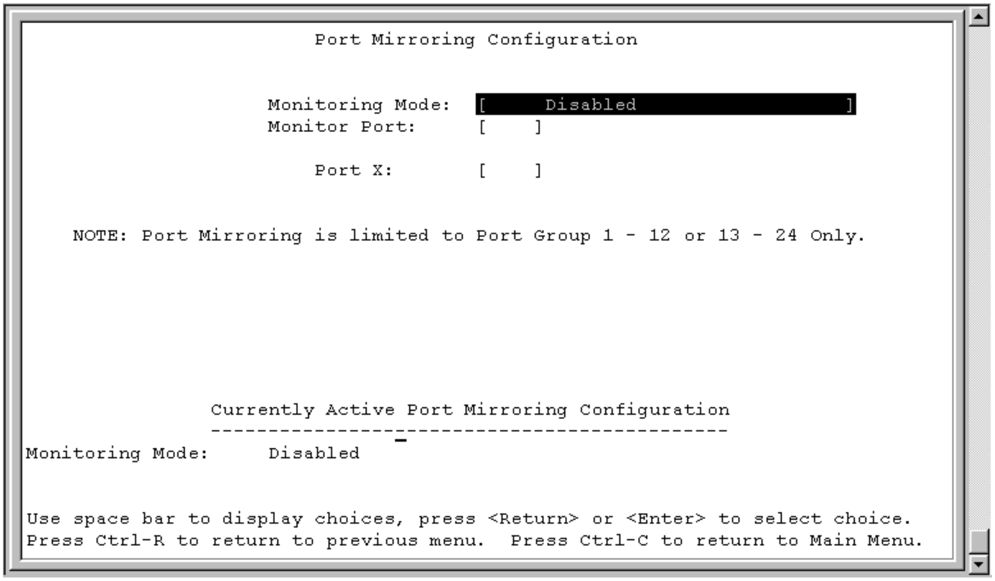
For more information about the port mirroring feature, see "Port mirroring (conversation steering)" on page 42.

Figure 70 shows an example of a Port Mirroring Configuration screen.

To open the Port Mirroring Configuration screen:

➔ Choose Port Mirroring Configuration (or press i) from the Switch Configuration Menu screen.

Figure 70 Port Mirroring Configuration screen



```
                         Port Mirroring Configuration


                     Monitoring Mode:   [      Disabled                  ]
                     Monitor Port:      [    ]

                         Port X:        [    ]


    NOTE: Port Mirroring is limited to Port Group 1 - 12 or 13 - 24 Only.






                Currently Active Port Mirroring Configuration
                ---------------------------------------------
Monitoring 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 29 describes the Port Mirroring Configuration screen fields.

Table 29 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 30 on page 144). 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 30 on page 144
Monitor 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 29 Port Mirroring Configuration screen fields (continued)

Field	Description	
Port X	Indicates one of the ports 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 30).	
	Default Value	Zero-length string
	Range	(depends on model type)

Table 30 describes the various monitoring modes available from the Port Mirroring Configuration screen.

Table 30 Monitoring modes

Field	Description
Port-based:	
Disabled	Default value for this feature.
-> Port X	Monitor all traffic received by Port X.

Port Statistics screen

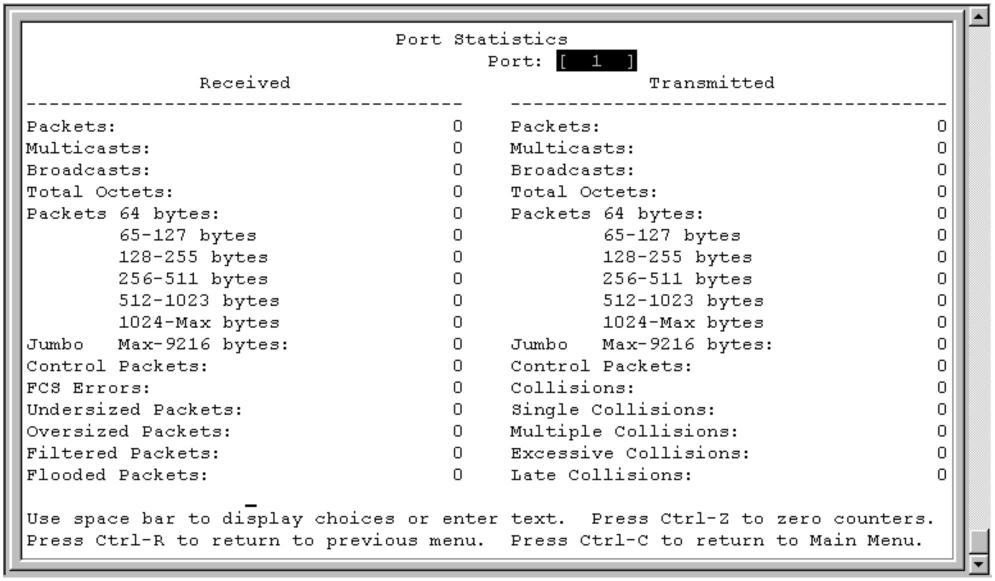
The Port Statistics screen (Figure 71) allows you to view detailed information about any switch or port in a standalone configuration. The screen is divided into two sections (Received and Transmitted) so that you can compare and evaluate throughput or other port parameters. All screen data is updated 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 108).

To open the Port Statistics screen:

➔ Choose Display Port Statistics (or press d) from the Switch Configuration Menu screen.

Figure 71 Port Statistics screen



```
                         Port Statistics
                               Port: [  1  ]
               Received                                 Transmitted
--------------------------------------   --------------------------------------
Packets:                            0    Packets:                            0
Multicasts:                         0    Multicasts:                         0
Broadcasts:                         0    Broadcasts:                         0
Total Octets:                       0    Total Octets:                       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-Max bytes              0            1024-Max bytes              0
Jumbo   Max-9216 bytes:             0    Jumbo   Max-9216 bytes:             0
Control Packets:                    0    Control Packets:                    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    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 31 describes the Port Statistics screen fields.

Table 31 Port Statistics screen fields

Field	Description
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.

Table 31 Port Statistics screen fields (continued)

Field	Description
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.
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.
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-Max 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.
Max 9216 bytes (Jumbo)	Received column: Indicates the total number of 1519-byte packets to 9216 byte packets received on this port. Transmitted column: Indicates the total number of 1519-byte packets to 9216 byte packets transmitted successfully on this port.
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 1548 bytes (if MAC Security is disabled) and with proper CRC and framing (also known as oversized frames).
Filtered Packets	Indicates the number of packets filtered (not forwarded) by this port.

Table 31 Port Statistics screen fields (continued)

Field	Description
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.
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.
Control packets	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. 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.

System Log screen

The System Log screen (Figure 72) displays or clears messages obtained from system nonvolatile random access memory (NVRAM) or dynamic random access memory (DRAM) and NVRAM.

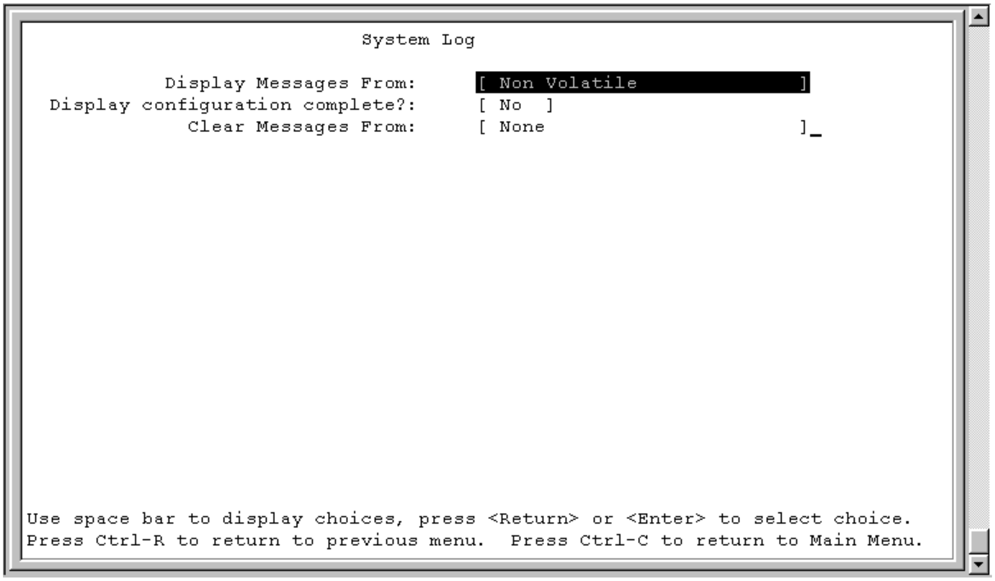
System Log messages operate as follows:

- 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 System Log screen:

➔ Choose Display System Log (or press y) from the main menu.

Figure 72 System Log screen



```
                                   System Log

             Display Messages From:      [ Non Volatile              ]
  Display configuration complete?:      [ No  ]
               Clear Messages From:      [ None                      ]_
```

```
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 System Log screen fields.

Table 32 System Log screen fields

Field	Description
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, 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

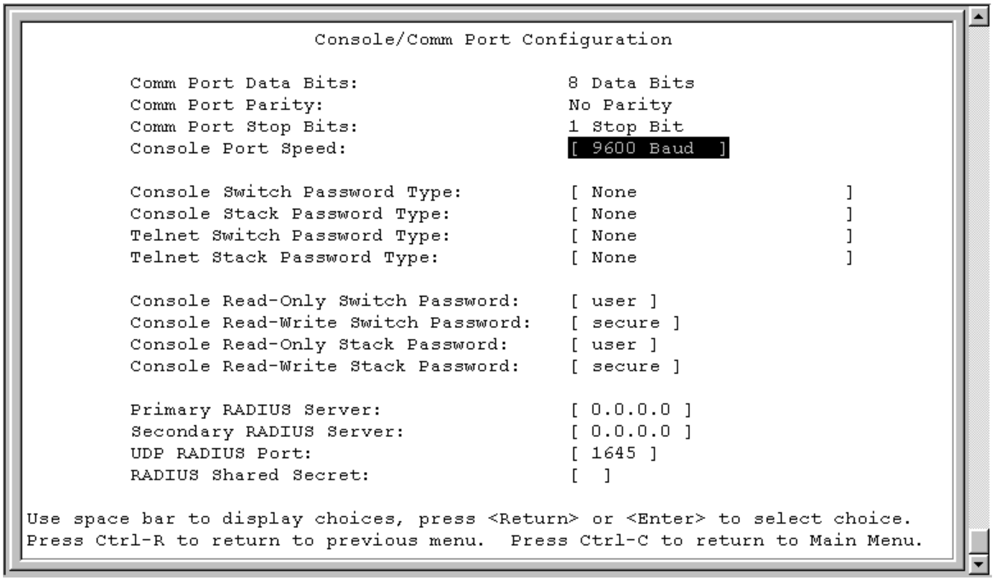
Console/Comm Port Configuration screen

The Console/Comm Port Configuration screen (Figure 73) allows you to configure and modify the console/comm port parameters and security features of a switch.

To open the Console/Comm Port Configuration screen:

➔ Choose Console/Comm Port Configuration (or press o) from the main menu.

Figure 73 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:                     [ 9600 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:      [ user ]
         Console Read-Write Switch Password:     [ secure ]
         Console Read-Only Stack Password:       [ user ]
         Console Read-Write Stack Password:      [ secure ]

         Primary RADIUS Server:                  [ 0.0.0.0 ]
         Secondary RADIUS Server:                [ 0.0.0.0 ]
         UDP RADIUS Port:                        [ 1645 ]
         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 33 describes the Console/Comm Port Configuration screen fields.

Table 33 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 33 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 33 Console/Comm Port Configuration screen fields (continued)

Field	Description
TELNET Switch Password Type	Enables password protection for accessing the console interface (CI) of a 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
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. 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:** 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.

Table 33 Console/Comm Port Configuration screen fields (continued)

Field	Description
	⛔ **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。
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

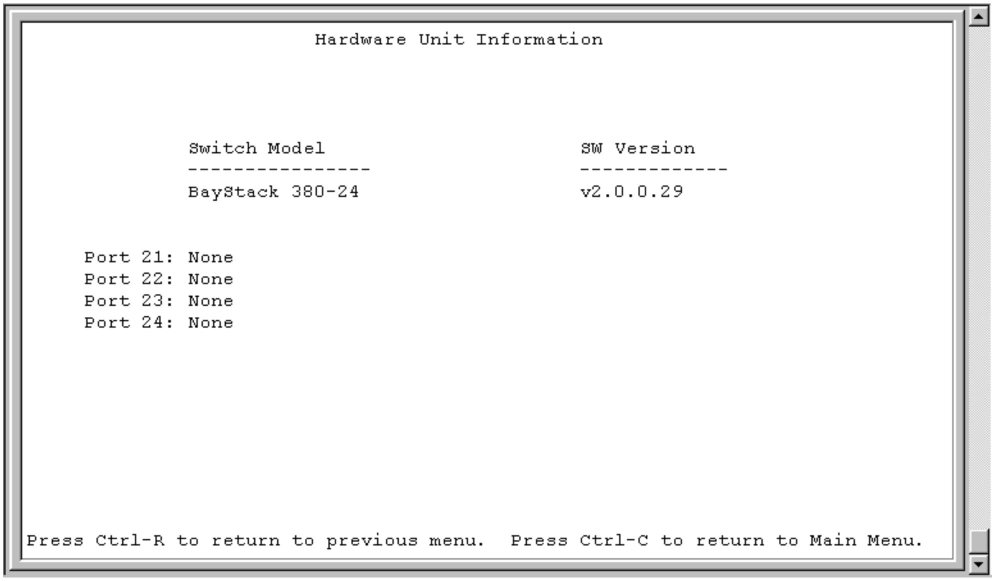
Hardware Unit Information screen

The Hardware Unit Information screen (Figure 74) lists the switch models, including any installed mini-GBICs that are configured in your standalone configuration.

To open the Hardware Unit Information screen:

➔ Choose Display Hardware Unit (or press h) from the main menu.

Figure 74 Hardware Unit Information screen



```
                           Hardware Unit Information



               Switch Model                        SW Version
               ----------------                    -------------
               BayStack 380-24                     v2.0.0.29


      Port 21:  None
      Port 22:  None
      Port 23:  None
      Port 24:  None









Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

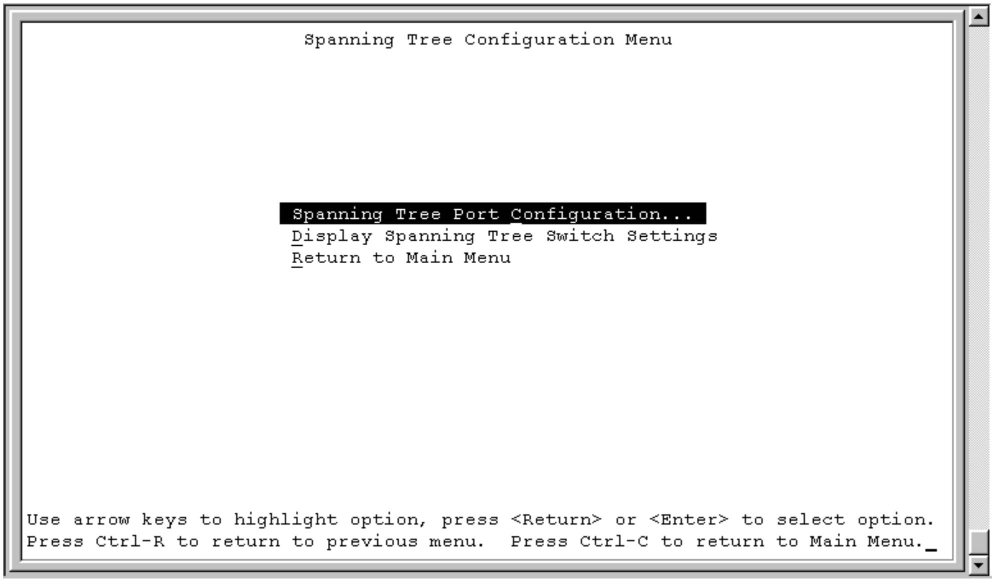
Spanning Tree Configuration Menu screen

The Spanning Tree Configuration Menu screen (Figure 75) allows you to view spanning tree parameters and configure individual switch ports to participate in the spanning tree algorithm (STA). To modify any of the spanning tree parameters, see your SNMP documentation.

To open the Spanning Tree Configuration Menu screen:

➔ Choose Spanning Tree Configuration (or press p) from the main menu.

Figure 75 Spanning Tree Configuration Menu screen



```
                    Spanning Tree Configuration Menu




                  Spanning Tree Port Configuration...
                  Display Spanning Tree Switch Settings
                  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 34 describes the Spanning Tree Configuration Menu options.

Table 34 Spanning Tree Configuration Menu options

Option	Description
Spanning Tree Port Configuration...	Displays the Spanning Tree Port Configuration screen (see "Spanning Tree Port Configuration screen" on page 156).
Spanning Tree Switch Settings	Displays the Spanning Tree Switch Settings screen (see "Spanning Tree Switch Settings screen" on page 159).
Return to Main Menu	Exits the Spanning Tree Configuration Menu and displays the main menu.

Spanning Tree Port Configuration screen

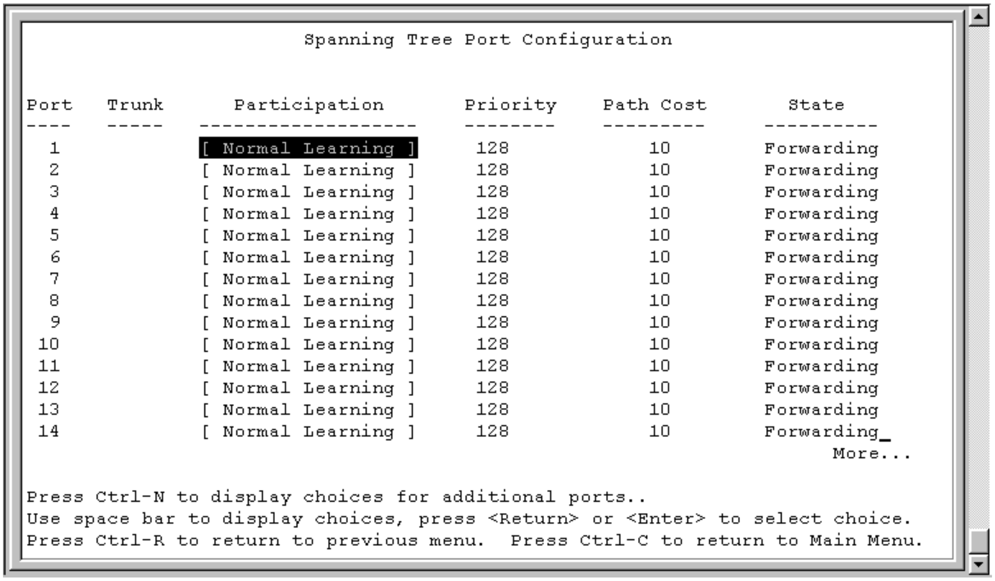
The Spanning Tree Port Configuration screen allows you to configure individual switch ports or all switch ports for participation in the spanning tree.

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 76 and Figure 77 show sample port configurations for the two Spanning Tree Port Configuration screens.

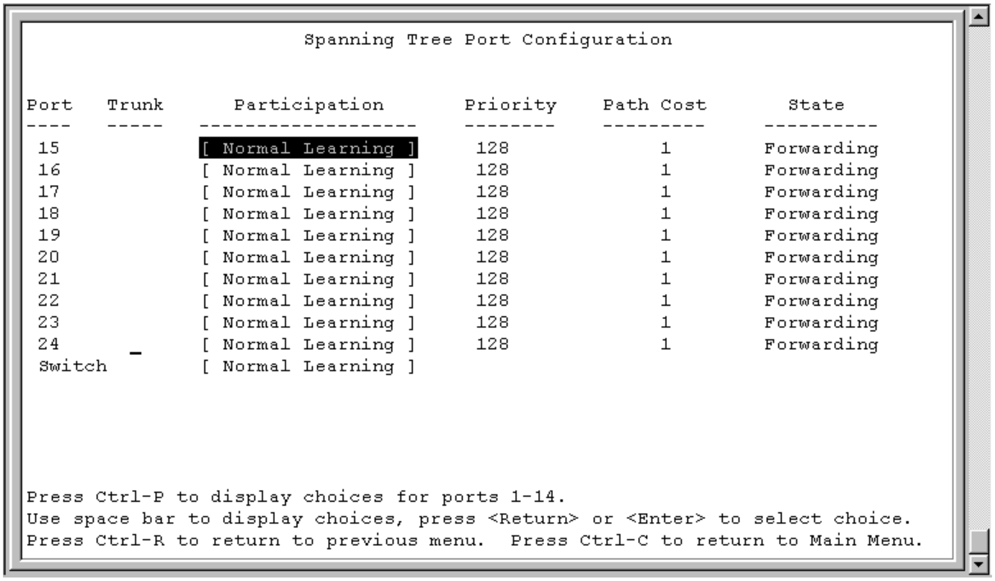
Choose Spanning Tree Port Configuration (or press c) from the Spanning Tree Configuration Menu to open the Spanning Tree Port Configuration screen.

Figure 76 Spanning Tree Port Configuration screen (1 of 2)



```
                        Spanning Tree Port Configuration


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.
```

Figure 77 Spanning Tree Port Configuration screen (2 of 2)



```
                        Spanning Tree Port Configuration


Port   Trunk      Participation       Priority   Path Cost      State
----   -----   -------------------    --------   ---------    ----------
 15            [ Normal Learning ]      128          1        Forwarding
 16            [ Normal Learning ]      128          1        Forwarding
 17            [ Normal Learning ]      128          1        Forwarding
 18            [ Normal Learning ]      128          1        Forwarding
 19            [ Normal Learning ]      128          1        Forwarding
 20            [ Normal Learning ]      128          1        Forwarding
 21            [ Normal Learning ]      128          1        Forwarding
 22            [ Normal Learning ]      128          1        Forwarding
 23            [ Normal Learning ]      128          1        Forwarding
 24       _    [ Normal Learning ]      128          1        Forwarding
 Switch        [ Normal Learning ]




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 35 describes the Spanning Tree Port Configuration screen fields.

Table 35 Spanning Tree 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). Note that the values in the *Switch* row affect all switch ports.
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 136).
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. 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 port's lowest path cost to the root. When one or more ports have the same path cost, the STA selects the path with the highest priority (lowest numerical value). See also Path Cost. Default Value: 128 Range: 0 to 255
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 the STA and transitions to the Forwarding state (the default). When the Participation field is set to Enabled, 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

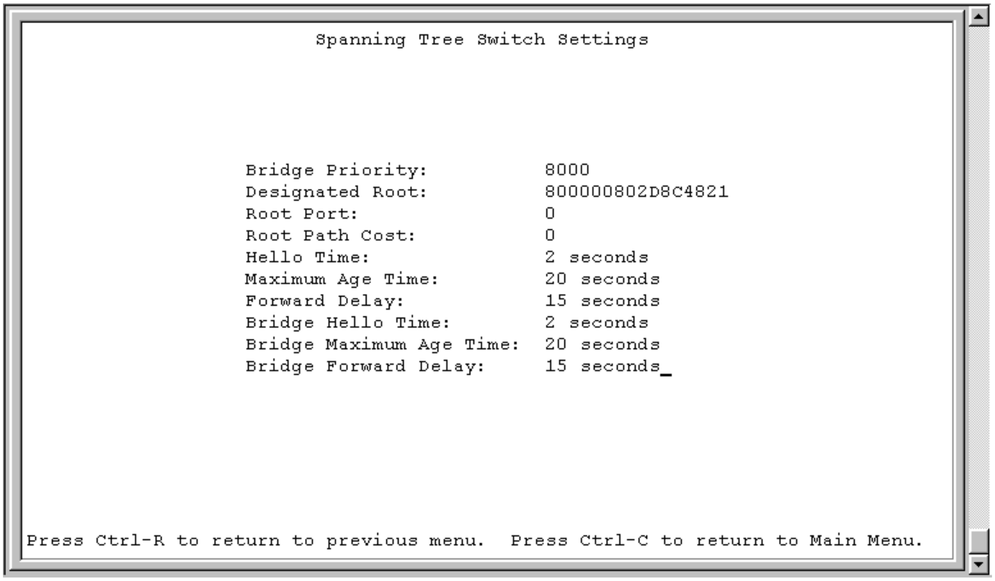
Spanning Tree Switch Settings screen

The Spanning Tree Switch Settings screen (Figure 78) allows you to view spanning tree parameter values for the BayStack 380 Switch.

To open the Spanning Tree Switch Settings screen:

➔ Choose Display Spanning Tree Switch Settings (or press d) from the Spanning Tree Configuration Menu screen.

Figure 78 Spanning Tree Switch Settings screen



```
                         Spanning Tree Switch Settings




                   Bridge Priority:           8000
                   Designated Root:           800000802D8C4821
                   Root Port:                 0
                   Root Path Cost:            0
                   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_





Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Table 36 describes the Spanning Tree Switch Settings parameters.

Table 36 Spanning Tree Switch Settings parameters

Parameter	Description
Bridge Priority	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 compared first, followed by the hardware addresses. Default Value 8000 Range 0 to 65535
Designated Root	Indicates the bridge ID of the root bridge, as determined by the STA. Default Value 8000 (bridge_id) Range 0 to 65535
Root Port	Indicates the switch port number that offers the lowest path cost to the root bridge. Default Value 0 Range Port: 24
Root Path Cost	Indicates the path cost from this switch port to the root bridge. Default Value 0 Range Not applicable
Hello Time	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. Default Value 2 seconds Range 1 to 10 seconds
Maximum Age Time	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. Default Value 20 seconds Range 6 to 40 seconds

Table 36 Spanning Tree Switch Settings parameters (continued)

Parameter	Description
Forward Delay	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. Default Value 15 seconds Range 4 to 30 seconds
Bridge Hello Time	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 Maximum Age Time	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	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

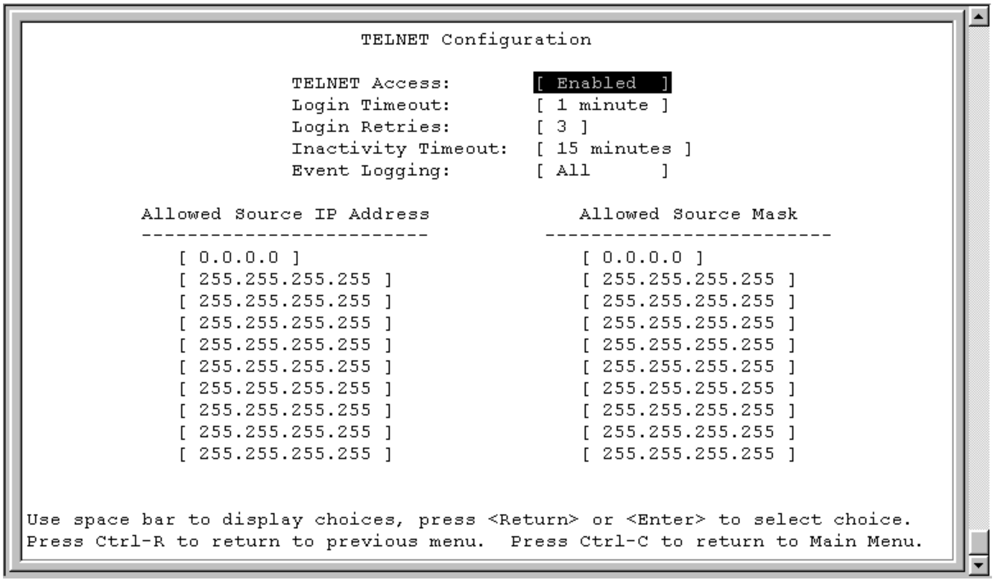
TELNET Configuration screen

The TELNET Configuration screen (Figure 79) allows a user at a remote console terminal to communicate with the BayStack 380 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 Configuration screen:

➔ Choose TELNET Configuration (or press t) from the main menu.

Figure 79 TELNET Configuration screen



```
                         TELNET Configuration

                   TELNET Access:          [ Enabled  ]
                   Login Timeout:          [ 1 minute ]
                   Login Retries:          [ 3 ]
                   Inactivity Timeout:     [ 15 minutes ]
                   Event Logging:          [ All       ]

          Allowed Source IP Address                Allowed Source Mask
          -------------------------                -------------------------
             [ 0.0.0.0 ]                              [ 0.0.0.0 ]
             [ 255.255.255.255 ]                      [ 255.255.255.255 ]
             [ 255.255.255.255 ]                      [ 255.255.255.255 ]
             [ 255.255.255.255 ]                      [ 255.255.255.255 ]
             [ 255.255.255.255 ]                      [ 255.255.255.255 ]
             [ 255.255.255.255 ]                      [ 255.255.255.255 ]
             [ 255.255.255.255 ]                      [ 255.255.255.255 ]
             [ 255.255.255.255 ]                      [ 255.255.255.255 ]
             [ 255.255.255.255 ]                      [ 255.255.255.255 ]
             [ 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 37 describes the TELNET Configuration screen fields.

Table 37 TELNET Configuration screen fields

Field	**Description**
TELNET Access	Allows a user remote access to the CI 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 147. 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 37 TELNET Configuration screen fields (continued)

Field	Description
Allowed Source IP Address	Specifies up to 10 user-assigned host IP addresses that are allowed Telnet access to the CI. 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 80 and Figure 81) allow you to revise the BayStack 380 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。

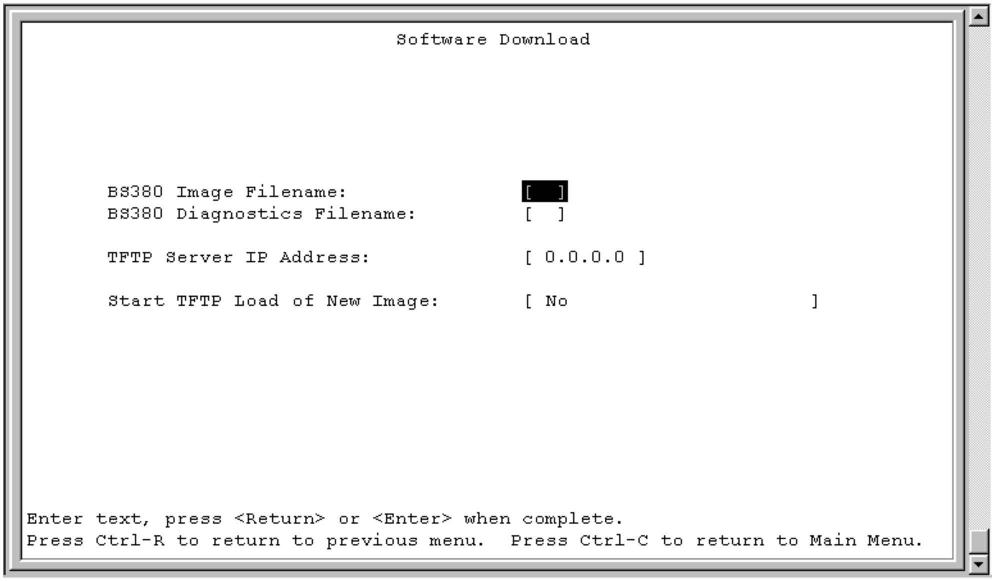
To download the software image, you need a properly configured Trivial File Transfer Protocol (TFTP) server in your network, and an IP address for the switch. To learn how to configure the switch IP address, refer to "IP Configuration/Setup screen" on page 99.

To open the Software Download screen:

➔ Choose Software Download (or press f) from the main menu.

You can monitor the software download process by observing the LEDs (see "LED Indications during the download process" on page 167).

Figure 80 Software Download screen for a BayStack 380 Switch



```
                         Software Download




   BS380 Image Filename:                  [  ]
   BS380 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.
```

Table 38 describes the Software Download screen fields.

Table 38 Software Download screen fields

Field	Description
BayStack 380 Image Filename	The BayStack 380 Switch software image load file name. **NOTE:** Certain software releases may require you to download two images: the *boot code image* and the *agent image*. For proper operation of the switch, the new boot code image must be downloaded *before* the agent image is downloaded. Default Value Zero-length string Range An ASCII string of up to 30 printable characters
BayStack 380 Diagnostics Filename	The BayStack 380 Switch diagnostics file name. Default Value Zero-length string Range An ASCII string of up to 30 printable characters

Table 38 Software Download screen fields (continued)

Field	Description
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 Yes. 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 Yes, No

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, the Software Download screen displays error codes that define the problem. The error codes are described in Chapter 4, “Troubleshooting,” on page 171.

LED Indications during the download process

During the software image download, the link and speed LEDs turn to green and begin a browsing display pattern. The two rows of 10/100/1000 LEDs illuminate from in to out. After the download, the system automatically reboots and the LEDs return to the initialization state.

Configuration File Download/Upload screen

The Configuration File Download/Upload screen (Figure 81) allows you to store your switch configuration parameters on a TFTP server.

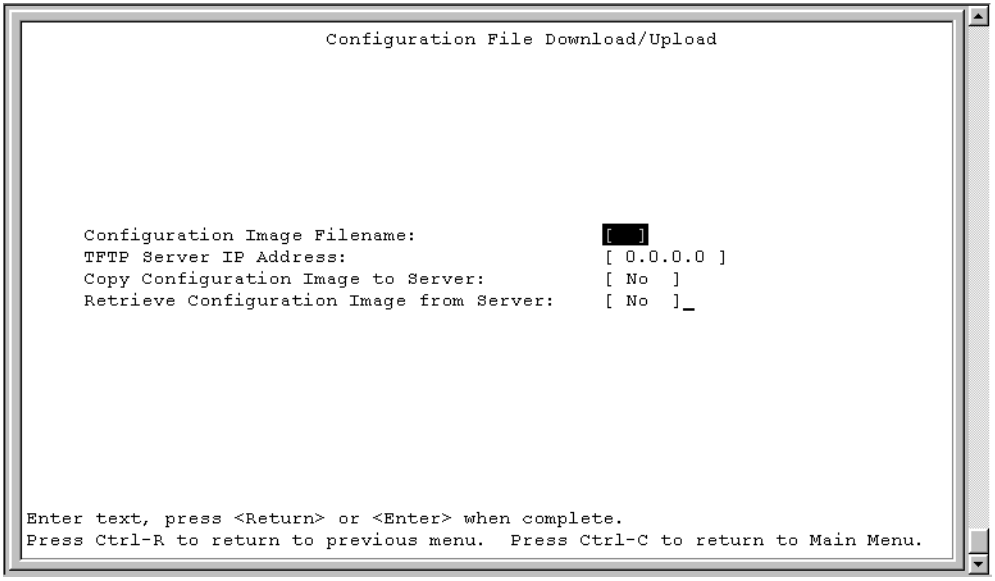
You can retrieve the configuration parameters of a switch and use the retrieved parameters to automatically configure a replacement switch. Certain requirements apply when automatically configuring a switch using this feature. You must set up the file on your TFTP server and set the filename read/write permission to enabled before you can save the configuration parameters.

Although most configuration parameters are saved to the configuration file, certain parameters are not saved (see Table 40 on page 170).

To open the Configuration File Download/Upload screen:

➔ Choose Configuration File (or press g) from the main menu.

Figure 81 Configuration File Download/Upload screen



```
                     Configuration File Download/Upload




     Configuration Image Filename:                  [   ]
     TFTP Server IP Address:                        [ 0.0.0.0 ]
     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 39 describes the Configuration File Download/Upload screen fields.

Table 39 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 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 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 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

Table 40 describes configuration file parameter information.

Table 40 Parameters not saved to the configuration file

These parameters are not saved:	**Used in this screen:**	**See page:**
In-Band Switch IP Address		
In-Band Subnet Mask		
Default Gateway		
Console Read-Only Switch Password	Console/Comm Port Configuration	149
Console Read-Write Switch Password		
Configuration Image Filename	Configuration File Download/Upload	168
TFTP Server IP Address		

Chapter 4 Troubleshooting

This chapter describes how to isolate and diagnose problems with your BayStack 380 Switch and covers the following topics:

- "Interpreting the LEDs," next
- "Diagnosing and correcting problems" on page 174
  - Normal power-up sequence
  - Port connection problems

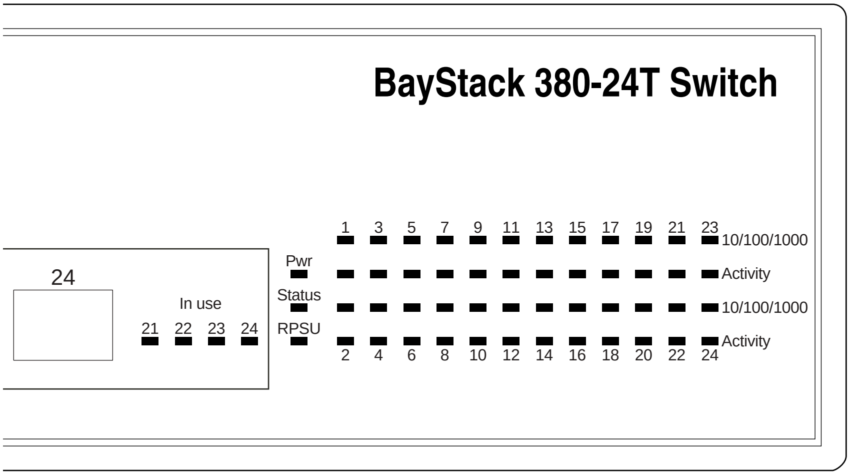
The chapter topics lead you through a logical process for troubleshooting the BayStack 380 Switch. For example, because LEDs provide visual indications of certain problems, see "Interpreting the LEDs" on page 172 to understand the various states (Table 82) that your switch LEDs can exhibit during normal operation.

For more help in determining the problem, "Diagnosing and correcting problems" on page 174 describes symptoms and corrective actions (Table 42) you can perform to resolve specific problems. Subsequent sections give step-by-step procedures to correct the problems.

Interpreting the LEDs

Figure 82 shows the BayStack 380 Switch LED display panel. Table 41 describes the LEDs.

Figure 82 LED display panel



10473EA

Table 41 BayStack 380 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.

Table 41 BayStack 380 switch LED descriptions

Label	Type	Color	State	Meaning
10/100/1000	Speed/Link Status indicator	Alternating Green/ Amber (10)	On	The corresponding port is set to operate at 10 Mb/s, and the link is good.
			Blinking	The corresponding 10 Mb/s port has been disabled by software.
			Off	The link connection is bad, or there is no connection to this port.
		Solid Amber (100)	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.
			Off	The link connection is bad, or there is no connection to this port.
		Solid Green (1000)	On	The corresponding port is set to operate at 1000 Mb/s and the link is good.
			Blinking	The corresponding 1000 Mb/s port has been disabled by software.
			Off	The link connection is bad, or there is no connection to this port.
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.

Note: The speed indicator LED for a port operating at 10 Mb/s is solid amber for 5 seconds, then switches to green for 1 second. It alternates in this way while the switch is on.

Diagnosing and correcting problems

Before you perform the problem-solving steps in this section, cycle the power to the BayStack 380 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. After the self-test, the remaining port LEDs indicate their operational status, as described in Table 42.

Table 42 Corrective actions

Symptom	Probable cause	Corrective action
All LEDs are off.	The switch is not receiving AC power. The fans are not operating or the airflow is blocked, causing the unit to overheat.	Verify that the AC power cord is fastened securely at both ends and that power is available at the AC power outlet. 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.

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.

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).

The BayStack 380 Switch negotiates port speeds according to the IEEE 802.3u, IEEE 802.3z, and IEEE 802.3ab autonegotiating standards. The switch adjusts (autonegotiates) its port speed and duplex mode to match the best service provided by the connected station, up to 1000 Mb/s in full-duplex mode as follows:

- If the connected station uses a form of autonegotiation that is not compatible with the IEEE autonegotiating standard, the BayStack 380 Switch cannot negotiate a compatible mode for correct operation.
- If the autonegotiation feature is not present or not enabled at the connected station, the BayStack 380 Switch may not be able to determine the correct duplex modes.

In both situations, the BayStack 380 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 “Port Configuration screen” on page 131).
2. Manually set the Speed/Duplex field to match the speed/duplex mode of the connected station (see Table 24 on page 132).

   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 BayStack 380 Switch port.

Port interface

Ensure that the devices are connected using the appropriate crossover or straight-through cable (see Appendix D, “Connectors and pin assignments,” on page 201), or that autonegotiation is active.

➡ **Note:** IEEE 1000BASE-TX requires full duplex mode operation with autonegotiation enabled.

➡ **Note:** Auto-MDI-X and auto-polarity both require that auto-negotiation be enabled.

Appendix A
Technical specifications

This appendix provides technical specifications for the BayStack 380 10/100/1000 Switch.

Environmental

Table 43 lists environmental specifications for the BayStack 380 Switch.

Table 43 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)	12,096 m (40,000 ft)

Electrical

Table 44 lists power electrical parameters for the BayStack 380 Switch.

Table 44 Electrical parameters

Parameter	Electrical specification
Input Voltage	100 to 240 VAC @ 47 to 63 Hz
Input Power Consumption	150 W maximum
Input current	1.5 A @ 100 VAC 0.6 A @ 240 VAC
Maximum thermal output	250 BTU/hr

Physical dimensions

Table 45 lists physical dimensions for the BayStack 380 Switch.

Table 45 Physical dimensions

Parameter	Specifications
Height	2.77 in (7.04 cm)
Width	17.25 in (43.82 cm)
Depth	12.75 in (32.34 cm)
Weight	10.6 lb (4.8 kg)

Performance specifications

Table 46 lists performance specifications for the BayStack 380 Switch.

Table 46 Performance specifications

Parameter	Specifications
Frame Forward Rate (64-byte packets)	Up to 3.35 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 • For 1000 Mb/s: 1,488,100 pps maximum
Address Database Size	32,000 entries at line rate
Addressing	48-bit MAC address
Frame Length	64 to 9,216 bytes (IEEE 802.1Q Tagged)

Network protocol and standards compatibility

The following are protocols and standards used by the BayStack 380 Switch:

- IEEE 802.3 10BASE-T (ISO/IEC 8802-3, Clause 14)
- IEEE 802.3u 100BASE-TX (ISO/IEC 8802-3, Clause 25)
- IEEE 802.3ab 1000BASE-T
- IEEE 802.3z (gigabit ethernet)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.3x (Flow Control with 802.1D compliant device)
- IEEE 802.1D (Spanning tree protocol)
- IEEE 802.1p (Prioritization)

Safety agency certification

- The safety certifications follow for the BayStack 380 Switch:
- UL Listed (UL 1950)
- IEC 950/EN60950 (CB report) with all national deviations
- C22.2 No. 950 (CUL)
- UL-94-V1 flammability requirements for PC board
- NOM (NOM-019)

Electromagnetic emissions

- The electromagnetic emission standards for the BayStack 380 Switch:
- 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 BayStack 380 Switch meets the EN50082-1:1997 standard.

Appendix B
Installing SFP and CWDM Gigabit Interface Converters (GBICs)

This appendix describes how to install a Small Form Factor Pluggable (SFP) Gigabit Interface Converter (GBIC) or a Coarse Wavelength Division Multiplex (CWDM) GBIC to the BayStack 380 switch. It also provides a description of the SFP GBIC, the SFP GBIC label, and SFP GBIC specifications.

➡ **Note:** In the BayStack 380, ports 21 through 24 are shared copper and fiber ports. A copper port is always active until a SFP GBIC is inserted with an active link.

Product description

SFP GBICs are hot-swappable input/output enhancement components designed for use with Nortel Networks products to allow Gigabit Ethernet ports to link with fiber optic networks.

Table 47 lists and describes the Nortel Networks SFP GBIC models.

Table 47 Nortel Networks SFP GBIC models

Model number	Product number	Description
1000BASE-SX (LC Type)	AA1419013	Small Form Factor Pluggable, short wavelength 550 m
1000BASE-SX (MT-RJ Type)	AA1419014	Small Form Factor Pluggable, short wavelength 550 m
1000BASE-LX (LC Type)	AA1419015	Small Form Factor Pluggable, long wavelength 5 km

Note: The cable distance may vary depending on the quality of fiber optic cable used.

Handling, safety, and environmental guidelines

Before installing your SFP GBIC, read the following handling, safety, and environmental guidelines:

- SFP GBICs are static sensitive. To prevent damage from electrostatic discharge (ESD), follow your normal board and component handling procedures.
- SFP GBICs are dust sensitive. When storing a SFP GBIC, or when a SFP GBIC is disconnected from a fiber optic cable, always keep the dust cover over a SFP GBIC's optical bores.
- To clean contaminants from the optical bores of a SFP GBIC, use an alcohol swab or equivalent to clean the ferrules of the optical connector.
- Dispose of this product according to all national laws and regulations.

Warning: Fiber optic equipment can emit laser or infrared light that can injure your eyes. Never look into an optical fiber or connector port. Always assume that fiber optic cables are connected to a light source.

Installing an SFP GBIC

SFP GBIC bays are covered by spring-loaded filler panels that rotate out of the way as you push the SFP GBIC into place. You can install or replace an SFP GBIC in a BayStack 380 Switch without turning off power to the switch.

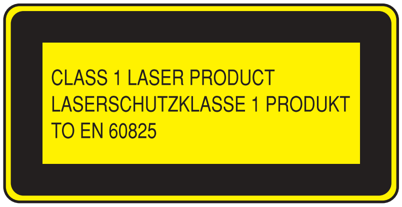
⚠ **Warning:** Fiber optic equipment can emit laser or infrared light that can injure your eyes. Never look into an optical fiber or connector port. Always assume that fiber optic cables are connected to a light source.

⚠ **Vorsicht:** Glasfaserkomponenten können Laserlicht bzw. Infrarotlicht abstrahlen, wodurch Ihre Augen geschädigt werden können. Schauen Sie niemals in einen Glasfaser-LWL oder ein Anschlußteil. Gehen Sie stets davon aus, daß das Glasfaserkabel an eine Lichtquelle angeschlossen ist.

⚠ **Avertissement:** L’équipement à fibre optique peut émettre des rayons laser ou infrarouges qui risquent d’entraîner des lésions oculaires. Ne jamais regarder dans le port d’un connecteur ou d’un câble à fibre optique. Toujours supposer que les câbles à fibre optique sont raccordés à une source lumineuse.

⚠ **Advertencia:** Los equipos de fibra óptica pueden emitir radiaciones de láser o infrarrojas que pueden dañar los ojos. No mire nunca en el interior de una fibra óptica ni de un puerto de conexión. Suponga siempre que los cables de fibra óptica están conectados a una fuente luminosa.

⚠ **Avvertenza:** Le apparecchiature a fibre ottiche emettono raggi laser o infrarossi che possono risultare dannosi per gli occhi. Non guardare mai direttamente le fibre ottiche o le porte di collegamento. Tenere in considerazione il fatto che i cavi a fibre ottiche sono collegati a una sorgente luminosa.



CLASS 1 LASER PRODUCT
LASERSCHUTZKLASSE 1 PRODUKT
TO EN 60825

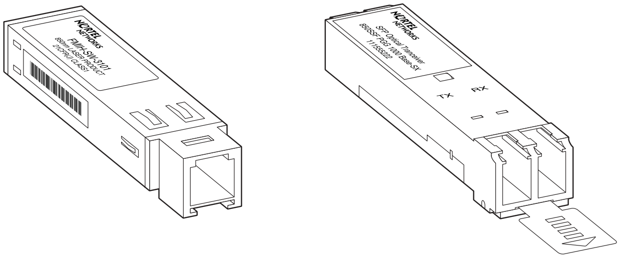
8769EA

Product models

Small Form Factor Pluggable Gigabit Interface Converters (SFP GBICs) are hot-swappable input/output enhancement components designed for use with Nortel Networks products to allow Gigabit Ethernet ports to link with fiber optic networks.

Figure 83 shows the SFP GBIC

Figure 83 SFP GBIC



MTRJ GBIC model with extractor button

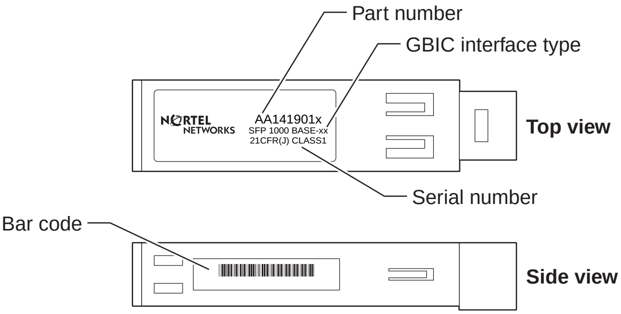
LC GBIC model with extractor tab

10515FA

SFP GBIC labeling

The Nortel Networks label on a typical SFP GBIC (Figure 84) contains a Nortel Networks serial number, a bar code, a manufacturer's code, an interface type, and a part number.

Figure 84 Nortel Networks SFP GBIC label



10516EA

Note: When you contact a Nortel Networks service representative for troubleshooting purposes, you must have the following information available:

- Nortel Networks serial number
- Manufacturer’s code
- Interface type
- GBIC part number

Installing a Small Form Factor Pluggable SFP GBIC

This section lists the steps to install an SFP GBIC.

To install an SFP GBIC:

1. Remove the SFP GBIC from its protective packaging.
2. Verify that the SFP GBIC is the correct model for your network configuration (Table 47 on page 183).
3. Remove the dust cover from the SFP GBIC’s optical bores.
4. Grasp the SFP GBIC between your thumb and forefinger.
5. Insert the SFP GBIC into the slot on the front panel of the Gigabit Ethernet switching module (Figure 86).

Figure 85 Inserting an LC SFP GBIC

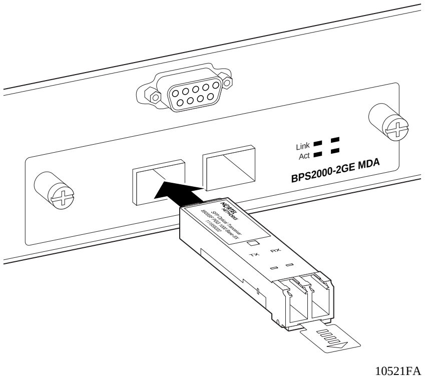
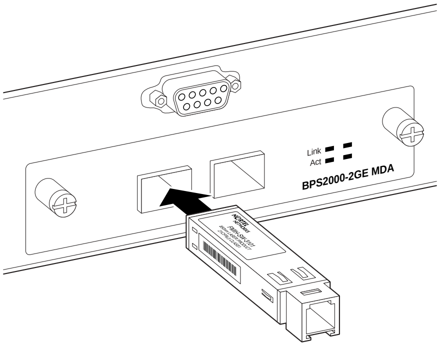


Figure 86 Inserting an MT-RJ SFP GBIC



Note: SFP GBICs are keyed to prevent incorrect insertion.

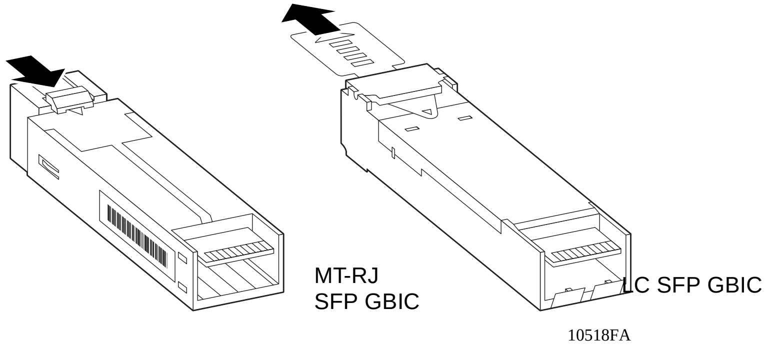
Removing a Small Form Factor Pluggable SFP GBIC

This section lists the steps for removing an SFP GBIC.

To remove an SFP GBIC:

1. Disconnect the network fiber cable from the SFP GBIC connector.
2. Depending on your SFP GBIC model, either pull the LC extraction tab located in the front of the SFP GBIC (below right) with your thumb and forefinger, or press the button on the bottom of the MT-RJ SFP GBIC (below left).

Figure 87 Removing an SFP GBIC (Bottom view)



3 Slide the SFP GBIC out of the Gigabit Ethernet module slot.

4 If the SFP GBIC does not slide easily from the module slot, use a gentle side-to-side rocking motion while firmly pulling the SFP GBIC from the slot.

5 Dispose of the SFP GBIC according to all national laws and regulations.

Note: If you are storing an SFP GBIC, remember to place a dust cover over the fiber optic bores.

Small Form Factor Pluggable SFP GBIC specifications

Table 48 describes general SFP GBIC specifications.

Table 48 SFP GBIC specifications

Specification	Descriptions
Dimensions (H x W x D)	0.53 x 0.33 x 2.22 inches (13.4 x 8.5 x 56.4 mm)
Connectors	Multimode fiber optic: LC or MT-RJ Single-mode fiber optic: LC

Standards, connectors, cabling, and distance

This section describes SFP GBIC standards, connectors, cabling, and distance; and provides specifications for the following SFP GBICs:

- "1000BASE-SX (LC Type)" on page 190
- "1000BASE-LX (LC Type)" on page 191
- "1000BASE-SX (MT-RJ Type)" on page 193

1000BASE-SX (LC Type)

The Model 1000BASE-SX SFP GBIC provides 1000BASE-SX (850 nm, short wavelength, Gigabit Ethernet) connectivity using LC duplex multimode fiber connectors.The Model 1000BASE-SX SFP GBIC supports full-duplex operation only.

Table 49 describes standards, connectors, cabling, and distance for the Model 1000BASE-SX SFP GBIC.

Table 49 1000BASE-SX SFP GBIC specifications

Type	**Specifications**
Standards	Conformity to the following standards: 802.3z, 1000BASE-SX
Connectors	Duplex LC fiber optic connector
Cabling	62.5 µm MMF optic cable 50 µm MMF optic cable
Distance	902 ft. (275 m) using 62.5 µm MMF optic cable 1804 ft. (550 m) using 50 µm MMF optic cable
Wavelength	850 nm
Optical budget	7 dB
Laser Transmitter Characteristics	
Minimum launch power	-10 dBm
Maximum launch power	-4 dBm
Receiver Characteristics	
Minimum input power	-17 dBm
Maximum input power	0 dBm

1000BASE-LX (LC Type)

The Model 1000BASE-LX SFP SFP GBIC provides 1000BASE-LX (1300 nm, wavelength, Gigabit Ethernet) connectivity using LC duplex fiber connectors. The long wavelength optical transceivers used in the LX model provide variable distance ranges using both multimode and single-mode fiber optic cabling. The Model 1000BASE-LX SFP GBIC supports full-duplex operation only.

Table 50 describes standards, connectors, cabling, and distance for the Model 1000BASE-LX SFP GBIC.

Table 50 1000BASE-LX SFP GBIC specifications

Type	**Specifications**
Standards	Conformity to the following standards: 802.3z, 1000BASE-LX
Connectors	Duplex LC fiber optic connector
Cabling	10 µm SMF optic cable
Distance	16405 ft. (5 km) using 10 µm SMF optic cable
Wavelength	1300 nm
Optical budget	11.0 dB
Laser Transmitter Characteristics	
Minimum launch power	-9.0 dBm
Maximum launch power	-3 dBm
Receiver Characteristics	
Minimum input power	-20 dBm
Maximum input power	-3 dBm

1000BASE-SX (MT-RJ Type)

The Model 1000BASE-SX (MT-RJ Type) SFP GBIC provides Gigabit Ethernet connectivity using MT-RJ multi-mode fiber connectors.

Table 51 describes standards, connectors, cabling, and distance for the Model 1000BASE-SX (MT-RJ Type) SFP GBIC.

Table 51 1000BASE-SX (MT-RJ) SFP GBIC specifications

Type	**Specifications**
Standards	Conformity to the following standards: 802.3z, Ethernet full duplex
Connectors	Duplex MT-RJ fiber optic connector
Cabling	62.5 µm MMF optic cable 50 µm MMF optic cable
Distance	275 mm (62.5 µm MMF optic cable) 550 mm (50 µm MMF optic cable)
Optical budget	7 dB
Laser Transmitter Characteristics	
Wavelength	850 nm
Maximum spectral width	0.85 nm
Maximum launch power	-4.0 dBm
Minimum launch power	-10.0 dBm
Receiver Characteristics	
Wavelength	850 nm
Minimum input power	-17 dBm
Maximum input power	0 dBm

Coarse Wavelength Division Multiplexed (CWDM) Small Form Factor Pluggable (SFP) Gigabit Interface Converters

This section describes how the Nortel Networks* Coarse Wavelength Division Multiplexed Small Form Factor Pluggable Gigabit Interface Converter (CWDM SFP GBIC) works within the optical routing system. It also provides a list of CWDM SFP GBICs by wavelength and shows how they are labeled and color-coded.

CWDM SFP GBIC description

CWDM SFP GBICs are transceivers that link Gigabit Ethernet ports with fiber optic networks. WDM technology consolidates multiple optical channels, using specific wavelengths to expand available bandwidth, on a common optical fiber.

About the optical routing system

CWDM SFP GBICs are a component in the optical routing system designed to support high speed data communication for Metropolitan Area Networks (MANs). The system uses a grid of eight CWDM optical wavelengths in both ring and point-to-point configurations. All components are color-coded by wavelength.

CWDM SFP GBIC Listing

Table 52 lists the Nortel Networks CWDM SFP GBICs and describes their wavelengths, color codes, part numbers, and cable lengths.

Table 52 Nortel Networks CWDM SFP GBIC List

CWDM SFP GBIC	Product number	Maximum distance
1470nm/Gray	AA1419025 AA1419033	40 KM 70 KM
1490nm/Violet	AA1419026 AA1419034	40 KM 70 KM
1510nm/Blue	AA1419027 AA1419035	40 KM 70 KM

Table 52 Nortel Networks CWDM SFP GBIC List (continued)

CWDM SFP GBIC	Product number	Maximum distance
1530nm/Green	AA1419028 AA1419036	40 KM 70 KM
1550nm/Yellow	AA1419029 AA1419037	40 KM 70 KM
1570nm/Orange	AA1419030 AA1419038	40 KM 70 KM
1590nm/Red	AA1419031 AA1419039	40 KM 70 KM
1610nm/Brown	AA1419032 AA1419040	40 KM 70 KM

➡ **Note:** The cable distance may vary depending on the quality of fiber optic cable used.

➡ **Note:** CWDM SFP GBICs are installed and removed like any other LC type SFP GBIC.

CWDM SFP GBIC specifications

The following tables list the specifications for the 40 kilometer and 70 kilometer CWDM SFP GBICs

Table 53 40 Kilometer CWDM SFP GBIC specifications

Item	**Specification**	
Physical dimensions		0.457 X .604 X 2.18 inches (11.6 X 15.3 X 55.43 mm)
Connectors		Duplex LC fiber optic
Cabling		SMF, 9 µm
Data rate	Nominal range	50 to 1300 Mb/s
Average launch power	minimum maximum	-4.0 dBm +1.0 dBm
Transmitter extinction ratio	minimum	9 dB
Data format		8 B/10 B
Average receive power	minimum maximum	-21.0 dBm -3.0 dBm
Power supply	maximum	3.15 to 3.45 V, 175 mA
Operating temperature range		0^{o}C to 60^{o}C
Regulatory	Class 1 devices per FDA/CDRH and 1EC8251 Laser Safety Regulations	
Optical budget		17 dB

Table 54 70 Kilometer CWDM SFP GBIC specifications

Item	**Specification**	
Physical dimensions		0.457 X .604 X 2.18 inches (11.6 X 15.3 X 55.43 mm)
Connectors		Duplex LC fiber optic
Cabling		SMF, 9 µm
Data rate	Nominal range	50 to 1300 Mbaud
Average launch power	minimum maximum	-3.0 dBm +2.0 dBm
Transmitter extinction ratio	minimum	9 dB
Data format		8 B/10 B

Table 54 70 Kilometer CWDM SFP GBIC specifications (continued)

Item	**Specification**	
Average receive power	minimum maximum	-23.0 dBm -3.0 dBm
Power supply	maximum	3.15 to 3.45 V, 175 mA
Operating temperature range		0°C to 60°C
Regulatory	Class 1 devices per FDA/CDRH and 1EC8251 Laser Safety Regulations	
Optical budget		20 dB

Note: A minimum attenuation of 5 dB must be present between the transmitter and receiver. To avoid receiver saturation, you must insert a minimum attenuation of 5 dB when:

- testing the CWDM SFP GBIC in loopback mode
- using short runs of fiber with no intermediate CWDM OADM or CWDM OMUX

To determine the expected signal loss for a CWDM OADM, CWDM OMUX, or fiber length, see *Installation and Networking Guidelines for Optical Routing*, part number 212257-A.

Note: Given a loss budget of 24 dB and assuming fiber loss of .25 dB/km, up to 96 km reach is supported with no intermediate CWDM OADM or CWDM OMUX.

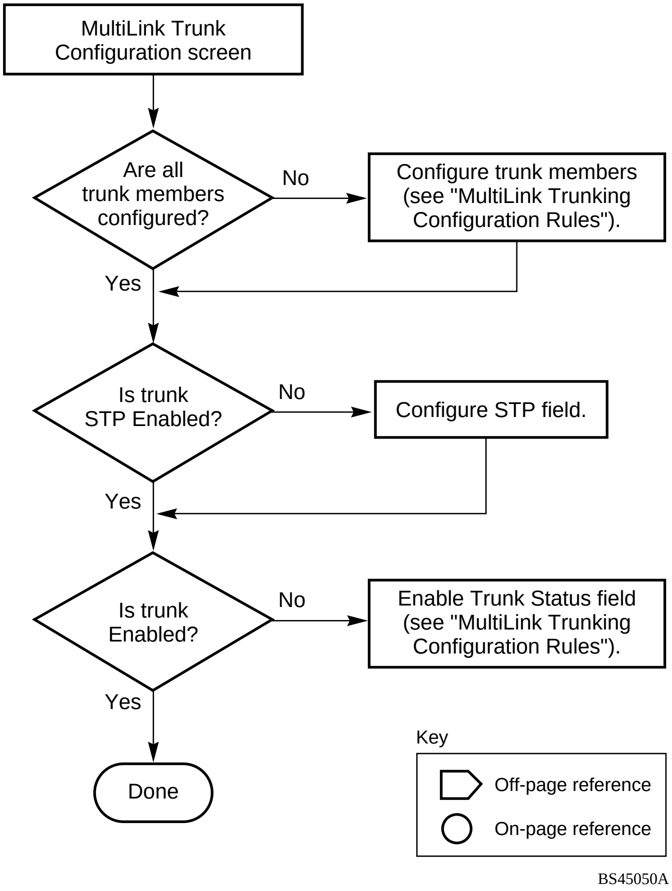
Appendix C
Quick configuration for MultiLink Trunking

If you are a system administrator with experience configuring BayStack 380 Switch MultiLink Trunking, use the flowchart in Figure 88 on page 200 as a quick configuration guide. The flowchart refers you to the "configuration rules" appropriate for this feature.

To open the MultiLink Trunk Configuration screen:

➔ Choose MultiLink Trunk Configuration (or press t) from the MultiLink Trunk Configuration Menu screen.

Figure 88 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

Appendix D
Connectors and pin assignments

This appendix describes the BayStack 380 Switch port connectors and pin assignments.

RJ-45 (10BASE-T/100BASE-TX/1000BASE-TX) port connectors

The RJ-45 port connectors (Figure 89) are wired as MDI-X ports to connect end stations without using crossover cables. (See “MDI and MDI-X devices” on page 203 for information about MDI-X ports.) For 10BASE-T connections, use Category 3 (or higher) UTP cable. For 100BASE-TX/1000BASE-TX connections, use only Category 5 UTP cable.

Figure 89 RJ-45 (8-pin modular) port connector

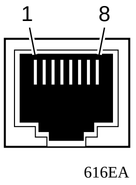


Table 55 lists the RJ-45 (8-pin modular) port connector pin assignments.

Table 55 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

For 1000BASE-T, all 8 pins are used for four pairs of bi-directional data.

Table 56 lists the types of bi-directional data for each of the 1000BASE-T pin connectors.

Table 56 1000BASE-T Pin Connectors

Pin	Type of Data
1	Bi-directional data A+
2	Bi-directional data A-
3	Bi-directional data B+
4	Bi-directional data C+
5	Bi-directional data C-
6	Bi-directional data B-
7	Bi-directional data D+
8	Bi-directional data D-

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

The BayStack 380 Switch features Auto-MDI/MDI-X detection. With auto-negotiation enabled, you can use straight Category 5 cables for MDI to MDI-X connections.

Auto-polarity

The BayStack 380 Switch features auto-polarity. With autonegotiation enabled, auto-polarity automatically reverses the polarity of a pair of pins from positive to negative or negative to positive. This corrects the polarity of the received data if the port detects that the polarity of the data has been reversed due to a wiring error.

DB-9 (RS-232-D) Console/Comm Port connector

The DB-9 Console/Comm Port connector (Figure 90) 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 90 DB-9 Console port connector

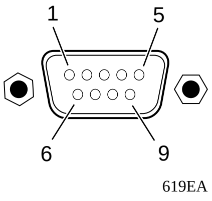


Table 57 lists the DB-9 Console port connector pin assignments.

Table 57 DB-9 Console port connector pin assignments

Pin	Signal	Description
1	CD	Not used
2	TXD	Transmit data (output)
3	RXD	Receive data (input)
4	DSR	
5	GND	Signal ground
6	DSR	Not used
7	CTS	
8	RTS	Not used
9	RI	Not used
Shell		Chassis ground

Appendix E
Default settings

Table 58 lists the factory default settings for the BayStack 380 Switch according to the console interface (CI) screens and fields for the settings.

Table 58 Factory default settings

Field	Default setting	Appears in this CI screen
BootP Request Mode	BootP Disabled	"IP Configuration/Setup screen" on page 99
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 104
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 106
sysName	Zero-length string	
sysLocation	Zero-length string	

Table 58 Factory default settings (continued)

Field	Default setting	Appears in this CI screen
Aging Time Find an Address	300 seconds 00-00-00-00-00-00 (no MAC address assigned)	"MAC Address Table screen" on page 110
MAC Address Security	Disabled	"MAC Address Security Configuration Menu screen" on page 111
MAC Address Security SNMP-Locked	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 115
Security	Disabled	
Find an Address	blank field	"MAC Address Security Table screens" on page 117
MAC Address	- - - - - - (no address assigned)	
Allowed Source	- (blank field)	
Display/Create MAC Address	00-00-00-00-00-00	
Create VLAN	1	"VLAN Configuration screen" on page 121
Delete VLAN	blank field	
VLAN Name	VLAN # (*VLAN number*)	
Management VLAN	Yes, VLAN #1	
VLAN Type	Port-based	
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)	
Port	1	
Filter Untagged Frames	No	

Table 58 Factory default settings (continued)

Field	**Default setting**	**Appears in this CI screen**
Port Name	Unit 1, Port 1	
PVID	1	
Tagging	Untagged Access	
Port	1	
PVID	1 (read only)	
Auto PVID	Disabled	
Port Name	Unit 1, Port 1 (read only)	
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 136
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 140

Table 58 Factory default settings (continued)

Field	Default setting	Appears in this CI screen
Monitoring Mode	Disabled	"Port Mirroring Configuration screen" on page 142
Monitor Port	Zero-length string	
Port	1	
Console Port Speed	9600 Baud	"Console/Comm Port Configuration screen" on page 149
Console Switch Password	Not Required	
Console Read-Only Switch Password	user	
Console Read-Write Switch Password	secure	
Participation	Normal Learning	
Priority	128	
Path Cost	10 or 100	
Bridge Priority	8000 (read only)	"Spanning Tree Switch Settings screen" on page 159
Designated Root	8000 (bridge_id) (read only)	
Root Port	0 (read only)	
Root Path Cost	0 (read only)	
Hello Time	2 seconds (read only)	
Maximum Age Time	20 seconds (read only)	
Forward Delay	15 seconds (read only)	
Bridge Hello Time	2 seconds (read only)	
Bridge Maximum Age Time	20 seconds (read only)	
Bridge Forward Delay	15 seconds (read only)	
TELNET Access	Enabled	"TELNET Configuration screen" on page 162
Login Timeout	1 minute	
Login Retries	3	
Inactivity Timeout	15 minutes	

Table 58 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)	
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 164
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 168
TFTP Server IP Address	0.0.0.0 (no IP address assigned)	
Copy Configuration Image to Server	No	
Retrieve Configuration Image from Server	No	

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
#
# 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= BS380_20046.img

# 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
#    boot file:                   BS380_20046.img
```

Index