Software Release V4.0.0

Part No. 309979-D Rev 00
March 2001

4401 Great America Parkway
Santa Clara, CA 95054

Using the BayStack 350 10/100/1000 Series Switch

NORTEL NETWORKS™

Copyright © 2001 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 is a trademark of Nortel Networks Inc.

Accelar, BayStack, Bay Networks, Centillion, EZ LAN, Optivity, Optivity Campus, Optivity Enterprise, StackProbe, and the Bay Networks logo are trademarks of Nortel Networks Inc.

Microsoft, MS, MS-DOS, Win32, Windows, and Windows NT are trademarks of Microsoft Corporation.

All other trademarks are the property of their respective owners.

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.

USA Requirements Only

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

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

European Requirements Only

EN 55 022 Statement

This is to certify that the Nortel Networks BayStack 350 switch is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class A (CISPR 22).

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

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

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

EC Declaration of Conformity

This product conforms (or these products conform) to the provisions of Council Directive 89/336/EEC and 73/23/EEC. Go to *http://libra2.corpwest.baynetworks.com/cgi-bin/ndCGI.exe/DocView/* on the Nortel Networks World Wide Web site for a copy of the Declaration of Conformity.

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。

Voluntary Control Council for Interference (VCCI) Statement

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

Taiwan Requirements

Bureau of Standards, Metrology and Inspection (BSMI) Statement

警告使用者:

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

Canada Requirements Only

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (BayStack 350 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 350 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, 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

Preface

Chapter 1
BayStack 350 10/100/1000 Series Switches

Chapter 2
Installing the BayStack 350 Switch

Chapter 3
Using the Console Interface

Chapter 4
Troubleshooting

Appendix A
Technical Specifications

Appendix B
Gigabit Fiber Optical Characteristics

Appendix C
Media Dependent Adapters

Appendix D
ATM Overview

Appendix E
Quick Steps to Features

Appendix F
Connectors and Pin Assignments

Appendix G
Default Settings

Appendix H
Sample BootP Configuration File

Figures

Tables

Preface

Congratulations on your purchase of the BayStack™ 350 switch, part of the Nortel Networks™ BayStack 10/100/1000 Switch line of communications products.

There are two versions of the BayStack 350 switch: the Model 350-24T, and the Model 350-12T. This guide describes the features, uses, and installation procedures for the two versions. (Unless otherwise specified, the terms "BayStack 350 switch" and "switch" refer to both switch versions.)

BayStack 350 switches include a dedicated Uplink/Expansion Module slot for attaching optional media dependent adapters (MDAs) that support a range of media types, including gigabit Ethernet and asynchronous transfer mode (ATM). Installation instructions are included with each MDA (see your Nortel Networks sales representative for ordering information).

For more information about the MDAs, refer to Appendix C, "Media Dependent Adapters."

Audience

This guide is intended for network installers and system administrators who are responsible for installing, configuring, or maintaining networks. This guide assumes that you understand the transmission and management protocols used on your network.

Organization

This guide has four chapters, eight appendixes, and an index:

If you want to:	Go to:
Learn about your BayStack 350 switch and its key features	Chapter 1
Install your BayStack 350 switch on a flat surface or in a 19-inch equipment rack, and verify its operation	Chapter 2
Connect to your BayStack 350 switch Console/Comm Port and learn how to use the console interface (CI) menus to configure and manage a standalone switch or a stack configuration	Chapter 3
Troubleshoot and diagnose problems with your BayStack 350 switch	Chapter 4
View BayStack 350 switch operational and environmental specifications	Appendix A
View gigabit fiber optical characteristics of the (optional) 1000BASE-SX/LX MDAs	Appendix B
Learn about optional MDAs you can use with your BayStack 350 switch	Appendix C
Learn important ATM terminology and concepts that relate to your BayStack 450-2M3/2S3 MDAs	Appendix D
View Quick-Step flowcharts for using your BayStack 350 switch features	Appendix E
Learn more about your BayStack 350 switch connectors (ports) and pin assignments	Appendix F
View a listing of the factory default settings for your BayStack 350 switch	Appendix G
View a sample BootP configuration file	Appendix H
View an alphabetical listing of the topics and subtopics in this guide, with cross-references to relevant information	Index

Text Conventions

This guide uses the following text conventions:

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.

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`

[Enter]

Named keys in text are enclosed in square brackets. The notation [Enter] is used for the Enter key and the Return key.

[Ctrl]-C

Two or more keys that must be pressed simultaneously are shown in text linked with a hyphen (-) sign.

Acronyms

This guide uses the following acronyms:

ATM	asynchronous transfer mode
BootP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
BUS	broadcast and unknown server
CI	console interface
CRC	cyclic redundancy check
CSMA/CD	carrier sense multiple access/collision detection
CTS	clear to send
DCE	data communications equipment
DSR	data set ready
DTE	data terminal equipment
EAP	Extensible Authentication Protol
EAPOL	Extensible Authentication Protol Over LANs
ECM	Entity Coordination Management
ELAN	emulated LAN
FID	filtering database identifier
HRPSU	high-power redundant power supply unit
IGMP	Internet Gateway Management Protocol
ILMI	Interim local management interface
IP	Internet Protocol
ISO	International Organization for Standardization
ISVN	interoperability software version number
LANE	LAN emulation
LEC	LAN emulation client
LECS	LAN emulation configuration server

(continued)

LED	light-emitting diode
LES	LAN emulation server
MAC	media access control
MDA	media dependent adapter
MDI	medium dependent interface
MDI-X	medium dependent interface-crossover
MIB	Management Information Base
MLT	MultiLink Trunk
NIC	network interface controller
NMS	network management station
PAE	port access entity
PID	Protocol Identifier
PVID	port VLAN identifier
RADIUS	Remote Authentication Dial-In User Services
RARP	Reverse Address Resolution Protocol
RMON	remote monitoring
RPSU	redundant power supply unit
SNMP	Simple Network Management Protocol
STA	Spanning Tree Algorithm
STP	Spanning Tree Protocol
TELNET	Network Virtual Terminal Protocol
TFTP	Trivial File Transfer Protocol
UNI	user-to-network interface
UTP	unshielded twisted pair
VC	virtual channel
VID	VLAN identifier
VLAN	virtual local area network
VP	virtual path

Related Publications

For more information about using the BayStack 350 switch, refer to the following publications:

- *Installing Media Dependent Adapters (MDAs)* (Part number 302403-F)

  Describes how to install optional MDAs on your BayStack 350 switch.

- *Gigabit Interface Converter (GBIC) Installation Guide* (Part number 208723-A)

  Provides a list of GBICS that are available from Nortel Networks, and includes procedures for installing/removing GBICs from supported devices, general specifications, cabling standards, and product descriptions for each model.

- *Wall Mounting Instructions* (Part number 304602-A)

  Describes how to mount up to two BayStack 350 or BayStack 450 switches on any wall that can safely support the weight of the switches, including any attached cables.

- *Reference for the BayStack 350/410/450 Management Software Operations* (Part number 210245-C)

  Describes the Nortel Networks Device Manager software, a set of graphical network management applications you can use to configure and manage the BayStack 350/410/450 switches.

- *Bay Networks Guide to Implementing BaySecure LAN Access for Ethernet* (Part number 345-1106A)

  Describes Nortel Networks real-time security system that safeguards Ethernet networks from unauthorized surveillance and intrusion.

- *Managing Network Access with Optivity SecureLAN* (Part number 312688-A)

  Describes how you can use the Nortel Networks Optivity SecureLAN application to control network access to your switch or stack.

You can print selected technical manuals and release notes free, directly from the Internet. Go to the *www25.nortelnetworks.com/library/tpubs/* Web address. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe Acrobat Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to the Adobe Systems Web address at *www.adobe.com* to download a free copy of Acrobat Reader.

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

How to Get Help

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

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

Technical Solutions Center	**Telephone**
Billerica, MA	800-4NORTEL or (800) 466-7835
Santa Clara, CA	800-4NORTEL or (800) 466-7835
Valbonne, France	(33) (4) 92-96-69-68
Sydney, Australia	(61) (2) 9927-8800
Tokyo, Japan	(8) (3) 5740-1700

Chapter 1
BayStack 350 10/100/1000 Series Switches

This chapter introduces the BayStack 350 switch and covers the following topics:

Physical Description

There are two versions of the BayStack 350 switch: the BayStack 350-24T switch and the BayStack 350-12T switch (Figure 1-1).

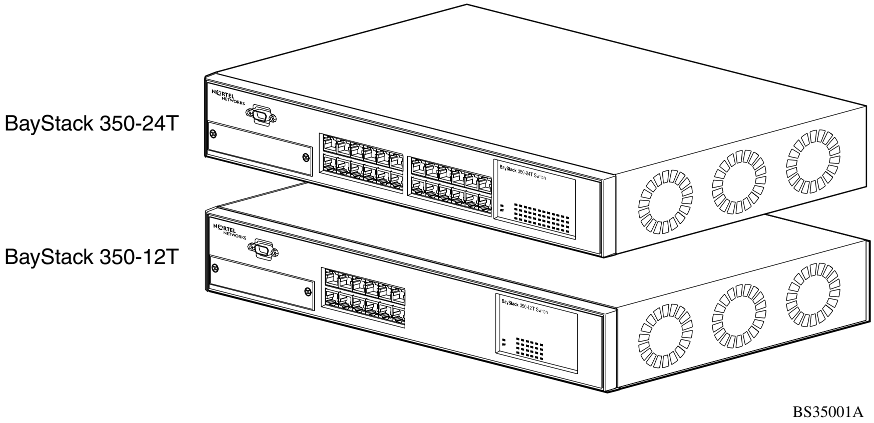
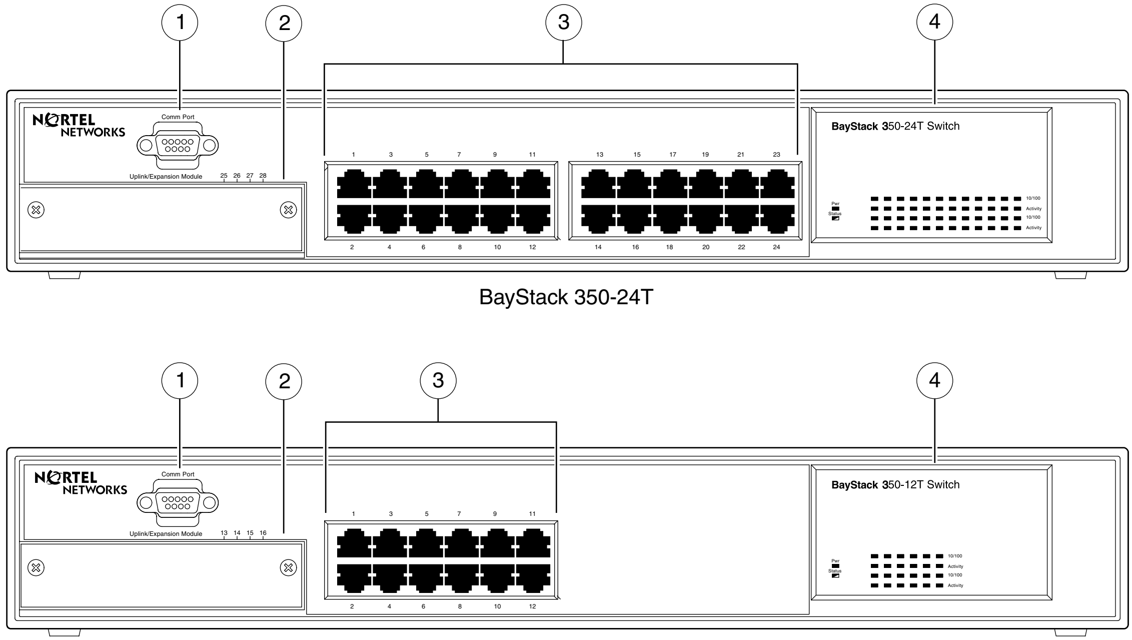


Figure 1-1. BayStack 350 Switch Versions

Front Panel

Figure 1-2 shows the front-panel configurations for the two BayStack 350 switch models. Descriptions of the front-panel components follow the figures.

For a description of the components located on the back panel of the BayStack 350 switch, see “Back Panel” on page 1-7.



BayStack 350-24T

BayStack 350-12T

1 = Comm Port

2 = Uplink/Expansion Module slot

3 = 10BASE-T/100BASE-TX port connectors

4 = LED display panel

BS35002B

Figure 1-2. **BayStack 350 Switch Front Panels**

Comm Port

The Comm Port (also referred to as the Console/Comm 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”).

The Console/Comm 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 switch by using a straight-through DB-9 to DB-9 standard serial port cable (see “Console/Comm Port” on page 2-10).

Note: The Console/Comm Port is configured as a data communications equipment (DCE) connector. Ensure that your RS-232 cable pinouts are configured for DCE connections (see “DB-9 (RS-232-D) Console/Comm Port Connector” on page F-5).

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

Uplink/Expansion Module Slot

The Uplink/Expansion Module slot allows you to attach optional MDAs that support a range of media types (see Appendix C, “Media Dependent Adapters” for more information about MDA types available from Nortel Networks).

10BASE-T/100BASE-TX Port Connectors

Your BayStack 350 switches use 10BASE-T/100BASE-TX RJ-45 (8-pin modular) port connectors.

Note: The RJ-45 port connectors on BayStack 350 switches manufactured prior to December 1998 are numbered 1 to 12 and 13 to 24, in succession from left to right. Later units use port connectors that are configured with one or two dual, six-port groups, numbered 1 to 12 and 13 to 24. The top rows are odd numbered and the bottom rows are even numbered (see Figure 1-2 on page 1-3). Port-specific examples in this guide show the appropriate port connections when required; other examples apply to both versions.

The 10BASE-T/100BASE-TX port connectors are configured as MDI-X (media-dependent interface-crossover). These ports connect over straight cables to the network interface controller (NIC) card in a node or server, similar to a conventional Ethernet repeater hub. If you are connecting to another Ethernet hub or Ethernet switch, you need a crossover cable unless an MDI connection exists on the associated port of the attached device (see “MDI and MDI-X Devices” on page F-2).

The switches use autosensing ports that are designed to operate at 10 Mb/s or at 100 Mb/s, depending on the connecting device. These ports support the IEEE 802.3u autonegotiation standard, which means that when a port is connected to another device that also supports the IEEE 802.3u standard, the two devices negotiate the best speed and duplex mode.

The 10BASE-T/100BASE-TX switch ports also support half- and full-duplex mode operation (see “Connecting the 10BASE-T/100BASE-TX Ports” on page 2-8).

The switch uses 10BASE-T/100BASE-TX RJ-45 port connectors to connect to 10 Mb/s or 100 Mb/s Ethernet segments or nodes.

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

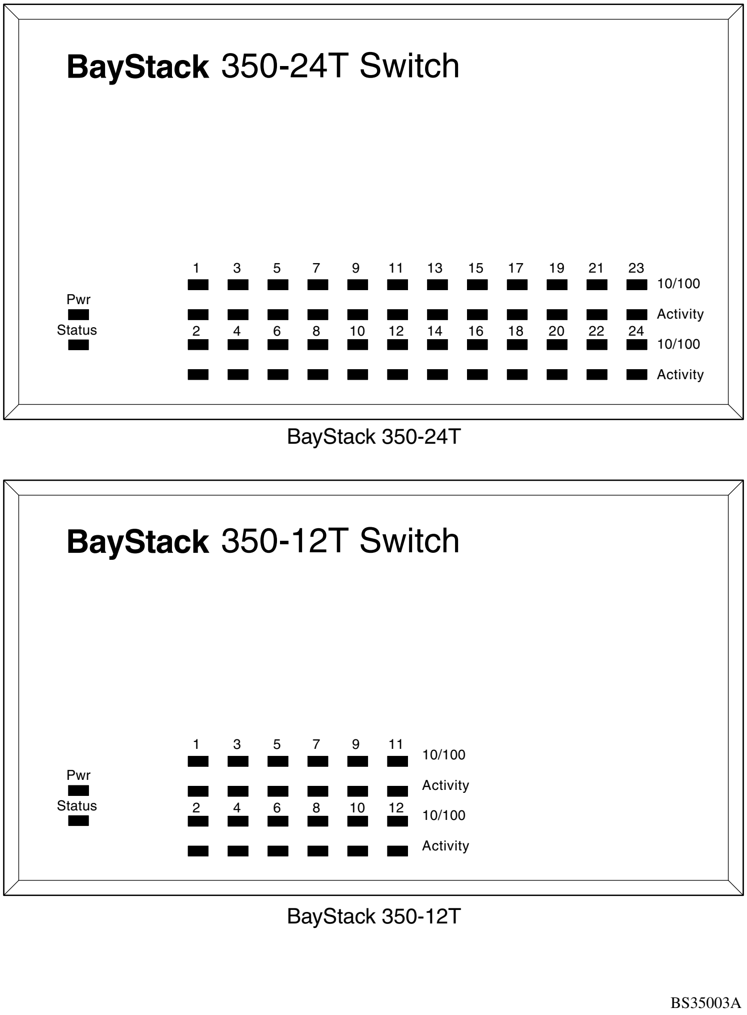
See Appendix F, “Connectors and Pin Assignments,” for more information about the RJ-45 port connectors.

LED Display Panel

Figure 1-3 shows the LED display panels for the BayStack 350-24T and the BayStack 350-12T models.

➡ **Note:** The LED display panel configuration for your switch may be different than shown in Figure 1-3, depending on the date of manufacturing (see the note in “10BASE-T/100BASE-TX Port Connectors” on page 1-4).

Refer to Table 1-1 for a description of the LEDs.



BayStack 350-24T

BayStack 350-12T

Figure 1-3. LED Display Panel

Table 1-1. 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.

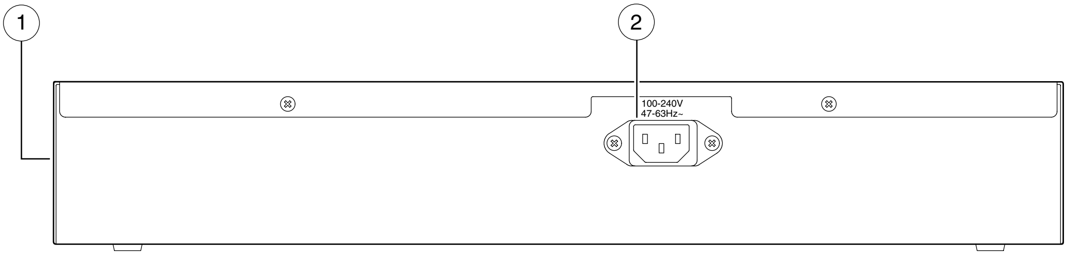
(continued)

Table 1-1. LED Descriptions (continued)

Label	Type	Color	State	Meaning
Status	System status	Green	On	Self-test passed successfully and switch is operational.
			Blinking	A nonfatal error occurred during the self-test.
			Off	The switch failed the self-test.
10/100	10/100 Mb/s port speed indicator	Green	On	The corresponding port is set to operate at 100 Mb/s and the link is good.
		Green	Blinking	The corresponding port has been disabled by software.
		Yellow	On	The corresponding port is set to operate at 10 Mb/s and the link is good.
		Yellow	Blinking	The corresponding 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.

Back Panel

The BayStack 350 switch back-panel components are the same for both switch versions (Figure 1-4). Descriptions of the back panel components follow the figure.



1 = Cooling fans (not shown)

2 = AC power receptacle

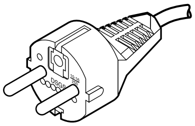
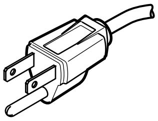
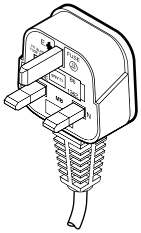
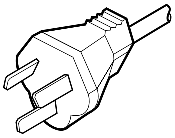
Figure 1-4. BayStack 350 Switch Back Panel

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 1-2 lists specifications for international power cords.

Table 1-2. 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
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

Cooling Fans

The variable-speed cooling fans (not shown) are located on one side of the BayStack 350 switch to provide cooling for the internal components. When you install the switch, be sure to allow enough space on *both sides* of the switch for adequate air flow.

Features

BayStack 350 switches provide 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).

BayStack 350 switches offer the following features:

- High-speed forwarding rate: Up to 3 million packets per second (peak)
- Store-and-forward switch: Full-performance forwarding at full line speed, using a 2.56-Gigabit/second switch fabric
- Learning rate: 3 million addresses per second (peak)
- Front-panel light-emitting diodes (LEDs) to monitor the following:
  - Power status
  - System status
  - Per-port status for the following:
    - 1000 Mb/s link
    - 100 Mb/s link
    - 10 Mb/s link
    - Half- and full-duplex transmission
    - Tx/Rx activity
    - Management enable/disable
- Address database size: 16,000 entries at line rate (32,000 entries without flooding)
- Spanning Tree Protocol (STP): Complies with IEEE 802.1D standard. STP can be disabled on the entire switch or on a per-port basis.

- IEEE 802.1Q port-based virtual LANs (VLANs)
- IGMP snooping
- IEEE 802.1p prioritizing
- MultiLink Trunking, supporting:
  - Switch-to-switch trunks
  - Switch-to-server trunks
- Port mirroring (conversation steering)
  - Port-based
  - MAC address-based
- Console/Comm port: Allows you to configure and manage the switch locally or remotely.
- Virtual local area networks (VLANs), supporting:
  - IEEE 802.1Q port-based VLANs
  - Protocol-based VLANs
- SNMP agent support
- Rate limiting: Adjustable broadcast or IP multicast packet-rate limits for control of broadcast and IP multicast storms
- TELNET:
  - Support for up to four simultaneous TELNET sessions
  - Optional password protection
  - Login time-out
  - Failed-login guard
  - Inactivity time-out
  - Allowed source addresses
  - Event logging
- High-speed Uplink/Expansion Module slot: Allows you to attach optional media dependent adapters (MDAs) that support a range of media types.

- IEEE 802.3u-compliant autonegotiation ports, with four modes:
  - 10BASE-T half-duplex
  - 10BASE-T full-duplex
  - 100BASE-TX half-duplex
  - 100BASE-TX full-duplex
- Remote monitoring (RMON), with four groups integrated:
  - Statistics
  - History
  - Alarms
  - Events
- Upgradeable device firmware in nonvolatile flash memory using the Trivial File Transfer Protocol (TFTP).
- Configuration file download/upload support: allows you to store your switch configuration parameters on a TFTP server.
- Security:
  - MAC address-based security: Allows you to limit access to the switch based on MAC addresses.
  - EAPOL-based security: EAP over LANs (EAPOL) security allows you to limit access to the switch based on the Extensible Authentication Protocol (EAP).
  - RADIUS-based security: Allows you to set up your switch with Remote Authentication Dial-In User Services (RADIUS) security, for authenticating TELNET logins.
  - SNMP-based security: Allows you to limit administration access to the switch via IP filtering.

Security

Your BayStack 350 switch security feature can provide four levels of security for your local area network (LAN):

- "MAC Address-Based Security" (page 1-14) -- Limits access to the switch based on allowed source MAC addresses.
- "EAPOL-Based Security" (page 1-15) -- Limits access to the switch based on an authentication mechanism that uses Extensible Authentication Protocol (EAP) to exchange authentication information between the switch and an authentication server.
- "RADIUS-Based Security" (page 1-22) -- Limits administrative access to the switch through user authentication.
- "SNMP-Based Security" (page 1-23) -- Limits administration access via selective IP filtering.

Figure 1-5 shows an example of a typical campus configuration using the BayStack 350 switch security features. In this configuration example, the following security measures are implemented:

- The switch

  The switch is located in a locked closet, accessible only by authorized Technical Services personnel.

  -- MAC address-based security allows up to 448 authorized stations (MAC addresses) access to one or more switch ports (see "MAC Address-Based Security" on page 1-14).

  -- EAPOL-based security provides port-based network access control to authenticate devices based on user authentication (see "EAPOL-Based Security" on page 1-15).

  -- RADIUS-based security limits administrative access through user authentication (see "RADIUS-Based Security" on page 1-22).

  -- SNMP-based security limits administrative access through selective IP filtering (see "SNMP-Based Security" on page 1-23).

- Student dormitory

  Dormitory rooms, typically occupied by two students, are 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.

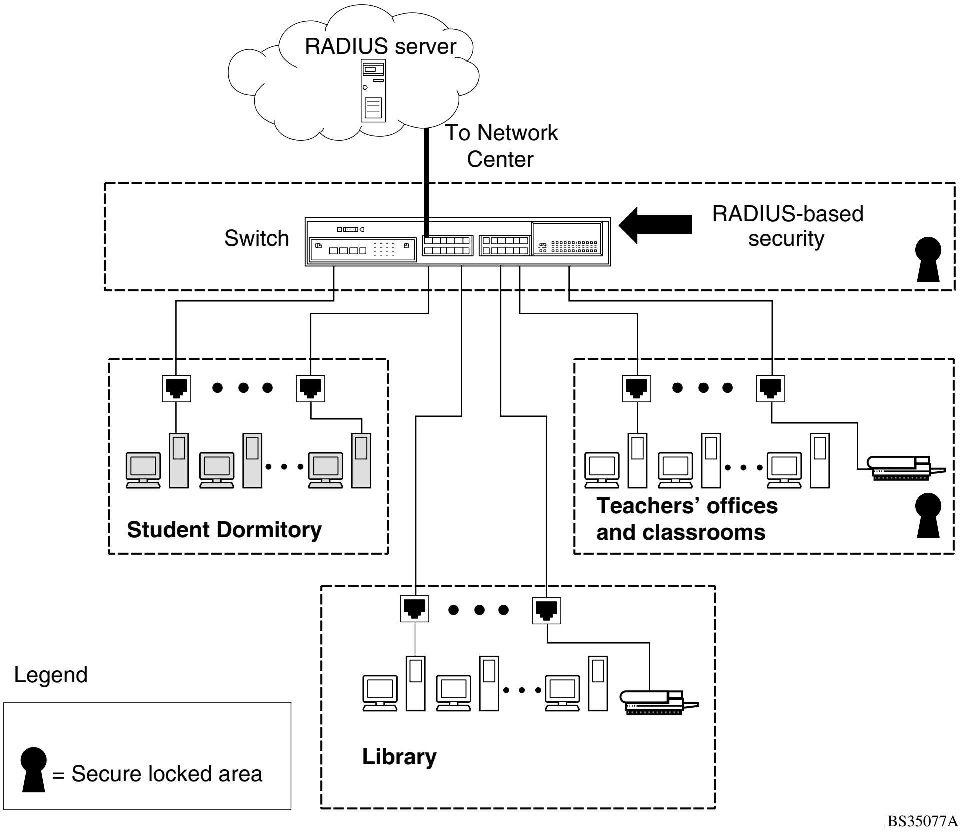


Figure 1-5. BaySack 350 Switch Security Feature Example

- 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 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.

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 or stack configuration. The 448 MAC addresses can be configured within a single standalone switch or they can be distributed in any order among the units in a single stack configuration.
- Specify which of your switch ports each MAC address is allowed to access.

  The options for allowed port access include: NONE, ALL, and single or multiple ports that are specified in a list, for example, 1/1-4,1/6,2/9 (see "Port List Syntax" on page 3-32).
- Specify actions your switch can take if the software detects a security violation.

  The switch can send a trap, turn on destination address (DA) filtering, disable the specific port, or use any combination of these three options.

For instructions on using the console interface (CI) to set up MAC address-based network access control, see "MAC Address-Based Security" on page 3-22.

See also Appendix E, "Quick Steps to Features," for configuration flowcharts that can help you use this feature.

➡ **Note:** You cannot configure a port for MAC address-based security if the port is currently configured for EAPOL-based security.

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. To learn more about Nortel Networks BaySecure LAN Access for Ethernet, refer to the *Bay Networks Guide to Implementing BaySecure LAN Access for Ethernet* (Part number 345-1106A).

EAPOL-Based Security

The EAPOL-based security feature uses the Extensible Authentication Protocol (EAP), as described in the IEEE Draft P802.1X, to allow you to set up network access control on internal LANs.

EAP allows the exchange of authentication information between any end station or server connected to the switch and an authentication server (such as a RADIUS server).

The EAPOL-based security feature operates in conjunction with a RADIUS-based server to extend the benefits of remote authentication to internal LAN clients (see "RADIUS-Based Security" on page 1-22).

This section covers the following topics:

- "Security Example" (page 1-16)
- "Overview and Terms" (page 1-17)
- "Dynamic VLAN Assignment" (page 1-18)
- "Setting Up the Authentication Server" (page 1-19)
- "Authentication Process" (page 1-20)
- "System Requirements" (page 1-21)
- "Configuration Rules" (page 1-22)

For instructions on using the console interface (CI) to set up MAC address-based network access control, see "MAC Address-Based Security" on page 3-22.

See also Appendix E, "Quick Steps to Features," for configuration flowcharts that can help you use this feature.

Security Example

The following example illustrates how the BayStack 350 switch, configured with the EAPOL-based security feature, reacts to a new network connection:

1. The switch detects a new connection on one of its ports (Figure 1-6).
    a. The switch requests a user ID from the new client (1).
    b. EAPOL encapsulates and forwards the user ID to the RADIUS server (2).
    c. The RADIUS server requests the user's password (3).

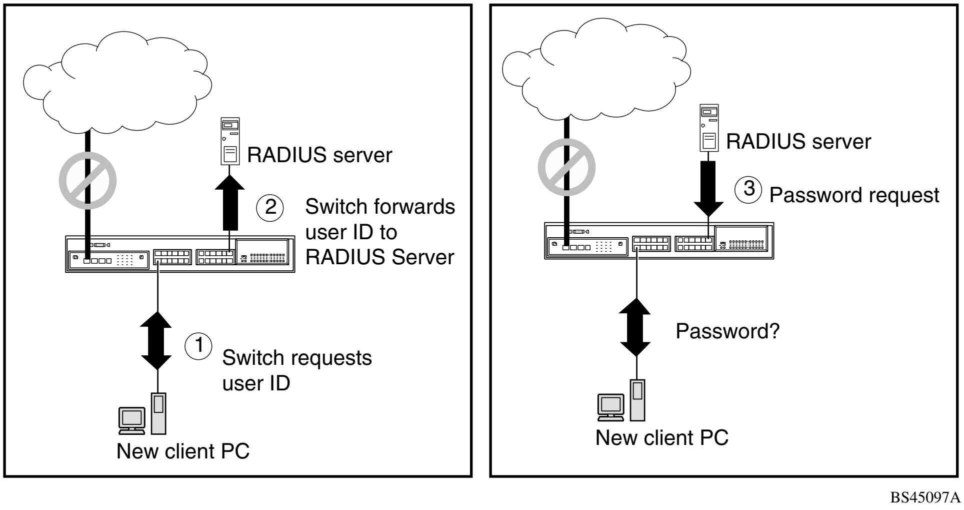


Figure 1-6. EAPOL-Based Security (1 of 2)

2. The new client forwards an encrypted password to the switch, within the EAPOL packet (Figure 1-7).
    a. The switch relays the EAPOL packet to the RADIUS server (4).
    b. If the RADIUS server validates the password (5), the new client is allowed access to the switch and the network (6).

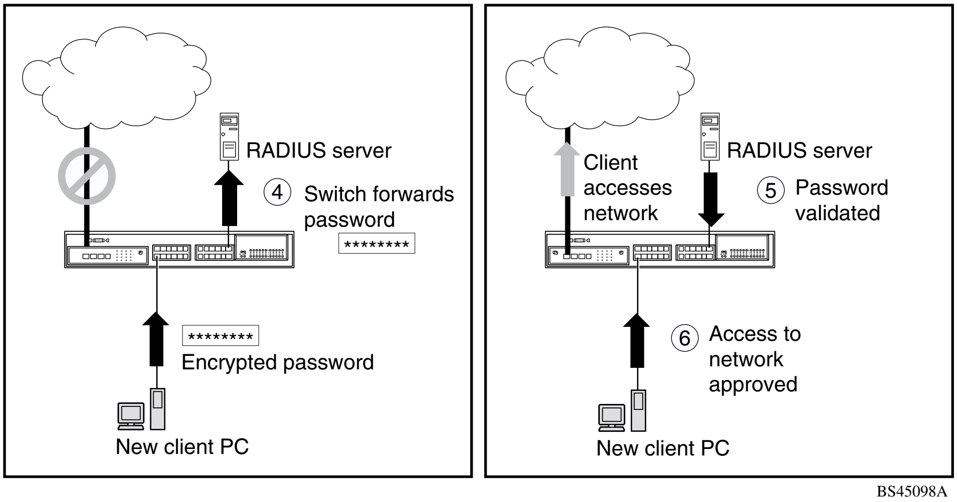


Figure 1-7. EAPOL-Based Security (2 of 2)

Overview and Terms

This section provides a detailed description of EAPOL-based security, including an overview of the components and terms used with this feature.

Some components of EAPOL-based security are:

- Supplicant -- the entity that the Authenticator is authorizing. The supplicant can be any end station or server that is connected to the switch. In the preceding example, the supplicant is the new client PC.
- Authenticator -- a software entity whose sole purpose is to authorize a *supplicant* that is attached to the other end of a LAN segment.
- Authentication Server -- a RADIUS server that provides authorization services to the Authenticator.
- Port Access Entity (PAE) -- a software entity associated with each port that supports the Authenticator or Supplicant functionality. In the preceding example, the Authenticator PAE resides on the switch.
- Controlled Port -- any switch port whose operational state is influenced by the Authenticator. In the previous example, the controlled port is the switch port that is connected to the new client PC.

The Authenticator communicates with the Supplicant using an encapsulation mechanism known as EAP over LANs (EAPOL). The Authenticator PAE encapsulates the EAP message into a RADIUS packet before sending the packet to the Authentication Server. It does not interfere with authentication exchanges that occur between the Supplicant and the Authentication Server (except for encapsulating the EAP message to make it suitable for the packet's destination).

The Authenticator also determines the *controlled* port's operational state. After the RADIUS server notifies the Authenticator PAE about the success or failure of the authentication, it changes the controlled port's operational state accordingly. The Authenticator PAE functionality is implemented for each controlled port on the switch. At system initialization, or when a supplicant is initially connected to the switch's controlled port, the controlled port's state is set to Blocking. During that time, only EAP packets can be received from the supplicant. When the Authentication server returns a "success" or "failure" message, the controlled port's state is changed accordingly. If the authorization is successful, the controlled port's operational state is set to Forwarding. Otherwise, the controlled port's state depends on the Operational Traffic Control field value in the EAPOL Security Configuration screen (see Figure 3-16 on page 3-38).

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

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

Dynamic VLAN Assignment

If EAPOL-based security is enabled on a port, and then the port is authorized, the EAPOL feature dynamically changes the port's VLAN configuration according to preconfigured values, and assigns a new VLAN. The new VLAN configuration values are applied according to previously stored parameters (based on the user_ID) in the Authentication server (see "Setting Up the Authentication Server" following this section). The following VLAN configuration values are affected:

- Port Membership
- PVID
- Port Priority

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

The following exceptions apply to dynamic VLAN assignments:

- The dynamic VLAN configuration values assigned by EAPOL are Not stored in the switch's NVRAM.
- You can override the dynamic VLAN configuration values assigned by EAPOL; however, the values you configure are not stored in NVRAM.
- If you configure values (other than VLAN configuration values) when EAPOL is enabled on a port, those values are applied and stored in NVRAM.

For more information about VLANs, see "Virtual Local Area Networks (VLANs)" on page 1-33.

Setting Up the Authentication Server

This section describes how to set up your Authentication server (RADIUS server) for EAPOL dynamic VLAN assignments. The Authentication server allows you to configure user-specific settings for VLAN memberships and port priority. When you log on to a system that has been configured for EAPOL authentication, the Authentication server recognizes your user ID and notifies the switch to assign preconfigured (user-specific) VLAN membership and port priorities to the switch. The configuration settings are based on configuration parameters that were customized for your user ID and previously stored on the Authentication server. To set up the Authentication server, set the following "Return List" attributes for all user configurations (refer to your Authentication server documentation):

- VLAN Membership Attributes
  - Tunnel-Type: value 13, Tunnel-Type-VLAN
  - Tunnel-Medium-Type: value 6, Tunnel-Medium-Type-802
  - Tunnel-Private-Group-Id: ASCII value 1 to 4094 (this value is used to identify the specified VLAN)
- Port Priority (Vendor-Specific) Attributes
  - Vendor Id: value 562, Nortel Networks vendor ID
  - Attribute Number: value 1, Port Priority
  - Attribute Value: value 0 (zero) to 7 (this value is used to indicate the port priority value assigned to the specified user)

Authentication Process

The flowcharts shown in Figures 1-8 and 1-9 describe the authentication process.

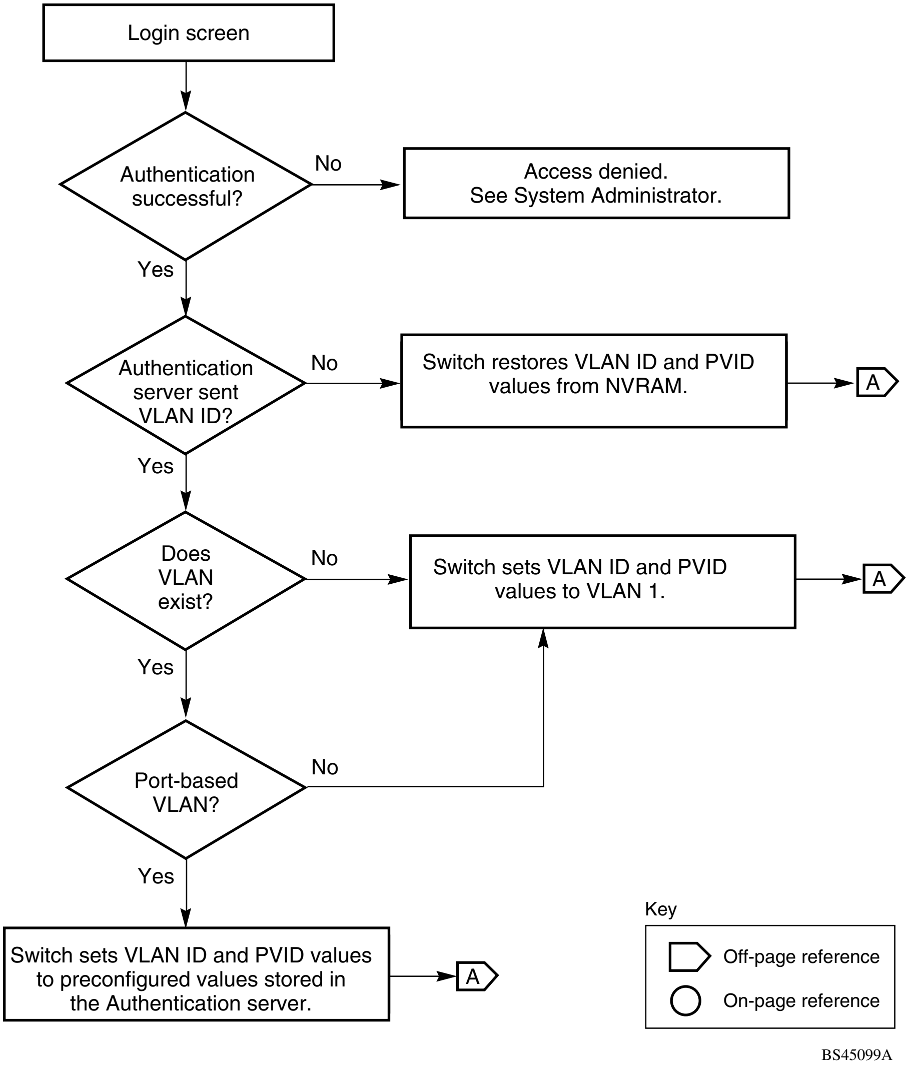

Login screen
Authentication successful?
No
Access denied. See System Administrator.
Yes
Authentication server sent VLAN ID?
No
Switch restores VLAN ID and PVID values from NVRAM.
A
Yes
Does VLAN exist?
No
Switch sets VLAN ID and PVID values to VLAN 1.
A
Yes
Port-based VLAN?
No
Yes
Switch sets VLAN ID and PVID values to preconfigured values stored in the Authentication server.
A
Key
Off-page reference
On-page reference
BS45099A

Figure 1-8. Authenticaton Process Flowchart (1 of 2)

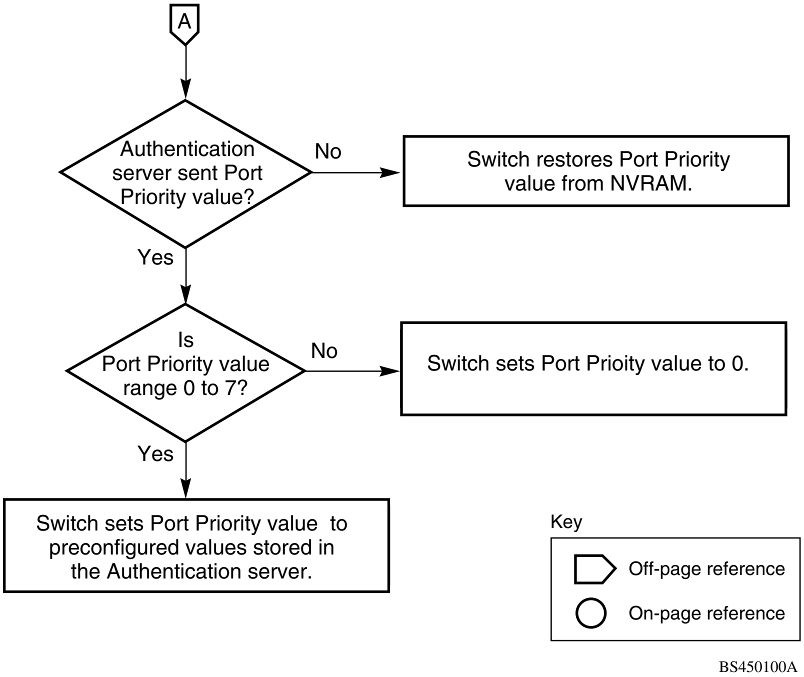

A
Authentication server sent Port Priority value?
No
Switch restores Port Priority value from NVRAM.
Yes
Is Port Priority value range 0 to 7?
No
Switch sets Port Prioity value to 0.
Yes
Switch sets Port Priority value to preconfigured values stored in the Authentication server.
Key
Off-page reference
On-page reference
BS450100A

Figure 1-9. Authenticaton Process Flowchart (2 of 2)

System Requirements

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

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

You must configure your BayStack 350/410-24T/450 switches and Business Policy Switch 2000 switches for port-based VLANs and EAPOL security (see the appropriate switch *User's Guide*.)

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

You can manage network access to your switch or stack using the CI menus and screens as described in Chapter 3, "Using the Console Interface," or you can use the Optivity SecureLAN application (refer to *Managing Network Access with Optivity SecureLAN* [Part number 312688-A]).

Configuration Rules

The follwing configuration rules apply to your BayStack 350 switch when using EAPOL-based security:

- Before configuring your switch, you must configure the Primary RADIUS Server and Shared Secret fields (see "Console/Comm Port Configuration" on page 3-95).
- You cannot configure EAPOL-based security on ports that are currently configured for:
  - MultiLink Trunking
  - MAC address-based security
  - IGMP (Static Router Ports)
  - ATM
  - Port mirroring
- You can connect a single client only on each port that is configured for EAPOL-based security.

RADIUS-Based 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 feature uses the RADIUS protocol to authenticate local console, TELNET, and EAPOL-authorized logins.You must 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 about setting up your RADIUS server, refer to your RADIUS server documentation.

For instructions on using the console interface (CI) to set up the RADIUS-based security feature, see "Console/Comm Port Configuration" on page 3-95.

SNMP-Based Security

The SNMP security feature allows you to set up network access control using selective IP filtering. SNMP-based security limits administration access to the switch, based on IP address filters.

For instructions on using the console interface (CI) to set up SNMP security, see "TELNET/SNMP Manager List Configuration" on page 3-111.

Flash Memory Storage

The following two sections describe switch parameters that are stored in flash memory.

Switch Software Image

Your switch's software image is stored in flash memory. The flash memory allows you to update your switch software image with a newer version, without changing the switch hardware (see "Software Download" on page 3-114). An in-band connection between the switch and the TFTP load host is required to download the software image.

If a BootP server is set up properly on the network and the BayStack 350 switch detects a corrupted software image during the self-test, the switch automatically uses TFTP to download a new software image.

Configuration Parameters

Certain configuration parameters, including the system characteristics strings, some VLAN parameters, IGMP configuration parameters, and the MultiLink Trunk names are stored in flash memory. These parameters are updated every 10 minutes *or whenever you issue the Save Current Settings command* (also, whenever you issue the Reset command).

➡ **Note:** Do not power off the switch within 10 minutes of changing any configuration parameters, *unless you first issue the Save Current Settings command*. Powering down the switch within 10 minutes of changing configuration parameters (without resetting) can cause the changed configuration parameters to be lost.

SNMP Support

The following two sections describe the SNMP support for the BayStack 350 switch.

MIBs

The BayStack 350 switch supports an SNMP agent with industry-standard MIBs, as well as private MIB extensions, which ensures compatibility with existing network management tools. The BayStack 350 switch supports the MIB-II (RFC 1213), the Bridge MIB (RFC 1493), and the RMON MIB (RFC 1757), which provide access to detailed management statistics.

The following MIBs are supported:

- EAPOL (IEEE 802.1X Port Access Control MIB)
- SNMPv2 (RFC 1907)
- Bridge MIB (RFC 1493)
- Ethernet MIB (RFC 1643)
- RMON MIB (RFC 1757)
- MIB-II (RFC 1213)
- Interface MIB (RFC 1573)
- ATM Forum LAN Emulation Client MIB

- Nortel Networks proprietary MIBs:
  - s5Chas MIB
  - s5Agent MIB
  - s5 Ethernet Multi-segment Topology MIB
  - s5 Switch BaySecure MIB
  - Rapid City MIB

SNMP Traps

The BayStack 350 switch supports an SNMP agent with industry standard SNMPv1 traps, as well as private SNMPv1 trap extensions (Table 1-3).

Table 1-3. Supported SNMP Traps

Trap Name	Configurable	Sent when:
RFC 1215 (Industry Standard):		
linkUp	Per port	A port’s link state changes to up.
linkDown	Per port	A port’s link state changes to down.
authenticationFailure	System wide	There is an SNMP authentication failure.
coldStart	Always on	The system is powered on.
warmStart	Always on	The system restarts due to a management reset.
s5Ctr MIB (Nortel Networks Proprietary Traps):		
s5CtrUnitUp	Always on	A unit is added to an operational stack.
s5CtrUnitDown	Always on	A unit is removed from an operational stack.
s5CtrHotSwap	Always on	A unit is hot-swapped in an operational stack.
s5CtrProblem	Always on	An assigned base unit fails.
s5EtrMgmAccessViolation	Always on	An SNMP management attempt by an “IP filtered” station is detected.
s5EtrSbsMacAccessViolation	System wide	A MAC address-based security violation is detected.

BootP Automatic IP Configuration/MAC Address

The BayStack 350 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 350 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. For an example of a BootP configuration file, see Appendix H, “Sample BootP Configuration File.”

Autosensing and Autonegotiation

BayStack 350 switches are autosensing and autonegotiating devices. The term *autosense* refers to a port’s ability to *sense* the speed of an attached device. The term *autonegotiation* refers to a standardized protocol (IEEE 802.3u) that exists between two IEEE 802.3u-capable devices.

Autonegotiation allows the BayStack 350 switch to select the best of both speed and duplex modes. Autosensing is used when the attached device is not capable of autonegotiation or is using a form of autonegotiation that is not compatible with the IEEE 802.3u autonegotiation standard. In this case, because it is not possible to sense the duplex mode of the attached device, the BayStack 350 switch reverts to half-duplex mode.

When autonegotiation-capable devices are attached to the BayStack 350 switch, the switch ports negotiate down from 100 Mb/s speed and full-duplex mode until the attached device acknowledges a supported speed and duplex mode.

For more information about autosensing and autonegotiation modes, see “Autonegotiation Modes” on page 4-6.

Configuration and Switch Management

The BayStack 350 switch is shipped directly from the factory ready to operate in any 10BASE-T or 100BASE-TX standard network. You can manage the switch using the Nortel Networks Optivity® network management software, Nortel Networks Device Manager Software, or any generic SNMP-based network management software; however, you must assign an IP address to the switch or stack, depending on the mode of operation (see "Initial Setup" on page 2-17).

You can also set up a BootP server to recognize the BayStack 350 switch BootP requests (see "BootP Automatic IP Configuration/MAC Address" on page 1-26).

For more information about using the Console/Comm Port to configure the switch, see Chapter 3, "Using the Console Interface."

Network Configurations

You can use BayStack 350 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 that is connected to the switch, or by creating a virtual LAN (VLAN) through the switch.

This section provides four network examples using BayStack 350 switches:

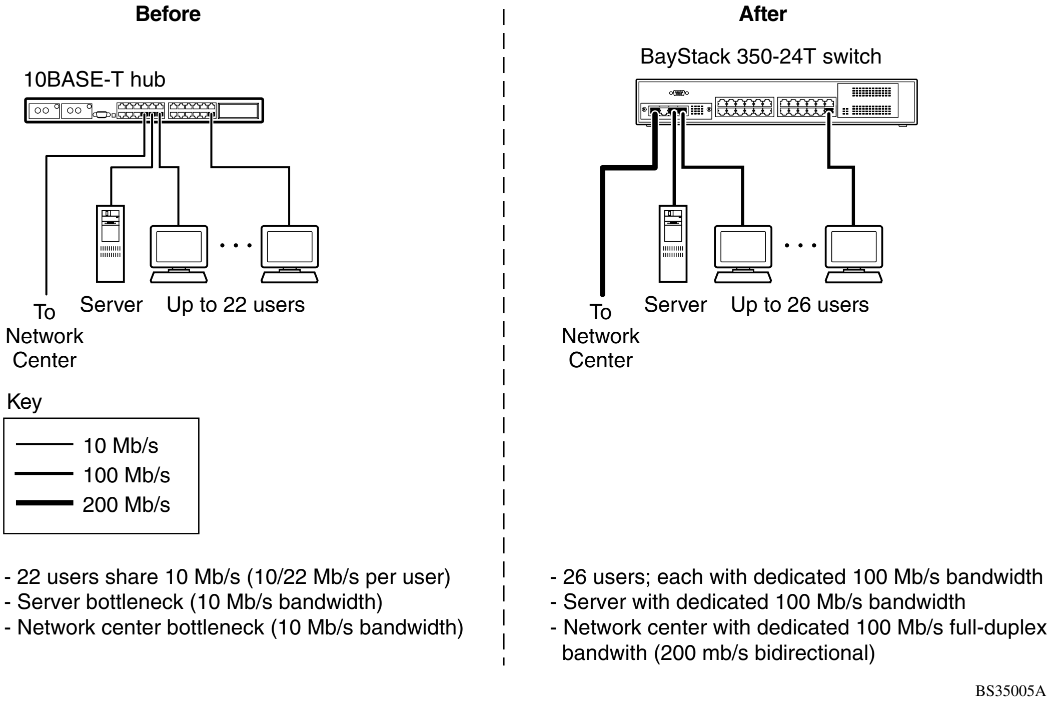
- Desktop switch application
- Segment switch application
- High-density switched workgroup application
- ATM application

➡ **Note:** All models of the BayStack 350 switch can be used interchangeably in the following network configuration examples.

Desktop Switch Application

Figure 1-10 shows the BayStack 350-24T switch used as a desktop switch, where desktop workstations are connected directly to switch ports.

This configuration provides dedicated 100 Mb/s connections to the network center, to the server, and up to 26 users. This configuration uses the optional 400-4TX MDA (10BASE-T/100BASE-TX MDA).



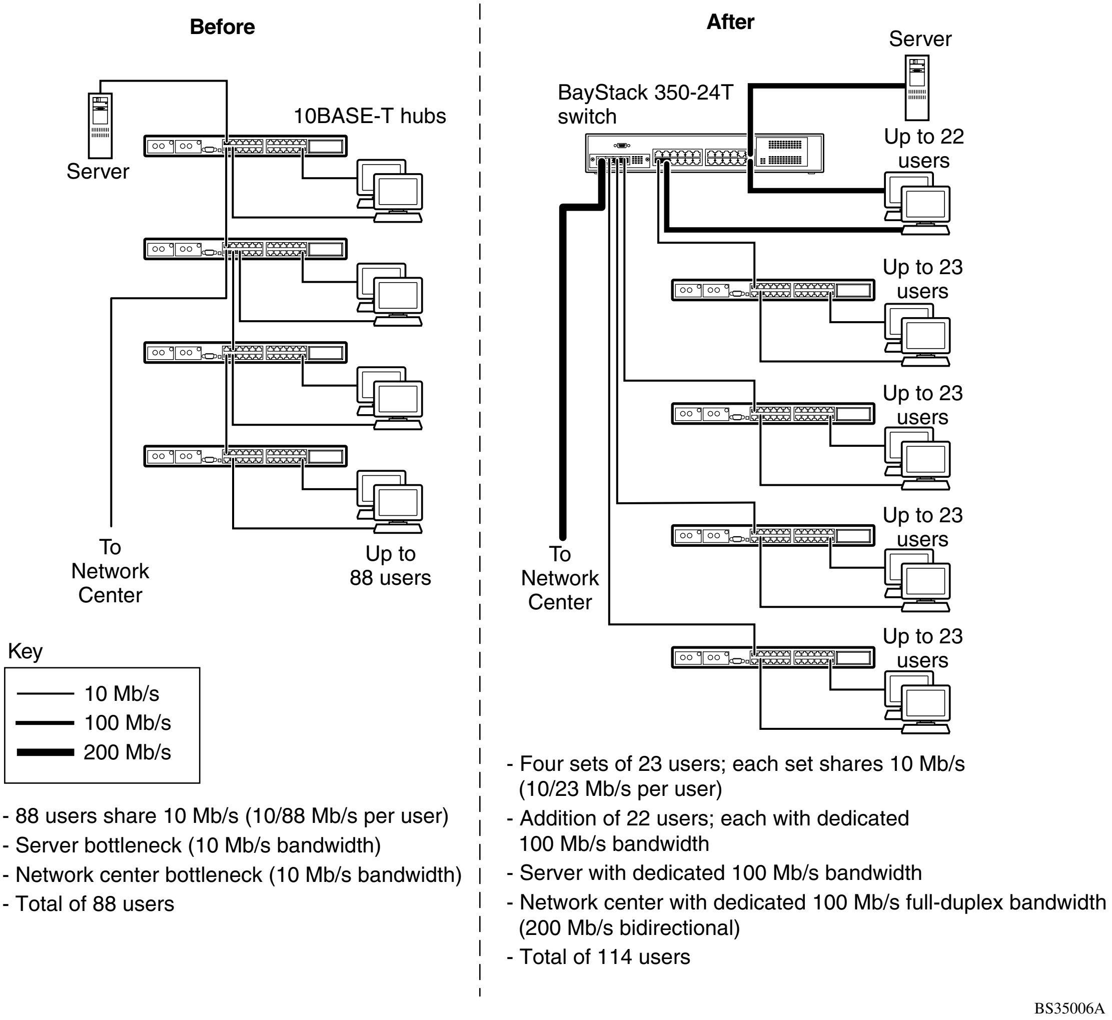
- 22 users share 10 Mb/s (10/22 Mb/s per user)
- Server bottleneck (10 Mb/s bandwidth)
- Network center bottleneck (10 Mb/s bandwidth)

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

Figure 1-10. BayStack 350-24T Used as a Desktop Switch

Segment Switch Application

Figure 1-11 shows the BayStack 350-24T switch used as a segment switch to alleviate user contention for bandwidth and eliminate server and network bottlenecks. Before segmentation, 88 users had a total bandwidth of only 10 Mb/s available. After segmentation, 92 users have 40 Mb/s, four times the previous bandwidth, while adding 22 dedicated 100 Mb/s connections. This configuration can be extended to add more segments without degrading performance.



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

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

Figure 1-11. BayStack 350-24T Used as a Segment Switch

High-Density Switched Workgroup Application

Figure 1-12 shows a BayStack 350-24T switch with a high-speed (gigabit) connection to a Nortel Networks Accelar™ 1100 switch. BayStack 303 and 304 switches are also shown in this example of a high-density switched workgroup.

As shown in Figure 1-12, the Accelar 1100 switch is used as a backbone switch, connecting to the BayStack 350 switch with an optional gigabit (1000BASE-SX) MDA for maximum bandwidth. The BayStack 303 and 304 switches have 100 Mb/s connections to the BayStack 350 switch, a 100BASE-TX hub, and a 100 Mb/s server and 10 Mb/s connections to DTE (data terminal equipment).

See the Nortel Networks library Web page: *www25.nortelnetworks.com/library/* for online documentation about the Nortel Networks Accelar 1100 switch and the BayStack 303 and 304 switches.

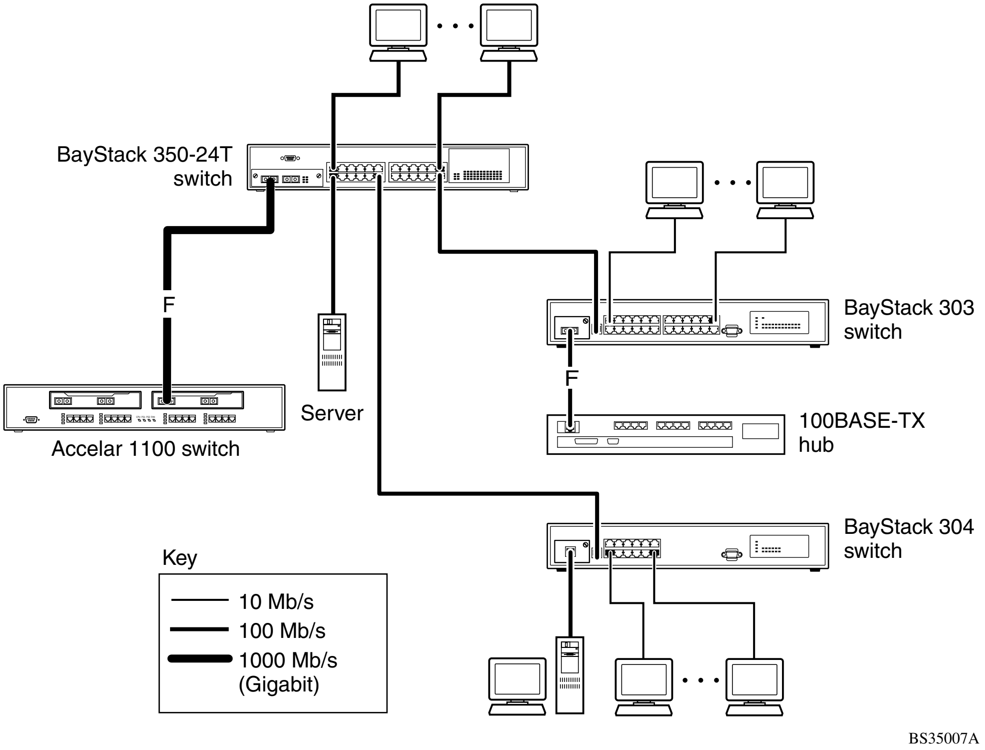


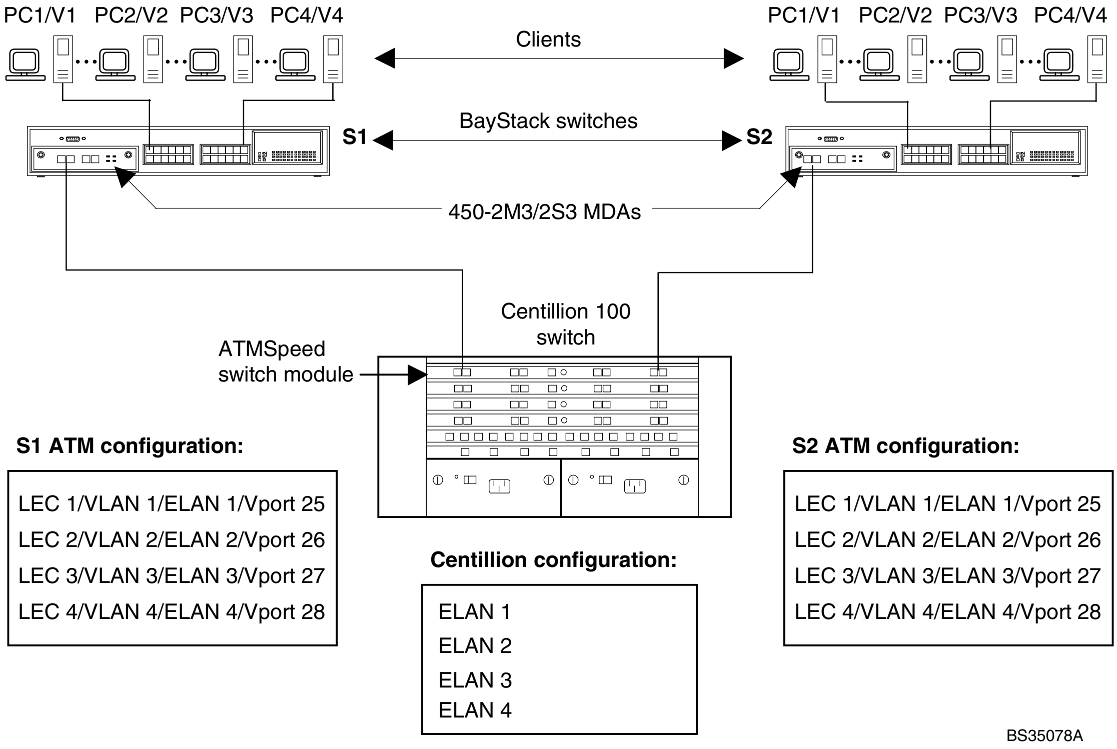
Figure 1-12. Configuring Power Workgroups and a Shared Media Hub

ATM Application

Figure 1-13 shows an example of using your BayStack 350 switches with optional BayStack 450-2M3/2S3 MDAs installed. You can configure each switch with up to four virtual ports that correspond to any of four LAN Emulation Clients (LECs) within the MDA.

In this example, the BayStack 450-2M3/2S3 MDAs provide asynchronous transfer mode (ATM) connections to a Nortel Networks Centillion™ 100 switch. Clients (PCs) that are connected to S1 can communicate with clients connected to S2, provided that the VLANs (with their respective client members) are mapped onto the same ELANs as shown.

See "Setting Up an ATM Configuration" on page 1-32 for more information about setting up your BayStack 450-2M3/2S3 MDA.



S1 ATM configuration:

LEC 1/VLAN 1/ELAN 1/Vport 25
LEC 2/VLAN 2/ELAN 2/Vport 26
LEC 3/VLAN 3/ELAN 3/Vport 27
LEC 4/VLAN 4/ELAN 4/Vport 28

Centillion configuration:

ELAN 1
ELAN 2
ELAN 3
ELAN 4

S2 ATM configuration:

LEC 1/VLAN 1/ELAN 1/Vport 25
LEC 2/VLAN 2/ELAN 2/Vport 26
LEC 3/VLAN 3/ELAN 3/Vport 27
LEC 4/VLAN 4/ELAN 4/Vport 28

Figure 1-13. Configuring an ATM Application

Setting Up an ATM Configuration

This section lists the steps required to set up the ATM configuration example shown in Figure 1-13 on page 1-31.

> **Note:** Certain spanning tree considerations apply when configuring Vports (see “Spanning Tree on LEC Ports” on page D-11).

For ATM terminology, as well as concepts and examples of how the BayStack 450-2M3/2S3 MDAs operate within an ATM environment, see Appendix D, “ATM Overview.”

To set up the ATM configuration:

1. **Create VLAN 1, including S1 (PC 1) and S2 (PC 1) as VLAN members, and also set the appropriate PVIDs for the respective PC ports.**

   See “VLAN Configuration Menu” on page 3-41, for help in creating VLANs.

2. **Create an ELAN (ELAN 1) on the Centillion 100 switch.**

   Refer to the Centillion 100 switch documentation.

3. **Configure a virtual port (Vport LEC 1) on S1 that corresponds to VLAN 1 and ELAN 1.**

   Refer to “ATM Configuration Menu” on page 3-85.

4. **Configure a virtual port (Vport LEC 1) on S2 that corresponds to VLAN 1 and ELAN 1.**

5. **Repeat steps 1 to 4 for each of the three remaining LECs within the BayStack 450-2M3/2S3 MDAs.**

For details about creating VLANs, see “VLAN Configuration Menu” on page 3-41.

For details about configuring the BayStack 450-2M3/2S3 MDA using the CI menus and screens, refer to“ATM Configuration Menu” on page 3-85.

Appendix E, “Quick Steps to Features,” provides flowcharts that you can use as quick configuration guides for the BayStack 350 switch features.

See the Nortel Networks library Web page: *www25.nortelnetworks.com/library/* for online documentation about the Nortel Networks Centillion 100 switch.

Virtual Local Area Networks (VLANs)

In a traditional shared-media network, traffic generated by a station is propagated 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.

Supported VLAN Types

Your BayStack 350 switch supports two types of VLANs:

- 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.

- Protocol-based VLANs

  A protocol-based VLAN is a VLAN in which you assign your switch ports as members of a broadcast domain, based on the protocol information within the packet. Protocol-based VLANs can localize broadcast traffic and assure that only the protocol-based VLAN ports are flooded with the specified protocol type packets. Your switch ports can be members of multiple protocol-based VLANs that are *not based* on the same protocol. Only tagged ports can be members of multiple protocol-based VLANs that *are based* on the same protocol.

You can create port-based VLANs and protocol-based VLANs, in any combination, as long as you do not exceed a total of 64 VLANs.

IEEE 802.1Q VLAN Workgroups

BayStack 350 switches support up to 64 VLANs with 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 IP 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 1-14). 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.

BayStack 350 switches allow you to assign ports to VLANs using the console, TELNET, or any generic SNMP-based network management software. 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.

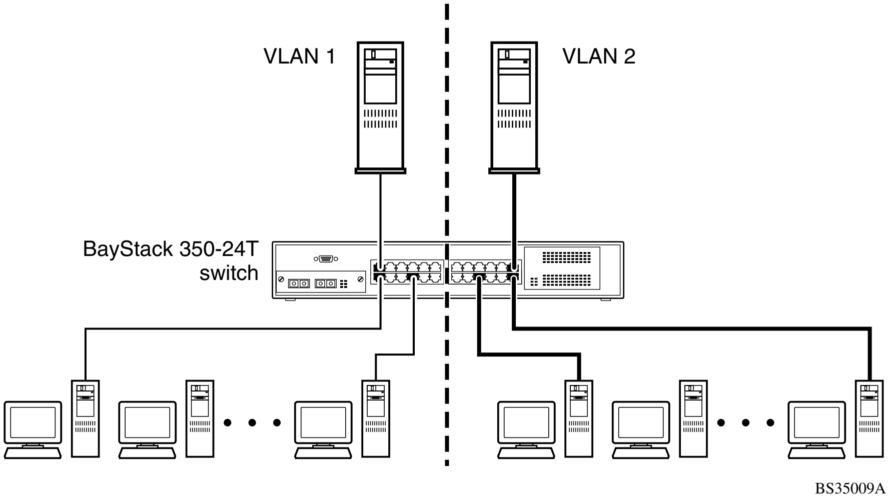


Figure 1-14. Port-Based VLAN Example

IEEE 802.1Q Tagging

BayStack 350 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.
- Port VLAN identifier (PVID) -- a classification mechanism that associates a port with a specific VLAN (see Figures 1-16 to 1-21).
- 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 VLAN assigned to that frame. 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, and therefore has a value of 0 through 7. This field allows the tagged frame to carry the user_priority value 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 frame's user_priority value. *Tagged* packets get their user_priority value from the 802.1Q frame header.
- Unregistered packet -- a tagged frame that contains a VID where the receiving port is not a member of that VLAN.

- Filtering database identifier (FID) -- the specific filtering/forwarding database within the BayStack 350 switch that is assigned to each VLAN. The current version of software assigns *all VLANs* to the same FID. This is referred to as Shared VLAN Learning in the IEEE 802.1Q specification.

The default configuration settings for BayStack 350 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 1-15, all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID = 1). Untagged packets enter and leave the switch unchanged.

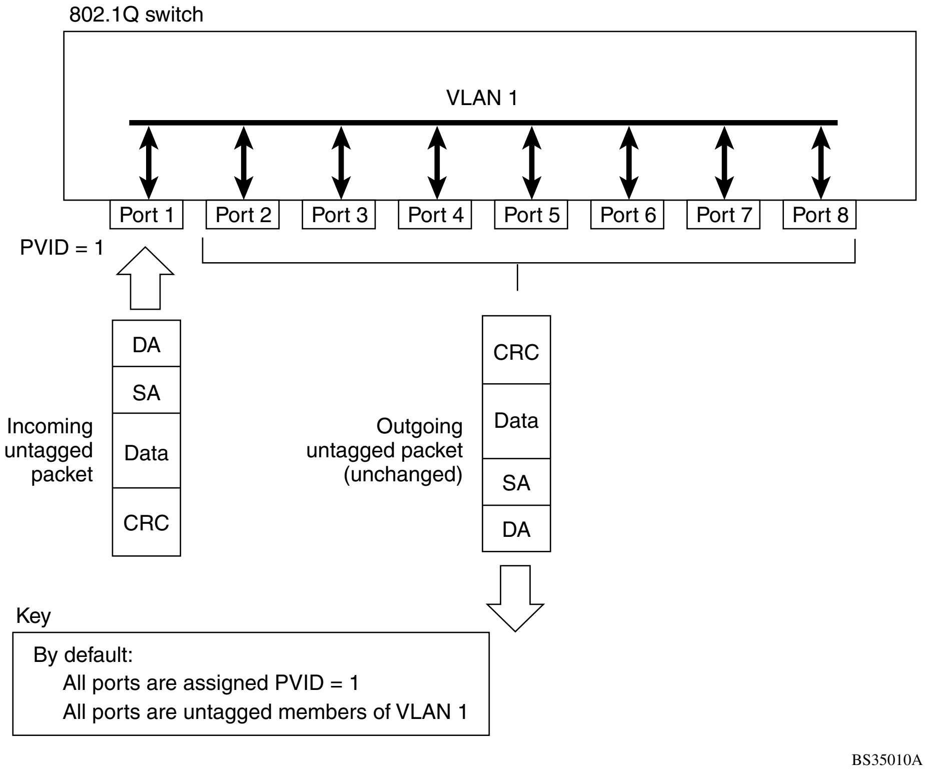


Figure 1-15. Default VLAN Settings

To configure VLANs, a user can reconfigure the switch ports as *tagged* or *untagged* members of specific VLANs (see Figures 1-16 to 1-21).

In Figure 1-16, 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.

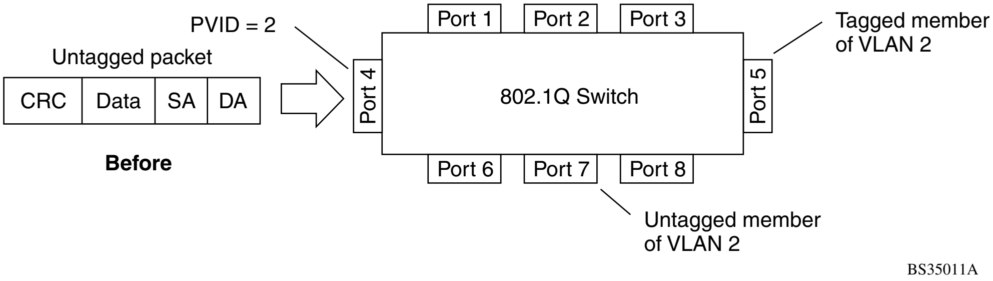


Figure 1-16. Port-Based VLAN Assignment

As shown in Figure 1-17, 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.

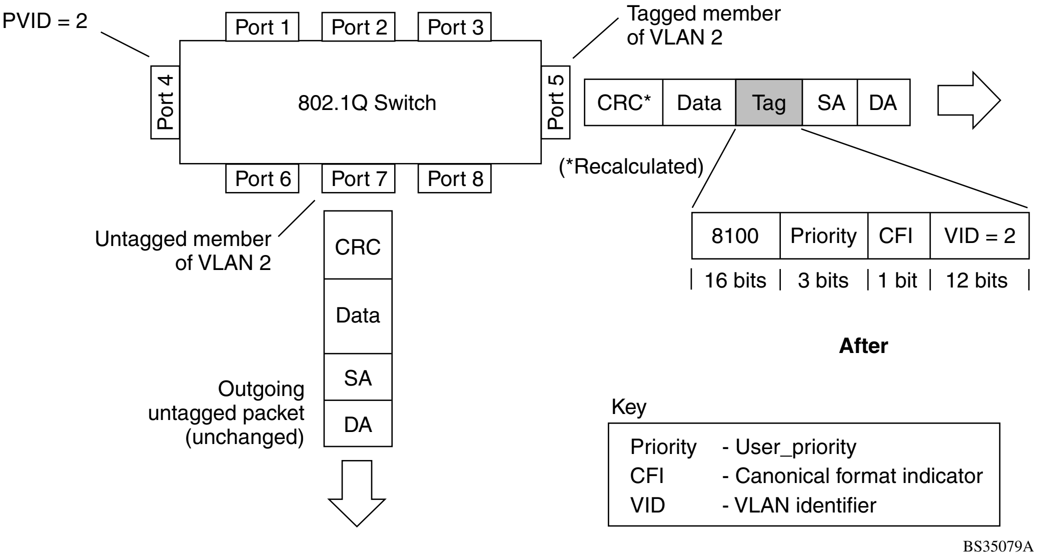


Figure 1-17. 802.1Q Tagging (After Port-Based VLAN Assignment)

In Figure 1-18, untagged incoming packets are assigned to VLAN 3 (IP Protocol VLAN = 3, PVID = 2). Port 5 is configured as a *tagged* member of VLAN 3, and port 7 is configured as an *untagged* member of VLAN 3.

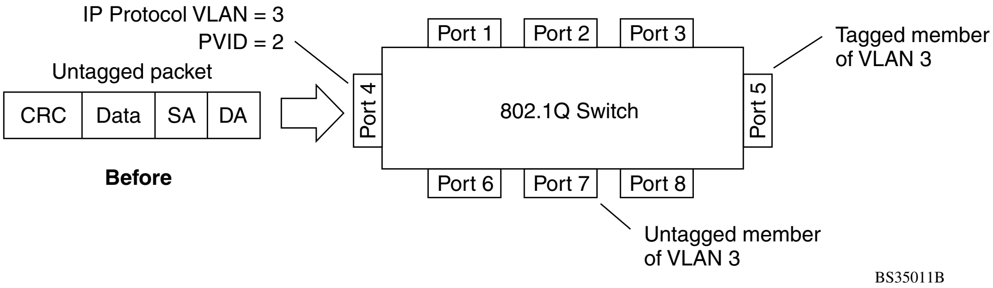


Figure 1-18. Protocol-Based VLAN Assignment

As shown in Figure 1-19, the untagged packet is marked (tagged) as it leaves the switch through port 5, which is configured as a tagged member of VLAN 3. The untagged packet remains unchanged as it leaves the switch through port 7, which is configured as an untagged member of VLAN 3.

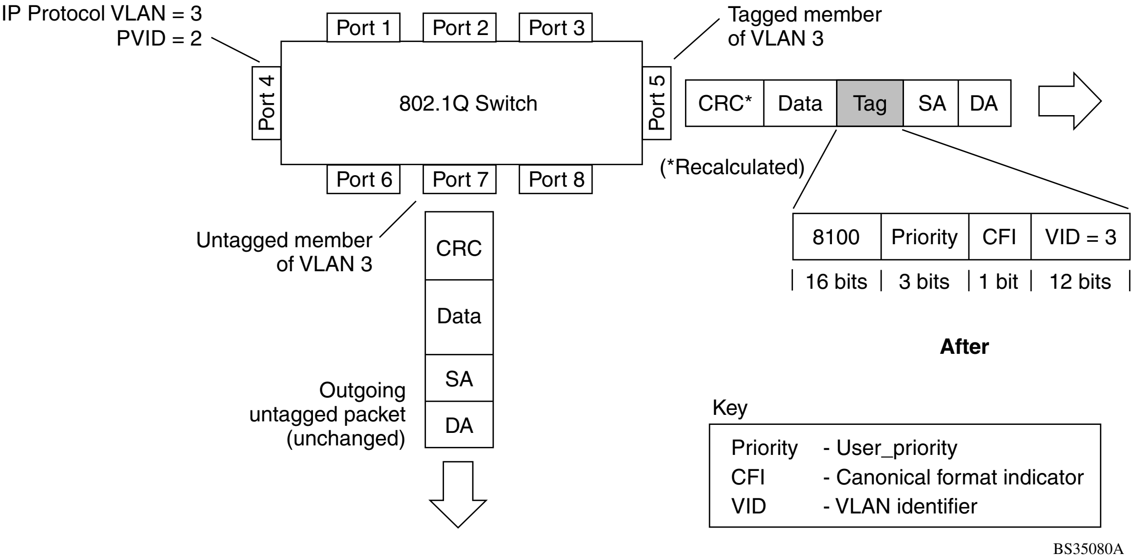


Figure 1-19. 802.1Q Tagging (After Protocol-Based VLAN Assignment)

In Figure 1-20, 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.

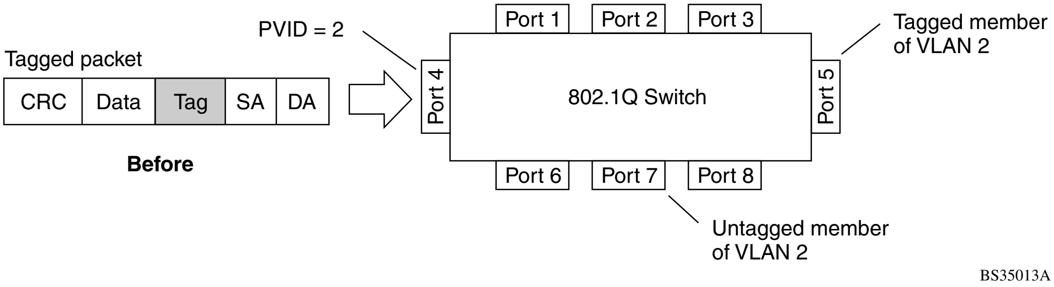


Figure 1-20. 802.1Q Tag Assignment

As shown in Figure 1-21, 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.

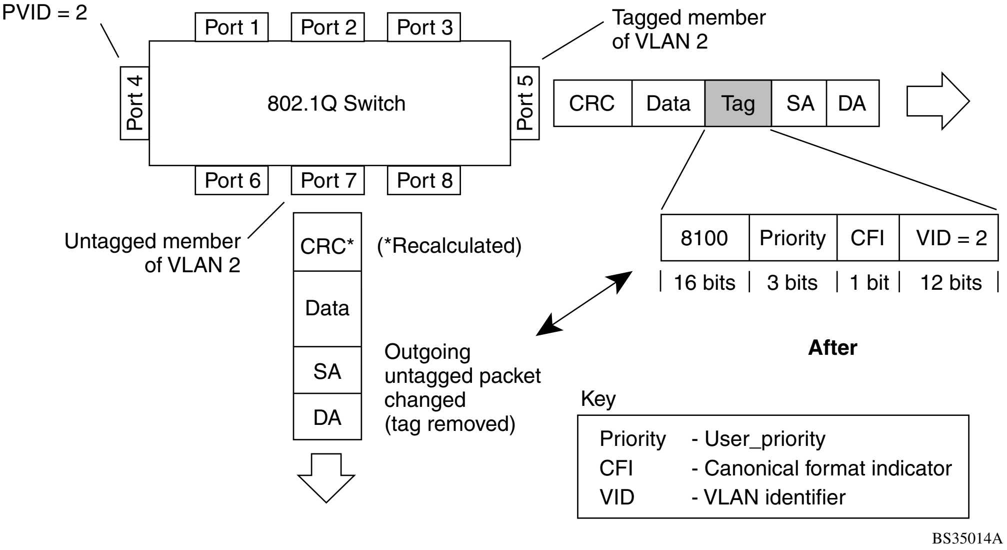


Figure 1-21. 802.1Q Tagging (After 802.1Q Tag Assignment)

VLANs Spanning Multiple Switches

You can use VLANs to segment a network within a switch. When connecting 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. Users 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 1-22 shows VLANs spanning two BayStack 350 switches. 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.

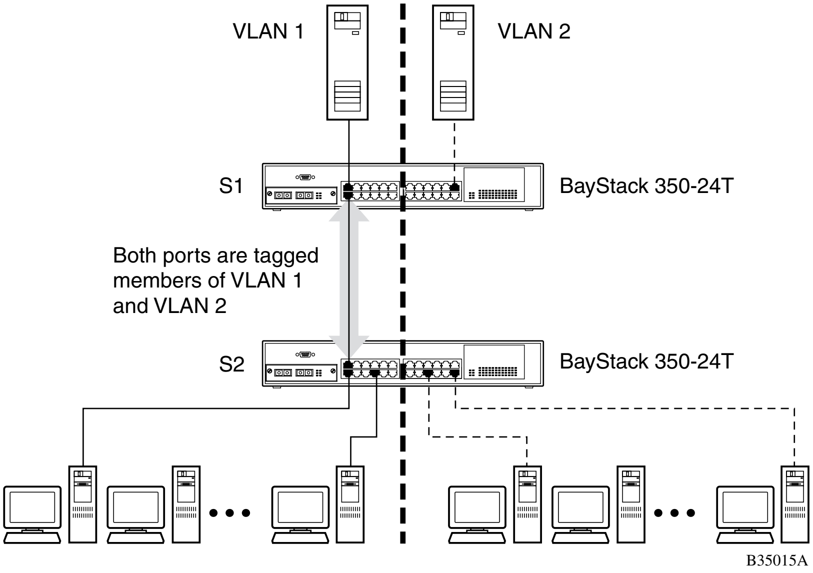


Figure 1-22. VLANs Spanning Multiple 802.1Q Tagged Switches

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 1-23 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).

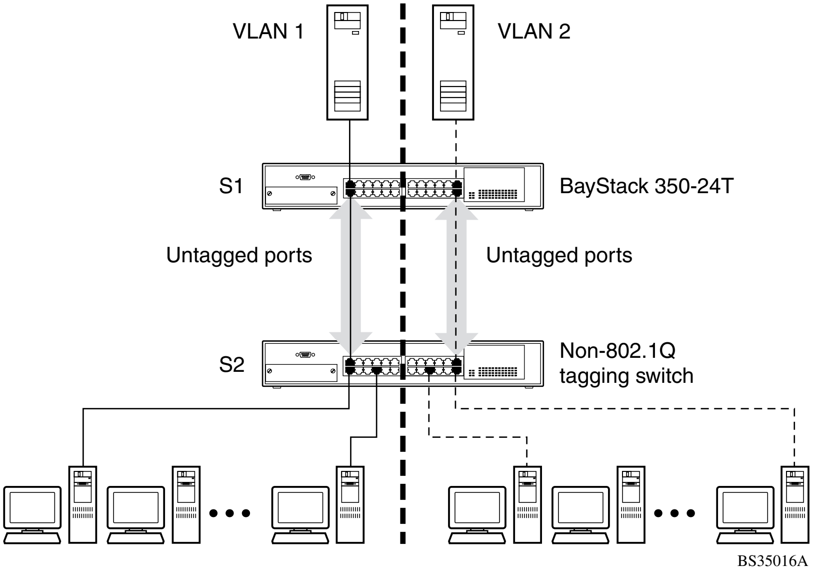


Figure 1-23. VLANs Spanning Multiple Untagged Switches

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, the STP must be disabled on all participating switch ports. Figure 1-24 shows possible consequences of enabling the STP when using VLANs between untagged (non-802.1Q tagged) switches.

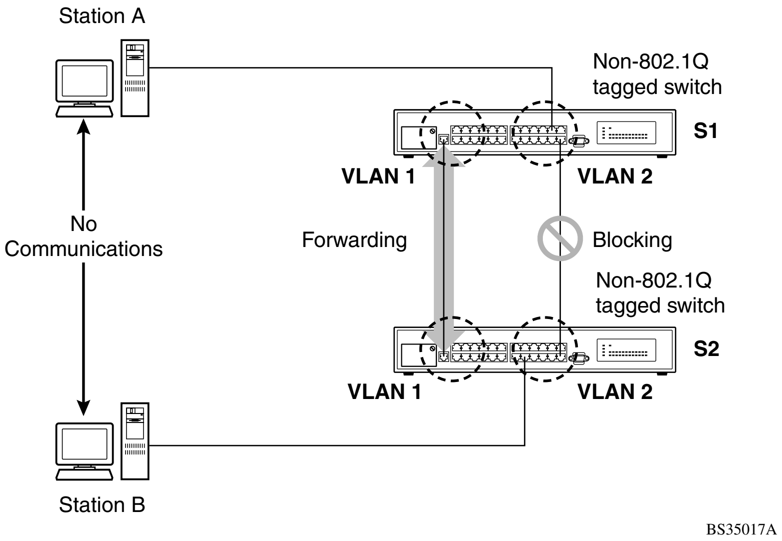


Figure 1-24. Possible Problems with VLANs and Spanning Tree Protocol

As shown in Figure 1-24, with STP enabled, only one connection between S1 and 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 link connecting VLAN 1 on switches S1 and S2 is selected as the forwarding link based on port speed, duplex mode, and port priority. Because the other link connecting VLAN 2 is placed into 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 350 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 1-25.

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.

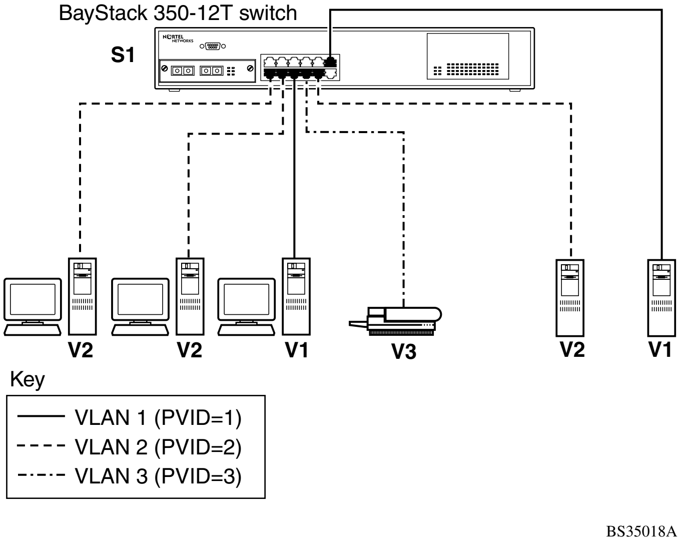


Figure 1-25. Multiple VLANs Sharing Resources

In the above configuration, all of the switch ports are set to participate as VLAN port members. This allows the switch to establish the appropriate broadcast domains within the switch (see Figure 1-26).

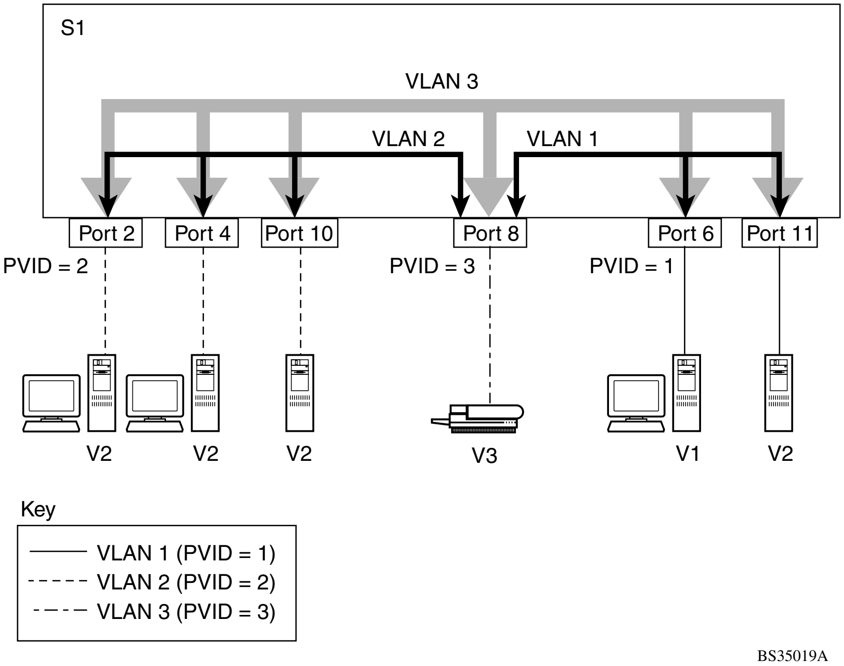


Figure 1-26. VLAN Broadcast Domains Within the Switch

For example, to create a broadcast domain for each VLAN shown in Figure 1-26, 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.

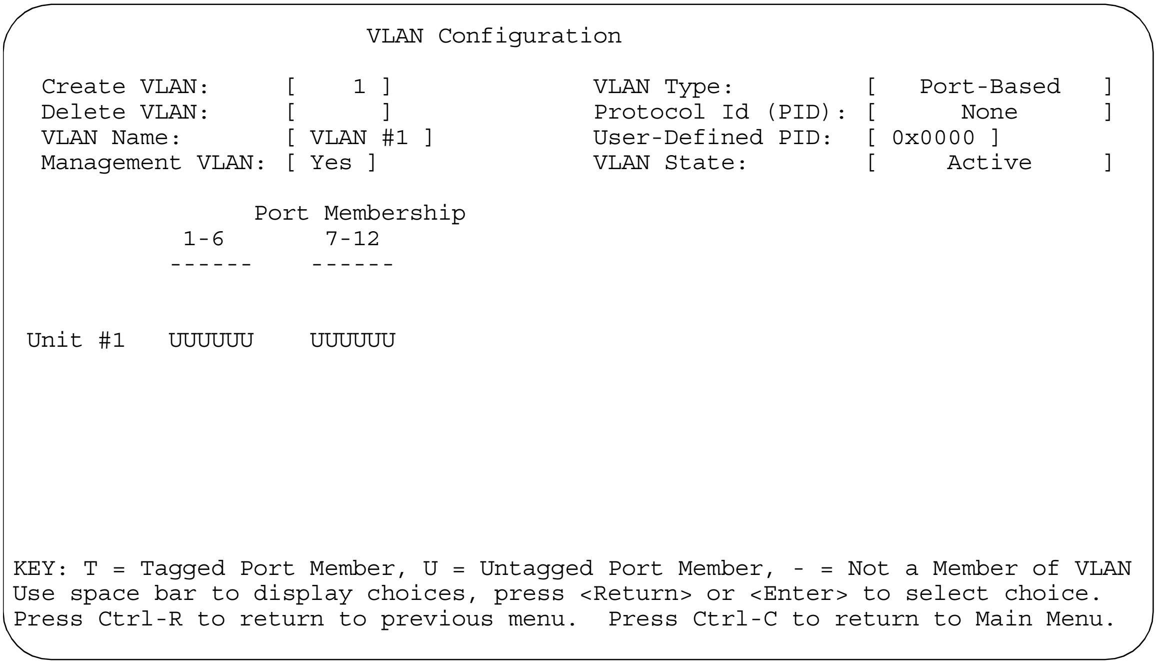
  The PVID/VLAN association for port 8 is: PVID = 3.

The following steps show how to use the VLAN configuration screens to configure the VLAN 3 broadcast domain shown in Figure 1-26.

To configure the VLAN port membership for VLAN 1:

1. **Select Switch Configuration from the BayStack 350-12T 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 1-27):



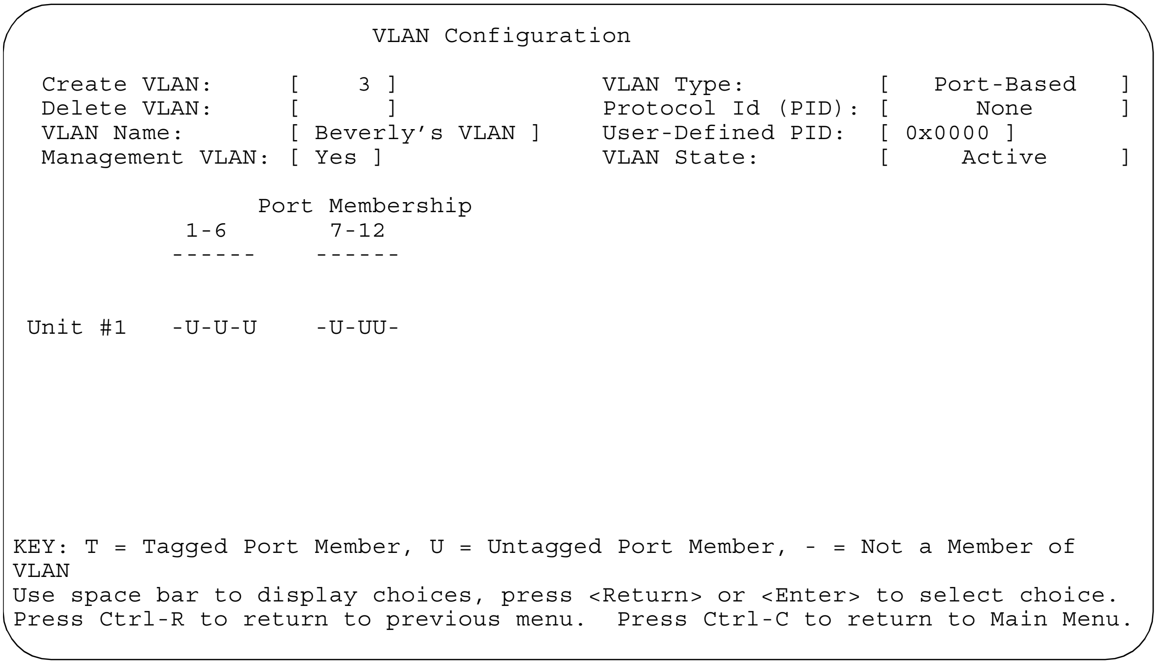
```
                         VLAN Configuration

  Create VLAN:      [    1 ]            VLAN Type:          [   Port-Based   ]
  Delete VLAN:      [      ]            Protocol Id (PID): [      None      ]
  VLAN Name:        [ VLAN #1 ]         User-Defined PID:   [ 0x0000 ]
  Management VLAN: [ Yes ]              VLAN State:         [     Active     ]

                 Port Membership
           1-6        7-12
          ------     ------


 Unit #1  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.
```

Figure 1-27. Default VLAN Configuration Screen Example

The VLAN Configuration screen settings shown in Figure 1-27 are default settings with all switch ports classified as *untagged* members of VLAN 1.

Figure 1-28 shows the VLAN Configuration screen after it is configured to support the VLAN 3 broadcast domain shown in Figure 1-26 (VLAN Name is optional).

Ports 2, 4, 6, 8, 10, and 11 are now untagged members of VLAN 3 as shown in Figure 1-26 on page 1-44.



```
                          VLAN Configuration

  Create VLAN:      [    3 ]              VLAN Type:          [   Port-Based   ]
  Delete VLAN:      [      ]              Protocol Id (PID):  [      None      ]
  VLAN Name:        [ Beverly's VLAN ]    User-Defined PID:   [ 0x0000 ]
  Management VLAN:  [ Yes ]               VLAN State:         [     Active     ]

                  Port Membership
              1-6       7-12
             ------    ------


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






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.
```

Figure 1-28. VLAN Configuration Screen Example

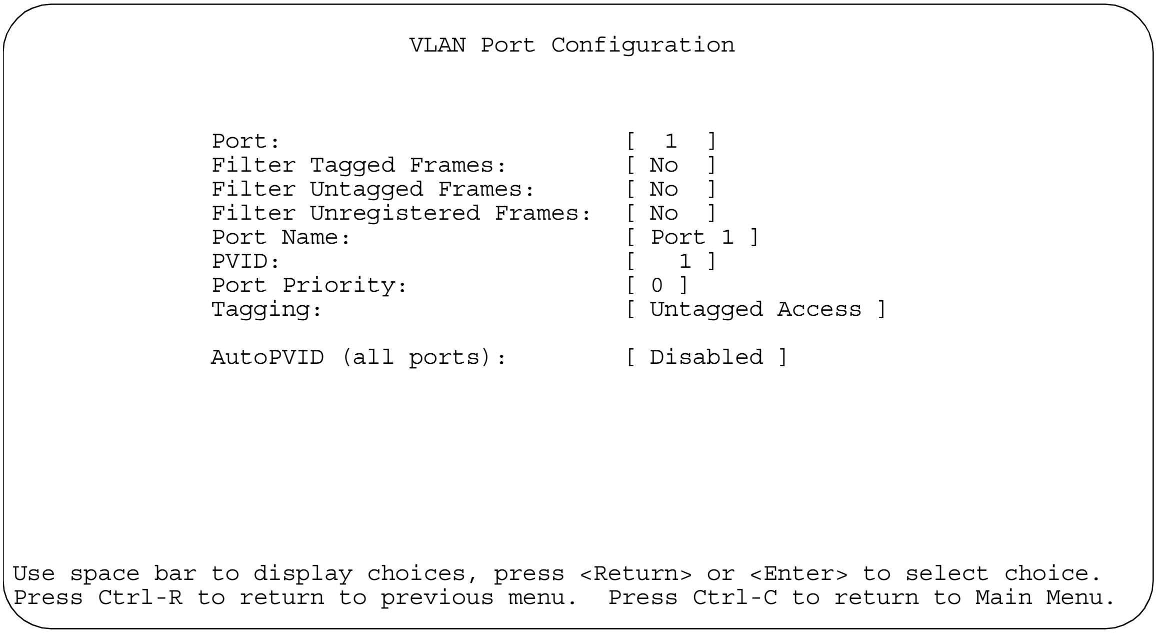
To configure the PVID (port VLAN identifier) for Port 8:

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 1-29).

The VLAN Port Configuration screen settings shown in Figure 1-29 are default settings.

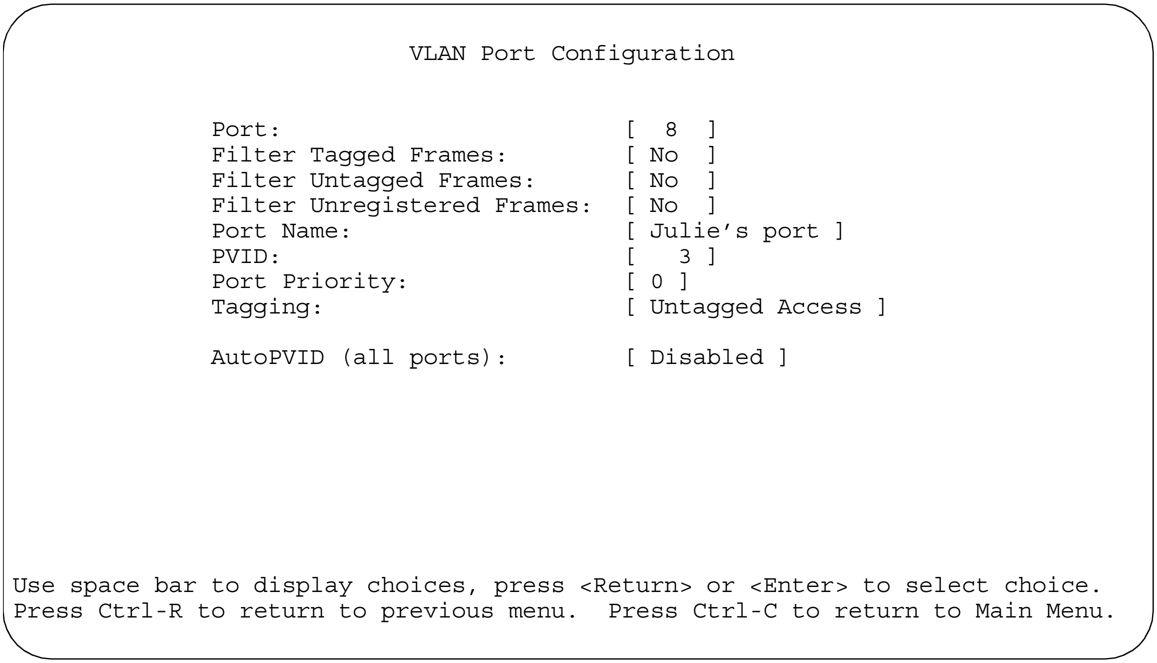


```
                           VLAN Port Configuration



              Port:                          [  1  ]
              Filter Tagged Frames:          [ No  ]
              Filter Untagged Frames:        [ No  ]
              Filter Unregistered 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 1-29. Default VLAN Port Configuration Screen Example

Figure 1-30 shows the VLAN Port Configuration screen after it is configured to support the PVID assignment for port 8, as shown in Figure 1-26 (Port Name is optional).

As shown in Figure 1-30, the PVID/VLAN association for VLAN 3 is now PVID = 3.



```
                        VLAN Port Configuration


            Port:                            [  8  ]
            Filter Tagged Frames:            [ No  ]
            Filter Untagged Frames:          [ No  ]
            Filter Unregistered Frames:      [ No  ]
            Port Name:                       [ Julie's port ]
            PVID:                            [   3 ]
            Port Priority:                   [ 0 ]
            Tagging:                         [ Untagged Access ]

            AutoPVID (all ports):            [ Disabled ]








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

Figure 1-30. VLAN Port Configuration Screen Example

Note: You can also automatically assign a PVID/VLAN association for each VLAN port membership you create.

The preceding example explains how to manually configure the PVID/VLAN association to PVID 3. However, if you set the AutoPVID field value to Enabled before creating the VLAN port memberships, the PVID/VLAN association is automatically assigned a value that is associated with the VLAN number you create.

See “VLAN Port Configuration” on page 3-49, for more information.

VLAN Workgroup Summary

This section summarizes the VLAN workgroup examples discussed in the previous sections of this chapter. As shown in Figure 1-31, switch S1 (a BayStack 350 switch) is configured with multiple VLANs:

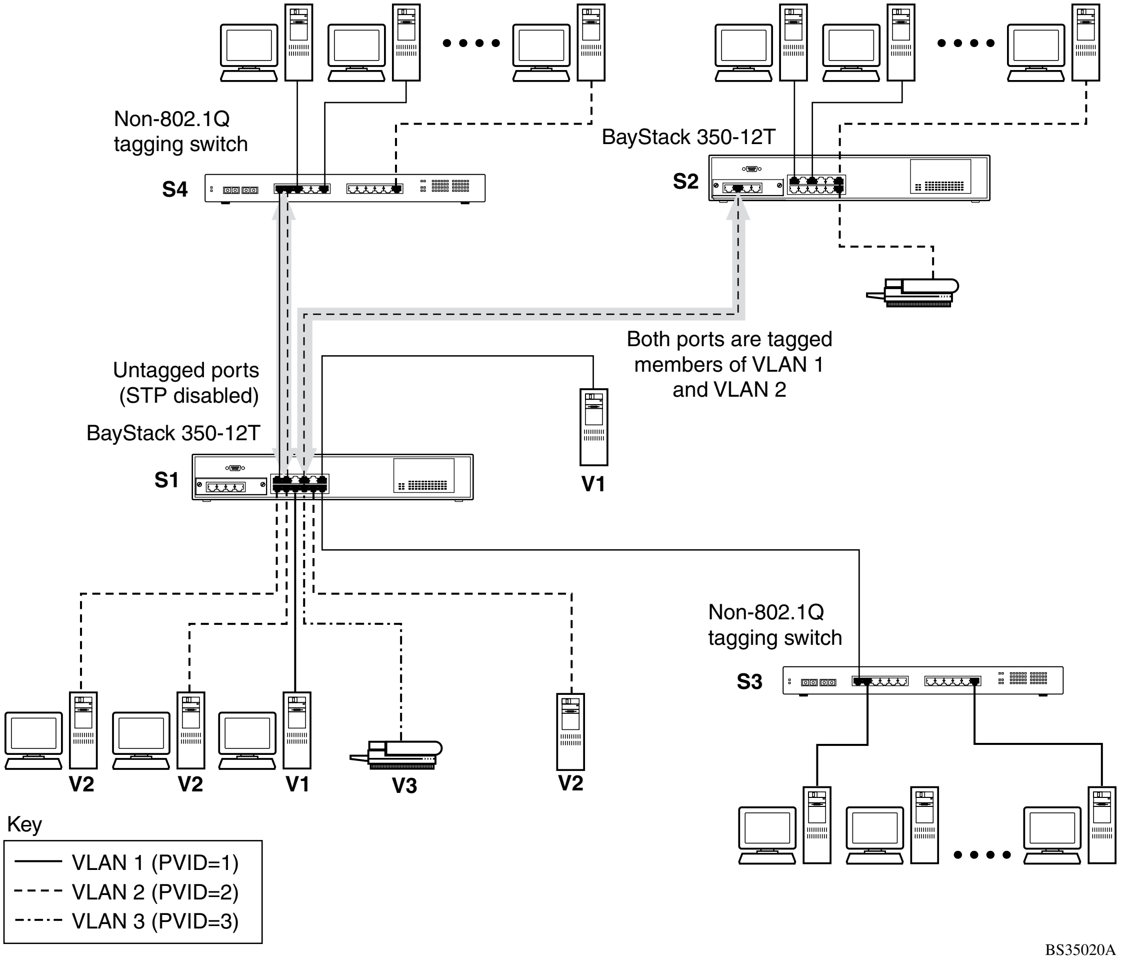


Figure 1-31. VLAN Configuration Spanning Multiple Switches

- 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 1-41).

The connection to S2 requires only one link between the switches because S1 and S2 are both BayStack 350 switches that support 802.1Q tagging (see “VLANs Spanning Multiple 802.1Q Tagged Switches” on page 1-40).

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:

- Your switch supports up to 64 VLANs. You can create port-based VLANs and protocol-based VLANs, in any combination, as long as you do not exceed a total of 64 VLANs.
- All ports that are involved in port mirroring must have memberships in the same VLANs. If a port is configured for port mirroring, the port’s VLAN membership cannot be changed.
- If a port is a trunk group member, all trunk members are added or deleted from the VLAN.
- All ports involved in trunking and port mirroring must have the same VLAN configuration. If a port is on a trunk with a mirroring port, the VLAN configuration cannot be changed.
- VLANs are not dependent on rate limiting settings.
- If a port is an IGMP member on any VLAN, and is removed from a VLAN, the port’s IGMP membership is also removed.
- If a port is added to a different VLAN, and it is already configured as a static router port, the port is configured as an IGMP member on that specific VLAN.

For more information about configuring VLANs, see “VLAN Configuration Menu” on page 3-41.

See also Appendix E, “Quick Steps to Features” for configuration flowcharts that can help you use this feature.

IGMP Snooping

BayStack 350 switches can sense Internet Group Management Protocol (IGMP) host membership reports from attached stations. The switches use this information to set up a dedicated path between the requesting station and a local IP multicast router. After the pathway is established, the BayStack 350 switch blocks the IP multicast stream from exiting any other port that does not connect to another host member, thus conserving bandwidth. The following discussion describes how BayStack 350 switches provide the same benefit as IP multicast routers, but in the local area.

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

Figure 1-32 shows how IGMP is used to set up the path between the client and server. As shown in this example, the IGMP host provides an IP multicast stream to designated routers that forward the IP multicast stream on their local network only if there is a recipient.

The client/server path is set up as follows:

1. The designated router sends out a *host membership query* to the subnet and receives *host membership reports* from end stations on the subnet.
2. The designated routers then set up a path between the IP multicast stream source and the end stations.
3. Periodically, the router continues to query end stations on whether to continue participation.
4. As long as any client continues to participate, all clients, including nonparticipating end stations on that subnet, receive the IP multicast stream.

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

IP multicast can be optimized in a LAN by using *IP multicast filtering switches,* such as the BayStack 350 switch.

As shown in Figure 1-32, a non-IP multicast filtering switch causes IP multicast traffic to be sent to all segments on the local subnet.

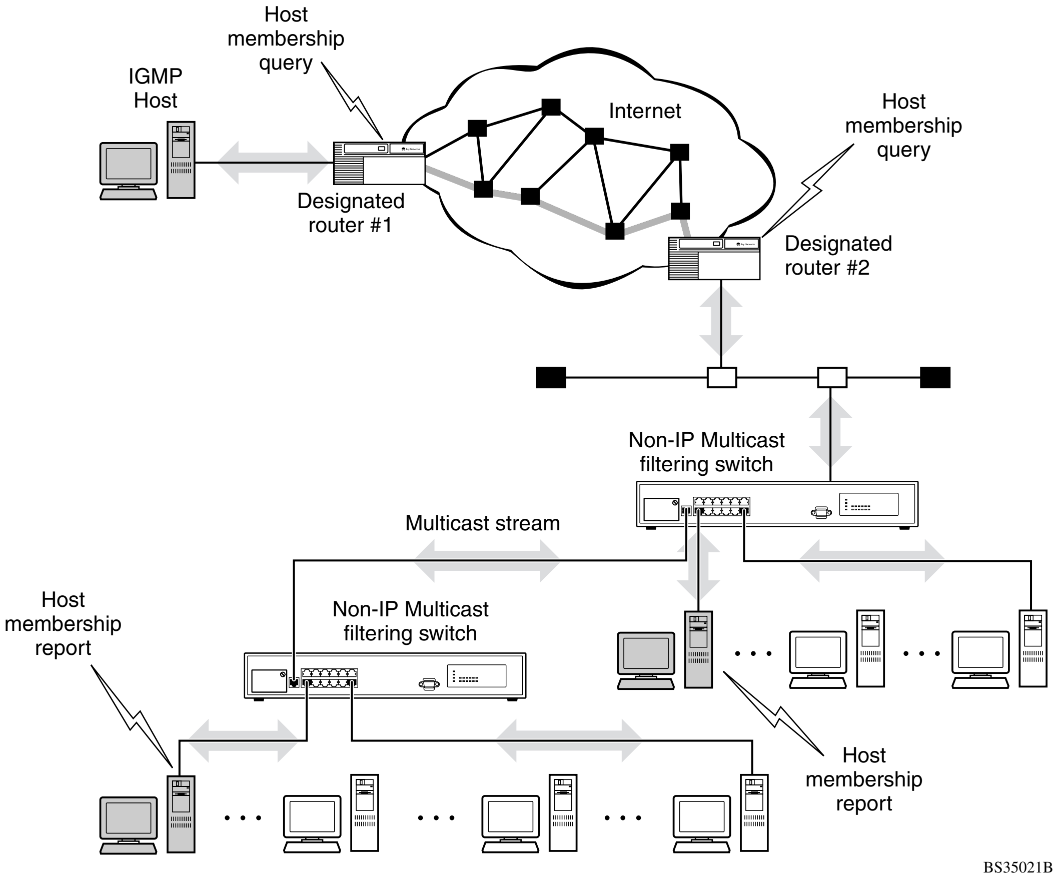


Figure 1-32. IP Multicast Propagation with IGMP Routing

The BayStack 350 switch can automatically set up IP multicast filters so the IP multicast traffic is directed only to the participating end nodes (see Figure 1-33).

In Figure 1-33, switches S1 to S4 represent a LAN connected to an IP multicast router. The router periodically sends Host Membership Queries to the LAN and listens for a response from end stations. All of the clients connected to switches S1 to S4 are aware of the queries from the router.

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

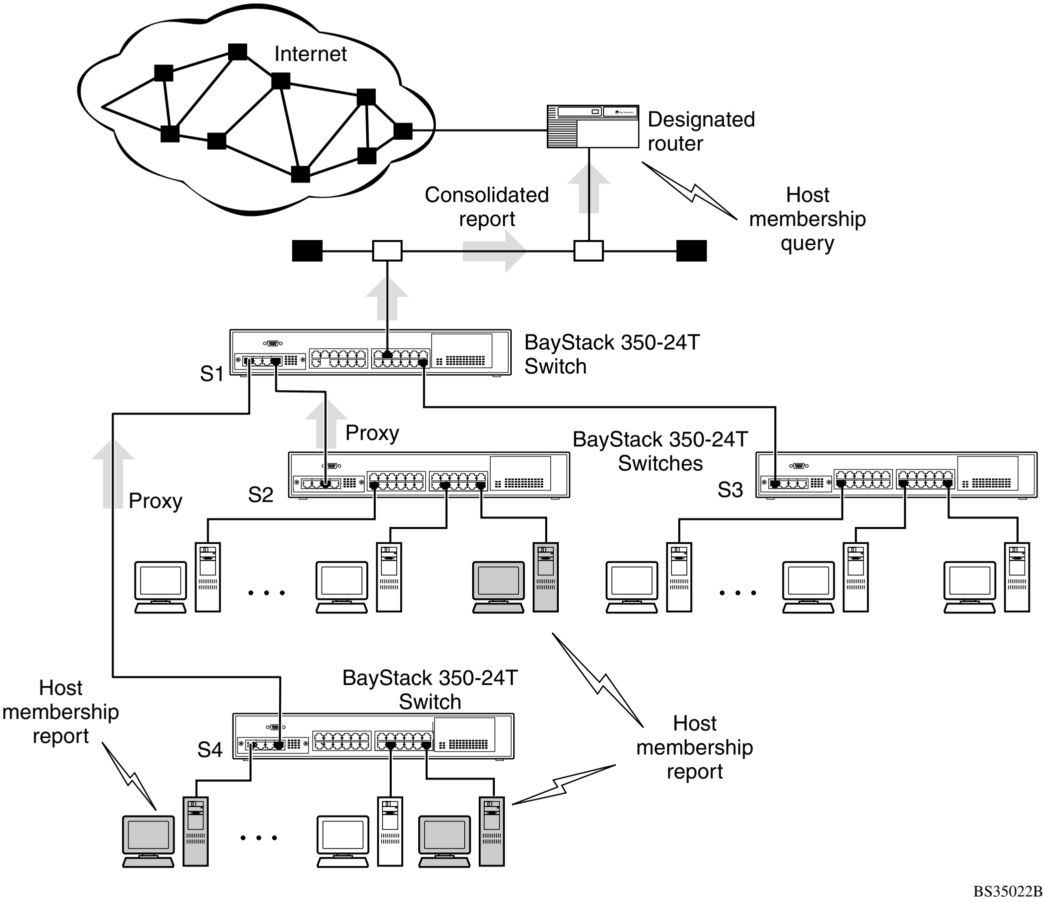


Figure 1-33. BayStack 350-24T Filtering IP Multicast Streams (1 of 2)

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

After the switches learn which ports are requesting access to the IP multicast stream, all other ports not responding to the queries are blocked from receiving the IP multicast (see Figure 1-34).

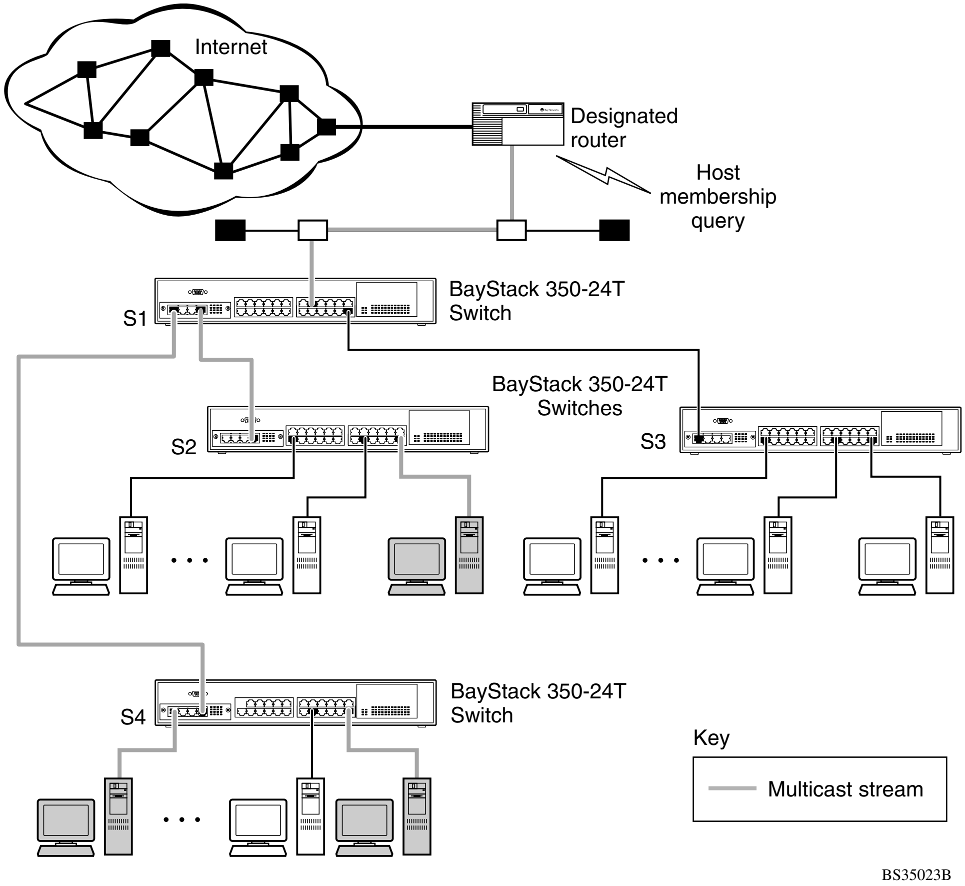


Figure 1-34. BayStack 350-24T switches Filtering IP Multicast Stream (2 of 2)

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

IGMP Snooping Configuration Rules

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

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

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

For more information about using the IGMP snooping feature, see “IGMP Configuration Menu” on page 3-74.

See also Appendix E, “Quick Steps to Features,” 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 (see Figure 1-35).

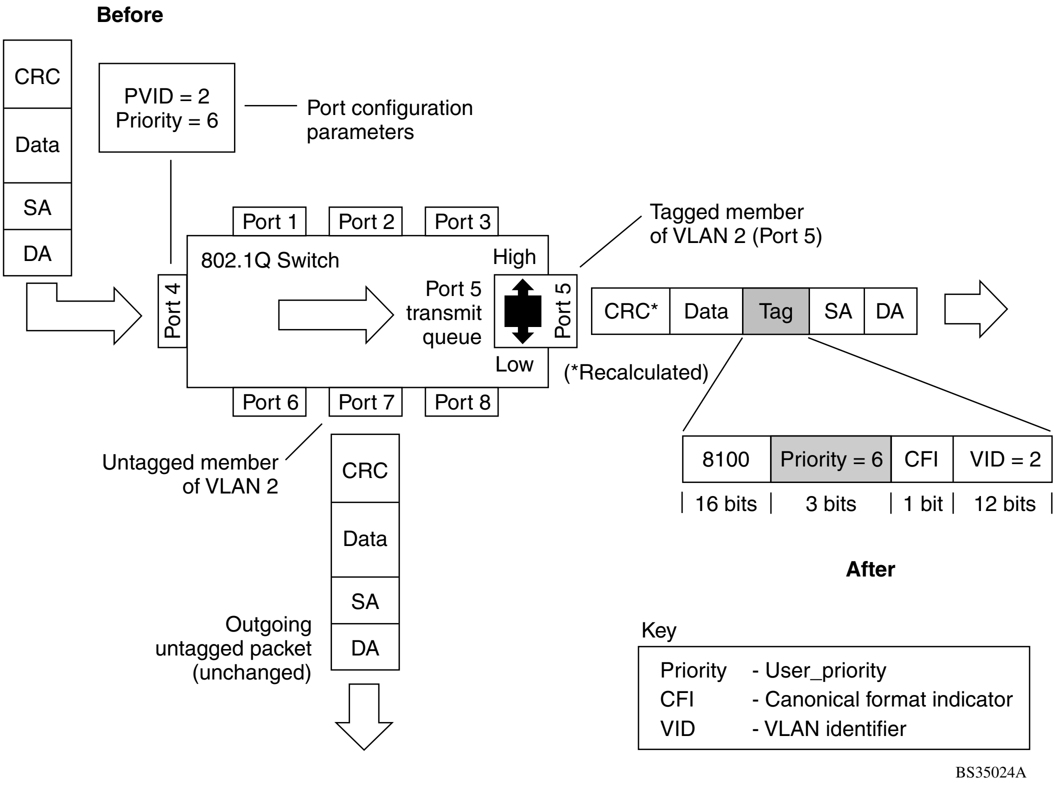


Figure 1-35. Prioritizing Packets

The newly tagged frame is read within the switch and sent to the port's high or low transmit queue for disposition (see Figure 1-36). The port transmit queue example shown in Figure 1-36 applies to all ports on the BayStack 350 switch.

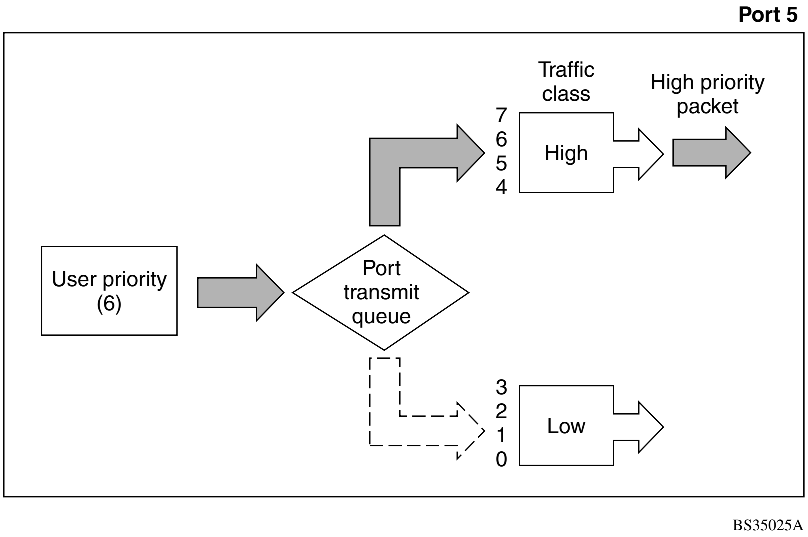


Figure 1-36. Port Transmit Queue

As shown in Figure 1-36, the switch provides two transmission queues, *High* and *Low*, 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 (Figure 1-37). The table indicates the corresponding traffic class that is assigned to the frame, for each possible 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 shown in the example Figure 1-35.

For more information about using the Traffic Class Configuration screen, see “Traffic Class Configuration” on page 3-54.

To configure the port priority level, follow these steps:

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

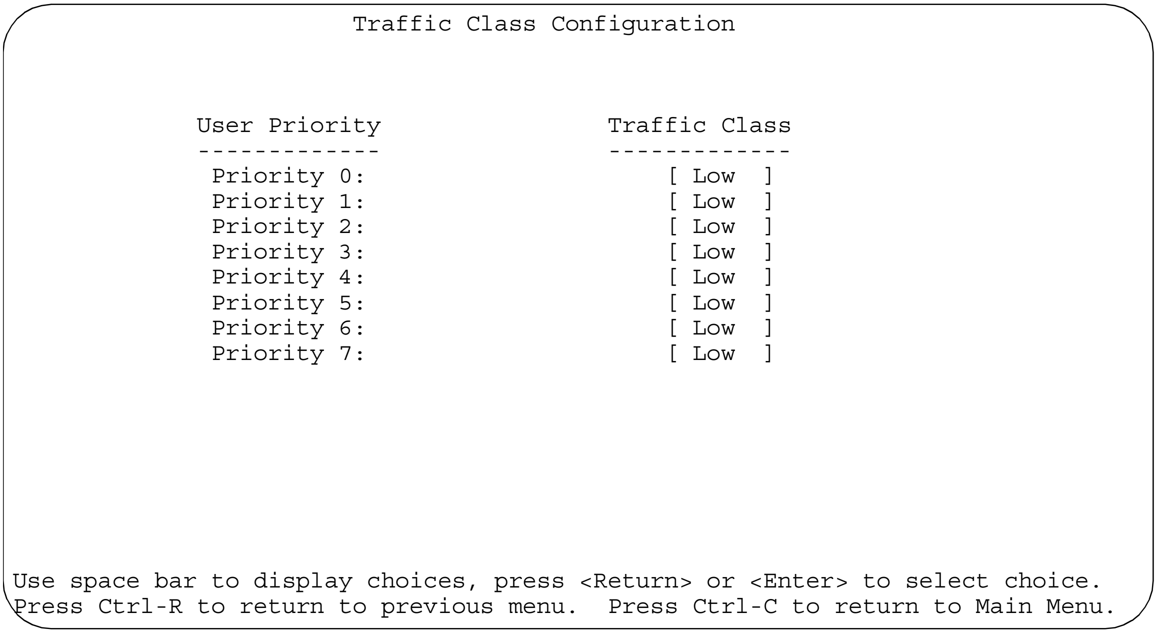
   User priority levels are assigned default settings in all BayStack 350 switches. The range is from 0 to 7. The traffic class table can be modified. Therefore, view the settings shown in the Traffic Class Configuration screen before setting the port priority in the VLAN Port Configuration screen.

2. **Select Switch Configuration from the BayStack 350-12T Main Menu (or press w).**

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

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

   The Traffic Class Configuration screen opens (Figure 1-37).



```
                         Traffic Class Configuration



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









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 1-37. Default Traffic Class Configuration Screen Example

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).**

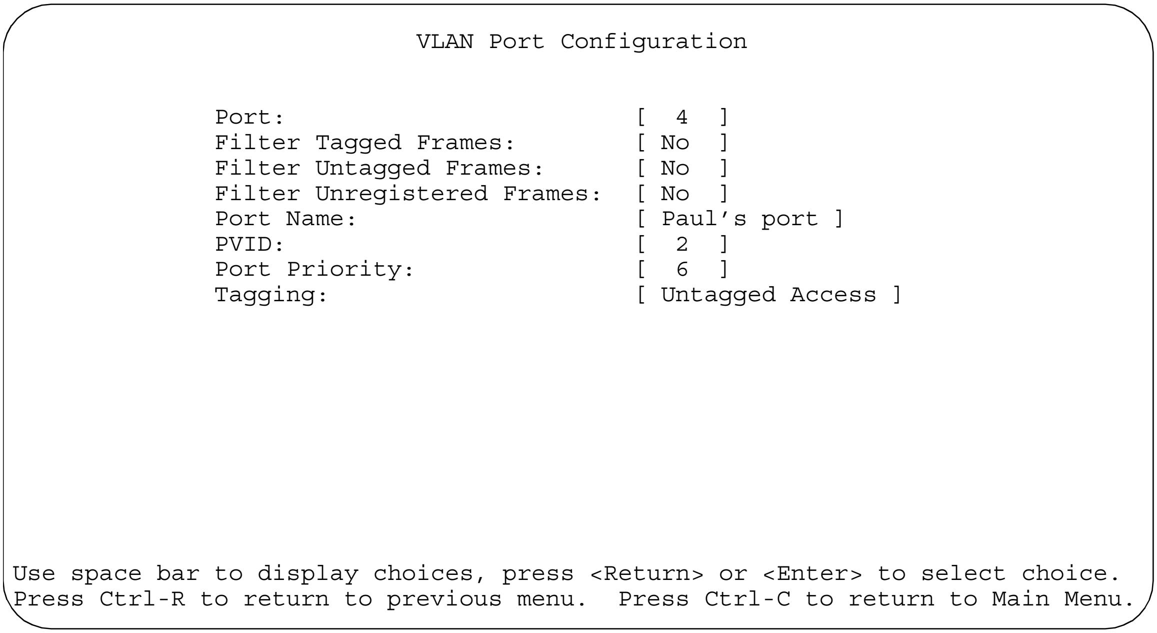
6. **Assign the priority level to ports using the VLAN Port Configuration screen:**

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

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

      The VLAN Port Configuration screen opens (Figure 1-38).

Figure 1-38 shows the VLAN Port Configuration screen setup for port 4 in Figure 1-35 on page 1-56.



```
                         VLAN Port Configuration


             Port:                         [  4  ]
             Filter Tagged Frames:         [ No  ]
             Filter Untagged Frames:       [ No  ]
             Filter Unregistered Frames:   [ No  ]
             Port Name:                    [ Paul's port ]
             PVID:                         [  2  ]
             Port Priority:                [  6  ]
             Tagging:                      [ Untagged Access ]








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 1-38. Setting Port Priority Example

For more information about using this feature, see “VLAN Port Configuration” on page 3-49.

MultiLink Trunks

A MultiLink Trunk (MLT)[1] allows you to group up to four switch ports to form a link to another switch or server. This can increase the aggregate throughput of the interconnection between devices as much as 800 Mb/s in full-duplex mode (up to 8000 Mb/s with optional gigabit MDA ports). You can configure up to six MultiLink Trunks. MLT software detects misconfigured (or broken) trunk links and redirects traffic on the misconfigured or broken trunk link to other trunk members within that MLT.

You can use the MultiLink Trunk Configuration screen to create switch-to-switch and switch-to-server MLT links (see Figure 1-39 and Figure 1-40).

Figure 1-39 shows two trunks (T1 and T2) connecting switch S1 to switches S2 and S3.

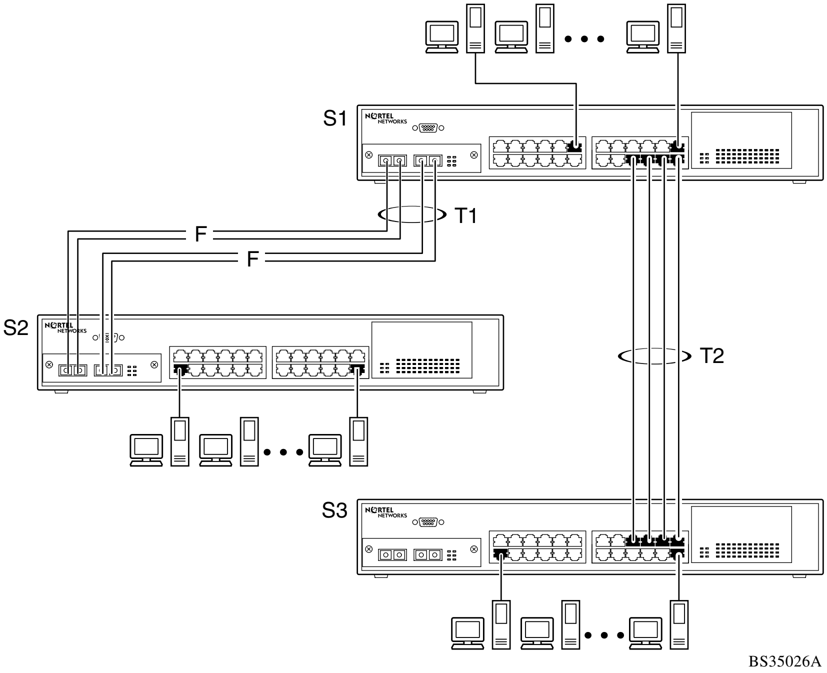


Figure 1-39. Switch-to-Switch Trunk Configuration Example

[1] In this guide, the terms “trunk” and “MLT” are used interchangeably to indicate a MultiLink Trunk.

Each of the trunks shown in Figure 1-39 can be configured with up to four switch ports to provide up to 800 Mb/s aggregate bandwidth through each trunk, in full-duplex mode. As shown in this example, when traffic between switch-to-switch connections approaches single port bandwidth limitations, creating a MultiLink Trunk can supply the additional bandwidth required to improve the performance.

Figure 1-40 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 controller (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.

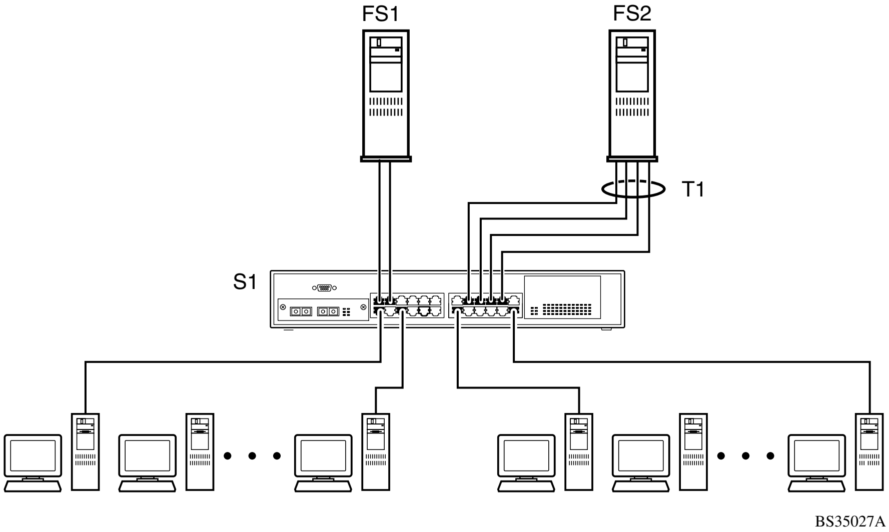


Figure 1-40. Switch-to-Server Trunk Configuration Example

Client/Server Configuration Using MultiLink Trunks

Figure 1-41 shows an example of how MultiLink Trunking can be used in a client/server configuration. In this example, both servers are connected 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 (see "IEEE 802.1Q VLAN Workgroups" on page 1-34).

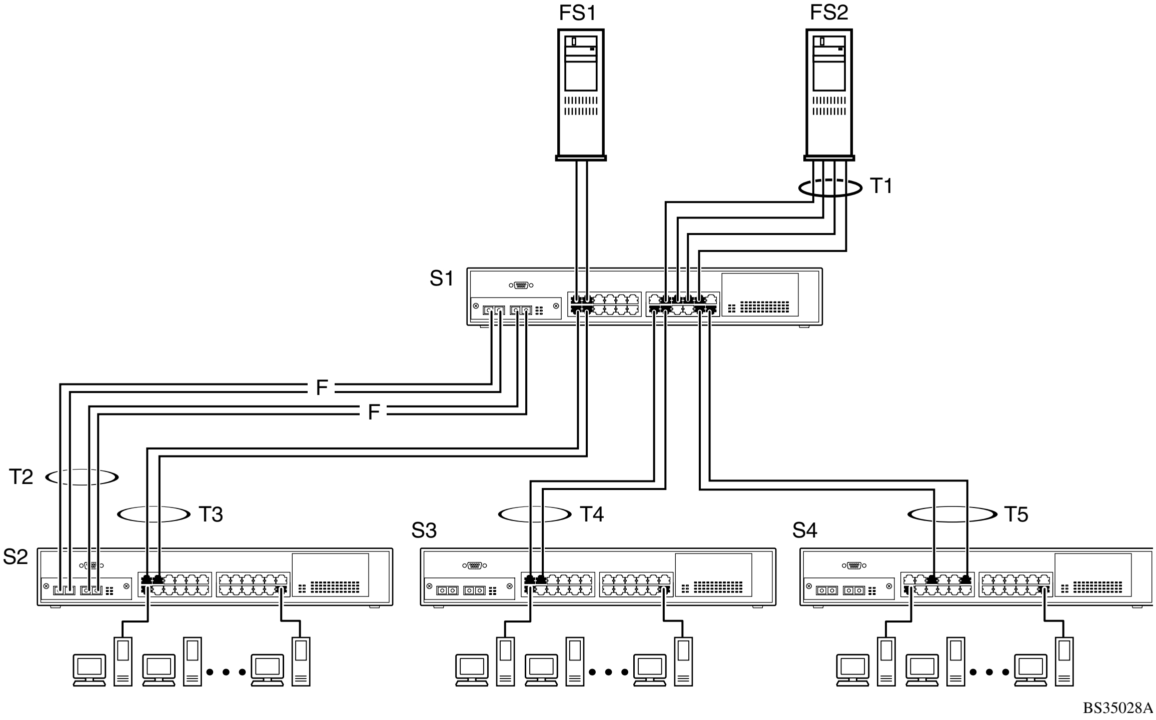


Figure 1-41. Client/Server Configuration Example

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" on page 3-61.

Trunk Configuration Screen Examples

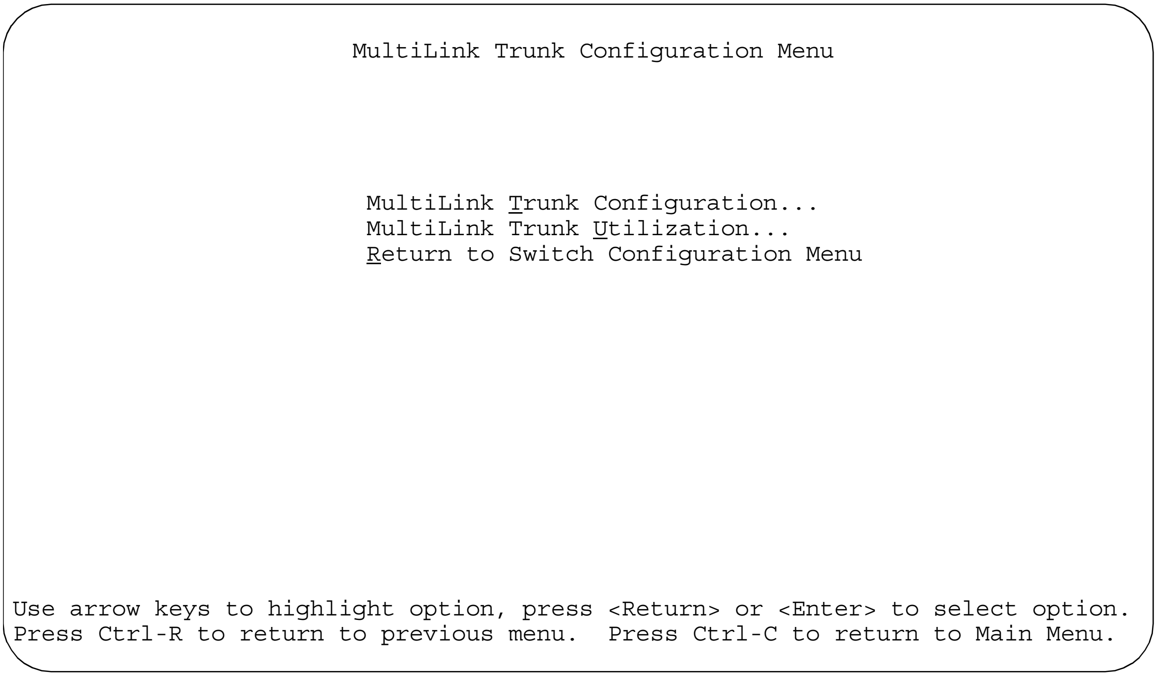
This section shows examples of the MultiLink Trunk configuration screens for the client/server configuration example shown in Figure 1-41 on page 1-62. The screens show how you could set up the trunk configuration screens for switches S1 to S4. See "Spanning Tree Considerations for MultiLink Trunks" on page 1-74, and "MultiLink Trunk Configuration" on page 3-61 for more information.

Trunk Configuration Screen for Switch S1

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

Setting Up the Trunk Configuration for S1:

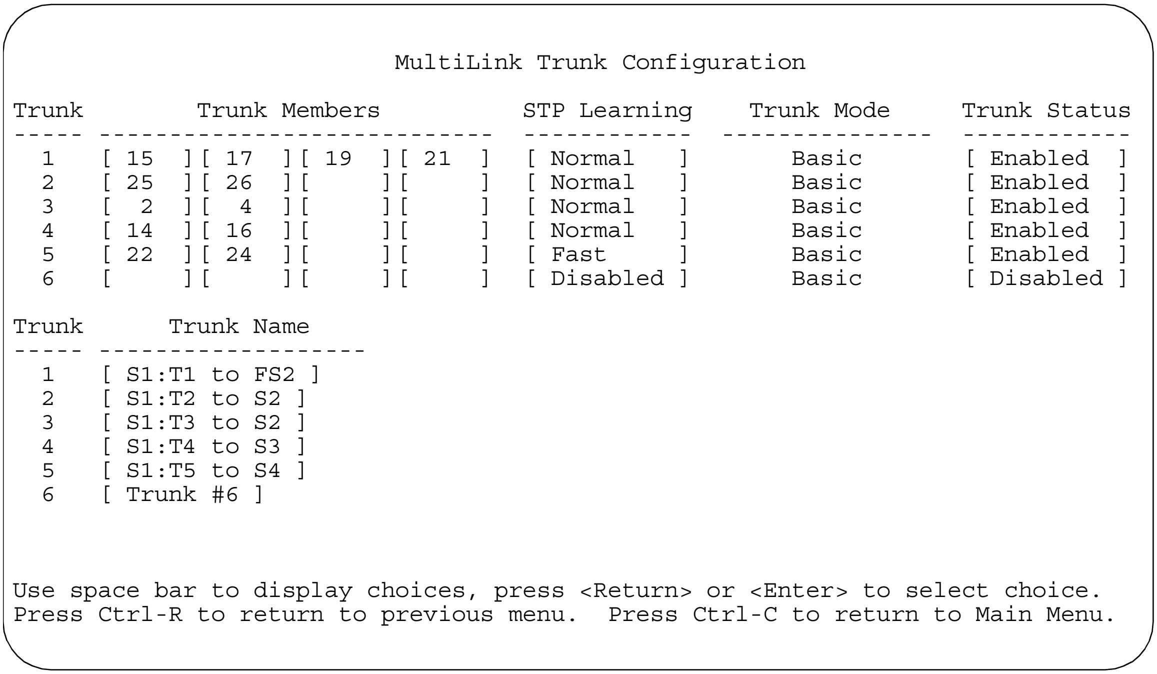
To set up the trunk configuration, choose MultiLink Trunk Configuration (or press t) from the MultiLink Trunk Configuration Menu (Figure 1-42).



```
                        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.
```

Figure 1-42. Choosing the MultiLink Trunk Configuration Screen

The MultiLink Trunk Configuration screen opens (Figure 1-43).



```
                           MultiLink Trunk Configuration

Trunk        Trunk Members          STP Learning    Trunk Mode     Trunk Status
----- ----------------------------  ------------  ---------------  ------------
  1   [ 15  ][ 17  ][ 19  ][ 21  ]  [ Normal   ]       Basic       [ Enabled  ]
  2   [ 25  ][ 26  ][     ][     ]  [ Normal   ]       Basic       [ Enabled  ]
  3   [  2  ][  4  ][     ][     ]  [ Normal   ]       Basic       [ Enabled  ]
  4   [ 14  ][ 16  ][     ][     ]  [ Normal   ]       Basic       [ Enabled  ]
  5   [ 22  ][ 24  ][     ][     ]  [ Fast     ]       Basic       [ Enabled  ]
  6   [     ][     ][     ][     ]  [ Disabled ]       Basic       [ Disabled ]

Trunk      Trunk Name
----- -------------------
  1   [ S1:T1 to FS2 ]
  2   [ S1:T2 to S2 ]
  3   [ S1:T3 to S2 ]
  4   [ S1:T4 to S3 ]
  5   [ S1:T5 to S4 ]
  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.
```

Figure 1-43. MultiLink Trunk Configuration Screen for Switch S1

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 15, 17, 19, and 21 are assigned as trunk members of trunk 1.

  -- Ports 25 and 26 are assigned as trunk members of trunk 2.

  -- Ports 2 and 4 are assigned as trunk members of trunk 3.

  -- Ports 14 and 16 are assigned as trunk members of trunk 4.

  -- Ports 22 and 24 are assigned as trunk members of trunk 5.

- **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 5 are set to Basic. Source MAC addresses are assigned statically to specific trunk members for flooding and forwarding. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.

- **Trunk 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.

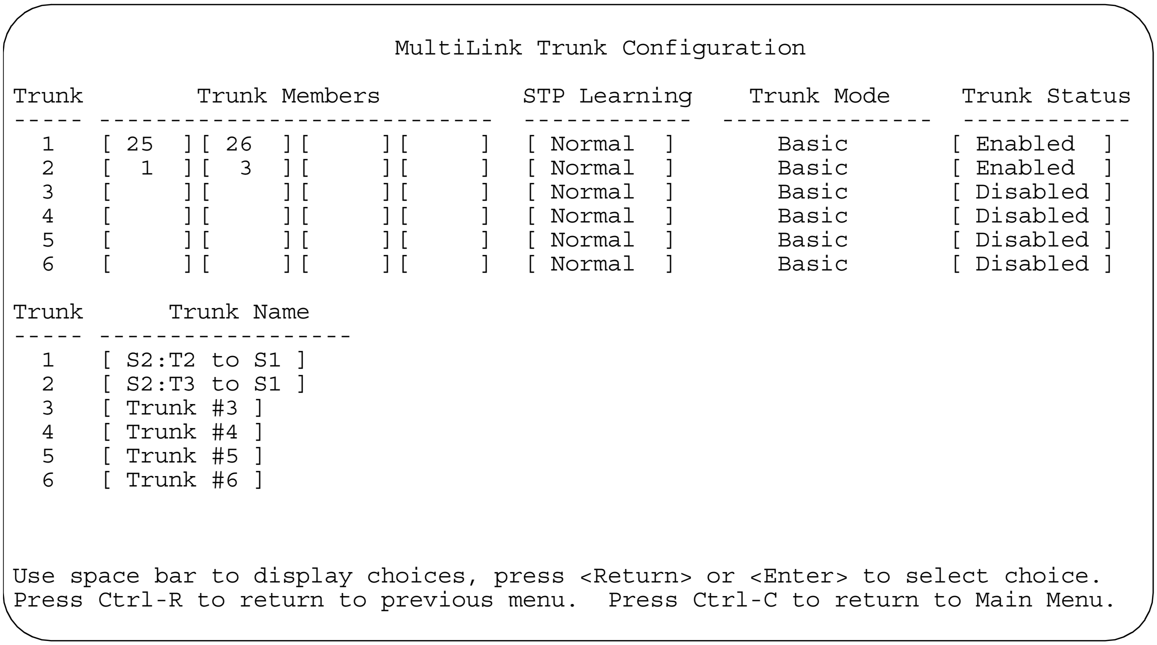
  The names chosen for this example provide meaningful information to the user of this switch (for example, S1:T1 to FS2 indicates that trunk 1, in switch S1, connects to file server 2).

Trunk Configuration Screen for Switch S2

As shown in Figure 1-41 on page 1-62, 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.

Figure 1-44 shows the MultiLink Trunk Configuration screen for switch S2.



```
                        MultiLink Trunk Configuration

Trunk         Trunk Members           STP Learning    Trunk Mode     Trunk Status
----- ----------------------------  ------------  ---------------  ------------
  1   [ 25  ][ 26  ][     ][     ]  [ Normal   ]      Basic       [ Enabled  ]
  2   [  1  ][  3  ][     ][     ]  [ Normal   ]      Basic       [ Enabled  ]
  3   [     ][     ][     ][     ]  [ Normal   ]      Basic       [ Disabled ]
  4   [     ][     ][     ][     ]  [ Normal   ]      Basic       [ Disabled ]
  5   [     ][     ][     ][     ]  [ Normal   ]      Basic       [ Disabled ]
  6   [     ][     ][     ][     ]  [ Normal   ]      Basic       [ Disabled ]

Trunk      Trunk Name
----- ------------------
  1   [ S2:T2 to S1 ]
  2   [ S2:T3 to S1 ]
  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.
```

Figure 1-44. MultiLink Trunk Configuration Screen for Switch S2

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 25 and 26 are assigned as trunk members of trunk 1.

  -- Ports 1 and 3 are assigned as trunk members of trunk 2.

- **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 assigned statically to specific trunk members for flooding and forwarding. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.

- **Trunk 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.

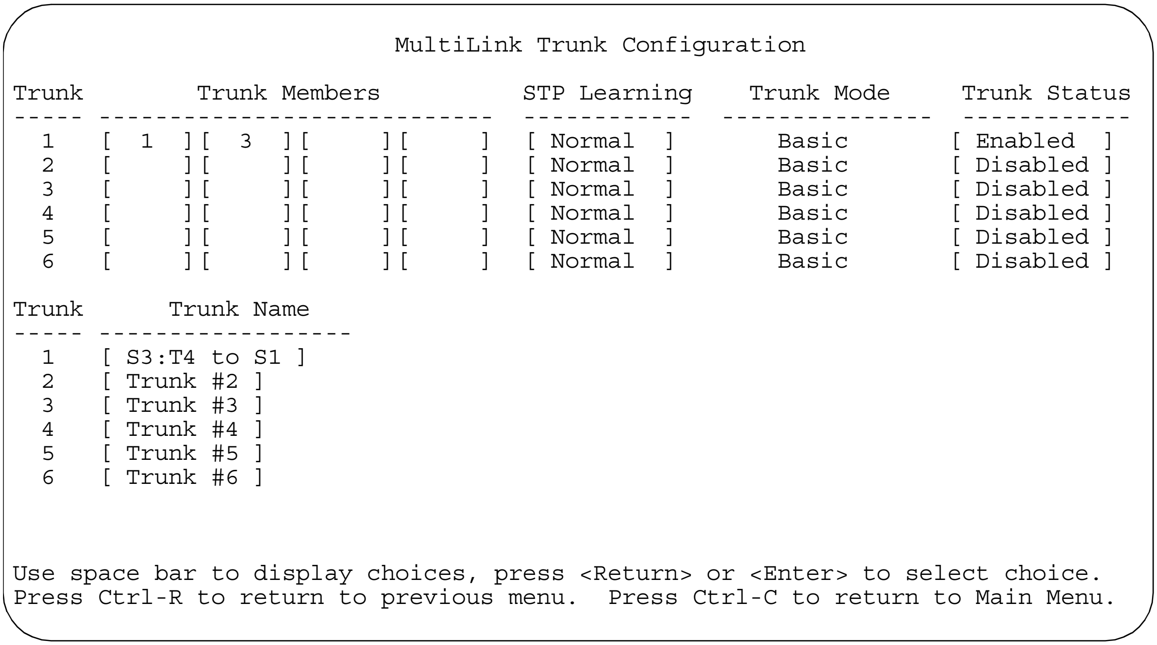
  The names chosen for this example provide meaningful information to the user of this switch (for example, S2:T2 to S1 indicates that trunk 1, in switch S2, connects to switch 1).

Trunk Configuration Screen for Switch S3

As shown in Figure 1-41 on page 1-62, 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 inter-switch trunk configuration choose MultiLink Trunk Configuration from the MultiLink Trunk Configuration Menu.

Figure 1-45 shows the MultiLink Trunk Configuration screen for switch S3.



```
                           MultiLink Trunk Configuration

Trunk        Trunk Members          STP Learning    Trunk Mode     Trunk Status
----- ----------------------------  ------------  ---------------  ------------
  1   [  1  ][  3  ][     ][     ]  [ 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   [ S3:T4 to S1 ]
  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.
```

Figure 1-45. MultiLink Trunk Configuration Screen for Switch S3

Switch S3 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 1 and 3 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 assigned statically to specific trunk members for flooding and forwarding. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.

- **Trunk 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.

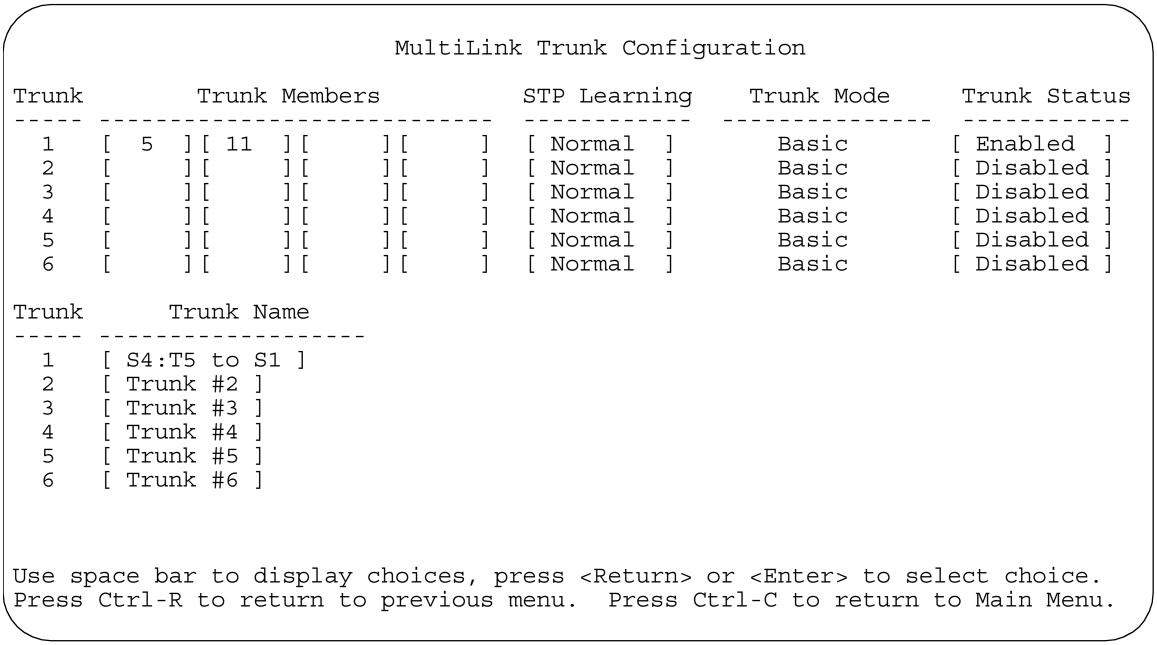
  The names chosen for this example provide meaningful information to the user of this switch (for example, S3:T4 to S1 indicates that trunk 1, in switch S3, connects to switch 1).

Trunk Configuration Screen for Switch S4

As shown in Figure 1-41, 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.

Figure 1-46 shows the MultiLink Trunk Configuration screen for switch S4.



```
                           MultiLink Trunk Configuration

Trunk        Trunk Members          STP Learning    Trunk Mode     Trunk Status
----- ----------------------------  ------------  ---------------  ------------
  1   [  5  ][ 11  ][     ][     ]  [ 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   [ S4:T5 to S1 ]
  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.
```

Figure 1-46. MultiLink Trunk Configuration Screen for Switch S4

Switch S4 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 5 and 11 are assigned as trunk members of trunk T1.
- **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 assigned statically to specific trunk members for flooding and forwarding. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.
- **Trunk 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 Configuring 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 configuring your MultiLink Trunk, you must consider these settings, along with specific configuration rules, as follows:

Before configuring any MultiLink Trunk:

1. **Read the configuration rules provided in the next section, "MultiLink Trunking Configuration Rules."**
2. **Determine which switch ports (up to four) are to become *trunk members* (the specific ports making up the trunk):**
   - A minimum of two ports are required for each trunk.
   - Ensure that the chosen switch ports are set to Enabled, using the Port Configuration screen (see "Port Configuration" on page 3-56) or through network management.
   - Trunk member ports must be in the same VLAN.
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 1-74).**
5. **Consider how existing VLANs will be affected by the addition of a trunk.**
6. **After completing the preceding steps, see "MultiLink Trunk Configuration" on page 3-61 for screen examples and field descriptions that will help you configure your MultiLink Trunks.**

MultiLink Trunking Configuration Rules

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

- Any port that is currently configured for EAPOL-based security cannot be configured as a MultiLink trunk member.

- Any port that participates in MultiLink Trunking must be an active port (set to Enabled via the Port Configuration screen or through network management).
- All trunk members must be configured into the same VLAN before the Trunk Configuration screen's Trunk Status field can be set to Enabled (See "VLAN Configuration Menu" on page 3-41).
- When an active port is configured in a trunk, the port becomes a *trunk member* when you set the Trunk Status field to Enabled. The spanning tree parameters for the port then change to reflect the new trunk settings.
- If you change the spanning tree participation of any trunk member to Enabled or Disabled, the spanning tree participation of all members of that trunk changes similarly (see "Spanning Tree Considerations for MultiLink Trunks" on page 1-74).
- When a trunk is enabled, the trunk's spanning tree participation setting takes precedence over that of any trunk member. When a trunk is active, you can change the trunk STP setting from either the Trunk Configuration screen or the Spanning Tree Configuration screen.
- If you change the VLAN settings of any trunk member, the VLAN settings of all members of that trunk change similarly.
- When you set any trunk member to Disabled (not active) through the Port Configuration screen or through network management, the trunk member is removed from the trunk. The removed trunk member must be reconfigured through the Trunk Configuration screen to rejoin the trunk. A screen prompt precedes this action. You cannot disable a trunk member if there are only two members on the trunk.
- You cannot configure a trunk member as a monitor port (see "Port Mirroring Configuration" on page 3-67).
- Trunks cannot be monitored by a monitor port; however, trunk members can be monitored (see "Port-Based Mirroring Configuration" on page 1-79).
- All trunk members must have identical IGMP snooping configurations.
- If you change the IGMP snooping configuration for any trunk member, the IGMP snooping settings for all trunk members change.

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 1-47 shows a four-port trunk (T1) with two port members operating at 100 Mb/s and two at 10 Mb/s. Trunk T1 provides an aggregate bandwidth of 220 Mb/s. The Path Cost for T1 is 4 (Path Cost = 1000/LAN speed, in Mb/s). Another three-port trunk (T2) is configured with an aggregate bandwidth of 210 Mb/s, with a comparable Path Cost of 4. When the Path Cost calculations for both trunks are equal, the software chooses the trunk with the larger aggregate bandwidth (T1) to determine the most efficient path.

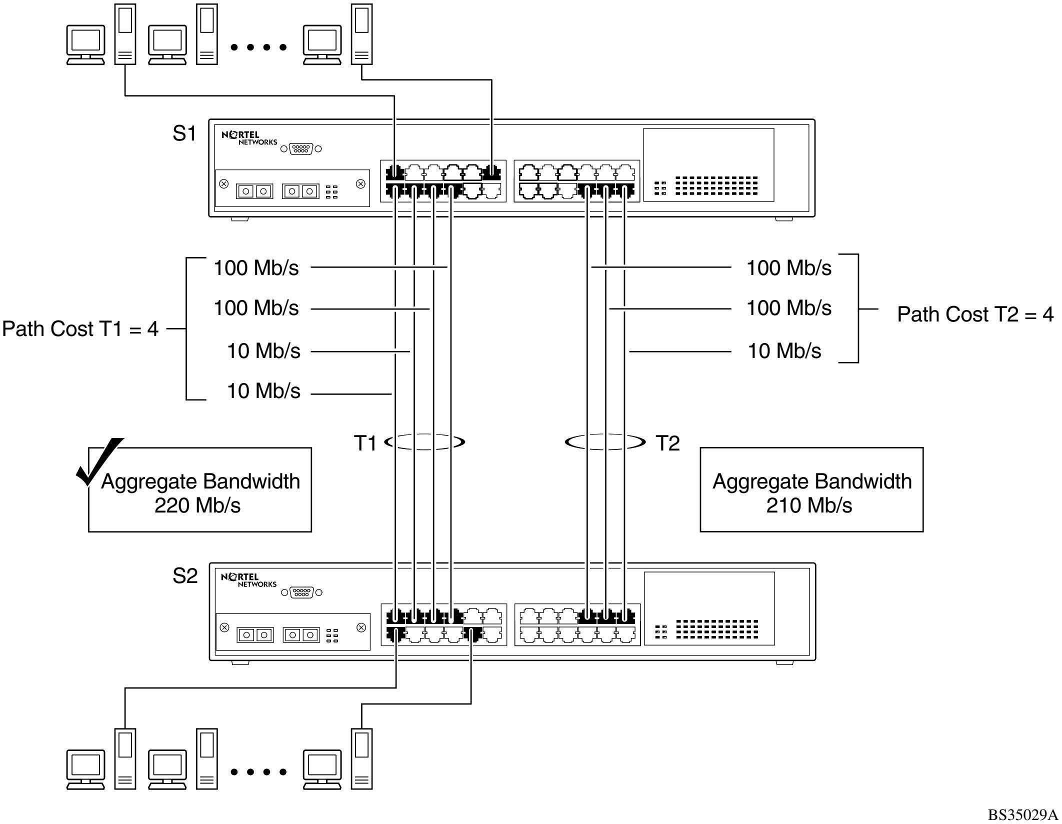
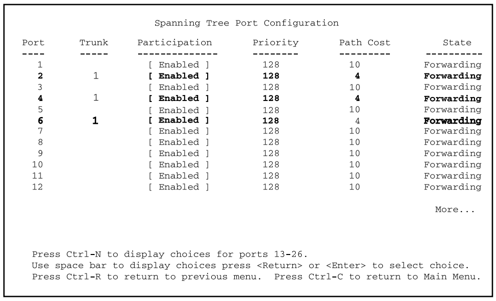


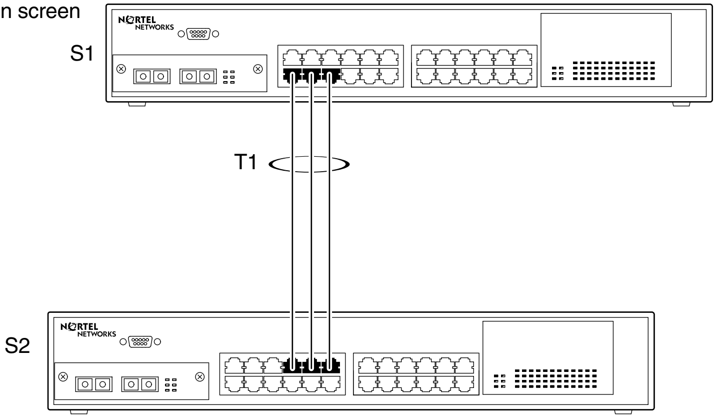
Figure 1-47. Path Cost Arbitration Example

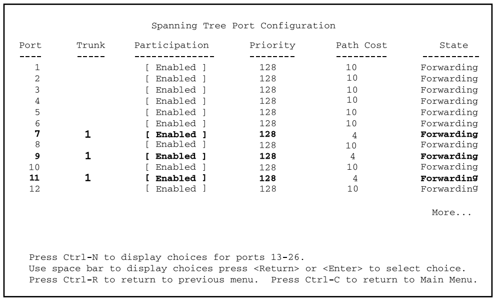
The switch can also detect trunk member ports that are physically misconfigured. For example, in Figure 1-48, trunk member ports 2, 4, and 6 of switch S1 are configured *correctly* to trunk member ports 7, 9, and 11 of switch S2. The Spanning Tree Port Configuration screen for each switch shows the State field for each port in the Forwarding state.



```
                       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





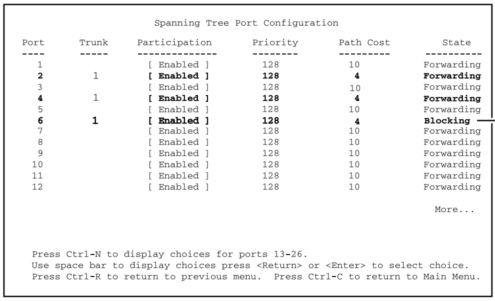
```
                       Spanning Tree Port Configuration

  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

BS35030A

Figure 1-48. Example 1: Correctly Configured Trunk

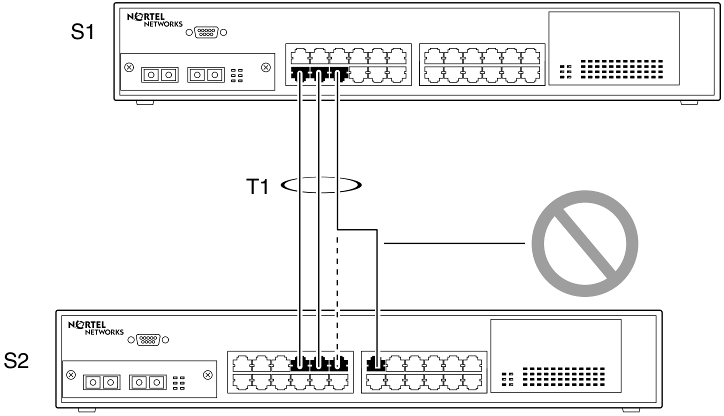
If switch S2's trunk member port 11 is physically disconnected and then reconnected to port 13, the Spanning Tree Port Configuration screen for switch S1 changes to show port 6 in the Blocking state (Figure 1-49).

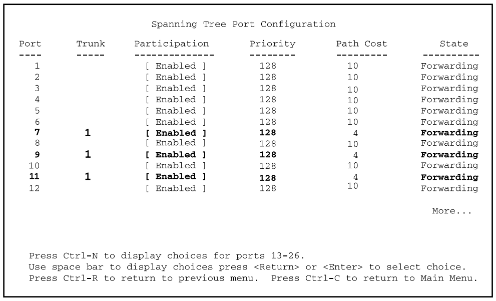


```
                    Spanning Tree Port Configuration

 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.
```

[Blocking]

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

BS35031A

Figure 1-49. Example 2: Detecting a Misconfigured Port

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 screen's 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 the Trunk Status field is set 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" on page 3-61.

Also see Appendix E, "Quick Steps to Features," for configuration flowcharts that can help you use this feature.

Port Mirroring (Conversation Steering)

The port mirroring feature (sometimes referred to as *conversation steering*) allows you to designate a single switch port as a traffic monitor for up to two specified ports or two media access control (MAC) addresses.

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

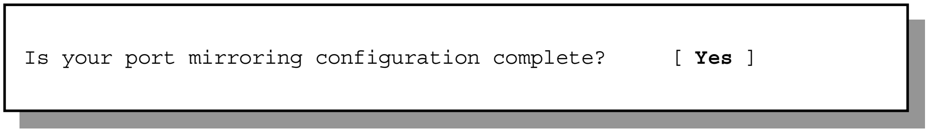
Note: A probe device, such as the Nortel Networks StackProbe* or equivalent, must be connected to the designated monitor port to use this feature (contact your Nortel Networks sales agent for details about the StackProbe).

The following sections provide example configurations for both monitoring modes available with the port mirroring feature:

- Port-based mirroring
- Address-based mirroring

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

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



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

Port-Based Mirroring Configuration

Figure 1-50 shows an example of a port-based mirroring configuration where port 23 is designated as the monitor port for ports 24 and 25 of switch S1. Although this example shows ports 24 and 25 monitored by the monitor port (port 23), any of the trunk members of T1 and T2 can also be monitored.

Note: Trunks cannot be monitored and trunk members cannot be configured as monitor ports (see "MultiLink Trunking Configuration Rules" on page 1-72).

Figure 1-51 shows the Port Mirroring Configuration screen setup for this example.

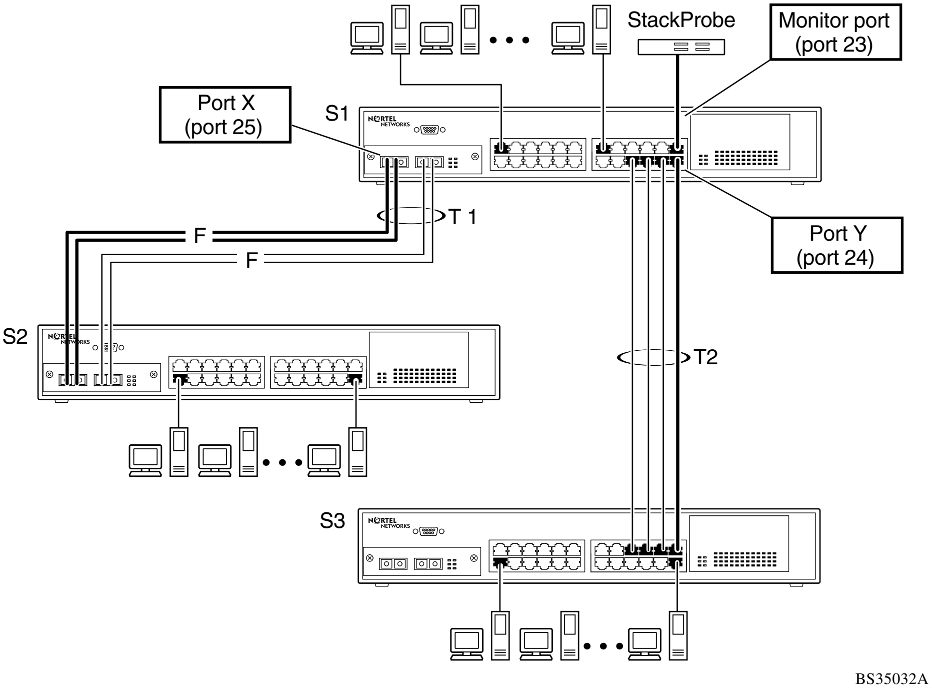


Figure 1-50. Port-Based Mirroring Configuration Example

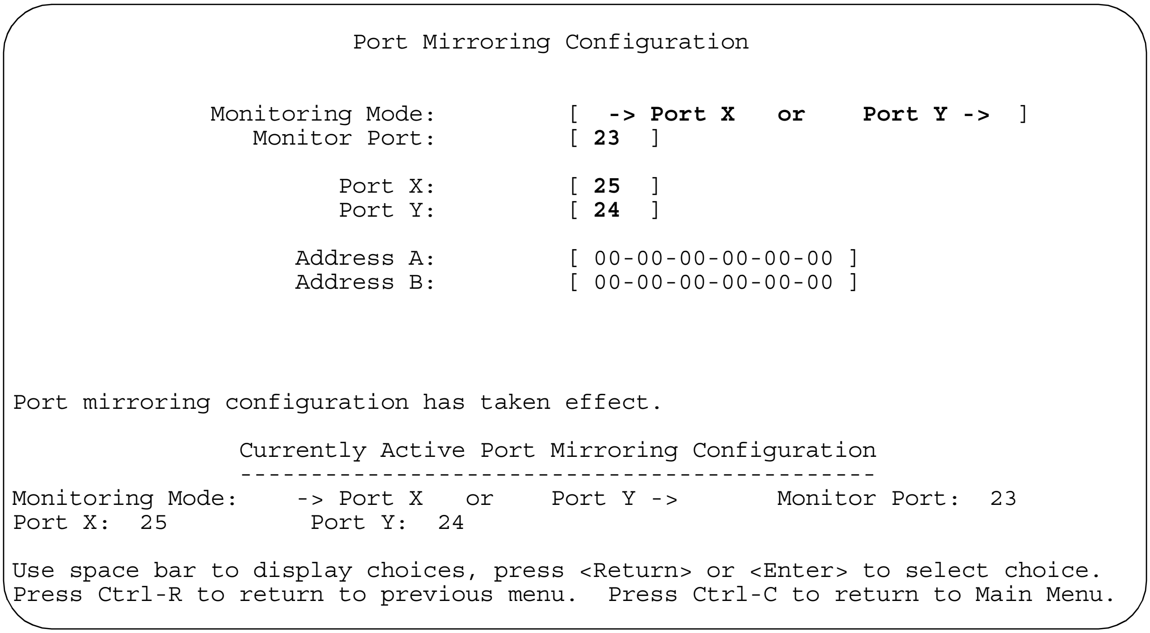
In the configuration example shown in Figure 1-50 on page 1-79, the designated monitor port (port 23) can be set to monitor traffic in any of the following modes:

- Monitor all traffic port X receives.
- Monitor all traffic port X transmits.
- Monitor all traffic port X receives and transmits.
- Monitor all traffic port X receives or port Y transmits.
- Monitor all traffic port X receives (destined to port Y) and then port Y transmits.
- Monitor all traffic port X receives/transmits and port Y receives/transmits (conversations between port X and port Y).

As shown in the Port Mirroring Configuration screen example (Figure 1-51), a user has designated port 23 as the Monitor Port for ports 24 and 25 in switch S1.

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

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



```
                         Port Mirroring Configuration


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

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

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




Port mirroring configuration has taken effect.

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

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

Figure 1-51. Port Mirroring Port-Based Screen Example

Address-Based Mirroring Configuration

Figure 1-52 shows an example of an address-based mirroring configuration where port 23, the designated monitor port for switch S1, is monitoring traffic occurring between address A and address B.

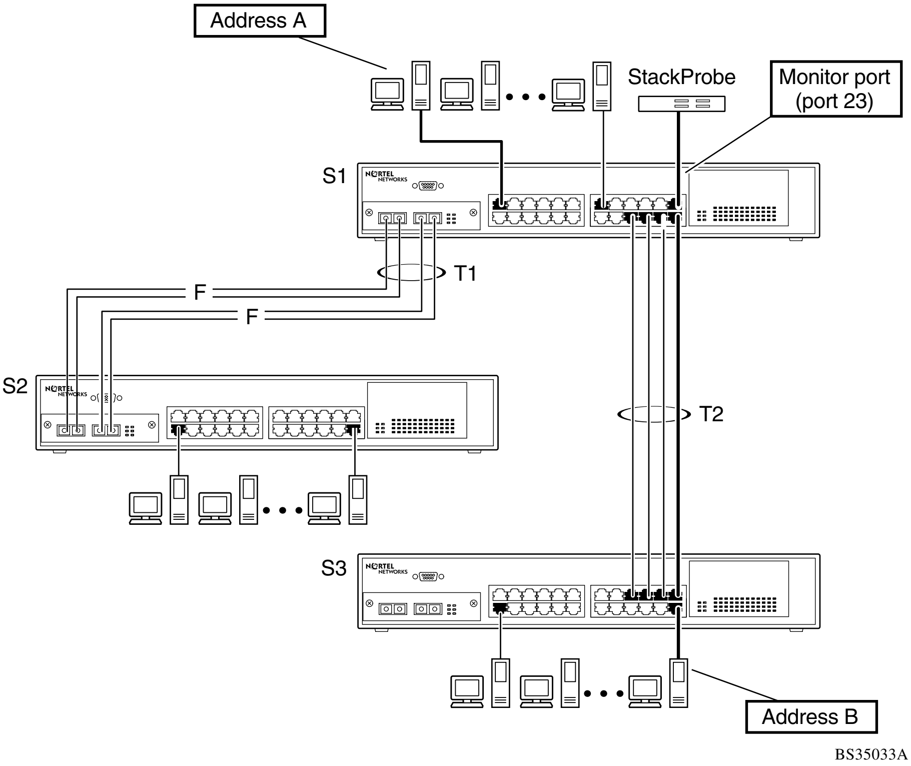


Figure 1-52. Address-Based Mirroring Configuration Example

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

- Monitor all traffic address A transmits to any address.
- Monitor all traffic address A receives from any address.
- Monitor all traffic address A receives or transmits.
- Monitor all traffic address A transmits to address B.
- Monitor all traffic between address A and address B (conversation between the two stations).

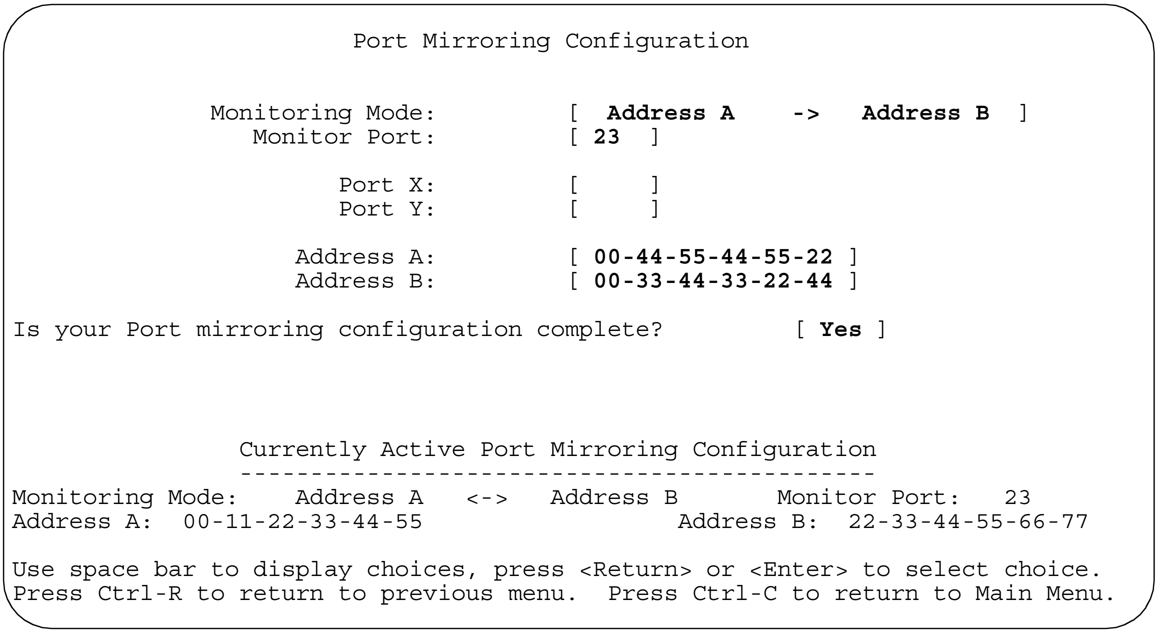
Figure 1-53 shows the Port Mirroring Configuration screen setup for this example.

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

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

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

Note: When you enter MAC addresses in this screen, they are also displayed in the MAC Address Table screen (see "MAC Address Table" on page 3-20).



```
                         Port Mirroring Configuration


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

                        Port X:         [     ]
                        Port Y:         [     ]

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

Is your Port mirroring configuration complete?        [ Yes ]



                 Currently Active Port Mirroring Configuration
                 ---------------------------------------------
Monitoring Mode:    Address A   <->   Address B      Monitor Port:   23
Address A:  00-11-22-33-44-55                  Address B:  22-33-44-55-66-77

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 1-53. Port Mirroring Address-Based Screen Example

Port Mirroring Configuration Rules

The following configuration rules apply to any port mirroring configuration:

- Any port that is currently configured for EAPOL-based security cannot be configured for port mirroring.
- You cannot configure a monitor port as a trunk member or IGMP member.
- A monitor port cannot be used for normal switch functions.
- When you configure a port as a monitor port, the port is automatically disabled from participating in the spanning tree. When you reconfigure the port as a standard switch port (no longer a monitor port), the port is enabled for spanning tree participation.
- When you create a *port-based* port mirroring configuration, be sure that the monitor port and both of the mirrored ports, port X and port Y, have the same configuration. Use the VLAN Configuration screen to configure the VLAN (see “VLAN Configuration Menu” on page 3-41).
- VLAN configuration settings for any ports configured for port-based mirroring cannot be changed. Use the Port Mirroring Configuration screen to disable port mirroring (or reconfigure the port mirroring ports), and then change the VLAN configuration settings.
- For port-based traffic monitoring, use one of the following modes for monitoring broadcast, IP multicast, or unknown DA frames:

  -- Monitor all traffic received by port X.

  -- Monitor all traffic transmitted by port X.

  -- Monitor all traffic received and transmitted by port X.

For more information about using the port mirroring feature, see “Port Mirroring Configuration” on page 3-67.

Also see Appendix E, “Quick Steps to Features,” for configuration flowcharts that can help you use this feature.

Chapter 2
Installing the BayStack 350 Switch

This chapter covers the following topics:

- "Installation Requirements" (page 2-1)
- "Installation Procedure" (page 2-3)
- "Connecting Power" (page 2-12)
- "Verifying the Installation" (page 2-14)
- "Initial Setup" (page 2-17)

Refer to Chapter 3, "Using the Console Interface," to further configure your BayStack 350 switch.

Installation Requirements

Before installing the BayStack 350 switch, verify that the package contains the items shown in Figure 2-1.

➡ **Note:** Be sure that the supplied AC power cord matches the requirements for your region; see "AC Power Receptacle" on page 1-8.

Install the BayStack 350 switch in a ventilated area that is dust free and away from heat vents, warm air exhaust from other equipment, and direct sunlight. Avoid proximity to large electric motors or other electromagnetic equipment. When choosing a location, observe the environmental guidelines listed in Appendix A, "Technical Specifications." You will need a Phillips screwdriver for the installation.

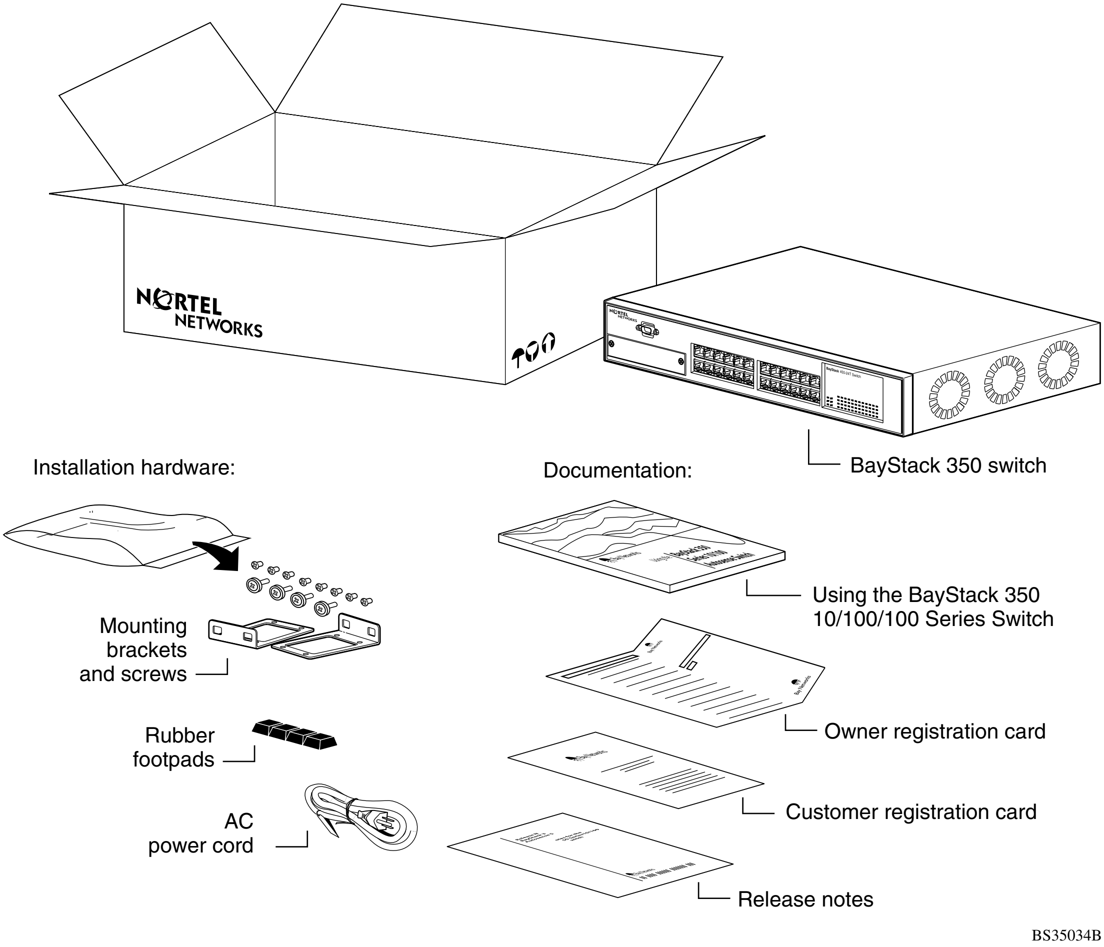


Figure 2-1. Package Contents

Note: Your shipping box may be configured differently than shown in Figure 2-1; the contents will be the same.

The number of boxes and their contents depends on the options you ordered. Open any accessories box and verify that the contents agree with your bill of materials. If any items are missing or damaged, contact the sales agent or the customer service representative from whom you purchased the BayStack 350 switch.

Installation Procedure

This section provides the requirements and instructions for installing the BayStack 350 switch on a flat surface or in a standard 19-inch utility rack. If you install the switch in a rack, ground the rack to the same grounding electrode used by the power service in the area. The ground path must be permanent and must not exceed 1 ohm of resistance from the rack to the grounding electrode.

Note: An optional wall mount kit is available for the BayStack 350 switch (Order Number A12018003). See your Nortel Networks sales representative for ordering information. Installation instructions are provided with the wall mount kit.

Installing the BayStack 350 Switch on a Flat Surface

Caution: When this device is installed on a shelf or tabletop, the accumulated weight of the port cables increases with the height of the shelf or tabletop.

Achtung: Wenn dieses Gerät in einem Stapel auf einem Tisch oder einem Regalboden installiert wird, erhöht sich das Gesamtgewicht der Schnittstellenkabel mit der Höhe des Regalbodens oder Tisches.

Attention: Si l'appareil est posé dans un rack ou sur une étagère, notez bien que le poids du câblage réseau augmente avec la hauteur de l'installation.

Precaución: Cuando este dispositivo se instala apilado en un estante o sobre una mesa, el peso acumulado de los cables de los puertos aumenta según la altura del estante o de la mesa.

Attenzione: Quando il dispositivo viene installato in stack su un ripiano o su un tavolo, il peso dei cavi connessi alle porte aumenta in proporzione all'altezza del ripiano o del tavolo.

注意： このディバイスを棚や台のスタックにインストールする場合、棚や台が高くなるにつれて、ポート・ケーブルの総重量が増します。

The BayStack 350 switch can be mounted onto any appropriate flat, level surface that can safely support the weight of a switch and its attached cables, as long as there is adequate space around the unit for ventilation and access to cable connectors.

To install the switch on a tabletop, shelf, or any other flat surface, follow these steps:

1. **Set the switch on the flat surface and check for proper ventilation.**

   Allow at least 2 inches (5.1 cm) on each side for proper ventilation and 5 inches (12.7 cm) at the back for power cord clearance.

2. **Attach rubber feet to each marked location on the bottom of the chassis.**

   The rubber feet are optional but recommended to keep the unit from slipping.

3. **Attach all devices to the ports.**

   See "Attaching Devices to the BayStack 350 Switch" on page 2-7.

Installing the BayStack 350 Switch in a Rack

Caution: When mounting this device in a rack, do not stack units directly on top of one another in the rack. Each unit must be secured to the rack with appropriate mounting brackets. Mounting brackets are not designed to support multiple units.

Achtung: Wenn Sie dieses Gerät in einem Gerätegestell installieren, stellen Sie die Geräte nicht direkt aufeinander. Jedes Gerät muß mit entsprechenden Halterungen im Gestell befestigt werden. Die Halterungen sind nicht dafür konzipiert, mehrere Geräte zu tragen.

Attention: Si cet appareil doit être encastré dans un rack, ne jamais empiler directement plusieurs unités les unes sur les autres. Chaque unité doit être correctement fixée avec les membrures appropriées. Les membrures ne sont pas conçues pour supporter le poids d'unités multiples.

Precaución: Al montar este dispositivo apilado con otros dispositivos, no apile las unidades directamente unas sobre otras. Cada unidad se debe fijar a la estructura mediante los soportes de montaje adecuados. Los soportes de montaje no están diseñados para soportar varias unidades.

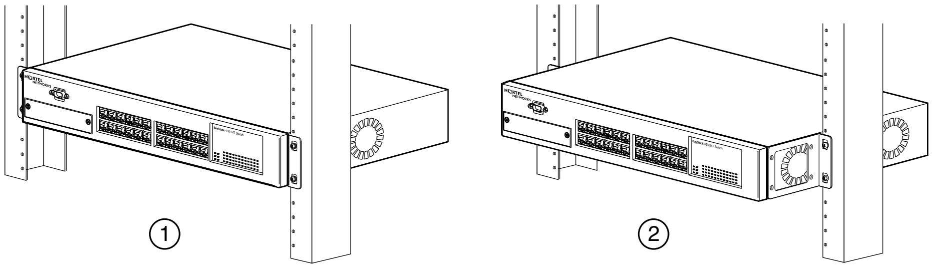
Attenzione: Se il dispositivo viene installato su una cremagliera, non impilarlo su un altro dispositivo montato sulla cremagliera. Ciascuna unità deve essere fissata alla cremagliera con le apposite staffe di montaggio. Tali staffe non possono essere utilizzate per fissare più unità.

注意：このディバイスをラックに据え付ける場合、スタック・ユニットを別のユニットの上に直接積み重ねないでください。各ユニットは、適切な据え付けブラケットでラックに固定してください。据え付けブラケットは、複数のユニットを支えるように設計されていません。

The BayStack 350 switch occupies a 1.6-unit (1.6u) rack space and can be installed in most standard 19-inch racks. Ground the rack to the same grounding electrode used by the power service in the area. The permanent ground path must not exceed 1 ohm of resistance from the rack to the grounding electrode.

To install the BayStack 350 switch in a rack, follow these steps:

1. **Determine how far you want the switch to protrude in front of the rack (see Figure 2-2).**



1 = Flush with rack
2 = Extended from rack

Figure 2-2. Positioning the Chassis in the Rack

You can install the switch flush to the rack or extended from the rack, depending on the orientation of the mounting brackets.

2. **Using a Phillips screwdriver, attach a mounting bracket to each side of the switch using the supplied screws (Figure 2-3).**

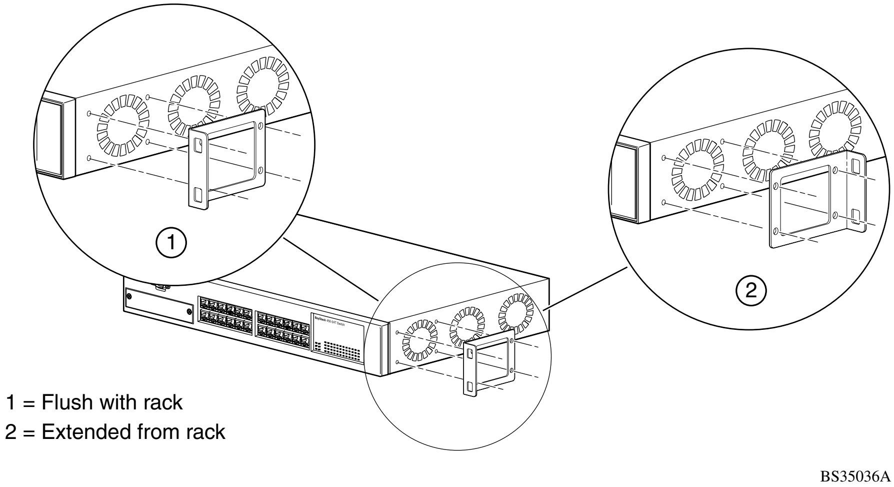


Figure 2-3. Attaching Mounting Brackets

3. **Position the switch in the rack and align the holes in the mounting bracket with the holes in the rack (see Figure 2-4).**

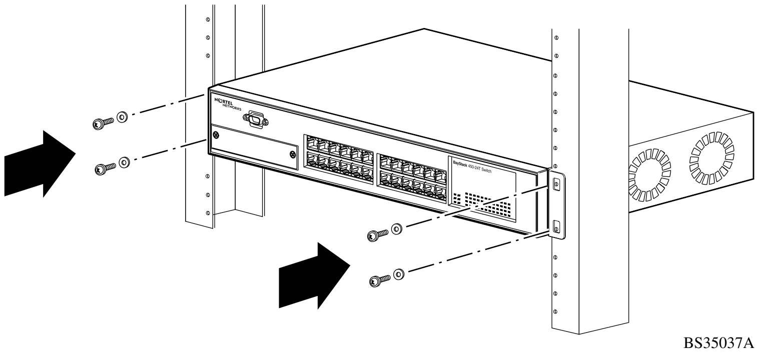


Figure 2-4. Installing the BayStack 350 Switch in an Equipment Rack

4. **Insert two screws, appropriate for your 19-inch rack, into each of the mounting brackets and tighten.**
5. **After the switch is secured in the rack, see the next section, "Attaching Devices to the BayStack 350 Switch."**

Attaching Devices to the BayStack 350 Switch

This section describes how to attach devices to the BayStack 350 switch ports and how to connect a console terminal to the switch Console/Comm port. You can use the console terminal to observe the power-on self-test results and set up the switch, if required, as described later in this chapter.

The BayStack 350 switch has an Uplink/Expansion slot that allows you to attach optional media dependent adapters (MDAs). The MDAs support a range of media types (see Appendix C, "Media Dependent Adapters," for more information about MDA types available from Nortel Networks). Refer to the documentation that came with your specific MDA for information about its cabling and LED indications.

Depending on your network configuration requirements, connect the RJ-45 port cables, the console port, and any optional MDA port cables. After attaching the devices to the BayStack 350 switch, see "Connecting Power" on page 2-12 to connect the AC power cord and power up the switch.

You can connect the BayStack 350 switch to any equipment that conforms to the IEEE 802.3 standard, such as the following devices:

- Ethernet networking devices
- Individual workstations or servers
- Other switches, bridges, or hubs

Connecting the 10BASE-T/100BASE-TX Ports

Connect devices to the 10BASE-T/100BASE-TX ports as shown in Figure 2-5.

The BayStack 350 switch 10BASE-T/100BASE-TX ports are configured with RJ-45 connectors that are wired as MDI-X ports. As in conventional Ethernet repeater hubs, the BayStack 350 switch ports connect via straight-through cables to the network interface card (NIC) in a node or server. When connecting to an Ethernet hub or to another switch, you must use a crossover cable. See Appendix F, “Connectors and Pin Assignments,” for more information.

By default, all BayStack 350 switch 10BASE-T/100BASE-TX switch ports are set with autonegotiation enabled. This feature allows any port to match the best service provided by the connected station, up to 100 Mb/s in full-duplex mode.

Note: The 10BASE-T/100BASE-TX ports must use Category 5 UTP cable to accommodate the 100BASE-TX functionality.

To connect the RJ-45 port cables, insert the cable plug into the appropriate port connector until the release tab snaps into the locked position (Figure 2-5).

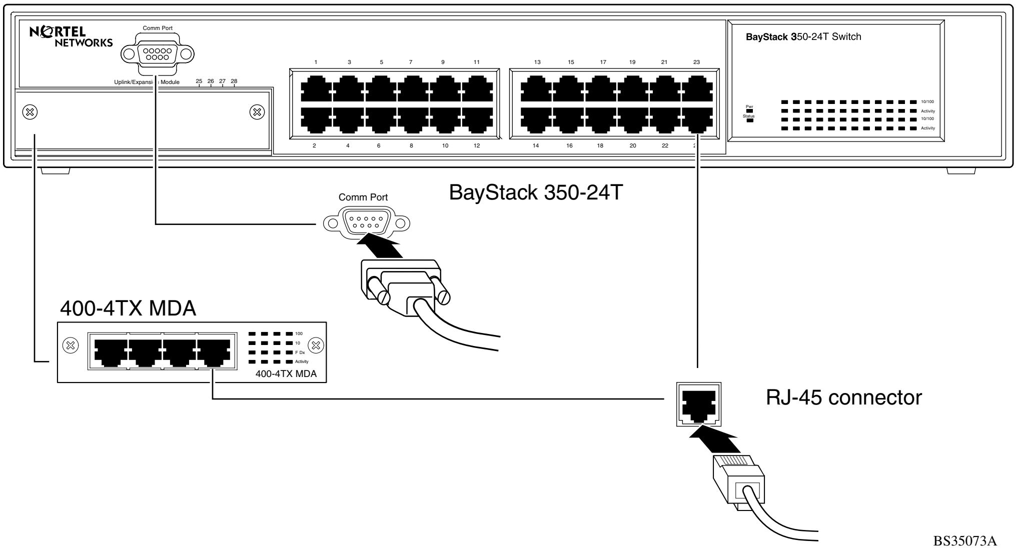


Figure 2-5. 10/100 Mb/s Port Connections

Connecting Fiber Optic Ports

Connect devices to the fiber optic ports as shown in Figure 2-6.

The (optional) 400-4FX MDA is a 100BASE-FX device that uses MT-RJ port connectors with 62.5/125-micron multimode fiber optic cable. The 400-2FX MDA is also a 100BASE-FX device but uses standard SC port connectors with 62.5/125 micron multimode fiber optic cable.

The 1000BASE-X MDAs (the 450-1SR/SX and the 450-1-LR/LX) use standard SC port connectors but special consideration is required for 1000BASE-LX connections (see "1000BASE-LX Multimode Applications" on page C-22).

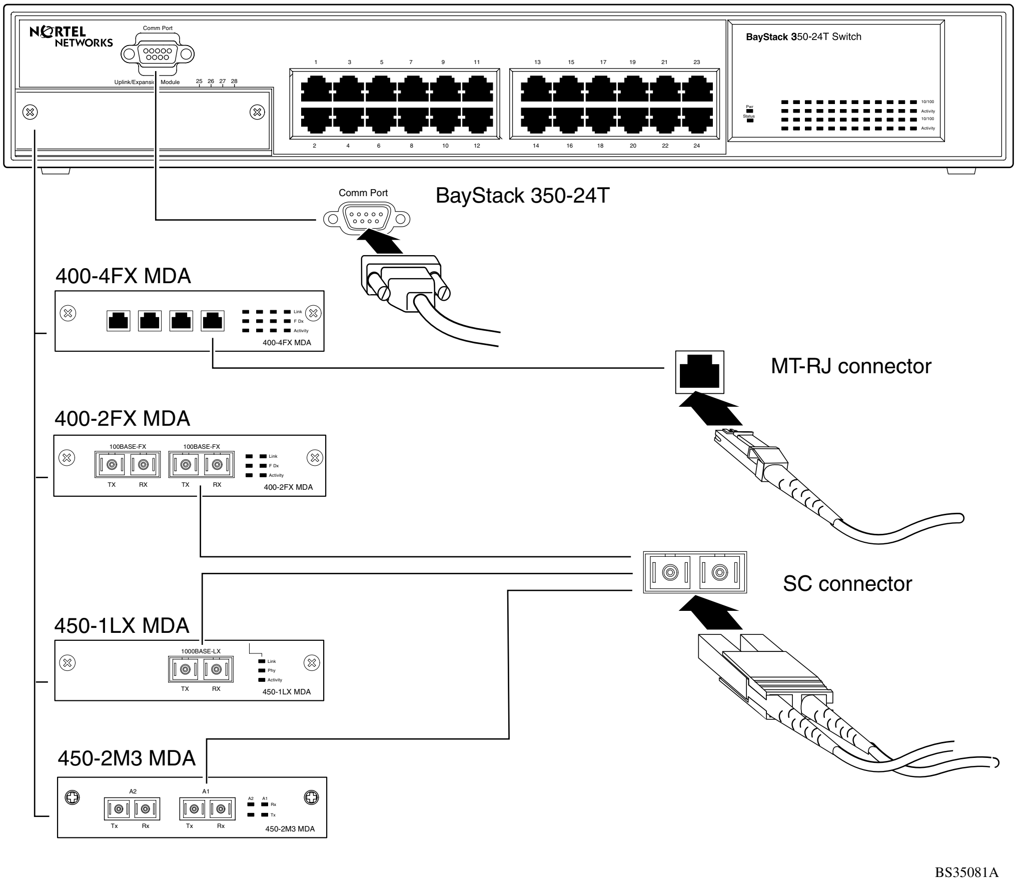


Figure 2-6. Fiber Optic Port Connections

Console/Comm Port

The serial console interface is an RS-232 port that enables a connection to a PC or terminal for monitoring and configuring the switch. You can also connect this port to an external modem to enable remote dial-in management of the switch. The port is a male DB-9 connector, implemented as a data communication equipment (DCE) connection.

To use the Console/Comm port, you need the following equipment:

- A terminal or TTY-compatible terminal, or a portable computer with a serial port and the ability to emulate a terminal.

  The terminal should have the following settings:

  -- 9600 baud

  -- No parity

  -- 8 bits

  -- 1 stop bit

  -- Window Terminal Emulator option set to NO

  -- Terminal Preferences: function, arrow, and control keys active

  -- Buffer size set to 24

- A UL-listed straight-through RS-232 cable with a female DB-9 connector for the console port on the switch.

  The other end of the cable must have a connector appropriate to the serial port on your computer or terminal. (Most terminals or computers use a male DB-25 connector.)

  Any cable connected to the console port must be shielded to comply with emissions regulations and requirements.

  See "DB-9 (RS-232-D) Console/Comm Port Connector," on page F-1 for a description of the pin assignments.

Connecting a Terminal to the Console/Comm Port

To connect a terminal to the console port:

1. **Set the terminal protocol as described in "Console/Comm Port" on page 2-10.**
2. **Connect the terminal (or a computer in terminal-emulation mode) to the console port using the RS-232 cable.**
   a. **Connect the female connector of the RS-232 cable directly to the Console/Comm Port on the switch, and then tighten the captive retaining screws (see Figure 2-7).**
   b. **Connect the other end of the cable to a terminal or the serial connector of a personal computer running communications software.**

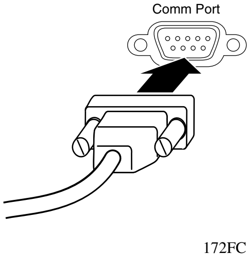


Figure 2-7. Connecting to the Console/Comm Port

3. **See the next section, "Connecting Power," to connect the AC power cord and power up the BayStack 350 switch.**

Connecting Power

The BayStack 350 switch does not have a power on/off switch. When you connect the AC power cord to a suitable AC power outlet, the switch powers up immediately.

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。

To connect the AC power cord, follow these steps:

1. **Plug one end of the AC power cord into the AC power receptacle on the switch back panel (Figure 2-8).**

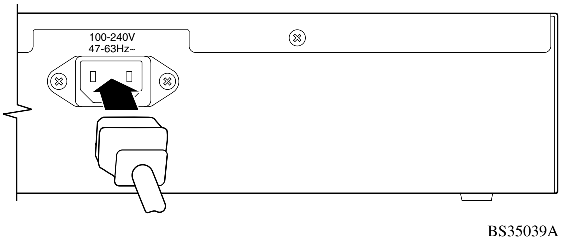


Figure 2-8. BayStack 350 Switch AC Power Receptacle

2. **Plug the other end of the AC power cord into the grounded AC power outlet (Figure 2-9).**

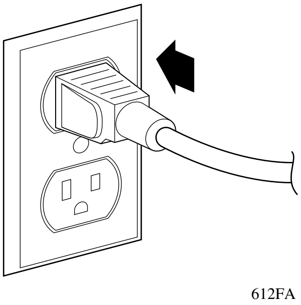


Figure 2-9. Grounded AC Power Outlet

3. **See the next section, "Verifying the Installation," to verify proper operation.**

Verifying the Installation

When power is applied to the switch, power-on self-tests are run.

You can verify proper operation of the BayStack 350 switch by observing the front-panel LEDs or by viewing the self-test results as displayed in the BayStack 350 switch Self-Test screen.

Verifying the Installation Using the LEDs

To verify the installation using the LEDs, check that the switch power-up sequence is as described in Table 2-1:

Table 2-1. Power-Up Sequence

Stage	Description	LED indication
1	Immediately after AC power is applied to the switch, DC power is available to the switch's internal circuitry.	The Power LED turns on within 5 seconds (Figure 2-10). If the Power LED does not turn on, verify that power is available at the AC power outlet and that the power cable is fastened securely at both ends. If the Power LED remains off, contact the sales agent or the customer service representative from whom you purchased the switch.
2	The switch initiates a self-test.	As the self-test initiates subroutines, the port status LEDs flash various patterns. When the switch passes the self-test (within 10 seconds), the Status LED turns on (Figure 2-10). If a nonfatal error occurs during self-test, the Status LED blinks. If the switch fails the self-test, the Status LED remains off. Contact the sales agent or the customer service representative from whom you purchased the switch.

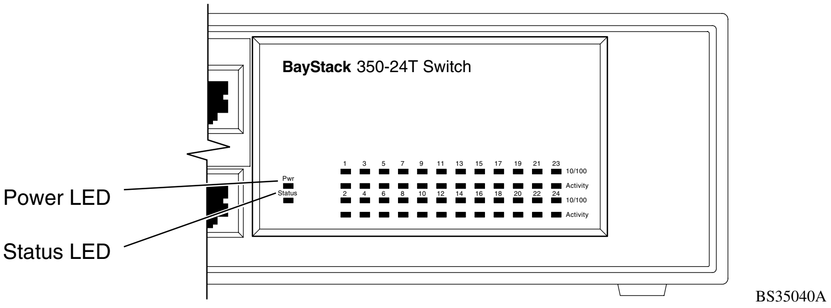


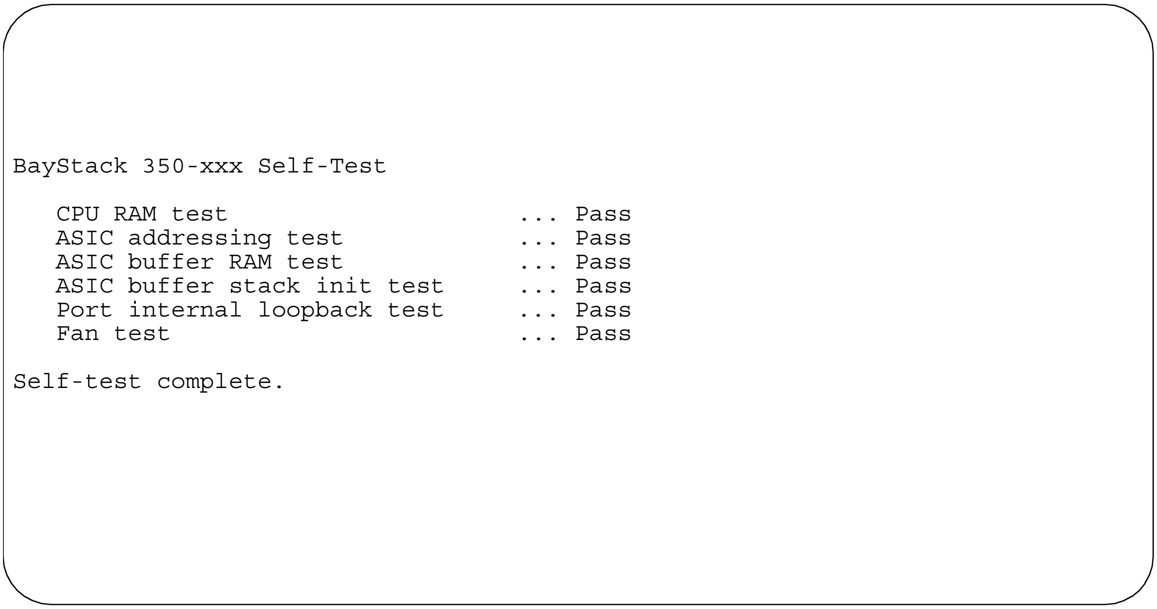
Figure 2-10. Observing LEDs to Verify Proper Operation

Verifying the Installation Using the Self-Test Screen

If a monitor is connected to the switch (see “Console/Comm Port” on page 2-10), you can observe the BayStack 350 switch Self-Test screen (Figure 2-11).

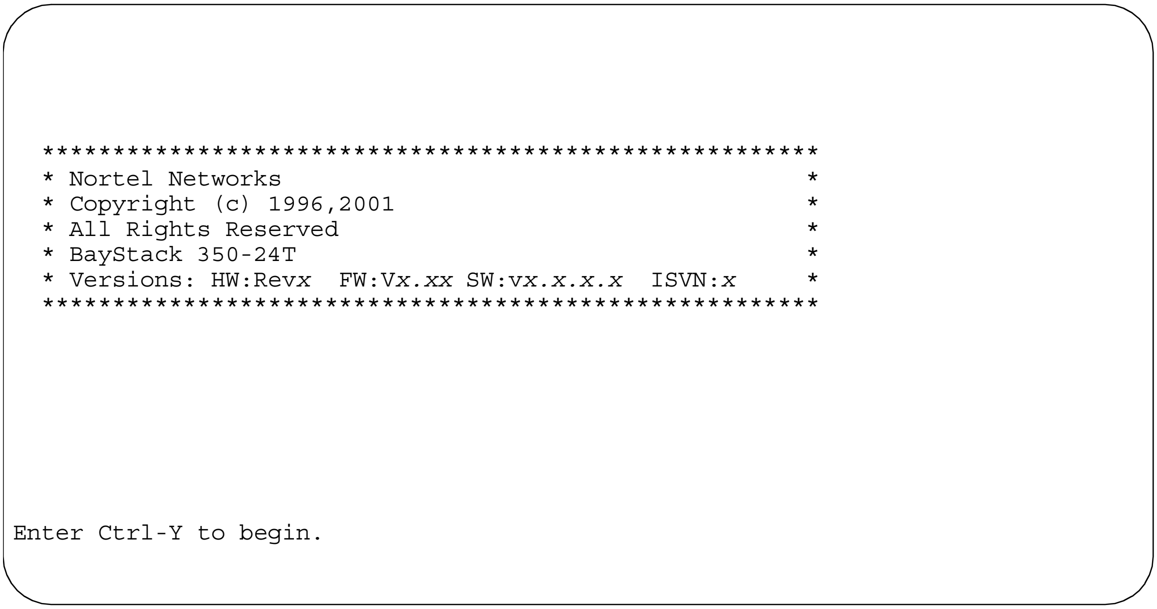
The results of the self-test are displayed briefly (5 or 10 seconds) in the Self-Test screen, which is followed by the Nortel Networks logo screen (Figure 2-12).

Note: The Self-Test screen remains displayed only if the self-test detects a fatal error.



```
BayStack 350-xxx Self-Test

   CPU RAM test                       ... Pass
   ASIC addressing test               ... Pass
   ASIC buffer RAM test               ... Pass
   ASIC buffer stack init test        ... Pass
   Port internal loopback test        ... Pass
   Fan test                           ... Pass

Self-test complete.
```

Figure 2-11. BayStack 350 Switch Self-Test Screen



```
  *******************************************************
  * Nortel Networks                                     *
  * Copyright (c) 1996,2001                             *
  * All Rights Reserved                                 *
  * BayStack 350-24T                                    *
  * Versions: HW:Revx  FW:Vx.xx SW:vx.x.x.x  ISVN:x     *
  *******************************************************






Enter Ctrl-Y to begin.
```

Figure 2-12. Nortel Networks Logo Screen

> ➡ **Note:** The Nortel Networks logo screen for your switch will display the correct model number and the current hardware, firmware, software, and ISVN versions.

Upon successful completion of the power-up self-tests, the switch is ready for normal operation.

To access the BayStack 350 Main Menu, press [Ctrl]-Y.

Initial Setup

In most cases the BayStack 350 switch can be installed and made operational using the system default settings (see Appendix G, “Default Settings” for a list of default settings for the BayStack 350 switch).

Although the BayStack 350 switch is designed for plug-and-play operation, certain parameters must be configured for the switch *management* function to become fully operational.

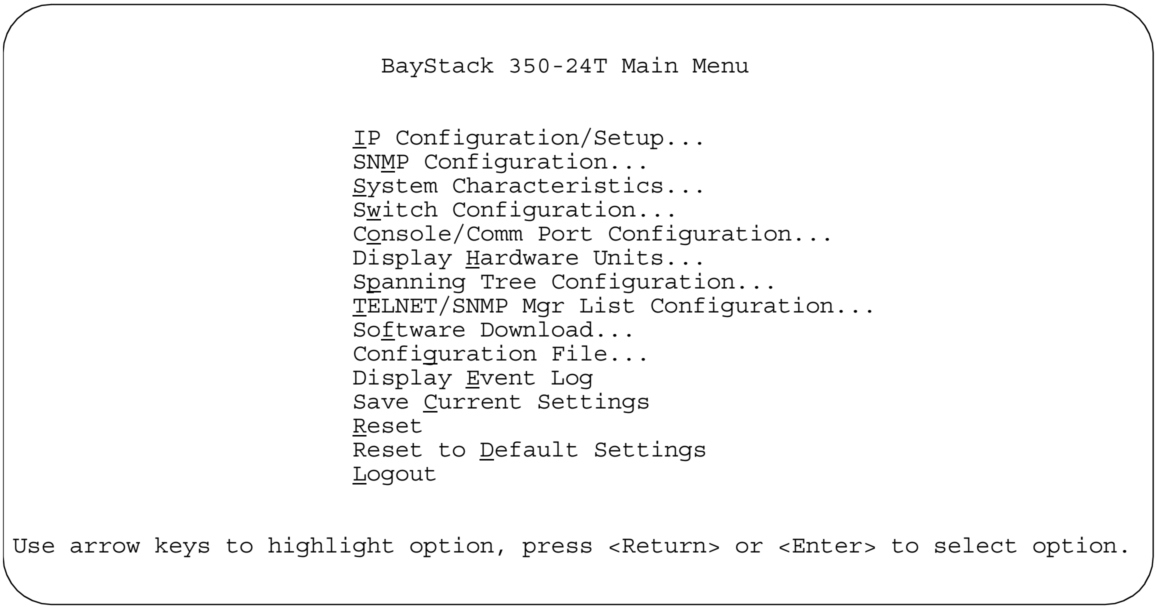
A minimal configuration is required when you plan on remote management or TFTP operations. In that case, you need to enter the IP address of the switch, the subnet mask, and the gateway address.

To set the IP address, subnet mask, and gateway address for the switch, follow these steps:

1. **Apply power to the switch.**
2. **After the Nortel Networks logo screen appears, press [Ctrl]-Y.**

   The Main Menu is displayed (Figure 2-13).

   (The Main Menu hierarchy is described in Chapter 3, “Using the Console Interface.”)



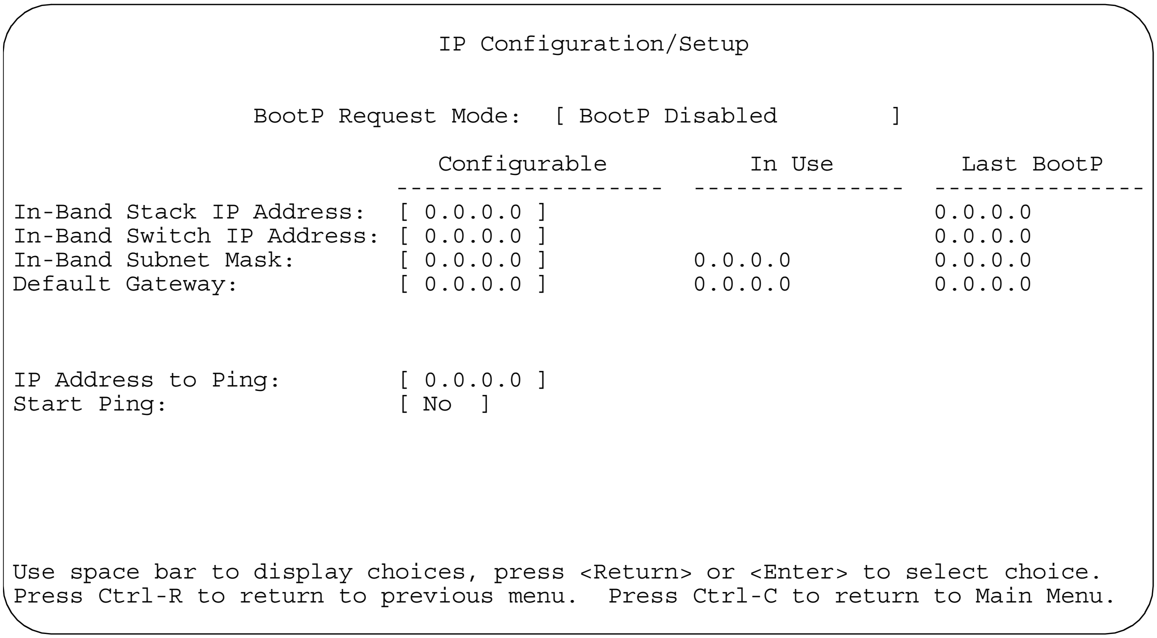
```
                           BayStack 350-24T Main Menu


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


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

Figure 2-13. Main Menu

3. **Select IP Configuration/Setup (or press i) from the Main Menu.**

   This selection displays the IP Configuration/Setup screen (Figure 2-14).

Note: The default management VLAN (IP interface) for the BayStack 350 switch is VLAN 1. However, you can specify which VLAN you want to be the management VLAN (see "VLAN Configuration on page 3-43).



```
                              IP Configuration/Setup


                 BootP Request Mode:  [ BootP Disabled        ]

                              Configurable          In Use         Last BootP
                           -------------------  ---------------  ---------------
In-Band Stack IP Address:  [ 0.0.0.0 ]                           0.0.0.0
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.
```

Figure 2-14. IP Configuration/Setup Screen

4. **Enter the IP address of the switch in the In-Band IP Address field, and then press [Enter].**

Note: When you enter the IP address in the In-Band Switch IP Address field, and the In-Band Subnet Mask field is not present, the software provides an *in-use* default value for the In-Band Subnet Mask field, based on the class of the entered IP address.

5. **Enter the IP subnet mask address in the In-Band Subnet Mask field, and then press [Enter].**

6. **Enter the default gateway address in the Default Gateway field, and then press [Enter].**

After setting up your switch, see Chapter 3, “Using the Console Interface,” for detailed descriptions of the menus and screens you can use to customize your configuration.

Chapter 3
Using the Console Interface

This chapter describes how to configure and manage the BayStack 350 switch using the menu-driven console interface (CI).

This chapter covers the following topics:

Accessing the CI Menus and Screens

You can access the CI menus and screens locally through a console terminal, remotely through a dial-up modem connection, or in-band through a TELNET session (see “Console/Comm Port” on page 2-10).

You can also manage the BayStack 350 switch using Nortel Networks Optivity network management software or any generic SNMP-based management software; however, for the switch management function to become fully operational, you must supply certain parameters, such as the switch IP address (see “Initial Setup” on page 2-17).

Note: If you have a properly configured BootP server in your network, it will detect 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 the BayStack 350 switch.

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.

Some options allow you to toggle between several possible settings; 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:

  a. Use the arrow keys to highlight the option name.

  b. 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 settings in a form:

  a. Use the spacebar to highlight the setting.

  b. Press [Enter].

- To clear a string field:

  a. Position the cursor in the string field.

  b. Press [Ctrl]-K.

- To return to the previous menu, press [Ctrl]-R.
- To return to the main menu at any time, press [Ctrl]-C.
- Press [Backspace] to delete entered text.
- Accelerator keys

  You can use accelerator keys to enter repetitive data into the fields of certain screens. The accelerator keys can be used only on fields that require entering a list, which includes the MAC Address Security Port Lists screen and the MAC Address Security Table screen.

  For more information about using the accelerator keys, see "Accelerator Keys for Repetitive Tasks" on page 3-32.

Map of CI Menus and Screens

Figure 3-1 shows a map of the CI screens. The remainder of this chapter describes the CI screens and their fields, beginning with the main menu.

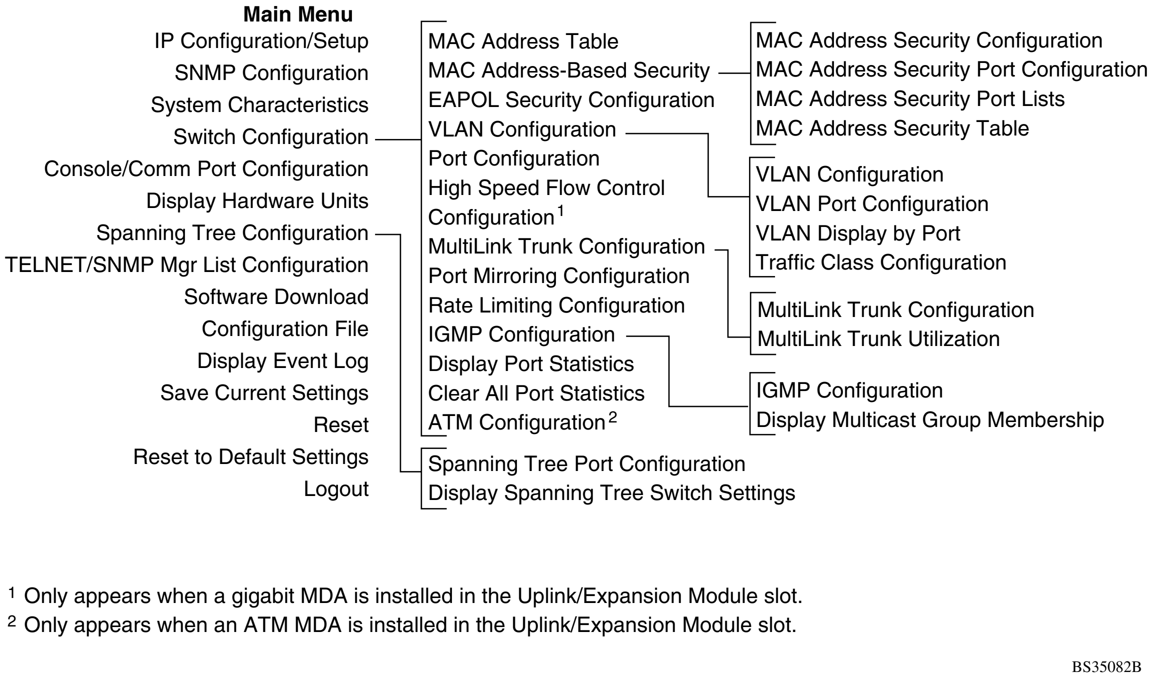

Main Menu
IP Configuration/Setup
SNMP Configuration
System Characteristics
Switch Configuration
Console/Comm Port Configuration
Display Hardware Units
Spanning Tree Configuration
TELNET/SNMP Mgr List Configuration
Software Download
Configuration File
Display Event Log
Save Current Settings
Reset
Reset to Default Settings
Logout
MAC Address Table
MAC Address-Based Security
EAPOL Security Configuration
VLAN Configuration
Port Configuration
High Speed Flow Control Configuration[1]
MultiLink Trunk Configuration
Port Mirroring Configuration
Rate Limiting Configuration
IGMP Configuration
Display Port Statistics
Clear All Port Statistics
ATM Configuration[2]
MAC Address Security Configuration
MAC Address Security Port Configuration
MAC Address Security Port Lists
MAC Address Security Table
VLAN Configuration
VLAN Port Configuration
VLAN Display by Port
Traffic Class Configuration
MultiLink Trunk Configuration
MultiLink Trunk Utilization
IGMP Configuration
Display Multicast Group Membership
Spanning Tree Port Configuration
Display Spanning Tree Switch Settings
[1] Only appears when a gigabit MDA is installed in the Uplink/Expansion Module slot.
[2] Only appears when an ATM MDA is installed in the Uplink/Expansion Module slot.
BS35082B

Figure 3-1. Map of Console Interface Screens

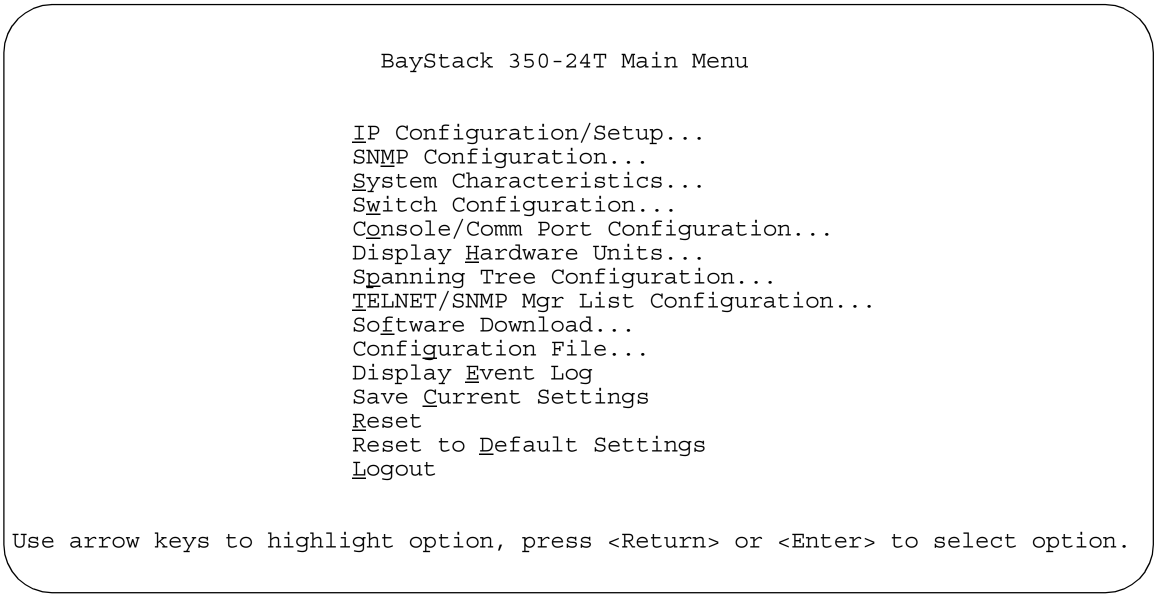
The CI screens for your specific switch model will show the correct model name in the main menu screen title and the correct number of ports and port types in the Port Configuration screen.

➡ **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 3-2). 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.



```
                         BayStack 350-24T Main Menu

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

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

Figure 3-2. Console Interface Main Menu

Table 3-1 describes the CI main menu options.

Table 3-1. Console Interface Main Menu Options

Option	Description
IP Configuration/ Setup...	Displays the IP Configuration/Setup screen (see "IP Configuration/Setup" on page 3-9). This screen allows you to set or modify your IP configuration parameters and to verify a station's IP address using the ping feature.
SNMP Configuration...	Displays the SNMP Configuration screen (see "SNMP Configuration" on page 3-14). This screen allows you to set or modify the SNMP read-only community and read-write community strings, enable or disable the authentication trap, set the IP address of trap receivers, set the trap community strings, and enable or disable the switch's participation in autotopology.
System Characteristics...	Displays the System Characteristics screen (see "System Characteristics" on page 3-16). This screen allows you to view switch characteristics, including number of resets, power status, hardware, firmware, software, ISVN version, and the MAC address. This screen also contains three user-configurable fields: sysContact, sysName, and sysLocation.
Switch Configuration...	Displays the Switch Configuration Menu (see "Switch Configuration" on page 3-18). This menu provides the following options: MAC Address Table, MAC Address-Based Security, EAPOL Security Configuration, VLAN Configuration, Port Configuration, High Speed Flow Control Configuration, MultiLink Trunk Configuration, Port Mirroring Configuration, Rate Limiting Configuration, IGMP Configuration, Display Port Statistics, Clear All Port Statistics, and ATM Configuration.
Console/Comm Port Configuration...	Displays the Console/Comm Port Configuration screen (see "Console/Comm Port Configuration" on page 3-95). This screen allows you to configure and modify the console/Comm port parameters, including the console port speed and password settings.
Display Hardware Units...	Displays the Hardware Unit Information screen (see "Hardware Unit Information" on page 3-102). This screen identifies your switch model and any installed MDA.
Spanning Tree Configuration...	Displays the Spanning Tree Configuration Menu (see "Spanning Tree Configuration" on page 3-103). This menu provides the following options: Spanning Tree Port Configuration and Display Spanning Tree Switch Settings.
TELNET/SNMP Mgr List Configuration...	Displays the TELNET/SNMP Manager List Configuration screen (see "TELNET/SNMP Manager List Configuration" on page 3-111). This screen allows you to specify up to 10 user-assigned host IP addresses that are allowed TELNET and SNMP access to the switch. You can set your switch to enable a user at a remote console terminal to communicate with the BayStack 350 switch as if the console terminal were directly connected to it.You can have up to four active TELNET sessions at one time.

(continued)

Table 3-1. Console Interface Main Menu Options *(continued)*

Option	Description
Software Download...	Displays the Software Download screen (see "Software Download" on page 3-114). This screen allows you to revise the BayStack 350 switch software image that is located in nonvolatile flash memory.
Configuration File...	Displays the Configuration File Download/Upload screen (see "Configuration File" on page 3-118). 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 or other switches with the same parameters.
Display Event Log	Displays the Event Log screen (see "Display Event Log" on page 3-120).
Save Current Settings	Saves your current configuration settings *without resetting your switch* (see "Save Current Settings" on page 3-123). When you select this option a confirmation prompt appears. Enter Yes to save your configuration settings; enter No to abort the option.
Reset	Resets the switch with the current configuration settings. When you select this option a confirmation prompt appears. Enter Yes to save your configuration settings; enter No to abort the option. If 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 350 Main Menu.
Reset to Default Settings	Resets the switch to the factory default configuration settings (see "Reset to Default Settings" on page 3-126). When you select this option a confirmation prompt appears. Enter Yes to reset the switch to the factory default configuration settings; enter No to abort the option. When you activate this option, the switch resets, runs a self-test, and then displays the Nortel Networks logo screen. **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.

(continued)

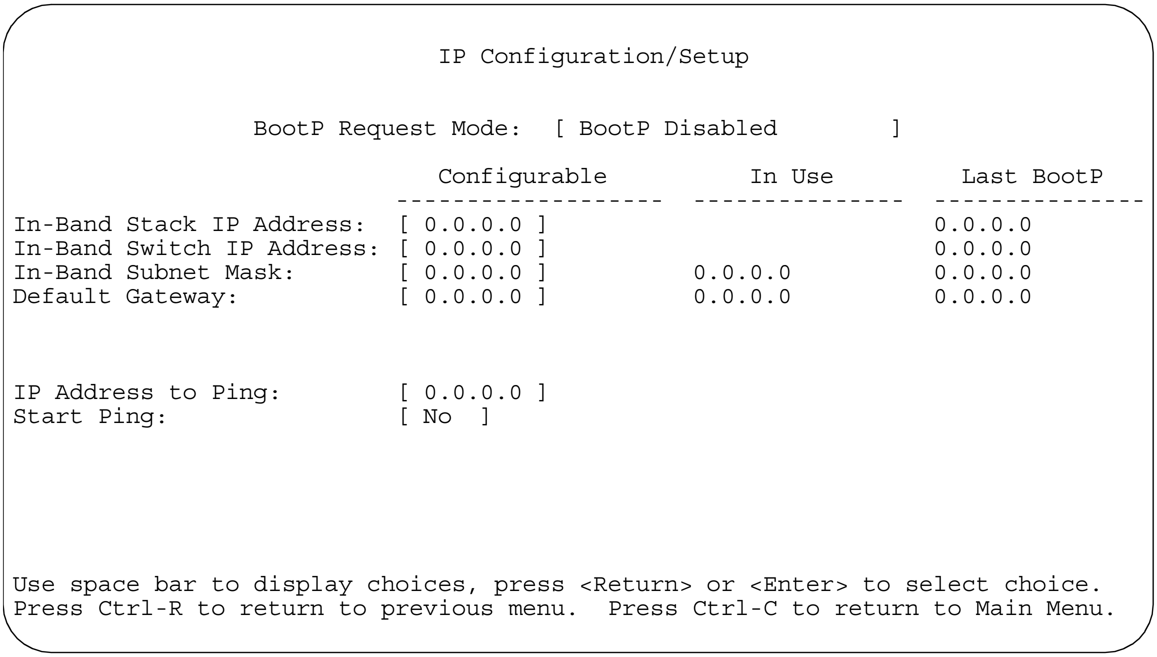
Table 3-1. Console Interface Main Menu Options *(continued)*

Option	Description
	⛔ **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。
	Enter Yes to reset the switch to factory default configuration settings; enter No to abort the option. When you select this option, the switch resets, runs a self-test, and then displays the Nortel Networks logo screen. Press [Ctrl]-Y to access the BayStack 350 Main Menu.
Logout	The Logout option allows a user in a TELNET session or a user working at a password-protected console terminal, to terminate the session (see “Logout” on page 3-129).

IP Configuration/Setup

The IP Configuration/Setup screen (Figure 3-3) allows you to set or modify the BayStack 350 switch IP configuration parameters and to verify a station’s IP address using the ping feature. Data that you enter in the user-configurable fields takes effect as soon as you press [Enter].

Choose IP Configuration/Setup (or press i) from the main menu to open the IP Configuration/Setup screen.



```
                               IP Configuration/Setup


                 BootP Request Mode:   [ BootP Disabled        ]

                               Configurable          In Use         Last BootP
                            -------------------  ---------------  ---------------
In-Band Stack IP Address:   [ 0.0.0.0 ]                           0.0.0.0
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.
```

Figure 3-3. IP Configuration/Setup Screen

Note: The read-only fields in this screen are updated based on the BootP mode specified in the BootP Request Mode field. (See “BootP Request Mode” on page 3-11 for more information.)

Table 3-2 describes the IP Configuration/Setup screen fields.

Table 3-2. IP Configuration/Setup Screen Fields

Field	Description	
BootP Request Mode	One of four modes of operation for BootP. (See "BootP Request Mode" on page 3-11 for details about the four modes.)	
	Default	BootP Disabled
	Range	BootP Disabled, BootP or Last Address, BootP When Needed, BootP Always
Configurable	Column header for the user-configurable fields in this screen. The data displayed in this column represents parameters that you can configure (or that are currently configured).	
In Use	Column header for the read-only fields in this screen. The read-only data displayed in this column represents data 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 data obtained from the last BootP reply received.	
In-Band Stack IP Address	**Accessible with BayStack 450 and BayStack 410-24T switch models only:** (Allows the in-band *stack* IP address field to be set for stackable switch models).	
In-Band Switch IP Address	The in-band IP address of the BayStack 350 switch.	
	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
➡	**Note:** When the IP address is entered in the In-Band Switch 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 Switch IP Address field.	
In-Band Subnet Mask	The subnet address mask associated with the in-band IP address shown on the screen. 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	0.0.0.0 (no subnet mask assigned)
	Range	Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point.

(continued)

Table 3-2. IP Configuration/Setup Screen Fields *(continued)*

Field	Description	
Default Gateway	The IP address of the default gateway.	
	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.
IP Address to Ping	The IP address of the station you want to verify using the ping feature.	
	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
Start Ping	Allows you to ping the target IP address entered in the IP Address to Ping field (above).	
	Default	No
	Range	No, Yes

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 Disabled
- BootP or Last Address
- BootP When Needed
- BootP Always

Note: Whenever the switch is broadcasting BootP requests, the BootP process will time out if a reply is not received within (approximately) 7 minutes. When the process times out, the BootP request mode automatically changes to BootP Disabled mode. To restart the BootP process, change the BootP request mode to any of the three following modes: BootP When Needed, BootP Always, or to BootP or Last Address.

BootP Disabled

Allows the switch to be managed only by using the IP address set from the console terminal (this is the default mode for your switch).

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 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.

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-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 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:

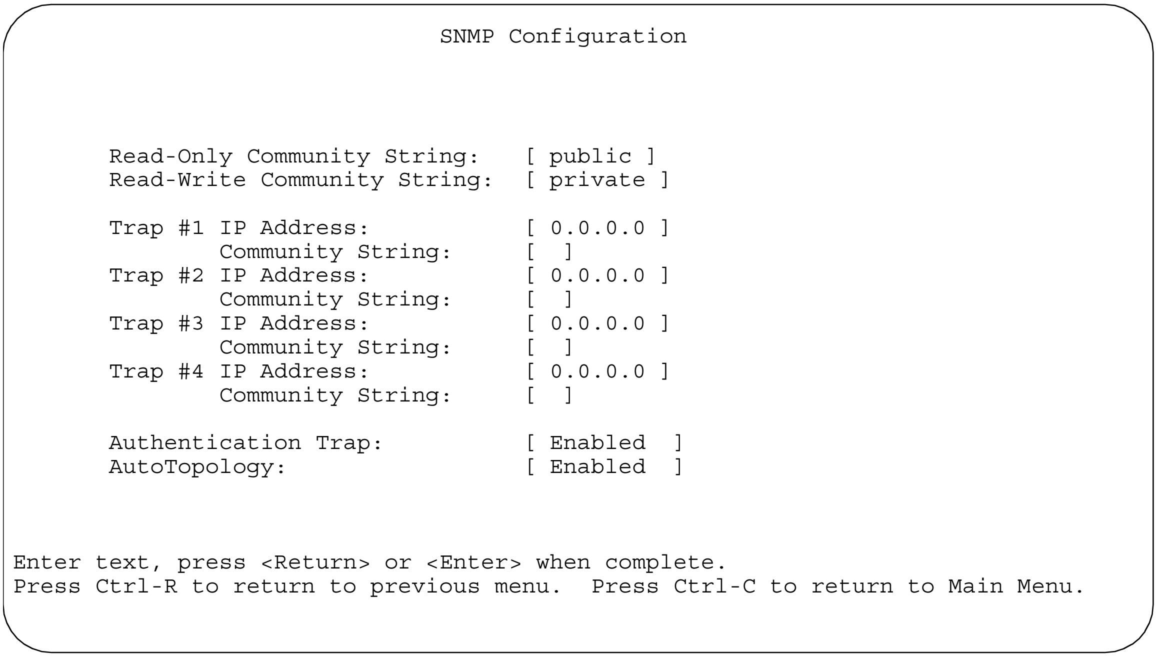
- The switch continues to broadcast BootP requests, regardless of whether an in-band IP address is set from the console terminal.
- If the switch receives a BootP reply that contains an in-band IP address, the switch uses this new in-band IP address.
- If the switch does not receive a BootP reply, the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

SNMP Configuration

The SNMP Configuration screen (Figure 3-4) allows you to set or modify the SNMP configuration parameters.

Choose SNMP Configuration (or press m) from the main menu to open the 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.
```

Figure 3-4. SNMP Configuration Screen

Table 3-3 describes the SNMP Configuration screen fields.

Table 3-3. SNMP Configuration Screen Fields

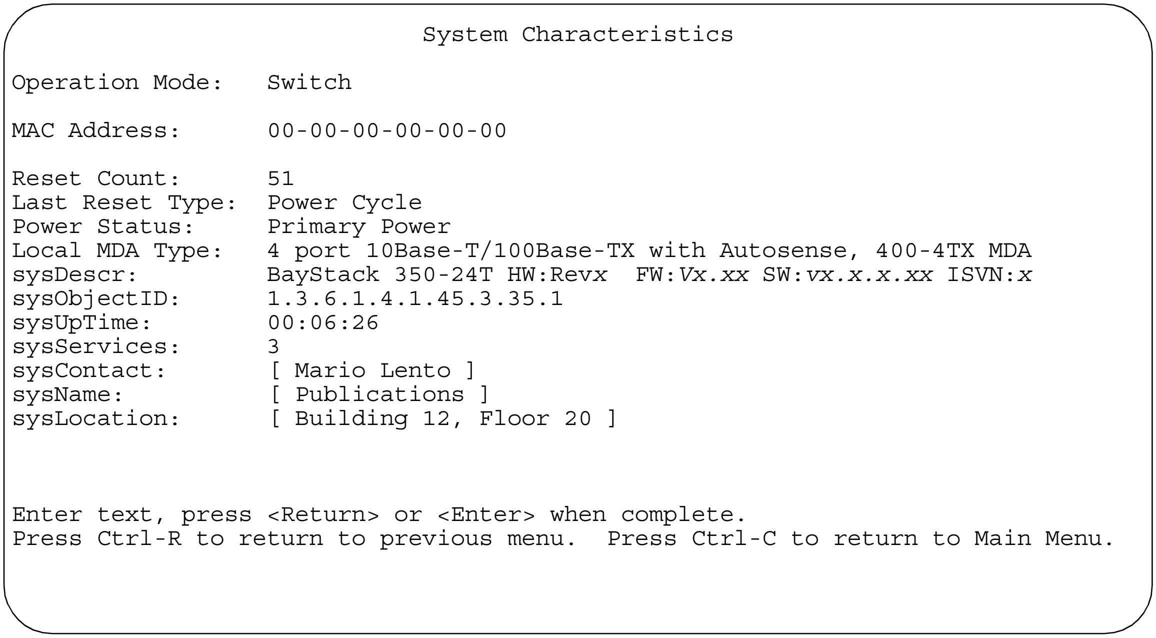
Field	Description	
Read-Only Community String	The community string used for in-band read-only SNMP operations.	
	Default	public
	Range	Any ASCII string of up to 32 printable characters
Read-Write Community String	The community string used for in-band read-write SNMP operations.	
	Default	private
	Range	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	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	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	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	Enabled
	Range	Enabled, 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 Valid or 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. When a Trap IP Address is entered from the console, the row status is always set to Valid.

System Characteristics

The System Characteristics screen (Figure 3-5) allows you to view system characteristics. The screen contains three user-configurable fields: sysContact, sysName, and sysLocation.

Choose System Characteristics (or press s) from the main menu to open the System Characteristics screen.



```
                             System Characteristics

Operation Mode:   Switch

MAC Address:      00-00-00-00-00-00

Reset Count:      51
Last Reset Type:  Power Cycle
Power Status:     Primary Power
Local MDA Type:   4 port 10Base-T/100Base-TX with Autosense, 400-4TX MDA
sysDescr:         BayStack 350-24T HW:Revx  FW:Vx.xx SW:vx.x.x.xx ISVN:x
sysObjectID:      1.3.6.1.4.1.45.3.35.1
sysUpTime:        00:06:26
sysServices:      3
sysContact:       [ Mario Lento ]
sysName:          [ Publications ]
sysLocation:      [ Building 12, Floor 20 ]



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

Figure 3-5. System Characteristics Screen

Table 3-4 describes the System Characteristics screen fields.

Table 3-4. System Characteristics Screen Fields

Field	Description
Operation Mode	Read-only field that indicates the operating mode of the switch.
MAC Address	The MAC address of the BayStack 350 switch.

(continued)

Table 3-4. System Characteristics Screen Fields *(continued)*

Field	Description	
Reset Count	A read-only field that indicates the number of resets since the operational firmware was first loaded on the switch.	
	Default	1
	Range	0 to 2^{32} -1
Last Reset Type	A read-only field that indicates the last type of reset.	
	Default	Power Cycle
	Range	Power Cycle, Software Download, Management Reset, Management Factory Reset
Power Status	A read-only field that indicates the current power source.	
	Default	Primary Power
Local MDA Type	A read-only field that indicates the MDA type that is configured in this switch.	
sysDescr	A read-only field that indicates your switch's model type, hardware version, firmware version, software version, and the ISVN. The Interoperability Software Version Number (ISVN) is used with stackable switches only.	
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. 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	Zero-length string
	Range	Any ASCII string of up to 56 printable characters[1]
sysName	A name that uniquely identifies the switch.	
	Default	Zero-length string
	Range	Any ASCII string of up to 56 printable characters[1]
sysLocation	The physical location of the switch.	
	Default	Zero-length string
	Range	Any ASCII string of up to 56 printable characters[1]

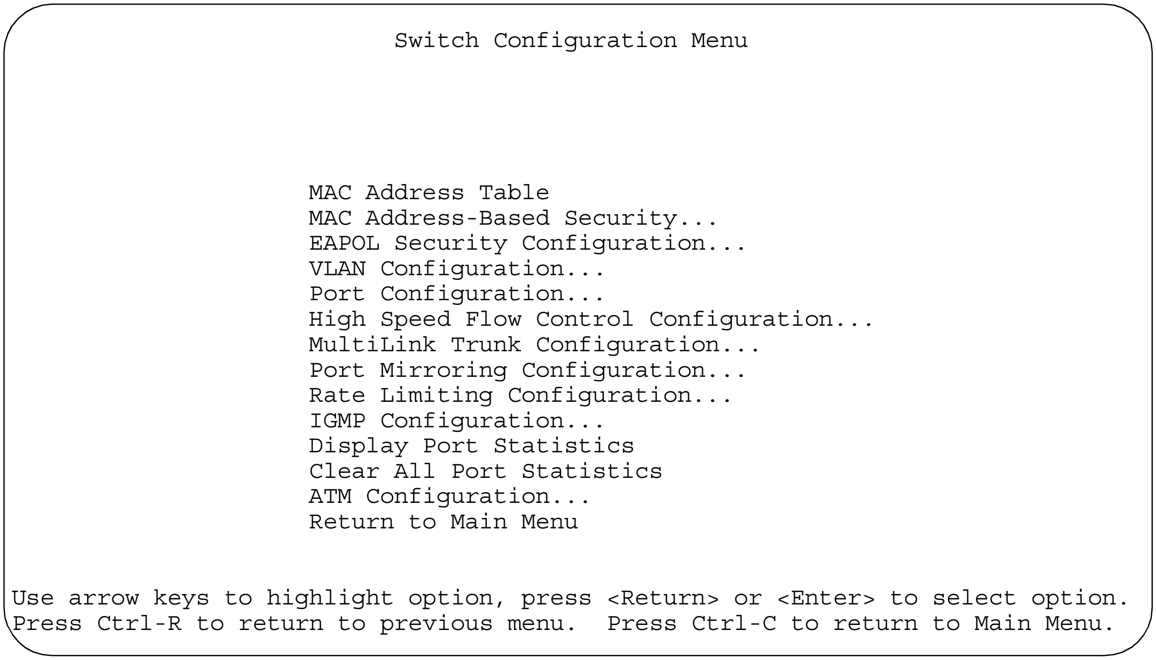
[1] Although this field can be set to up to 255 characters from a Network Management Station (NMS), only 56 characters are displayed on the console terminal.

Switch Configuration

The Switch Configuration Menu (Figure 3-6) allows you to set or modify your switch configuration.

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

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



```
                           Switch Configuration Menu




                     MAC Address Table
                     MAC Address-Based Security...
                     EAPOL Security Configuration...
                     VLAN Configuration...
                     Port Configuration...
                     High Speed Flow Control Configuration...
                     MultiLink Trunk Configuration...
                     Port Mirroring Configuration...
                     Rate Limiting Configuration...
                     IGMP Configuration...
                     Display Port Statistics
                     Clear All Port Statistics
                     ATM Configuration...
                     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.
```

Figure 3-6. Switch Configuration Menu Screen

Table 3-5 describes the Switch Configuration Menu options.

Table 3-5. Switch Configuration Menu Screen Options

Option	Description
MAC Address Table	Displays the MAC Address Table screen (see "MAC Address Table" on page 3-20). 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-Based Security...	Displays the MAC Address Security Configuration Menu (see "MAC Address-Based Security" on page 3-22). This menu provides the following options: MAC Address Security Configuration, MAC Address Security Port Configuration, MAC Address Security Port Lists, and MAC Address Security Table. This menu allows you to set up your MAC address-based security for your switch.
EAPOL Security Configuration...	Displays the EAPOL Security Configuration screen (see "EAPOL Security Configuration" on page 3-37). This screen allows you to configure your switch for EAPOL security.
VLAN Configuration...	Displays the VLAN Configuration Menu (see "VLAN Configuration Menu" on page 3-41). This menu provides the following options: VLAN Configuration, VLAN Port Configuration, VLAN Display by Port, and Traffic Class Configuration. This menu allows you to create and modify VLANs.
Port Configuration...	Displays the Port Configuration screen (see "Port Configuration" on page 3-56). This screen allows you to configure a specific switch port or all switch ports.
High Speed Flow Control Configuration...	This menu selection appears only when an optional gigabit MDA is installed in the Uplink Module slot. When the gigabit MDA is installed, selecting this option displays the High Speed Flow Control Configuration screen (see "High Speed Flow Control Configuration" on page 3-58).
MultiLink Trunk Configuration...	Displays the MultiLink Trunk Configuration Menu (see "MultiLink Trunk Configuration" on page 3-61). This menu provides the following options: MultiLink Trunk Configuration and MultiLink Trunk Utilization. This menu allows you to create and modify trunks, and to monitor the bandwidth utilization of configured trunks.
Port Mirroring Configuration...	Displays the Port Mirroring Configuration screen (see "Port Mirroring Configuration" on page 3-67). This screen allows you to designate a single switch port as a traffic monitor for up to two specified ports or addresses.

(continued)

Table 3-5. Switch Configuration Menu Screen Options *(continued)*

Option	Description
Rate Limiting Configuration...	Displays the Rate Limiting Configuration screen (see "Rate Limiting Configuration" on page 3-71). This screen allows you to limit the forwarding rate of broadcast and IP multicast packets.
IGMP Configuration...	Displays the IGMP Configuration Menu (see "IGMP Configuration Menu" on page 3-74). This screen allows you to optimize IP multicast traffic by setting up IGMP port memberships that filter IP multicast on a per port basis (see "IGMP Snooping" on page 1-51 for more information about this feature).
Display Port Statistics	Displays the Port Statistics screen (see "Port Statistics" on page 3-81). This screen allows you to view detailed information about any switch port.
Clear All Port Statistics	Allows you to clear all port statistics for all switch ports. This option is followed by a screen prompt that precedes the action. Enter Yes to clear all port statistics; enter No to abort the option.
ATM Configuration...	Displays the ATM Configuration Menu (see "ATM Configuration Menu" on page 3-85). This menu allows you to select the appropriate screens to configure or upgrade your ATM MDA.
Return to Main Menu	Exits the Switch Configuration Menu and displays the main menu.

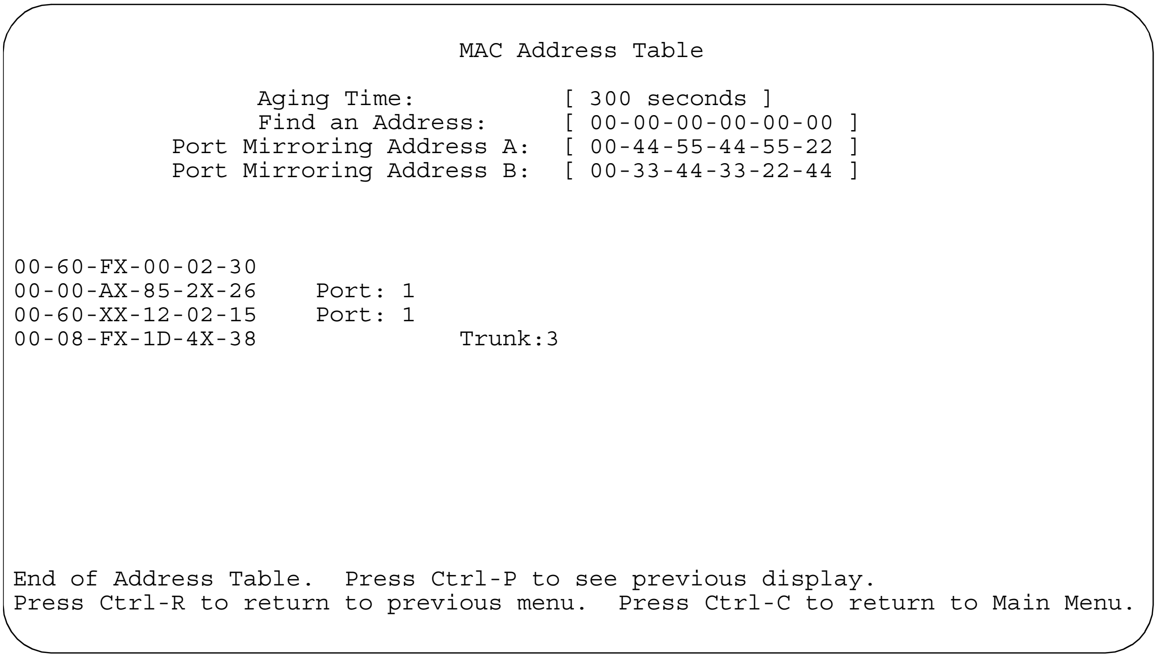
MAC Address Table

The MAC Address Table screen (Figure 3-7) allows you to view learned MAC addresses or to search for a specific MAC address.

The MAC Address 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" on page 3-67).

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

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



```
                               MAC Address Table

                 Aging Time:          [ 300 seconds ]
                 Find an Address:     [ 00-00-00-00-00-00 ]
           Port Mirroring Address A:  [ 00-44-55-44-55-22 ]
           Port Mirroring Address B:  [ 00-33-44-33-22-44 ]



00-60-FX-00-02-30
00-00-AX-85-2X-26    Port: 1
00-60-XX-12-02-15    Port: 1
00-08-FX-1D-4X-38              Trunk:3









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.
```

Figure 3-7. MAC Address Table Screen

Table 3-6 describes the MAC Address Table screen fields.

Table 3-6. 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	300 seconds
	Range	10 to 1,000,000 seconds
Find an Address	Allows the user to search for a specific MAC address.	
	Default	00-00-00-00-00-00 (no MAC address assigned)
	Range	00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF

(continued)

Table 3-6. MAC Address Table Screen Fields *(continued)*

Field	Description
Port Mirroring Address A	Appears only when you select any of the five *address-based* monitoring modes from the Port Mirroring Configuration screen. When you enter a MAC address in this field, it is also configured into the Port Mirroring Configuration screen. Conversely, when you enter the MAC address from the Port Mirroring Configuration screen, it also appears in this screen. See "Port Mirroring Configuration" on page 3-67 for more information. Default 00-00-00-00-00-00 (no MAC address assigned) Range 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF
Port Mirroring Address B	Appears only when you select any of the two *address-based* monitoring modes that use Address B from the Port Mirroring Configuration screen. When you enter a MAC address in this field, it is also configured into the Port Mirroring Configuration screen. Conversely, when you enter the MAC address from the Port Mirroring Configuration screen, it also appears in this screen. See "Port Mirroring Configuration" on page 3-67 for more information. Default 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-Based Security

The MAC Address Security Configuration Menu (Figure 3-8) allows you to choose the appropriate screen to specify a range of system responses to unauthorized network access to your switch. The system response can range from sending a trap to disabling the port. The network access control is based on the MAC addresses of the authorized stations.

You can specify a list of up to 448 MAC addresses that are authorized to access the switch. You can also specify the ports that each MAC address is allowed to access.

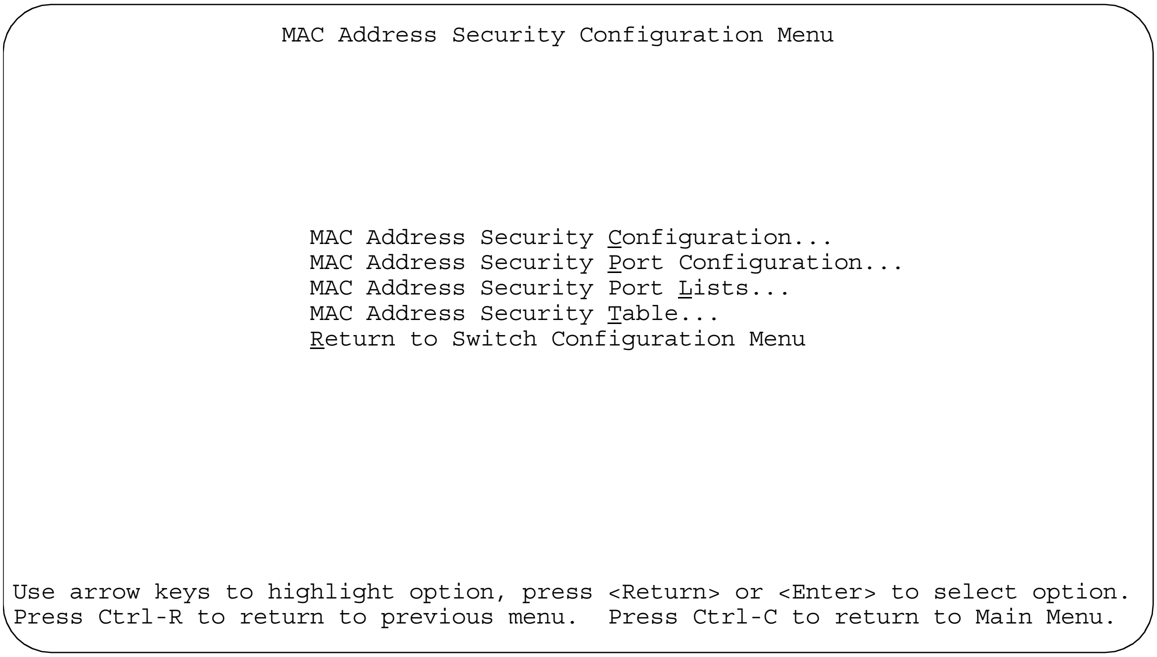
The options for allowed port access include: NONE, ALL, and single or multiple ports that are specified in a list, for example, 1/1-4, 2/6, 3/9, etc. (see "Accelerator Keys for Repetitive Tasks" on page 3-32).

When the switch software detects a security violation, you can set the system to respond in any of the following ways:

- Send a trap
- Turn on destination address (DA) filtering
- Disable the specific port

You can also combine any of the three preceding options.

Choose MAC Address-Based Security (or press s) from the Switch Configuration Menu to display the MAC Address Security Configuration Menu.



```
                        MAC Address Security Configuration Menu







                          MAC Address Security Configuration...
                          MAC Address Security Port Configuration...
                          MAC Address Security Port Lists...
                          MAC Address Security Table...
                          Return to Switch Configuration Menu








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

Figure 3-8. MAC Address Security Configuration Menu

Table 3-7 describes the MAC Address Security Configuration Menu options.

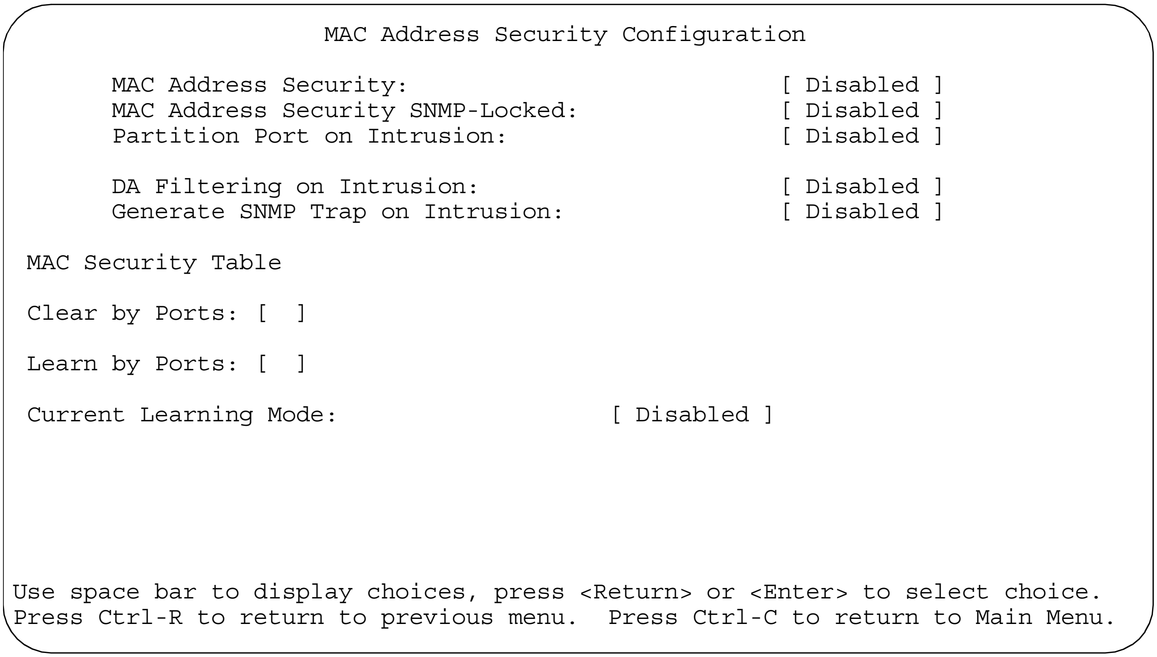
Table 3-7. MAC Address Security Configuration Menu Options

Option	Description
MAC Address Security Configuration...	Displays the MAC Address Security Configuration screen (see "MAC Address Security Configuration" on page 3-24). 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" on page 3-28). This screen allows you to enable or disable MAC Security for each port.
MAC Address Security Port Lists...	Displays the MAC Address Security Port Lists screen (see "MAC Address Security Port Lists" on page 3-30). This screen allows you to create port lists that can be used as an *allowed source port list* for a MAC address in the MAC Address Security Table screen.
MAC Address Security Table...	Displays the MAC Address Security Table screen (see "MAC Address Security Port Configuration" on page 3-28). 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 and displays the Switch Configuration Menu.

MAC Address Security Configuration

The MAC Address Security Configuration screen (Figure 3-9) allows you to enable (or disable) the MAC Address Security feature and to specify the appropriate system response to any unauthorized network access to your switch.

Choose MAC Address Security Configuration (or press c) from the MAC Address Security Configuration Menu to display the MAC Address Security Configuration screen.



```
                      MAC Address Security Configuration

       MAC Address Security:                             [ Disabled ]
       MAC Address Security SNMP-Locked:                 [ Disabled ]
       Partition Port on Intrusion:                      [ Disabled ]

       DA Filtering on Intrusion:                        [ Disabled ]
       Generate SNMP Trap on Intrusion:                  [ Disabled ]

 MAC Security Table

 Clear by Ports: [  ]

 Learn by Ports: [  ]

 Current Learning Mode:                       [ Disabled ]





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

Figure 3-9. MAC Address Security Configuration Screen

Table 3-8 describes the MAC Address Security Configuration screen fields.

Table 3-8. MAC Address Security Configuration Screen Fields

Field	Description
MAC Address Security	When set to Enabled, the software checks source MAC addresses of packets that arrive on secure ports against MAC addresses listed in the MAC Address Security Table for allowed membership (see "MAC Address Security Port Configuration" on page 3-28). If the software detects any source MAC address that is not an allowed member, a MAC intrusion event is registered. 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
Partition Port on Intrusion	This field value determines how the switch reacts to an intrusion event. When an intrusion event is detected (see MAC Address Security field description) the specified port is set to Disabled (partitioned from other switch ports). When this field is set to: • Disabled -- the port remains Enabled even if an intrusion event is detected. • Enabled -- the port becomes Disabled, and then automatically resets to Enabled depending on the value set in the Partition Time field (see Partition Time field description). • Forever -- the port becomes Disabled, and remains Disabled (partitioned). The Partition Time field cannot be used to automatically reset the port to Enabled if you set this field to Forever. You can manually set the port's status field to Enabled using the Port Configuration screen (see your switch's *User Guide* for more information). Default Disabled Range Disabled, Forever, Enabled
Partition Time	This field appears only if the Partition Port on Intrusion field is set to Enabled (see Partition Port on Intrusion Detected field). This field value determines the length of time a partitioned port remains Disabled. This field is not operational when the Partition Port on Intrusion field is set to Forever. Default 1 second Range 0-65536 seconds (the value 0 indicates forever)

(continued)

Table 3-8. MAC Address Security Configuration Screen Fields *(continued)*

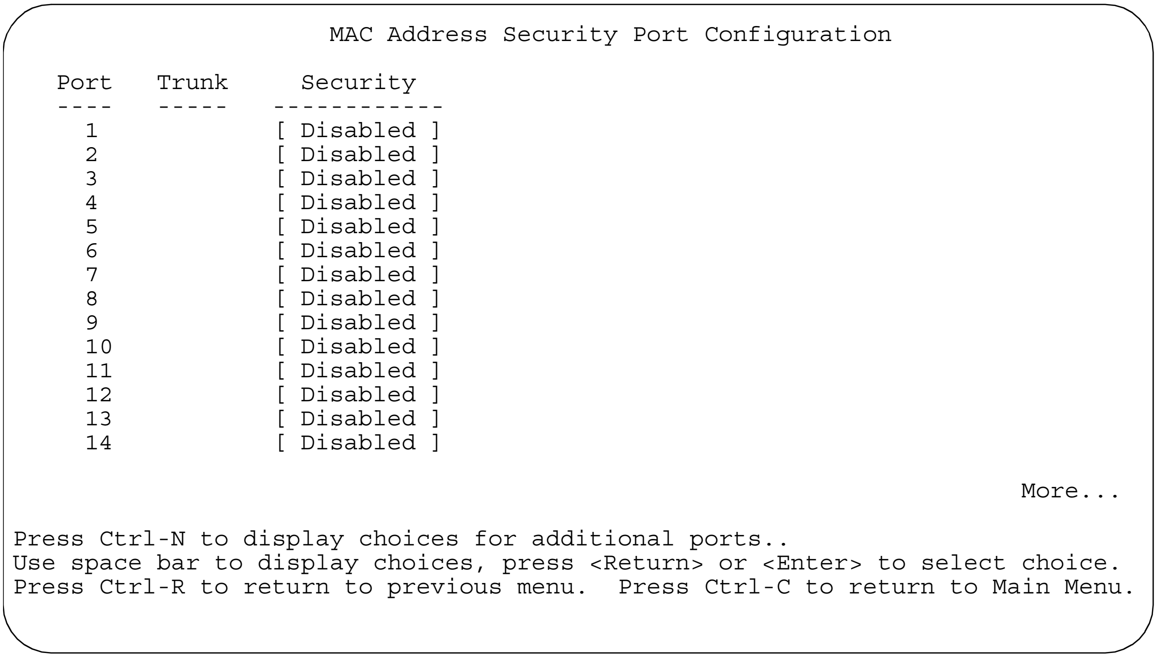
Field	Description
DA Filtering on Intrusion	When set to Enabled, this field isolates the intruding node by filtering (discarding) packets sent to that MAC address. Default Disabled Range Disabled, Enabled
Generate SNMP Trap on Intrusion	When set to Enabled and a MAC intrusion event is detected, the software issues an SNMP trap message to all registered SNMP trap addresses. Default Disabled Range Disabled, Enabled
Clear by Ports	This field clears the specified port (or ports) that are listed in the Allowed Source field of the MAC Address Security Table screen (see "MAC Address Security Table" on page 3-34). 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 clear the Allowed Source field (leaving a blank field) for any entry, the associated MAC address for that entry is also cleared. This field also clears the associated Port List field in the MAC Address Security Port Lists screen (Figure 3-13). Default NONE Range NONE, ALL, a port number list (for example, 1-4,6,ALL)
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 (see next field description) is set to Enabled. You cannot include any of the ports that are enabled for MAC address security (see "MAC Address Security Port Configuration" on page 3-28). Default NONE Range NONE, ALL, a port number list (for example, 1-4,6,ALL)
Current Learning Mode	Indicates the current learning mode for the switch ports. When this field is set to Enabled, 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). Default Disabled Range Disabled, Enabled

MAC Address Security Port Configuration

The MAC Address Security Port Configuration screens (Figures 3-10 and 3-11) allow you to enable or disable the MAC address security for each port.

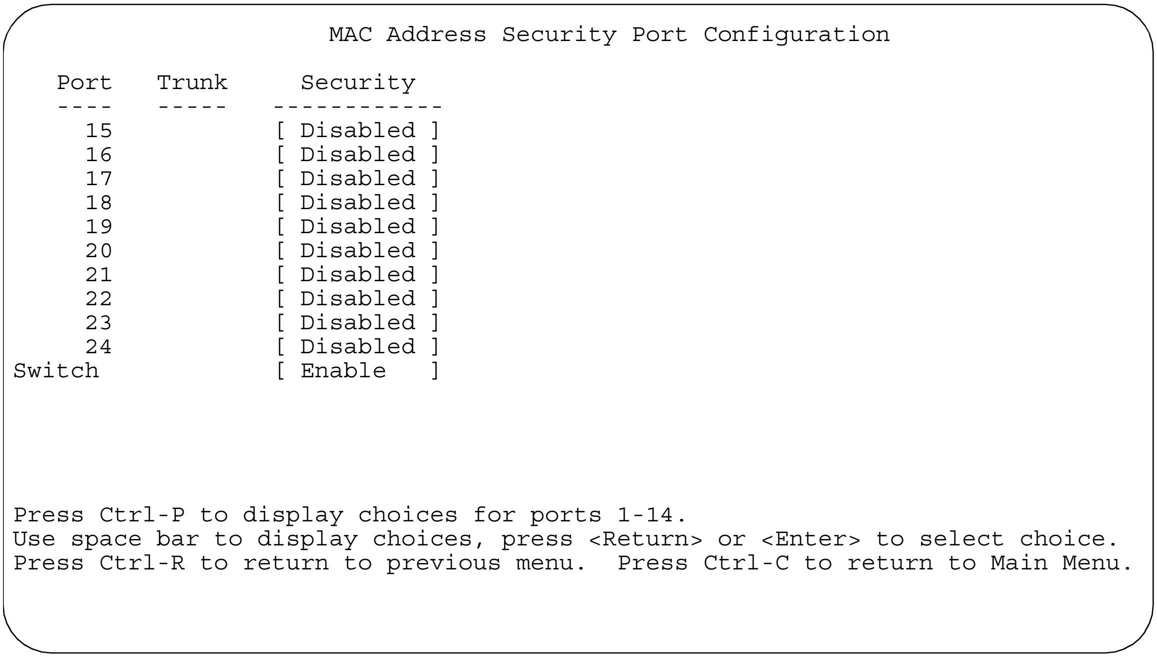
Note: You cannot enable MAC address security on a port that is currently configured for EAPOL-based security.

Choose MAC Address Security Port Configuration (or press p) from the MAC Address Security Configuration Menu to display the MAC Address Security Port Configuration screen.



```
                      MAC Address 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 3-10. MAC Address Security Port Configuration (Screen 1 of 2)



```
                                 MAC Address 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.
```

Figure 3-11. MAC Address Security Port Configuration (Screen 2 of 2)

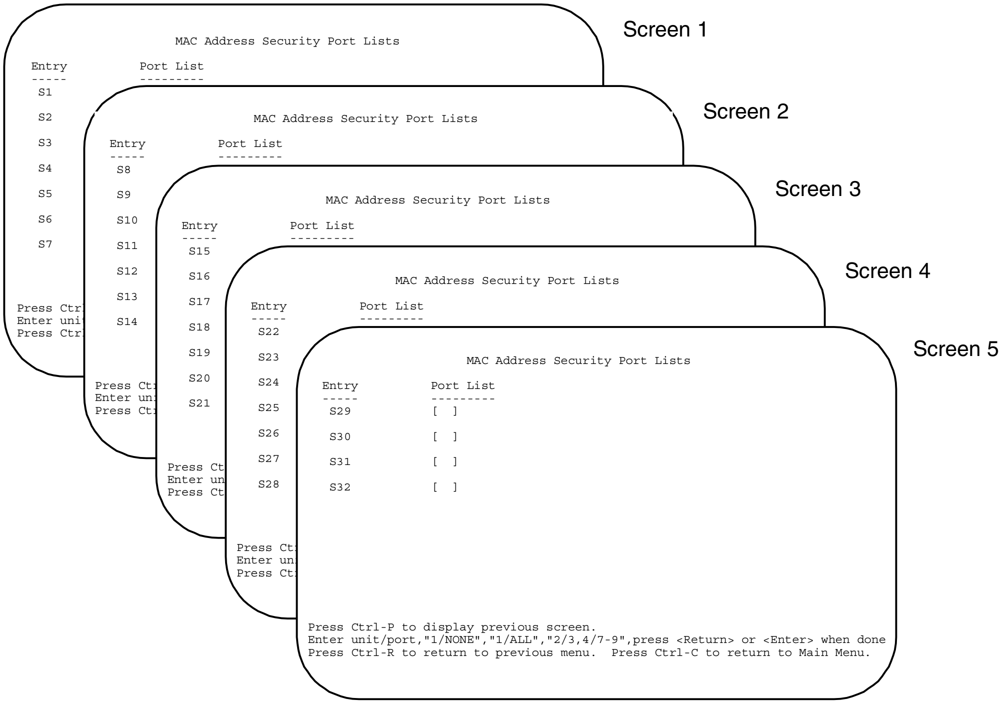
Table 3-9 describes the MAC Address Security Port Configuration screen fields.

Table 3-9. MAC Address Security 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 value that you set in the *Switch* row affects all switch ports.
Trunk	The read-only data displayed in this column indicates the MultiLink Trunks that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen.
Security	Allows you to enable or disable the security for the specified port. **Note:** If an (optional) BayStack 450-2M3/2S3 MDA is installed in your switch, the Security field value you set for a single LEC VPort applies automatically to the three remaining LEC VPorts. Default Disabled Range Disabled, Enabled

MAC Address Security Port Lists

The MAC Address Security Port Lists screens allow you to create port lists that can be used as *allowed source port lists* for a specified MAC address in the MAC Address Security Table screen. You can create as many as 32 port lists, using up to five MAC Address Security Port Lists screens (see Figure 3-12).



```
               MAC Address Security Port Lists

Entry          Port List
-----          ---------
 S1
 S2
 S3
 S4
 S5
 S6
 S7

Press Ctr
Enter uni
Press Ctr
```

```
               MAC Address Security Port Lists

Entry          Port List
-----          ---------
 S8
 S9
 S10
 S11
 S12
 S13
 S14

Press Ct
Enter un
Press Ct
```

```
               MAC Address Security Port Lists

Entry          Port List
-----          ---------
 S15
 S16
 S17
 S18
 S19
 S20
 S21

Press Ct
Enter un
Press Ct
```

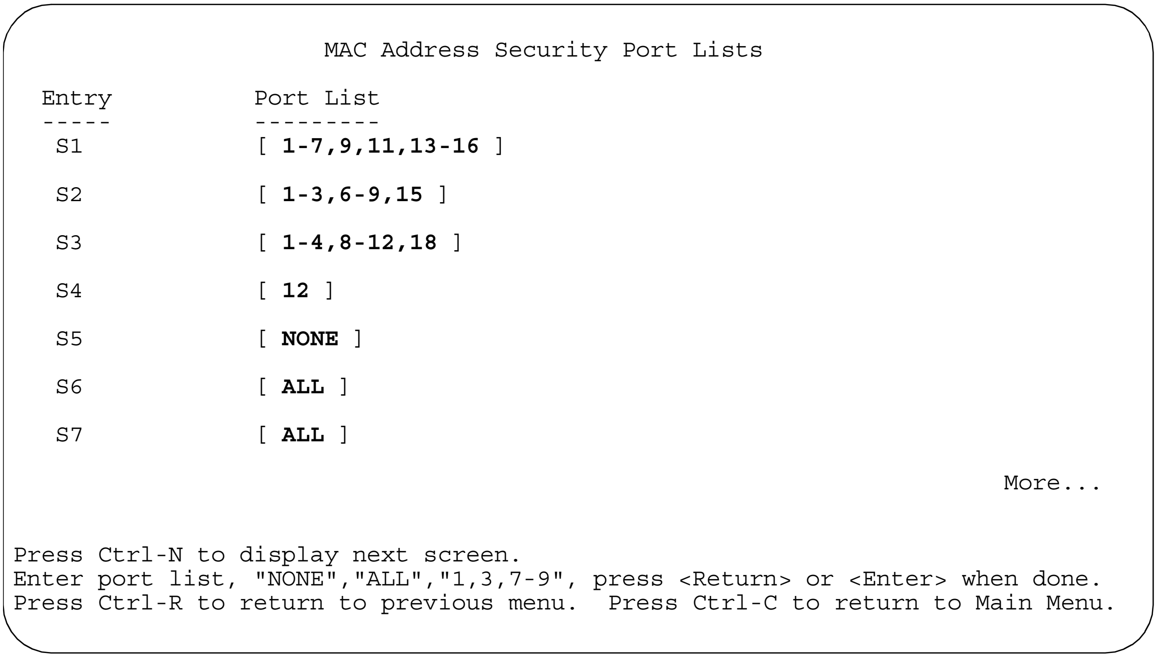
```
               MAC Address Security Port Lists

Entry          Port List
-----          ---------
 S22
 S23
 S24
 S25
 S26
 S27
 S28

Press Ct
Enter un
Press Ct
```

```
               MAC Address Security Port Lists

Entry          Port List
-----          ---------
 S29           [  ]
 S30           [  ]
 S31           [  ]
 S32           [  ]

Press Ctrl-P to display previous screen.
Enter unit/port,"1/NONE","1/ALL","2/3,4/7-9",press <Return> or <Enter> when done
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Figure 3-12. MAC Address Security Port Lists Screens (5 Screens)

Choose MAC Address Security Port Lists (or press l) from the MAC Address Security Configuration Menu to display the MAC Address Security Port Lists screen (Figure 3-13).

Note: The following screen shows an example of typical user input in boldface type.



```
                         MAC Address Security Port Lists

  Entry              Port List
  -----              ---------
   S1                [ 1-7,9,11,13-16 ]

   S2                [ 1-3,6-9,15 ]

   S3                [ 1-4,8-12,18 ]

   S4                [ 12 ]

   S5                [ NONE ]

   S6                [ ALL ]

   S7                [ ALL ]
                                                                        More...


Press Ctrl-N to display next screen.
Enter port list, "NONE","ALL","1,3,7-9", press <Return> or <Enter> when done.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Figure 3-13. MAC Address Security Port Lists Screen

Table 3-10 describes the MAC Address Security Port Lists screen fields.

Table 3-10. MAC Address Security Port Lists Screen Fields

Field	Description
Entry	Indicates the port list number (S1 to S32) that corresponds to the values you set in the Port List field.
Port List	Allows you to create a port list that you can use as an “Allowed Source” in the MAC Address Security Table screen (see “Port List Syntax” on page 3-32).

Port List Syntax

When you enter a port list, you must specify either a port number list, NONE, or ALL.

Note: NONE and ALL must be entered in uppercase characters as shown in the screen prompt.

A port number list is composed of one or more list items, each of which can be a single number or a range of numbers (where the number represents one or more ports).

For example, 1-7,9,11,13-16 is a valid unit/port number list (see entry S1 in Figure 3-13 on page 3-31).

It represents the following port order:

Ports 1 to 7, port 9, port 11, and ports 13 to 16.

See "Accelerator Keys for Repetitive Tasks" following this section for more information about creating port lists.

Accelerator Keys for Repetitive Tasks

You can use certain keystrokes as "accelerator keys" to help speed up repetitive tasks. For example, suppose you want to modify the Port List field in the MAC Address Security Port List screen (Figure 3-13 on page 3-31). You can modify the port list in any of the following ways:

- Add a new port to an existing port number list
- Remove a port from an existing port number list
- Copy an existing field into an adjacent field

Adding a New Port to an Existing Port Number List:

In the example shown in Figure 3-13 on page 3-31, S3 shows the Port List field values as:

1-4,8-12,18

If you want to add another port (for example, port **14**) to the existing port number list, you could highlight the field and then type another port list, including the new port number: 1-4,8-12,**14,**18 [Enter].

This works but is quite time consuming.

Instead, you can highlight the field, and then enter **+14** [Enter]. The existing field keeps the previous list, and adds the new port number (14) between ports 8-12 and 18.

(If you had chosen to add port **13** to the existing port number list, the field accepts the new port 13 but shows the new port number list field as: 1-4,**8-13**,18.)

Removing a Port from an Existing Port Number List:

To remove a port from the port number list, use the minus sign (-) character instead of the plus sign (+) character as described above.

Copying an Existing Field into an Adjacent Field:

You can use the period (.) character to copy a previously entered field value into the field directly next to it. For example, to copy the Allowed Source S3 (shown in Figure 3-15 on page 3-35) into the next field (entry 6):

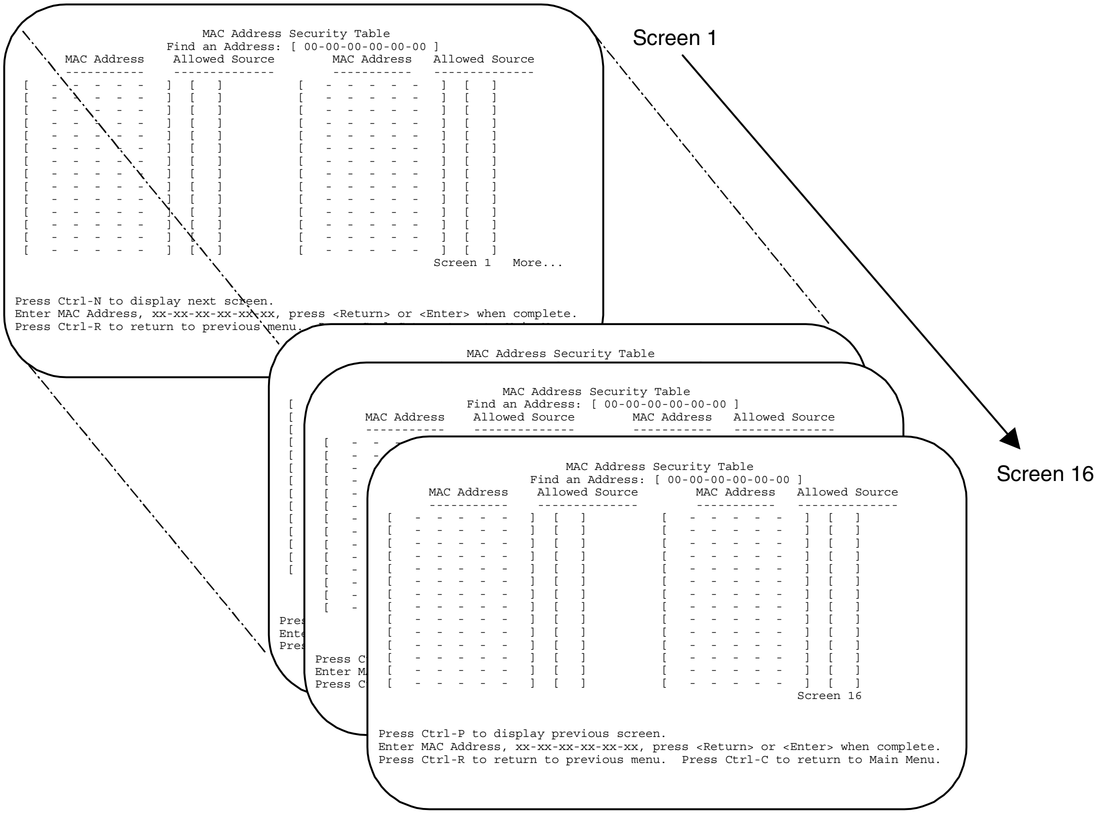
1. **Enter a MAC address into the next MAC Address field.**
2. **Highlight the (blank) Allowed Source field.**
3. **Enter the period character (.) and press [Enter].**

The port number list from the previous entry is copied into the new field.

MAC Address Security Table

The MAC Address Security Table screen allows you to specify the ports that each MAC address is allowed to access. You must also include the MAC addresses of any routers and switches that are connected to any secure ports.

There are 16 available MAC Address Security Table screens you can use to create as many as 448 MAC address entries. Twenty-eight MAC address entries are displayed on each screen (see Figure 3-14).



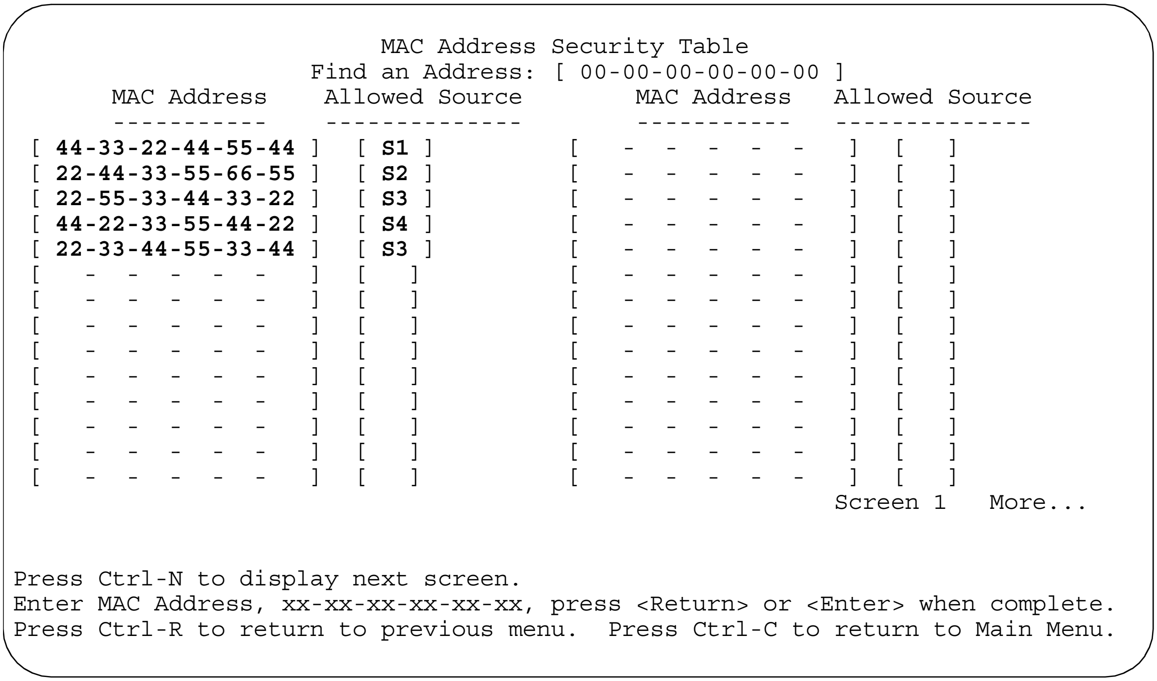
```
                    MAC Address Security Table
               Find an Address: [ 00-00-00-00-00-00 ]
    MAC Address    Allowed Source        MAC Address   Allowed Source
    -----------    --------------        -----------   --------------
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
                                                      Screen 1   More...


Press Ctrl-N to display next screen.
Enter MAC Address, xx-xx-xx-xx-xx-xx, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu.
```

```
                    MAC Address Security Table
               Find an Address: [ 00-00-00-00-00-00 ]
    MAC Address    Allowed Source        MAC Address   Allowed Source
    -----------    --------------        -----------   --------------
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
[   -  -  -  -  -  -   ]  [   ]         [   -  -  -  -  -  -   ]  [   ]
                                                           Screen 16


Press Ctrl-P to display previous screen.
Enter MAC Address, xx-xx-xx-xx-xx-xx, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Figure 3-14. MAC Address Security Table Screens (16 Screens)

Choose MAC Address Security Table (or press t) from the MAC Address Security Configuration Menu to display the MAC Address Security Table screen.

Note: The following screen shows an example of typical user input in boldface type.



```
                          MAC Address Security Table
                     Find an Address:  [ 00-00-00-00-00-00 ]
       MAC Address    Allowed Source         MAC Address   Allowed Source
       -----------    --------------         -----------   --------------
 [ 44-33-22-44-55-44 ]  [ S1 ]         [   -  -  -  -  -   ]  [   ]
 [ 22-44-33-55-66-55 ]  [ S2 ]         [   -  -  -  -  -   ]  [   ]
 [ 22-55-33-44-33-22 ]  [ S3 ]         [   -  -  -  -  -   ]  [   ]
 [ 44-22-33-55-44-22 ]  [ S4 ]         [   -  -  -  -  -   ]  [   ]
 [ 22-33-44-55-33-44 ]  [ S3 ]         [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]          [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]          [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]          [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]          [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]          [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]          [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]          [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]          [   -  -  -  -  -   ]  [   ]
 [   -  -  -  -  -   ]  [   ]          [   -  -  -  -  -   ]  [   ]
                                                          Screen 1   More...


Press Ctrl-N to display next screen.
Enter MAC Address, xx-xx-xx-xx-xx-xx, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Figure 3-15. MAC Address Security Table Screen

Table 3-11 describes the MAC Address Security Configuration screen fields.

Table 3-11. MAC Address Security Table Screen Fields

Field	Description	
Find an Address	Allows you to search for a specific MAC address that is used in any of the MAC Address Security Table screens.	
MAC Address	Allows you to specify up to 448 MAC addresses that are authorized to access the switch. You can specify the ports that each MAC address is allowed to access using the Allowed Source field (see next field description). The specified MAC address does not take effect until the Allowed Source field is set to some value (a single unit/port number or a port list value that you previously configured in the MAC Address Security Port Lists screen). You can clear an existing MAC address field by entering zero (0) in the field and pressing [Enter].	
	Default	- - - - - (no address assigned)
	Range	A range of 6 hexadecimal octets, separated by dashes (IP multicast[1] and broadcast addresses are not allowed).
Allowed Source	Allows you to specify the ports that each MAC address is allowed to access. The options for the Allowed Source field include a single port number or a port list value that you have previously configured in the MAC Address Security Port Lists screen.	
	Default	- (Blank field)
	Range	A single port or a port list value (for example, 3,6,8,S1,S5).

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

EAPOL Security Configuration

The EAPOL Security Configuration screen (Figure 3-16) allows you to selectively limit access to the switch based on an authentication mechanism that uses Extensible Authentication Protocol (EAP) to exchange authentication information between the switch and an authentication server. For more information about the EAPOL security feature and system requirements, see "EAPOL-Based Security" on page 1-15.

Note: Before you use the EAPOL Security Configuration screen, you must configure your Primary RADIUS Server and RADIUS Shared Secret (see "Console/Comm Port Configuration" on page 3-95).

You will also need to set up specific user accounts on your RADIUS server:

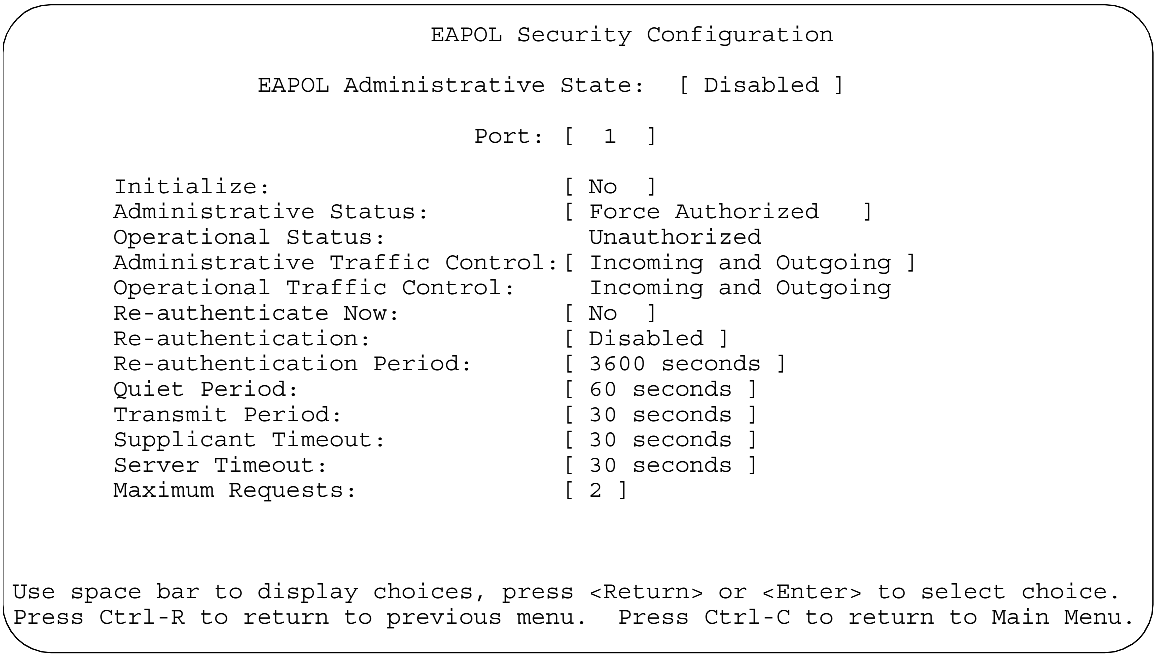
- User names
- Passwords
- VLAN IDs
- Port priority

You can set up these parameters directly on your RADIUS server, or by using the Optivity SecureLAN application.

For detailed instructions about configuring your RADIUS server, refer to your RADIUS server documentation; or if you are using the Optivity SecureLAN application, refer to *Managing Network Access with Optivity SecureLAN* (Part number 312688-A).

Note: Do not enable EAPOL security on the switch port that is connected to the RADIUS server.

Choose EAPOL Security Configuration (or press e) from the Switch Configuration Menu to display the EAPOL Security Configuration screen.



```
                          EAPOL Security Configuration

                EAPOL Administrative State:  [ Disabled ]

                             Port: [  1  ]

      Initialize:                  [ No  ]
      Administrative Status:       [ Force Authorized   ]
      Operational Status:            Unauthorized
      Administrative Traffic Control:[ Incoming and Outgoing ]
      Operational Traffic Control:   Incoming and Outgoing
      Re-authenticate Now:         [ No  ]
      Re-authentication:           [ Disabled ]
      Re-authentication Period:    [ 3600 seconds ]
      Quiet Period:                [ 60 seconds ]
      Transmit Period:             [ 30 seconds ]
      Supplicant Timeout:          [ 30 seconds ]
      Server Timeout:              [ 30 seconds ]
      Maximum Requests:            [ 2 ]


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

Figure 3-16. EAPOL Security Configuration Screen

Table 3-12 describes the EAPOL Security Configuration screen options.

Table 3-12. EAPOL Security Configuration Screen Options

Option	Description	
EAPOL Administrative State	Allows you to enable or disable EAPOL for you switch. When this field is set to Disabled (the default state), the Operational Status for all of the switch ports is set to Authorized (no security restriction).	
	Default	Disabled
	Range	Disabled, Enabled

(continued)

Table 3-12. EAPOL Security Configuration Screen Options *(continued)*

Option	Description	
Port	Allows you to select a port number to view or configure. To view or configure another port, type its port number and press [Enter], or press the spacebar to toggle the port numbers. If you set this field value to ALL, other screen field values you modify apply to *all* switch ports.	
	Default	1
	Range	1 to 28,ALL
Initialize	Allows you to activate EAPOL authentication for the specified port.	
	Default	No
	Range	No,Yes
Administrative Status	Allows you to set the EAPOL authorization status for the specified port. • Force Authorized means the specified port authorization status is *always* authorized. • Force Unauthorized means the specified port authorization status is *always* Unauthorized. • Auto means the specified port authorization status depends on the EAP authentication results.	
	Default	Force Authorized
	Range	Force Authorized,Force Unauthorized,Auto
Operational Status	A read-only field that shows the current authorization status for the specified port. This read-only field does not appear when the Port field is set to ALL.	
	Default	Authorized
	Range	Authorized,Unauthorized
Administrative Traffic Control	Allows you to choose whether EAPOL authentication is set for incoming and outgoing traffic or for incoming traffic only. For example, if you set the specified unit/port field value to Incoming and Outgoing, and the EAPOL authentication fails, then both incoming and outgoing traffic on the specified port is blocked.	
	Default	Incoming and Outgoing
	Range	Incoming and Outgoing,Incoming Only
Operational Traffic Control	A read-only field that indicates the current administrative traffic control configuration for the specified port (see preceding field description). This read-only field does not appear when the Port field value is set to ALL.	
	Default	Incoming and Outgoing
	Range	Incoming and Outgoing,Incoming Only

(continued)

Table 3-12. EAPOL Security Configuration Screen Options *(continued)*

Option	Description	
Re-authenticate Now	Allows you to activate EAPOL authentication for the specified unit/port immediately, without waiting for the Re-authentication Period to expire.	
	Default	No
	Range	No,Yes
Re-authentication	Allows you to repeat EAPOL authentication for the specified unit/port according to the time interval value configured in the Re-authentication Period field (see next field description).	
	Default	Enabled
	Range	Enabled,Disabled
Re-authentication Period	When the Re-authentication field value (see preceding field) is set to Enabled, this field allows you to specify the time period between successive EAPOL authentications for the specified unit/port.	
	Default	3600 seconds
	Range	1 to 604800 seconds
Quiet Period	Allows you to specify the time period between any single EAPOL authentication failure and the start of a new EAPOL authentication attempt.	
	Default	60 seconds
	Range	0 to 65535 seconds
Transmit Period	Allows you to specify how long the switch waits for the supplicant to respond to EAP Request/Identity packets.	
	Default	30 seconds
	Range	1 to 65535 seconds
Supplicant Timeout	Allows you to specify how long the switch waits for the supplicant to respond to all EAP packets, except EAP Request/Identity packets.	
	Default	30 seconds
	Range	1 to 65535 seconds
Server Timeout	Allows you to specify how long the switch waits for the RADIUS server to respond to all EAP packets.	
	Default	30 seconds
	Range	1 to 65535 seconds
Maximum Requests	Allows you to specify the number of times the switch attempts to resend EAP packets to a supplicant.	
	Default	2 attempts
	Range	1 to 10 attempts

VLAN Configuration Menu

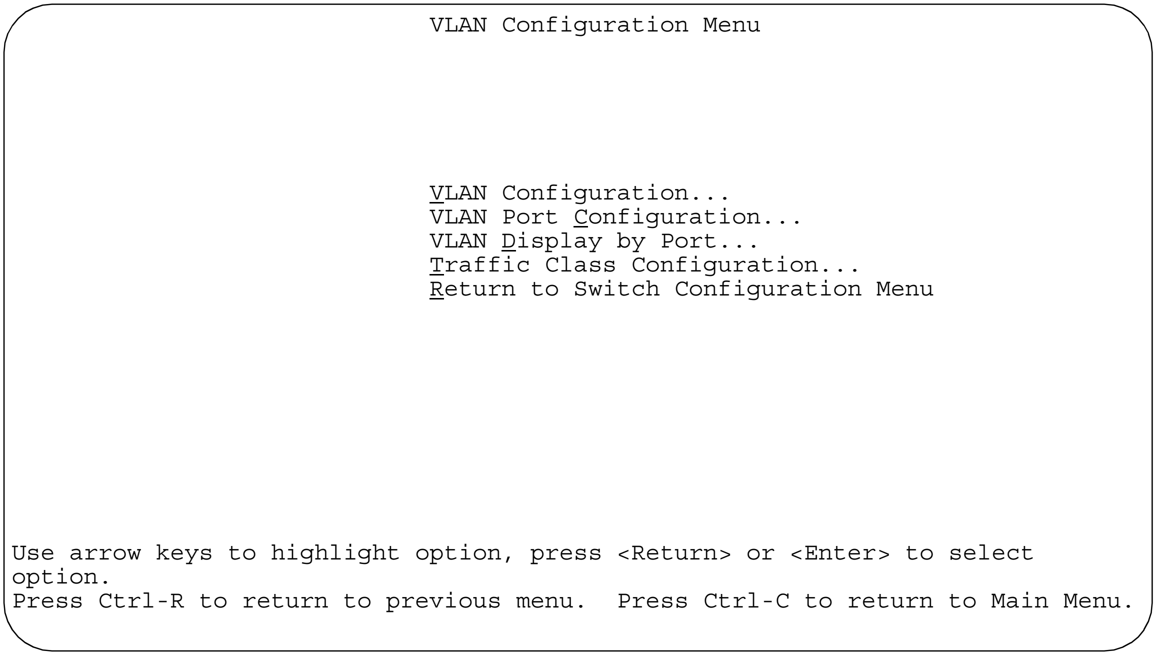
The VLAN Configuration Menu (Figure 3-17) allows you to select the appropriate screen to configure up to 64 VLANs (VLAN 1 is port-based, by default).

You can configure as many as 63 protocol-based VLANs, with up to 15 different protocols. The number of different protocols you can configure depends on the number of hexadecimal values (PID values) associated with the protocol type (some protocol types use more than one PID value, see Table 3-15 on page 3-47).

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.

See “IEEE 802.1Q VLAN Workgroups” on page 1-34 for detailed information about configuring VLANs.

Choose VLAN Configuration (or press v) from the Switch Configuration Menu to open the VLAN Configuration Menu.



```
                            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.
```

Figure 3-17. VLAN Configuration Menu Screen

Table 3-13 describes the VLAN Configuration Menu options.

Table 3-13. VLAN Configuration Menu Screen Options

Option	Description
VLAN Configuration...	Displays the VLAN Configuration screen (see "VLAN Configuration" on page 3-43). This screen allows you to set up VLAN workgroups.
VLAN Port Configuration...	Displays the VLAN Port Configuration screen (see "VLAN Port Configuration" on page 3-49). 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" on page 3-52).
Traffic Class Configuration...	Displays the Traffic Class Configuration screen (see "Traffic Class Configuration" on page 3-54).
Return to Switch Configuration Menu	Exits the VLAN Configuration Menu and displays the Switch Configuration Menu.

VLAN Configuration

The VLAN Configuration screen (Figure 3-18) allows you to assign *VLAN port memberships* to your switch ports. You can also create port-based VLANs and protocol-based VLANs:

- Port-based VLANs allow you to explicitly configure switch ports as VLAN port members.
- Protocol-based VLANs allow you to configure your switch ports as members of a broadcast domain, based on the protocol information within a packet.

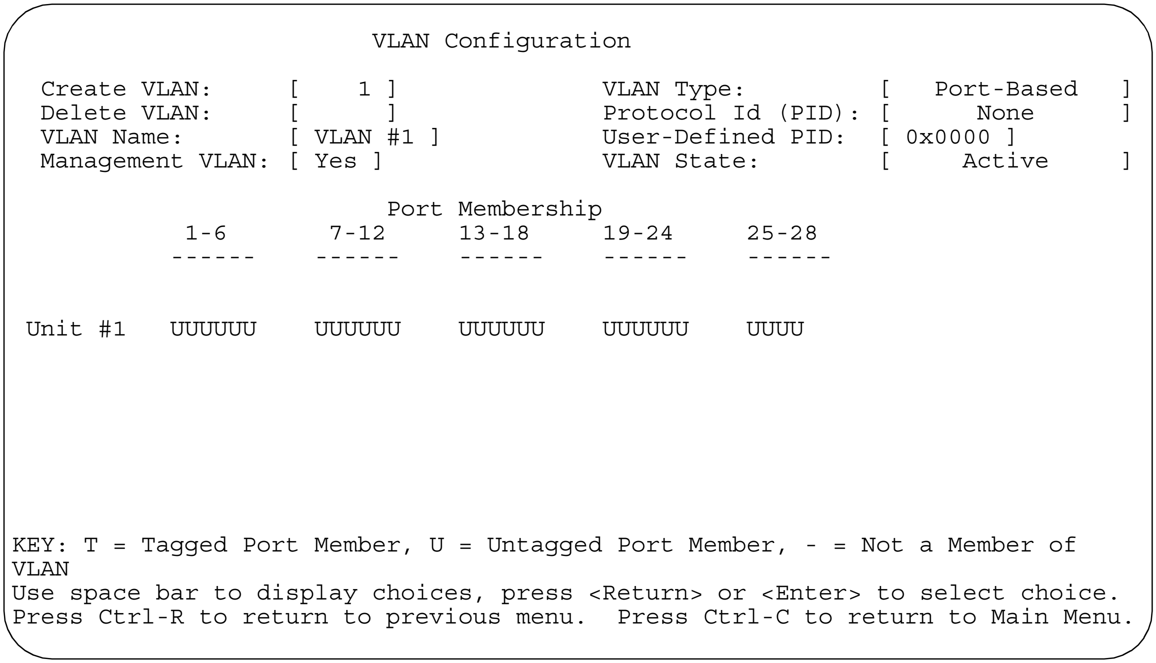
  Protocol-based VLANs can localize broadcast traffic and assure that only the protocol-based VLAN ports are flooded with the specified protocol-type packets.

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 assign VLAN port members attributes that allow the individual ports to operate in accordance with the IEEE 802.1Q tagging rules. You can define each of the VLAN port members as *tagged* or *untagged* (see “IEEE 802.1Q Tagging” on page 1-35 for a description of important terms used with 802.1Q VLANs).

You can also use this screen to create or delete specific VLANs, assign VLAN names, and assign any VLAN as the management VLAN.

Choose VLAN Configuration (or press v) from the VLAN Configuration Menu to open the VLAN Configuration screen.



```
                         VLAN Configuration

  Create VLAN:      [    1 ]              VLAN Type:          [   Port-Based   ]
  Delete VLAN:      [      ]              Protocol Id (PID):  [      None      ]
  VLAN Name:        [ VLAN #1 ]           User-Defined PID:   [ 0x0000 ]
  Management VLAN:  [ Yes ]               VLAN State:         [     Active     ]

                          Port Membership
           1-6       7-12     13-18     19-24     25-28
          ------    ------    ------    ------    ------


 Unit #1  UUUUUU    UUUUUU    UUUUUU    UUUUUU    UUUU







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.
```

Figure 3-18. VLAN Configuration Screen

Table 3-14 describes the VLAN Configuration screen fields.

Table 3-14. 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, and then press [Enter]. The Port Membership fields indicate the corresponding VLAN workgroup configuration, if configured, or all dashes (-), indicating no VLAN Members configured. Alternatively, you can use the spacebar to toggle through the various configured VLAN workgroups. You can create up to 64 different VLANs (including VLAN 1). Default 1 Range 2 to 4094

(continued)

Table 3-14. VLAN Configuration Screen Fields *(continued)*

Field	Description	
Delete VLAN	Allows you to delete a specified VLAN, except the assigned management VLAN (see Management VLAN field). Enter the number of the VLAN you want to delete, and then press [Enter], or use the spacebar to toggle through the selection until you reach the specific VLAN you want to delete, and then press [Enter]. The specified VLAN is deleted as soon as you press [Enter]. The software does not prompt you to confirm 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 1-34 for more information.	
	Default	blank field
	Range	2 to 4094
VLAN Name	Allows you to assign a name 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, and the VLAN Type field value must be Port-Based or Protocol-Based (with the Protocol Id (PID) field value set to IpEther2).	
	Default	Yes
	Range	Yes, No
VLAN Type	Allows you to select the type of VLAN (port-based or protocol-based) to create. To set this field, the VLAN State field value must be Inactive.	
	Default	Port-Based
	Range	Port-Based, Protocol-Based
Protocol Id (PID)	Allows you to set the protocol type of your protocol-based VLAN (to set this field, the VLAN State field value must be Inactive). You can choose from any of 15 predefined supported protocols (see “Predefined Protocol Identifier (PID) Description” on page 3-47), or you can create your own user-defined protocol-based VLAN (see the User-defined PID field description for more information).	
	Default	None
	Range	None, Ip Ether2, Ipx 802.3, Ipx 802.2, Ipx Snap, Ipx Ether2, AplTk Ether2Snap, Declat Ether2, DecOth Ether2, Sna 802.2, Sna Ether2, NetBios 802.2, Xns Ether2, Vines Ether2, Ipv6 Ether2, User-Defined, Rarp Ether2

(continued)

Table 3-14. VLAN Configuration Screen Fields *(continued)*

Field	Description	
User-Defined PID	Allows you to create your own user-defined protocol-based VLAN where you specify the Protocol Identifier (PID) for the VLAN. To set this field, the VLAN State field must be set to Inactive (some restrictions apply, see “User-Defined Protocol Identifier (PID) Description” on page 3-48).	
	Default	0x0000
	Range	Any 4-bit hexadecimal value (for example, 0xABCD)
VLAN State	Allows you to activate your newly created VLAN: • The following associated field values: VLAN Type, Protocol Id (PID), and 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 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 deleted also.	
	Default	Inactive
	Range	Inactive, Active
Port Membership	Allows you to assign VLAN port memberships to your switch ports. The ports can be configured in one or more VLANs. To set this field, you must set the VLAN State field value to Active. Certain restrictions apply for gigabit ports and when using the BayStack 410-24T switch ports as participants of protocol-based VLANs (see “Gigabit Ports and BayStack 410-24T Switch Ports Restriction” on page 3-49). This field depends on the Tagging field value in the VLAN Port Configuration screen (see the Tagging field description in Table 3-17 on page 3-50). For example: • When the Tagging field is set to *Untagged Access*, you can set the Port Membership field as an untagged port member (U) or as a non-VLAN port member (-). • When the Tagging field is set to *Tagged Trunk*, you can set the Port Membership field as a tagged port member (T) or as a non-VLAN port member (-). The Port Membership fields are displayed in six-port groups (for example, 1-6, 7-12, 13-18). The number of ports displayed depends on the switch model or type of optional MDA installed in the Uplink Module slot.	
	Default	U (All ports are assigned as untagged members of VLAN 1.)
	Range	U, T, and -

Predefined Protocol Identifier (PID) Description

Table 3-15 defines the standard protocol-based VLAN and PID types that the BayStack 350 switch supports:

Table 3-15. Prefined Protocol Identifier (PID)

PID Name	Encapsulation	PID Value (hex)	VLAN Type
Ip Ether2	Ethernet Type 2	0800, 0806	Standard IP on Ethernet Type 2 frames
Ipx 802.3	Ethernet 802.2	FF FF	Novell IPX on Ethernet 802.3 frames
Ipx 802.2	Ethernet 802.2	E0 E0	Novell IPX on Ethernet 802.2 frames
Ipx Snap	Ethernet Snap	8137, 8138	Novell IPX on Ethernet SNAP frames
Ipx Ether2	Ethernet Type 2	8137, 8138	Novell IPX on Ethernet Type 2 frames
AplTk Ether2Snap	Ethernet Type 2 or Ethernet Snap	809B, 80F3	AppleTalk on Ethernet Type 2 and Ethernet Snap frames
Declat Ether2	Ethernet Type 2	6004	DEC LAT protocol
DecOther Ether2	Ethernet Type 2	6000 - 6003, 6005 - 6009, 8038	Other DEC protocols
Sna 802.2	Ethernet 802.2	04 **, ** 04	IBM SNA on IEEE 802.2 frames
Sna Ether2	Ethernet Type 2	80D5	IBM SNA on Ethernet Type 2 frames
NetBios 802.2	Ethernet Type 2	F0 **, ** F0	NetBIOS Protocol
Xns Ether2	Ethernet Type 2	0600, 0807	Xerox XNS
Vines Ether2	Ethernet Type 2	0BAD	Banyan VINES
Ipv6 Ether2	Ethernet Type 2	86DD	IP version 6
User-Defined	Ethernet Type 2, Ethernet 802.2, or Ethernet Snap	User-defined 16-bit value	User-defined protocol-based VLAN (see "User-Defined Protocol Identifier (PID) Description" on page 3-48).
Rarp Ether2	Ethernet Type 2	8035	Reverse Address Resolution Protocol (RARP): RARP is a protocol used by some old diskless devices to obtain IP addresses by providing the MAC layer address. When you create a VLAN based on RARP, you can limit the RARP broadcasts to the ports that lead to the RARP server.

User-Defined Protocol Identifier (PID) Description

In addition to the standard *predefined* protocols, user-defined protocol-based VLANs are supported. For user-defined protocol-based VLANs, you specify the Protocol Identifier (PID) for the VLAN. Any frames that match the specified PID in any of the following ways are assigned to that user-defined VLAN:

- The ethertype for Ethernet Type 2 frames
- The PID in Ethernet SNAP frames
- The DSAP or SSAP value in Ethernet 802.2 frames

The following PIDs (see Table 3-16) are reserved and are not available for user-defined PIDs:

Table 3-16. Reserved PIDs

PID Value (hex)	Comments
04 **, ** 04	Sna 802.2
F0 **, ** F0	NetBios 802.2
AAAA	SNAP
0 - 05DC	Overlaps with 802.3 frame length
0600, 0807	Xns Ether2
0BAD	Vines Ether2
4242	IEEE 802.1D BPDUs
6000 - 6009, 8038	Dec
0800, 0806	Ip Ether2 (including Arp)
8035	Rarp Ether2
809B, 80F3	AplTk Ether2Snap
8100	IEEE 802.1Q for tagged frames
8137, 8138	Ipx
80D5	Sna Ether2
86DD	Ipv6 Ether2
8808	IEEE 802.3x pause frames
9000	Diagnostic loopback frame

Gigabit Ports and BayStack 410-24T Switch Ports Restriction

Gigabit ports and the BayStack 410-24T switch ports do not have the ability to assign incoming untagged frames to a protocol-based VLAN.

To allow Gigabit ports and BayStack 410-24T switch ports to participate in protocol-based VLANs, you must set the Tagging field value in the VLAN Port Configuration screen to Tagged Trunk.

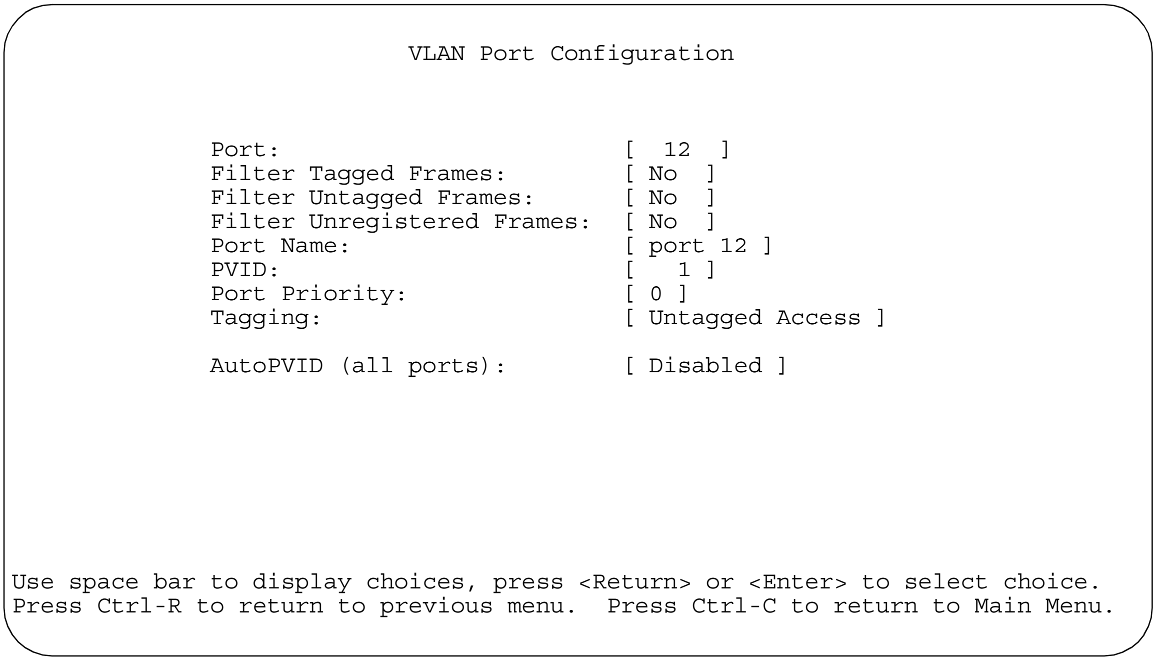
VLAN Port Configuration

The VLAN Port Configuration screen (Figure 3-19) 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 1-43 for more information about setting up VLAN broadcast domains).

You can configure specified switch ports to filter (discard) all received tagged frames, untagged frames, or unregistered frames (see “IEEE 802.1Q Tagging” on page 1-35).

You can also prioritize the order in which the switch forwards packets, on a per-port basis (see “Virtual Local Area Networks (VLANs)” on page 1-33).

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



```
                         VLAN Port Configuration



             Port:                         [  12  ]
             Filter Tagged Frames:         [ No   ]
             Filter Untagged Frames:       [ No   ]
             Filter Unregistered Frames:   [ No   ]
             Port Name:                    [ port 12 ]
             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 3-19. VLAN Port Configuration Screen

Table 3-17 describes the VLAN Port Configuration screen fields.

Table 3-17. 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 Tagged Frames	Allows you to set this port to filter (discard) all received tagged packets. Default No Range No, Yes
Filter Untagged Frames	Sets this port to filter (discard) all received untagged frames. **Restriction:** If this port is a gigabit port or a BayStack 410-24T switch port that is a protocol-based VLAN member, you cannot set this field value to No.

(continued)

Table 3-17. VLAN Port Configuration Screen Fields *(continued)*

Field	Description
	This restriction also applies if this port is a MultiLink Trunk member with a gigabit port or a BayStack 410-24T switch port that is a protocol-based VLAN member. Default No Range No, Yes
Filter Unregistered Frames	Sets this port to filter (discard) all received unregistered packets. 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 Unit *x*, Port *x* Range Any ASCII string of up to 16 printable characters
PVID	Associates the port (specified in the Port field) with a specific VLAN. For example, if you associate a specific port with a PVID of 3, all untagged frames received on the specified port are assigned to VLAN 3 (see also “AutoPVID (all ports)” field description, later in this table). Default 1 Range 1 to 4094
Port Priority	Prioritizes the order in which the switch forwards packets received on specified ports (see “IEEE 802.1p Prioritizing” on page 1-56). Default 0 Range 0 to 7
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. • Tagged Trunk: Any VLAN that this port is a member of will be 802.1Q tagged. The Port Membership field in the VLAN Configuration screen is dependent on the Tagging field value (see the Port Membership field description in Table 3-14 on page 3-44). **Restriction:** If this port is a gigabit port or a BayStack 410-24T switch port that is a protocol-based VLAN member, you cannot set this field value to Untagged Access.

(continued)

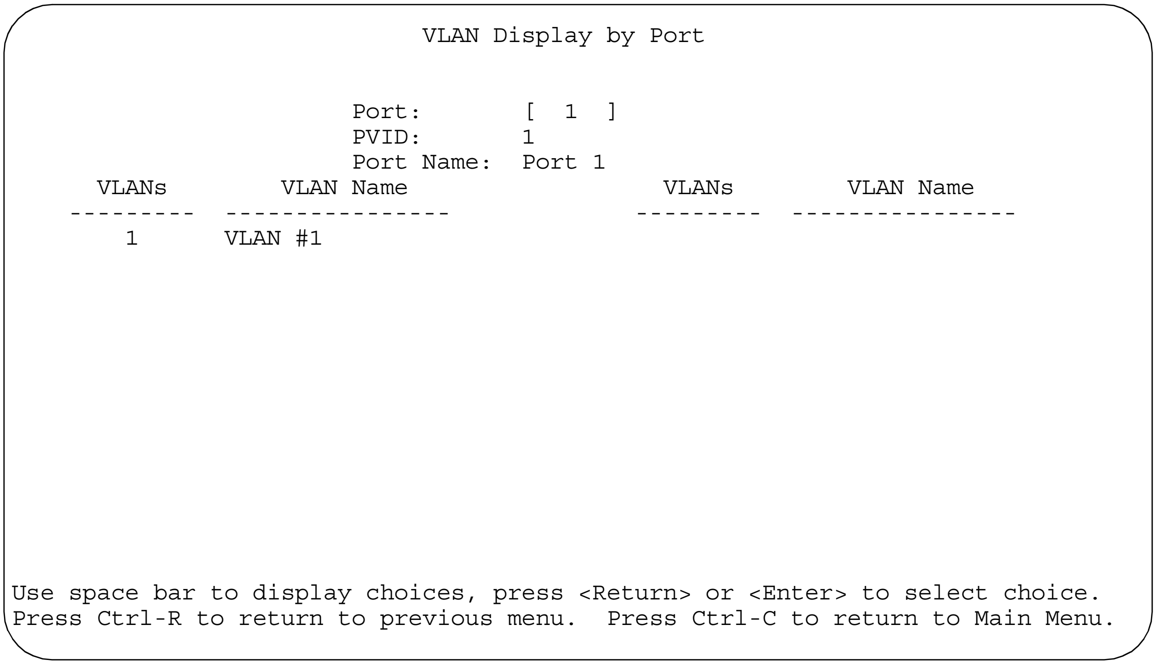
Table 3-17. VLAN Port Configuration Screen Fields *(continued)*

Field	Description
	This restriction also applies if this port is a MultiLink Trunk member with a gigabit port or a BayStack 410-24T switch port that is a protocol-based VLAN member. Default Untagged Access Range Untagged Access, Tagged Trunk
AutoPVID (all ports)	Enables or disables the AutoPVID feature. When you set this field to Enabled, the AutoPVID feature automatically assigns a PVID/VLAN association for any VLAN port membership you create thereafter (see "Shared Servers" on page 1-43). When you enable the AutoPVID feature, the feature is activated for all switch ports. **Note:** This feature is operational with untagged ports and port-based VLANs only. Default Disabled Range Disabled,Enabled

VLAN Display By Port

The VLAN Display by Port screen (Figure 3-18) 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 to open the 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.
```

Figure 3-20. VLAN Display by Port Screen

Table 3-18 describes the VLAN Display by Port screen fields.

Table 3-18. VLAN Display by Port Screen Fields

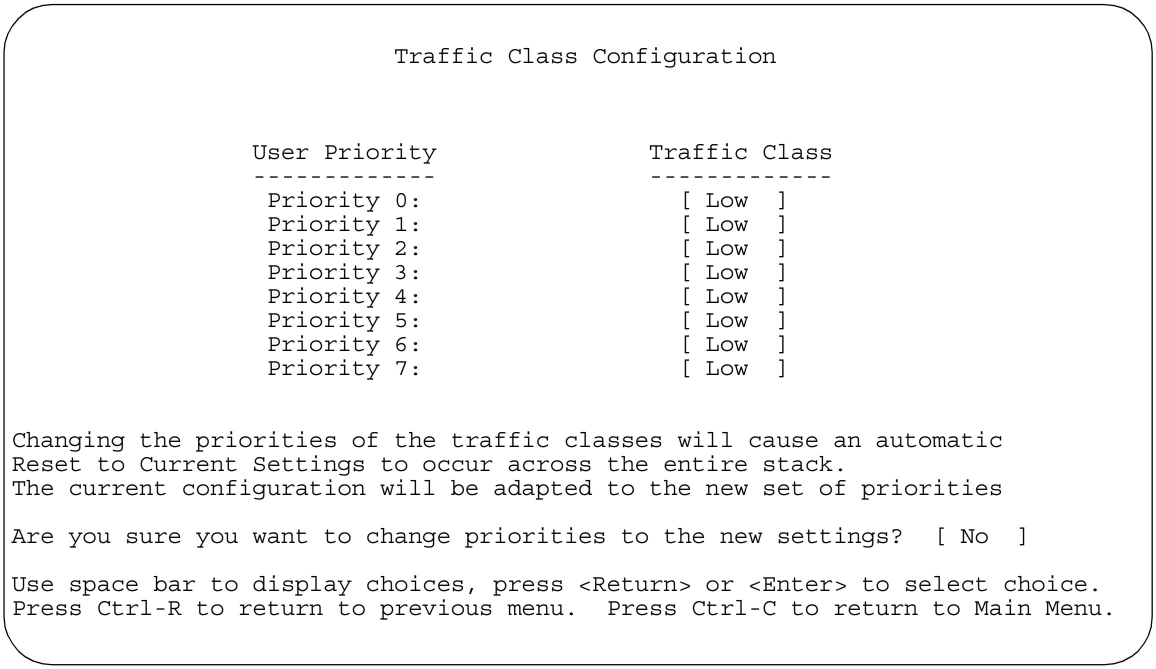
Field	Description
Port	Allows you to select the number of the port you want to view. To view another port, type its port number and press [Enter], or press the spacebar on your keyboard to toggle the port numbers.
PVID	Read-only field that indicates the PVID setting for the specified port.
Port Name	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.

Traffic Class Configuration

The Traffic Class Configuration screen (Figure 3-21) allows you to assign a Low or High traffic classification to any of eight (0 to 7) user_priority values assigned to a received frame on specified switch ports.

See “IEEE 802.1p Prioritizing” on page 1-56 for more information about this screen.

Choose Traffic Class Configuration (or press t) from the VLAN Configuration Menu to open the Traffic Class Configuration screen.



```
                         Traffic Class Configuration


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


Changing the priorities of the traffic classes will cause an automatic
Reset to Current Settings to occur across the entire stack.
The current configuration will be adapted to the new set of priorities

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.
```

Figure 3-21. Traffic Class Configuration Screen

Table 3-19 describes the Traffic Class Configuration screen fields.

Table 3-19. Traffic Class Configuration Screen Fields

Field	Description	
User Priority	Column header for the read-only fields that indicate the user priority values from 0 to 7. These values are derived from the 3-bit field in the header of 802.1Q tagged frames (see “IEEE 802.1Q Tagging” on page 1-35).	
Traffic Class	Column header for the eight user-configurable fields that correspond to the adjacent user priority levels.	
	Default	Low
	Range	Low, High

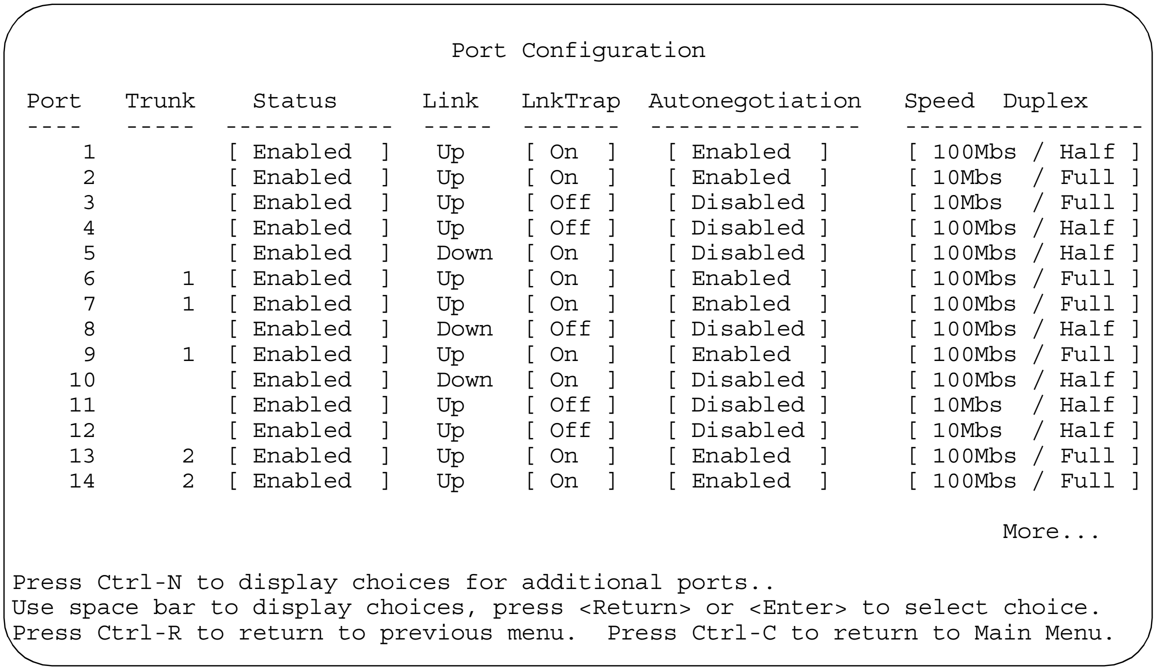
Port Configuration

The Port Configuration screen (Figures 3-22 and 3-23) allows you to configure a specific switch port or all switch ports. You can set the switch ports to autonegotiate for the highest available speed of the connected station, or you can set the speed for selected switch 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.

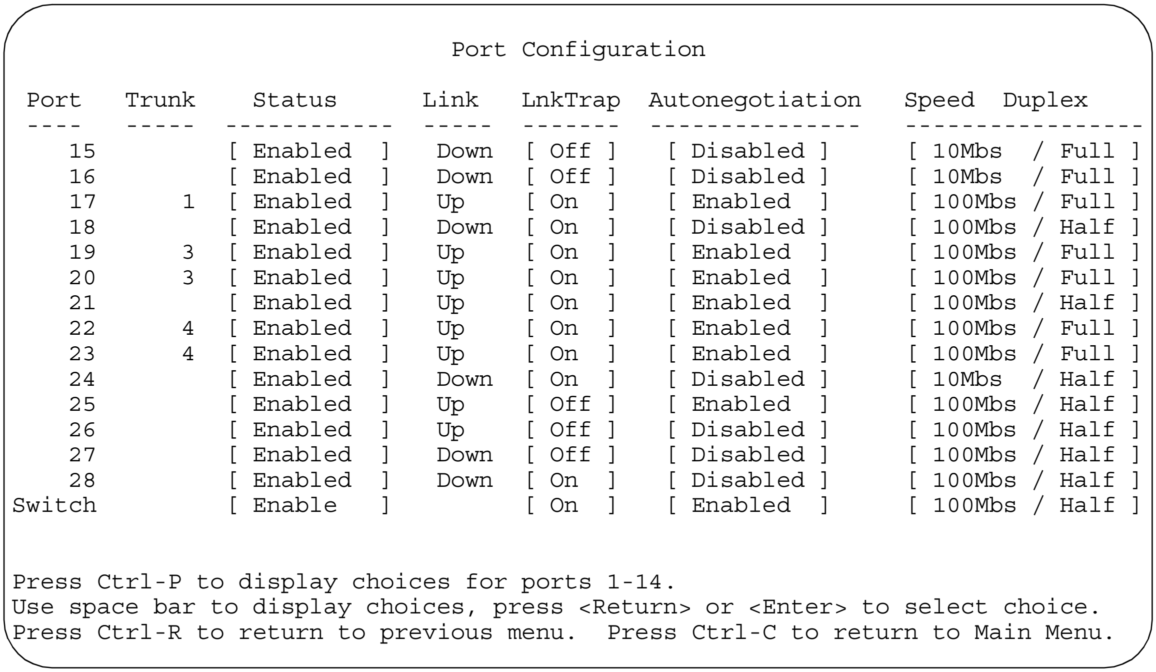
Note: The Autonegotiation, Link Trap, Speed, and Duplex fields are independent of MultiLink Trunking, rate limiting, VLANs, IGMP Snooping, and the STP.

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



```
                               Port Configuration

 Port   Trunk    Status      Link   LnkTrap  Autonegotiation   Speed  Duplex
 ----   -----  ------------  -----  -------  ---------------   -----------------
    1          [ Enabled  ]   Up    [ On  ]   [ Enabled  ]     [ 100Mbs / Half ]
    2          [ Enabled  ]   Up    [ On  ]   [ Enabled  ]     [ 10Mbs  / Full ]
    3          [ Enabled  ]   Up    [ Off ]   [ Disabled ]     [ 10Mbs  / Full ]
    4          [ Enabled  ]   Up    [ Off ]   [ Disabled ]     [ 100Mbs / Half ]
    5          [ Enabled  ]   Down  [ On  ]   [ Disabled ]     [ 100Mbs / Half ]
    6       1  [ Enabled  ]   Up    [ On  ]   [ Enabled  ]     [ 100Mbs / Full ]
    7       1  [ Enabled  ]   Up    [ On  ]   [ Enabled  ]     [ 100Mbs / Full ]
    8          [ Enabled  ]   Down  [ Off ]   [ Disabled ]     [ 100Mbs / Half ]
    9       1  [ Enabled  ]   Up    [ On  ]   [ Enabled  ]     [ 100Mbs / Full ]
   10          [ Enabled  ]   Down  [ On  ]   [ Disabled ]     [ 100Mbs / Half ]
   11          [ Enabled  ]   Up    [ Off ]   [ Disabled ]     [ 10Mbs  / Half ]
   12          [ Enabled  ]   Up    [ Off ]   [ Disabled ]     [ 10Mbs  / Half ]
   13       2  [ Enabled  ]   Up    [ On  ]   [ Enabled  ]     [ 100Mbs / Full ]
   14       2  [ Enabled  ]   Up    [ On  ]   [ Enabled  ]     [ 100Mbs / Full ]

                                                                       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 3-22. Port Configuration Screen (1 of 2)



```
                              Port Configuration

 Port   Trunk    Status      Link   LnkTrap  Autonegotiation    Speed  Duplex
 ----   -----  ------------  -----  -------  ---------------    -----------------
    15         [ Enabled  ]   Down  [ Off ]   [ Disabled ]      [ 10Mbs   / Full ]
    16         [ Enabled  ]   Down  [ Off ]   [ Disabled ]      [ 10Mbs   / Full ]
    17       1 [ Enabled  ]   Up    [ On  ]   [ Enabled  ]      [ 100Mbs / Full ]
    18         [ Enabled  ]   Down  [ On  ]   [ Disabled ]      [ 100Mbs / Half ]
    19       3 [ Enabled  ]   Up    [ On  ]   [ Enabled  ]      [ 100Mbs / Full ]
    20       3 [ Enabled  ]   Up    [ On  ]   [ Enabled  ]      [ 100Mbs / Full ]
    21         [ Enabled  ]   Up    [ On  ]   [ Enabled  ]      [ 100Mbs / Half ]
    22       4 [ Enabled  ]   Up    [ On  ]   [ Enabled  ]      [ 100Mbs / Full ]
    23       4 [ Enabled  ]   Up    [ On  ]   [ Enabled  ]      [ 100Mbs / Full ]
    24         [ Enabled  ]   Down  [ On  ]   [ Disabled ]      [ 10Mbs   / Half ]
    25         [ Enabled  ]   Up    [ Off ]   [ Enabled  ]      [ 100Mbs / Half ]
    26         [ Enabled  ]   Up    [ Off ]   [ Disabled ]      [ 100Mbs / Half ]
    27         [ Enabled  ]   Down  [ Off ]   [ Disabled ]      [ 100Mbs / Half ]
    28         [ Enabled  ]   Down  [ On  ]   [ Disabled ]      [ 100Mbs / Half ]
Switch         [ Enable   ]         [ On  ]   [ Enabled  ]      [ 100Mbs / 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.
```

Figure 3-23. Port Configuration Screen (2 of 2)

Note: When a gigabit MDA is installed, only the Status field for that MDA port is configurable. See "High Speed Flow Control Configuration" on page 3-58 to set the Autonegotiation field for the gigabit MDA port. The gigabit MDA only supports 1000 Mb/s in full-duplex mode.

Table 3-20 describes the Port Configuration screen fields.

Table 3-20. 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 (except the gigabit MDA ports or fiber optic ports, when installed).

(continued)

Table 3-20. Port Configuration Screen Fields *(continued)*

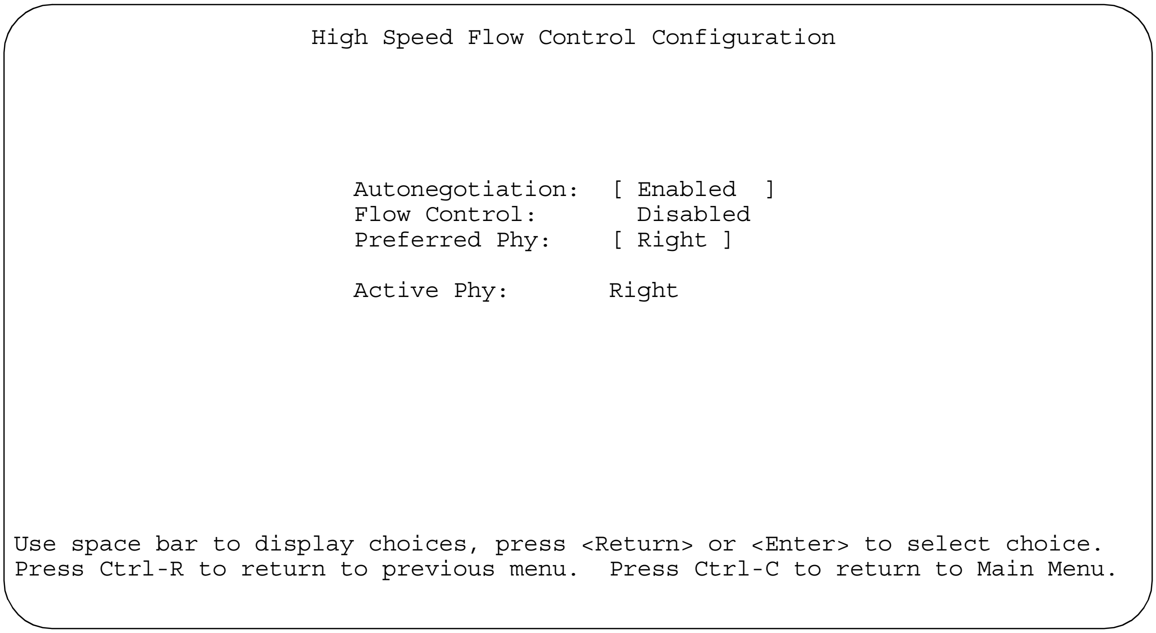
Field	Description	
Trunk	The read-only data displayed in this column indicates the trunk (1 to 4) that corresponds to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen (see "MultiLink Trunk Configuration" on page 3-61).	
Status	Allows you to disable any of the switch ports. You can also use this field to control access to any switch port.	
	Default	Enabled
	Range	Enabled, Disabled
Link	A read-only field that indicates the current link state of the corresponding port, as follows: • Up: The port is connected and operational. • Down: The port is not connected or is not operational.	
LnkTrap	Allows you to control whether link up/link down traps are sent to the configured trap sink from the switch.	
	Default	On
	Range	On, Off
Autonegotiation	When enabled, sets the corresponding port speed to match the best service provided by the connected station, up to 100 Mb/s in full-duplex mode. This field is disabled for all fiber optic ports.	
	Default	Enabled
	Range	Enabled, Disabled
Speed/Duplex	Allows you to manually configure any port to support an Ethernet speed of 10 Mb/s or 100 Mb/s, in half- or full-duplex mode. This field is set (by default) to 1000 Mb/s, full-duplex for gigabit MDA ports only.	
	Default	100Mbs/Half (when Autonegotiation is Disabled)
	Range	10Mbs/Half, 10Mbs/Full, 100Mbs/Half, 100Mbs/Full

High Speed Flow Control Configuration

The High Speed Flow Control Configuration screen (Figure 3-24) allows you to set the port parameters for installed gigabit MDAs.

➡ **Note:** This screen appears only when an optional gigabit MDA is installed in the Uplink Module slot.

Choose High Speed Flow Control Configuration (or press h) from the Switch Configuration Menu to open the High Speed Flow Control Configuration screen.



```
                     High Speed Flow Control Configuration



                        Autonegotiation:  [ Enabled  ]
                        Flow Control:       Disabled
                        Preferred Phy:    [ Right ]

                        Active Phy:       Right







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

Figure 3-24. High Speed Flow Control Configuration Screen

Table 3-21 describes the High Speed Flow Control Configuration screen fields.

Table 3-21. High Speed Flow Control Configuration Screen Fields

Field	Description	
Autonegotiation	Allows the port to advertise support for 1000 Mb/s operation, in full-duplex mode.	
	Default	Enabled
	Range	Enabled, Disabled
Flow Control	Allows you to control traffic and avoid congestion on the gigabit MDA port. Two modes are available (see “Choosing a High Speed Flow Control Mode” on page 3-60 for details about the two modes). The Flow Control field cannot be configured unless you set the Autonegotiation field value to Disabled.	
	Default	Disabled
	Range	Disabled, Symmetric, Asymmetric

(continued)

Table 3-21. High Speed Flow Control Configuration Screen Fields *(continued)*

Field	Description	
	Note: The following two fields appear only when a (single MAC) MDA with a separate redundant Phy port is installed.	
Preferred Phy	Allows you to choose a preferred Phy port, the other Phy port reverts to backup.	
	Default	Right
	Range	Right, Left
Active Phy	Indicates the operational Phy port.	
	Default	None
	Range	None, Right, Left

Choosing a High Speed Flow Control Mode

The High Speed Flow Control feature allows you to control traffic and avoid congestion on the gigabit full-duplex link. If the receive port buffer becomes full, the *gigabit MDA* 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 MDA issues a signal to resume the transmission. You can choose Symmetric or Asymmetric flow-control mode.

Symmetric Mode

This mode allows both the gigabit MDA port and its link partner to send flow control *pause* frames to each other. When a pause frame is received (by either the gigabit MDA port or its link partner), the port suspends transmission of frames for a number of slot times specified in the control frame or until a pause-release control frame is received. Both devices on the link must support this mode.

Asymmetric Mode

This mode allows the link partner to send flow control pause frames to the gigabit MDA port. When a pause frame is received, the receiving port suspends transmission of frames for a number of slot times specified in the control frame or until a pause-release control frames is received. In this mode the gigabit MDA port is disabled from transmitting pause frames to its link partner. This mode can be used if the gigabit MDA port is connected to a buffered repeater device.

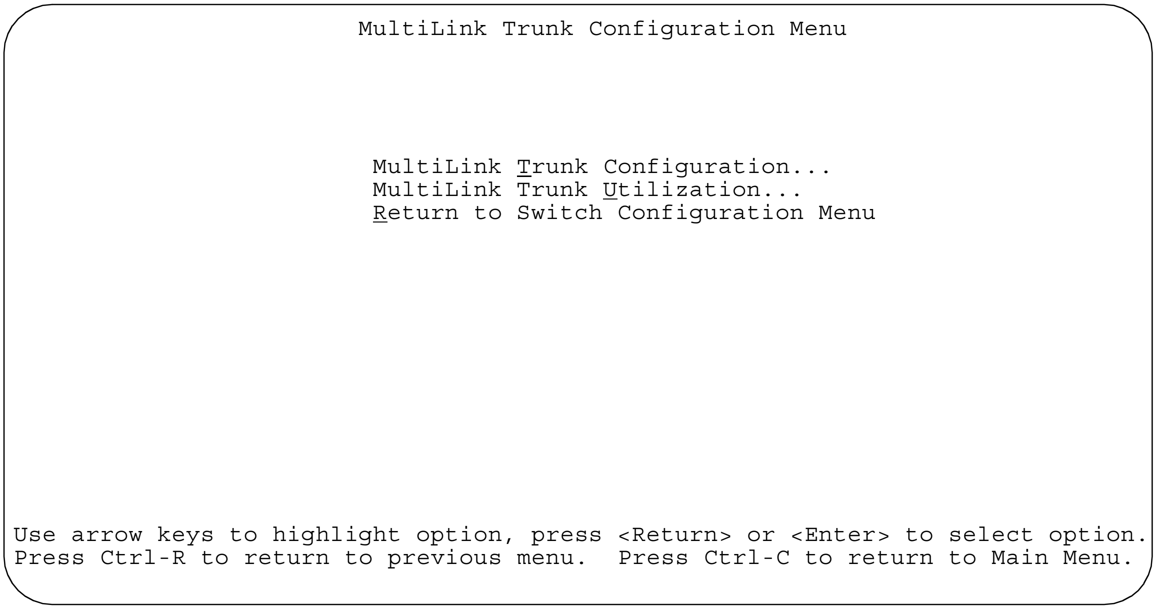
MultiLink Trunk Configuration

The MultiLink Trunk Configuration Menu (Figure 3-25) allows you to select the appropriate screen to configure up to six MultiLink trunks. You can group up to four switch ports to form each trunk, and you can use the trunks to link to another switch or to a server. Bandwidth utilization can be monitored for the trunk member ports within 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 1-60.

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.

Choose MultiLink Trunk Configuration (or press t) from the Switch Configuration Menu to open the MultiLink Trunk Configuration Menu.



```
                        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.
```

Figure 3-25. MultiLink Trunk Configuration Menu Screen

Table 3-22 describes the MultiLink Trunk Configuration Menu options.

Table 3-22. MultiLink Trunk Configuration Menu Options

Option	Description
MultiLink Trunk Configuration...	Displays the MultiLink Trunk Configuration screen (Figure 3-26). This screen allows you to configure up to six MultiLink trunks. You can group up to four switch ports to form each trunk.
MultiLink Trunk Utilization...	Displays the MultiLink Trunk Utilization screen (Figure 3-27 and Figure 3-28). This screen allows you to monitor the bandwidth utilization of the configured trunks.
Return to Switch Configuration Menu	Exits the MultiLink Trunk Configuration Menu and displays the Switch Configuration Menu.

MultiLink Trunk Configuration Screen

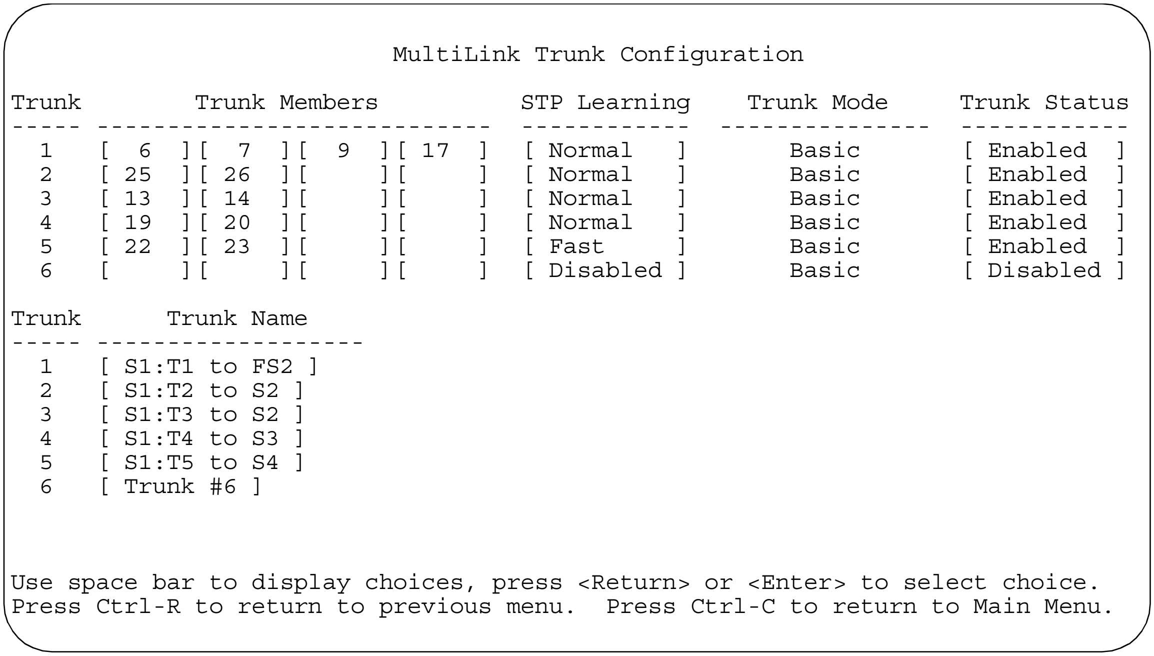
The MultiLink Trunk Configuration screen allows you to configure two to four switch ports together as members of a trunk. Up to six trunks can be created for each BayStack 350 switch.

➡ **Note:** Before configuring MultiLink Trunks, refer to “MultiLink Trunking Configuration Rules” on page 1-72.

Figure 3-26 shows an example of the MultiLink Trunk Configuration screen. In this screen example (previously discussed on page 1-63), five trunks are shown: One trunk is configured with four trunk members and the remaining four trunks are each configured with two trunk members. When a configured trunk is enabled, the trunk members (the specified switch ports) take on default settings necessary for correct operation of the MultiLink Trunking feature. These default settings can affect the correct operation of your configured network. See “MultiLink Trunks” on page 1-63 for more information.

➡ **Note:** If you disable a trunk, you may need to reconfigure the specific trunk members switch ports to return to the previous switch configuration.

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



```
                           MultiLink Trunk Configuration

Trunk        Trunk Members           STP Learning    Trunk Mode     Trunk Status
----- ----------------------------  ------------  ---------------  ------------
  1   [  6  ][  7  ][  9  ][ 17  ]  [ Normal   ]       Basic       [ Enabled  ]
  2   [ 25  ][ 26  ][     ][     ]  [ Normal   ]       Basic       [ Enabled  ]
  3   [ 13  ][ 14  ][     ][     ]  [ Normal   ]       Basic       [ Enabled  ]
  4   [ 19  ][ 20  ][     ][     ]  [ Normal   ]       Basic       [ Enabled  ]
  5   [ 22  ][ 23  ][     ][     ]  [ Fast     ]       Basic       [ Enabled  ]
  6   [     ][     ][     ][     ]  [ Disabled ]       Basic       [ Disabled ]

Trunk      Trunk Name
----- -------------------
  1   [ S1:T1 to FS2 ]
  2   [ S1:T2 to S2 ]
  3   [ S1:T3 to S2 ]
  4   [ S1:T4 to S3 ]
  5   [ S1:T5 to S4 ]
  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.
```

Figure 3-26. MultiLink Trunk Configuration Screen

Table 3-23 describes the MultiLink Trunk Configuration screen fields.

Table 3-23. 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	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. Gigabit ports cannot be configured as trunk members. Default blank field Range 1 to 28 (depending on model type)

(continued)

Table 3-23. MultiLink Trunk Configuration Screen Fields *(continued)*

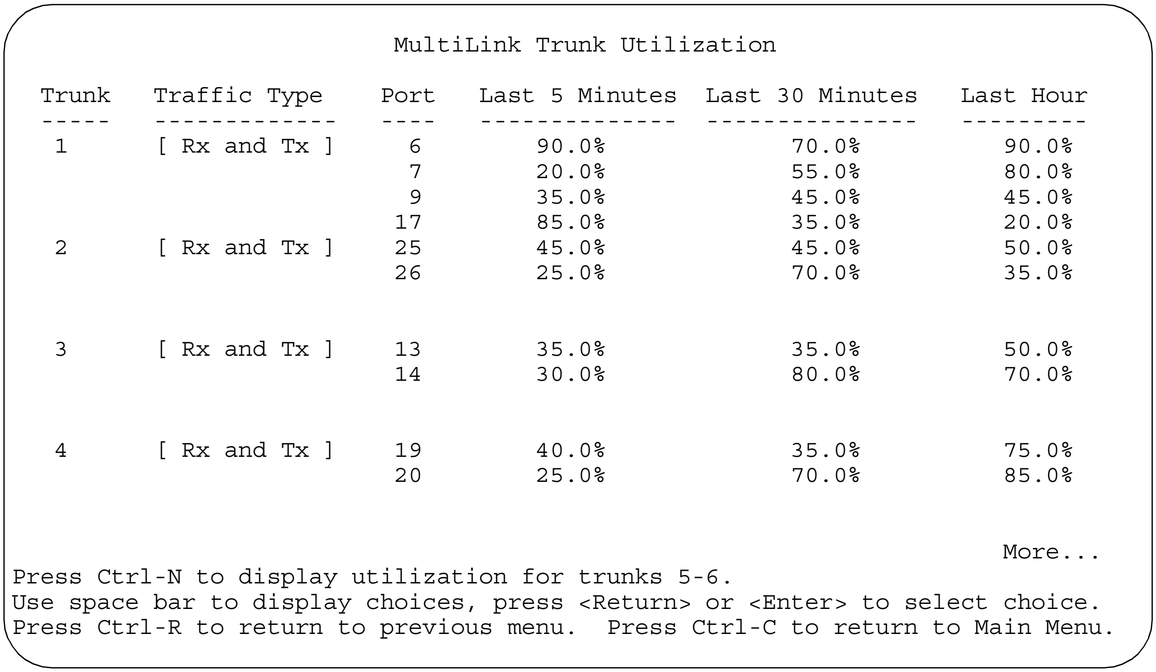
Field	Description	
STP Learning	Contains a single field for each row that, when enabled, allows the specified trunk to participate in the spanning tree. This setting overrides those of the individual trunk members. Fast is the same as Normal, except that the state transition timer is shortened to two seconds.	
	Default	Normal
	Range	Normal, Fast, Disabled
Trunk Mode	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. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.	
	Default	Basic
Trunk Status	Contains a single field for each row that allows users to enable or disable any of the trunks.	
	Default	Enabled
	Range	Enabled, Disabled
Trunk Name	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 (Figures 3-27 and 3-28) allows you to monitor the percentage of bandwidth used by configured trunk members. You can choose the type of traffic to monitor.

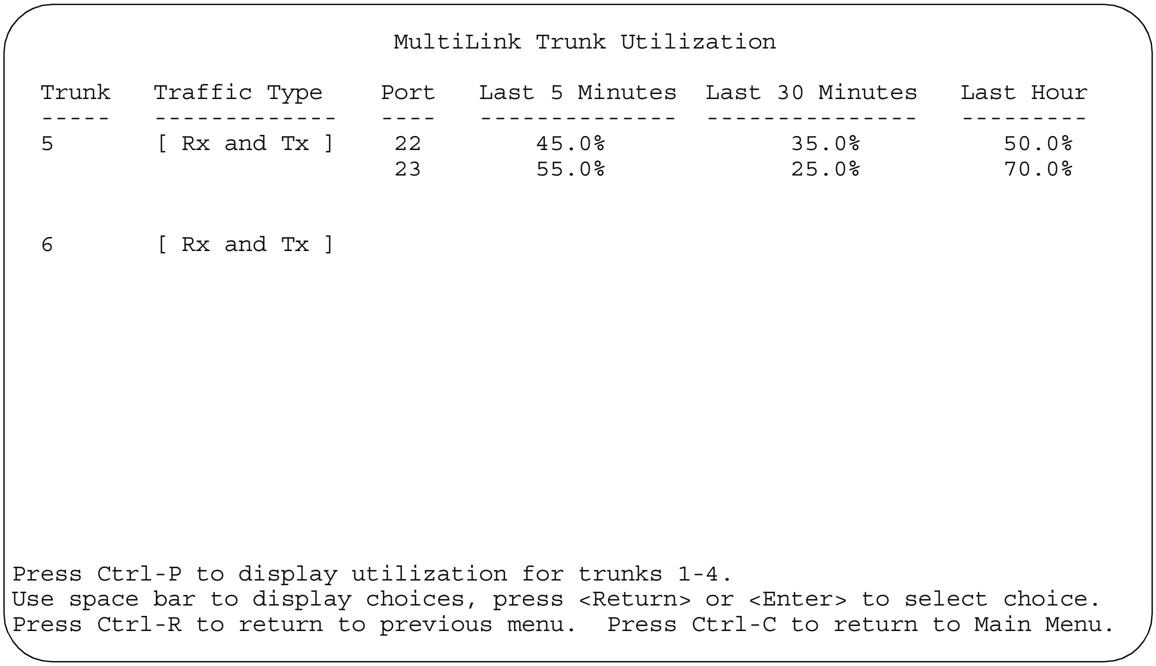
Figure 3-27 shows an example of bandwidth utilization rates for the trunk member ports configured in Figure 3-26. Because two screens are required to show all of the configured trunks (up to six), the screen prompts users to Press [Ctrl]-N to view trunks five and six.

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



```
                           MultiLink Trunk Utilization

  Trunk   Traffic Type    Port   Last 5 Minutes  Last 30 Minutes   Last Hour
  -----   -------------   ----   --------------  ---------------   ---------
   1      [ Rx and Tx ]     6        90.0%             70.0%          90.0%
                            7        20.0%             55.0%          80.0%
                            9        35.0%             45.0%          45.0%
                           17        85.0%             35.0%          20.0%
   2      [ Rx and Tx ]    25        45.0%             45.0%          50.0%
                           26        25.0%             70.0%          35.0%


   3      [ Rx and Tx ]    13        35.0%             35.0%          50.0%
                           14        30.0%             80.0%          70.0%


   4      [ Rx and Tx ]    19        40.0%             35.0%          75.0%
                           20        25.0%             70.0%          85.0%


                                                                      More...
Press Ctrl-N to display utilization for trunks 5-6.
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Figure 3-27. MultiLink Trunk Utilization Screen (1 of 2)



```
                              MultiLink Trunk Utilization

  Trunk    Traffic Type     Port    Last 5 Minutes  Last 30 Minutes    Last Hour
  -----    -------------    ----    --------------  ---------------    ---------
  5        [ Rx and Tx ]     22         45.0%             35.0%           50.0%
                             23         55.0%             25.0%           70.0%


  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.
```

Figure 3-28. MultiLink Trunk Utilization Screen (2 of 2)

Table 3-24 describes the MultiLink Trunk Utilization screen fields.

Table 3-24. 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 trunks (1 to 6) that correspond 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	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.	

(continued)

Table 3-24. MultiLink Trunk Utilization Screen Fields *(continued)*

Field	Description
Last 5 Minutes	This read-only field indicates the percentage of packets (of the type specified in the Traffic Type field) the port used in the last 5 minutes. This field provides a running average of network activity and is updated every 15 seconds.
Last 30 Minutes	This read-only field indicates the percentage of packets (of the type specified in the Traffic Type field) the port used 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) the port used in the last 60 minutes. This field provides a running average of network activity and is updated every 15 seconds.

Port Mirroring Configuration

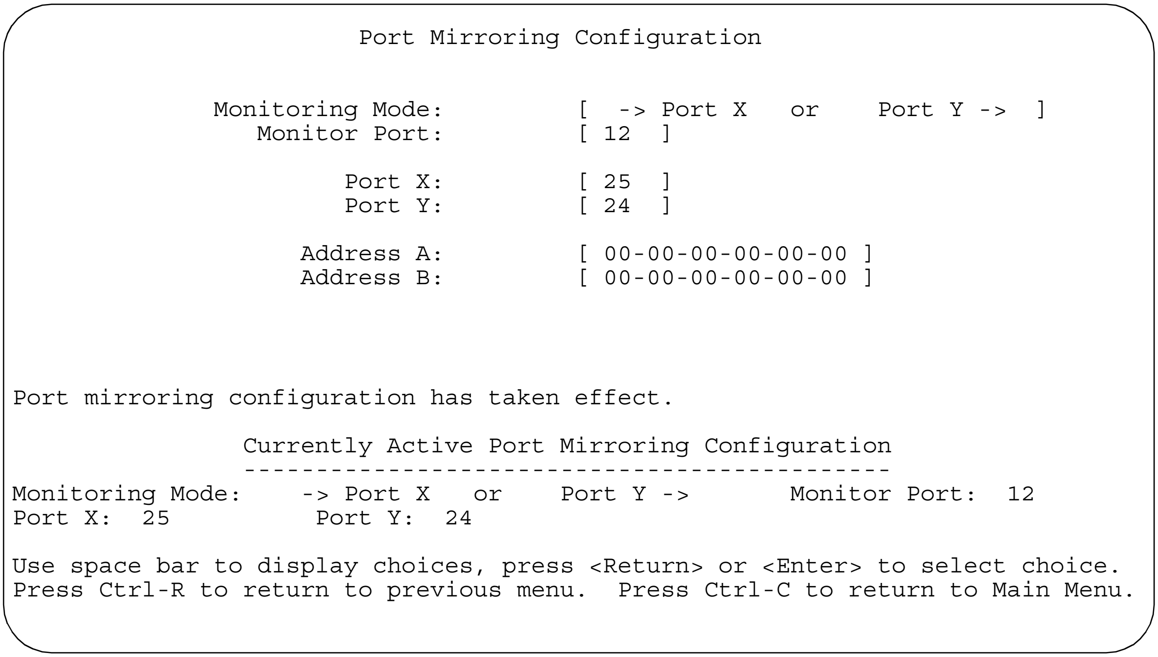
The Port Mirroring Configuration screen allows you to configure a specific switch port to monitor up to two specified ports or two MAC addresses. You can specify port-based monitoring or address-based monitoring.

For more information about the port mirroring feature, see "Port Mirroring (Conversation Steering)" on page 1-78.

Figure 3-29 shows an example of a Port Mirroring Configuration screen where switch port 12 is designated as the monitoring port for ports 24 and 25.

➡ **Note:** Before configuring port mirroring, see "Port Mirroring Configuration Rules" on page 1-84.

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



```
                        Port Mirroring Configuration


              Monitoring Mode:         [  -> Port X   or    Port Y ->  ]
                 Monitor Port:         [ 12  ]

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

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




Port mirroring configuration has taken effect.

                Currently Active Port Mirroring Configuration
                ---------------------------------------------
Monitoring Mode:    -> Port X   or    Port Y ->       Monitor Port:  12
Port X:  25          Port Y:  24

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

Figure 3-29. Port Mirroring Configuration Screen

Table 3-25 describes the Port Mirroring Configuration screen fields.

Table 3-25. Port Mirroring Configuration Screen Fields

Field	Description
Monitoring Mode	Allows you to select any one of six port-based monitoring modes or any one of five address-based monitoring modes (see Table 3-26): Selecting *any one* of the six *port-based modes* activates the port X and port Y screen fields, where you 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 you can specify MAC addresses to monitor. Default Disabled Range See Table 3-26

(continued)

Table 3-25. Port Mirroring Configuration Screen Fields *(continued)*

Field	Description
Monitor Port	Indicates the switch port designated as the monitor port. Default Zero-length string Range 1 to 28 (Model dependent)
Port X	Indicates one of the switch 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 3-26). Default Zero-length string Range 1 to 28 (Model dependent)
Port Y	Indicates one of the switch 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 Y in the Monitoring Mode field (see Table 3-26). Default Zero-length string Range 1 to 28 (Model dependent)
Address A	Indicates the MAC addresses that will be monitored by the designated port monitor when one of the address-based monitoring modes is selected. This port will be monitored according to the value of Address A in the selected Monitoring Mode field (see Table 3-26). Users can enter the MAC address from this screen or from the MAC Address Table screen. The entry is displayed and can be modified by either screen (see “MAC Address Table” on page 3-20). Default 00-00-00-00-00-00 (no MAC address assigned) Range 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF
Address B	Indicates the MAC addresses that will be monitored by the designated port monitor when one of the address-based monitoring modes is selected. This port will be monitored according to the value of Address B in the selected Monitoring Mode field (see Table 3-26). Users can enter the MAC address from this screen or from the MAC Address Table screen. The entry is displayed and can be modified by either screen (see “MAC Address Table” on page 3-20). Default 00-00-00-00-00-00 (no MAC address assigned) Range 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF

Table 3-26 describes the various monitoring modes available from the Port Mirroring Configuration screen.

Table 3-26. Monitoring Modes

Fields	Description
Port-based:	
Disabled	Default value for this feature.
-> Port X	Monitor all traffic Port X receives.
Port X ->	Monitor all traffic Port X transmits.
<-> Port X	Monitor all traffic Port X receives and transmits.
-> Port X or Port Y ->	Monitor all traffic Port X receives or Port Y transmits.
-> Port X and Port Y ->	Monitor all traffic Port X receives (destined to Port Y), and then Port Y transmits.
<-> Port X and Port Y <->	Monitor all traffic Port X receives/transmits and Port Y receives/transmits.
Address-based:	
Disabled	Default value for this feature.
Address A -> any Address	Monitor all traffic Address A transmits to any address.
any Address -> Address A	Monitor all traffic Address A receives from any address.
<-> Address A	Monitor all traffic Address A receives or transmits.
Address A -> Address B	Monitor all traffic Address A transmits to Address B.
Address A <-> Address B	Monitor all traffic between Address A and Address B (conversation between the two stations).

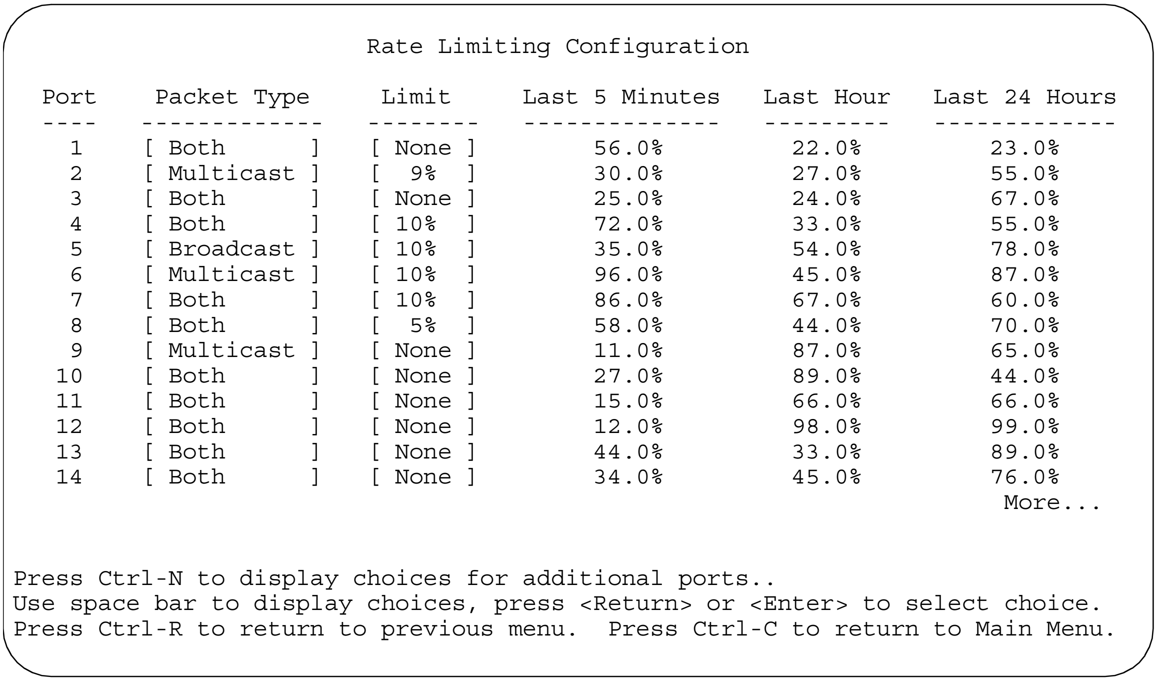
Rate Limiting Configuration

The Rate Limiting Configuration screen allows you to limit the forwarding rate of broadcast and IP multicast packets.

Figures 3-30 and 3-31 show sample rate-limiting settings for the two Rate Limiting Configuration screens.

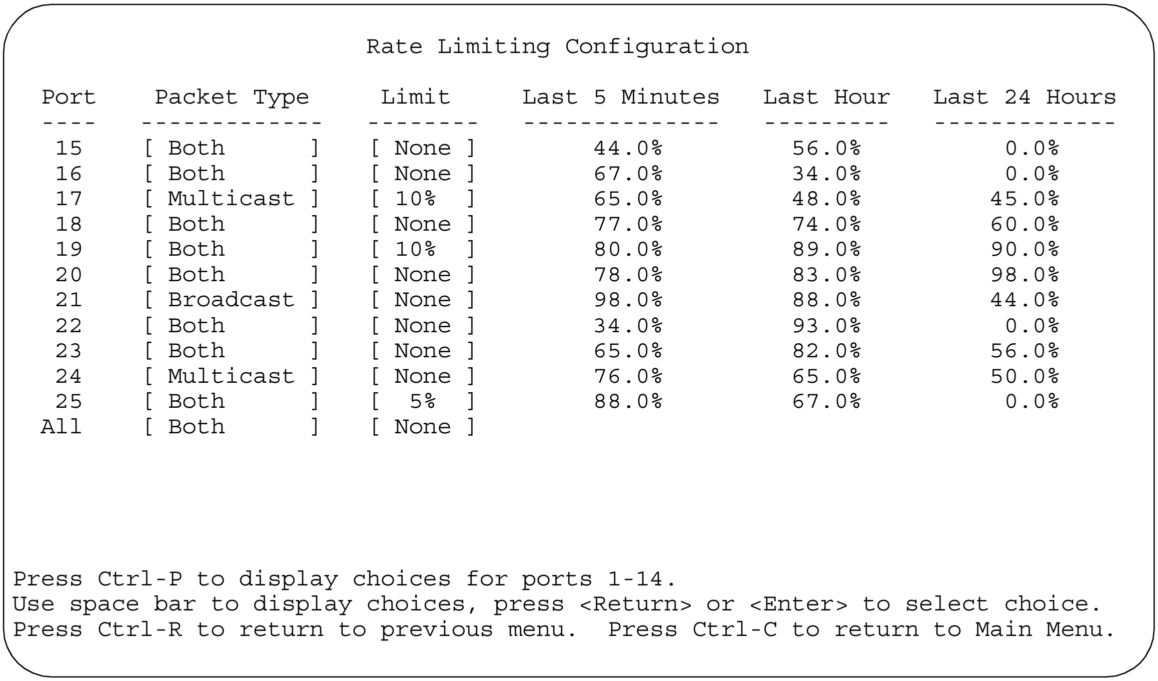
Note: If a port is configured for rate limiting, and it is a MultiLink trunk member, all trunk member ports implement rate limiting. Also, if a trunk member is implementing rate limiting and the port is disabled from rate limiting, all trunk members are disabled from rate limiting.

Choose Rate Limiting Configuration (or press l) from the Switch Configuration Menu to open the Rate Limiting Configuration screen.



```
                         Rate Limiting Configuration

  Port    Packet Type     Limit     Last 5 Minutes   Last Hour   Last 24 Hours
  ----   -------------   --------   --------------   ---------   -------------
    1    [ Both      ]   [ None ]       56.0%          22.0%         23.0%
    2    [ Multicast ]   [  9%  ]       30.0%          27.0%         55.0%
    3    [ Both      ]   [ None ]       25.0%          24.0%         67.0%
    4    [ Both      ]   [ 10%  ]       72.0%          33.0%         55.0%
    5    [ Broadcast ]   [ 10%  ]       35.0%          54.0%         78.0%
    6    [ Multicast ]   [ 10%  ]       96.0%          45.0%         87.0%
    7    [ Both      ]   [ 10%  ]       86.0%          67.0%         60.0%
    8    [ Both      ]   [  5%  ]       58.0%          44.0%         70.0%
    9    [ Multicast ]   [ None ]       11.0%          87.0%         65.0%
   10    [ Both      ]   [ None ]       27.0%          89.0%         44.0%
   11    [ Both      ]   [ None ]       15.0%          66.0%         66.0%
   12    [ Both      ]   [ None ]       12.0%          98.0%         99.0%
   13    [ Both      ]   [ None ]       44.0%          33.0%         89.0%
   14    [ Both      ]   [ None ]       34.0%          45.0%         76.0%
                                                                    More...


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

Figure 3-30. Rate Limiting Configuration Screen (1 of 2)



```
                         Rate Limiting Configuration

  Port    Packet Type     Limit     Last 5 Minutes   Last Hour   Last 24 Hours
  ----   -------------   --------   --------------   ---------   -------------
   15    [ Both      ]   [ None ]        44.0%         56.0%           0.0%
   16    [ Both      ]   [ None ]        67.0%         34.0%           0.0%
   17    [ Multicast ]   [ 10%  ]        65.0%         48.0%          45.0%
   18    [ Both      ]   [ None ]        77.0%         74.0%          60.0%
   19    [ Both      ]   [ 10%  ]        80.0%         89.0%          90.0%
   20    [ Both      ]   [ None ]        78.0%         83.0%          98.0%
   21    [ Broadcast ]   [ None ]        98.0%         88.0%          44.0%
   22    [ Both      ]   [ None ]        34.0%         93.0%           0.0%
   23    [ Both      ]   [ None ]        65.0%         82.0%          56.0%
   24    [ Multicast ]   [ None ]        76.0%         65.0%          50.0%
   25    [ Both      ]   [  5%  ]        88.0%         67.0%           0.0%
  All    [ Both      ]   [ None ]




Press Ctrl-P to display choices for ports 1-14.
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Figure 3-31. Rate Limiting Configuration Screen (2 of 2)

You can use this screen to view the percentage of either packet type (or both packet types) received on each port.

When the volume of either packet type is high, placing severe strain on the network (often referred to as a “storm”), you can set the forwarding rate of those packet types to *not exceed* a specified percentage of the total available bandwidth.

Table 3-27 describes the Rate Limiting Configuration screen fields.

Table 3-27. Rate Limiting Configuration Screen Fields

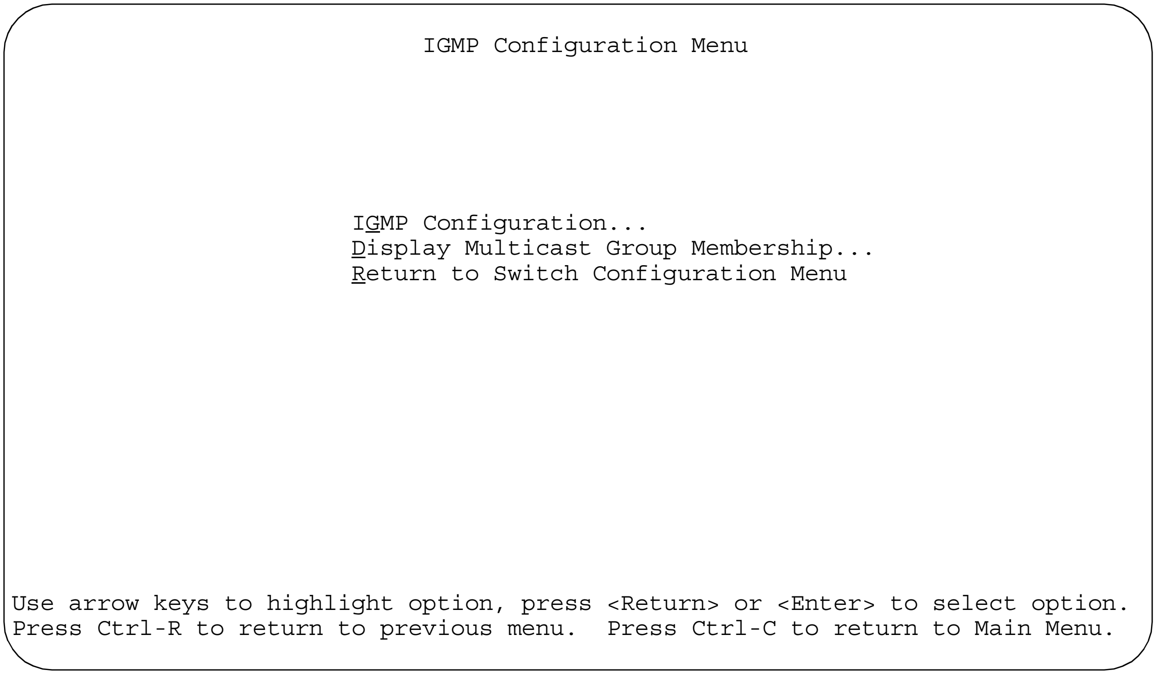
Field	Description	
Port	Indicates the switch port numbers that correspond to the field settings in that row of the screen (for example, the field settings in row 2 apply to switch port 2). Note that the values applied in the All row (bottom row) affect all switch ports.	
Packet Type	Allows you to select the packet types for rate limiting or viewing.	
	Default	Both
	Range	Both, Multicast, Broadcast
Limit	Sets the percentage of port bandwidth allowed for forwarding the packet types specified in the Packet Type field. When the threshold is exceeded, any additional packets (specified in the Packet Type field) are discarded[1].	
	Default	None
	Range	None, 10%, 9%, 8%, 7%, 6%, 5%, 4%, 3%, 2%, 1%
Last 5 Minutes	This read-only field indicates the percentage of packets (of the type specified in the Packet Type field) the port received in the last 5 minutes. This field provides a running average of network activity and is updated every 15 seconds. Note that this field indicates the receiving port's view of network activity, regardless of the rate-limiting setting.	
Last Hour	This read-only field indicates the percentage of packets (of the type specified in the Packet Type field) the port received in the last 60 minutes. This field provides a running average of network activity and is updated every 5 minutes. Note that this field indicates the receiving port's view of network activity, regardless of the rate-limiting setting.	
Last 24 Hours	This read-only field indicates the percentage of packets (of the type specified in the Packet Type field) the port received in the last 24 hours. This field provides a running average of network activity and is updated every hour. Note that this field indicates the receiving port's view of network activity, regardless of the rate-limiting setting.	

[1] Rate limiting is disabled if this field is set to None. This allows you to select and view the percentage of specific packet types present in the network, without inadvertently limiting the forwarding rate.

IGMP Configuration Menu

The IGMP Configuration Menu (Figure 3-32) allows you to select the appropriate screen to optimize IP multicast packets in a bridged Ethernet environment (see “IGMP Snooping” on page 1-51).

Choose IGMP Configuration (or press g) from the Switch Configuration Menu to open the IGMP Configuration Menu.



```
                              IGMP Configuration Menu





                         IGMP Configuration...
                         Display Multicast Group Membership...
                         Return to Switch Configuration Menu










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

Figure 3-32. IGMP Configuration Menu

Table 3-28 describes the IGMP Configuration Menu options.

Table 3-28. IGMP Configuration Menu Options

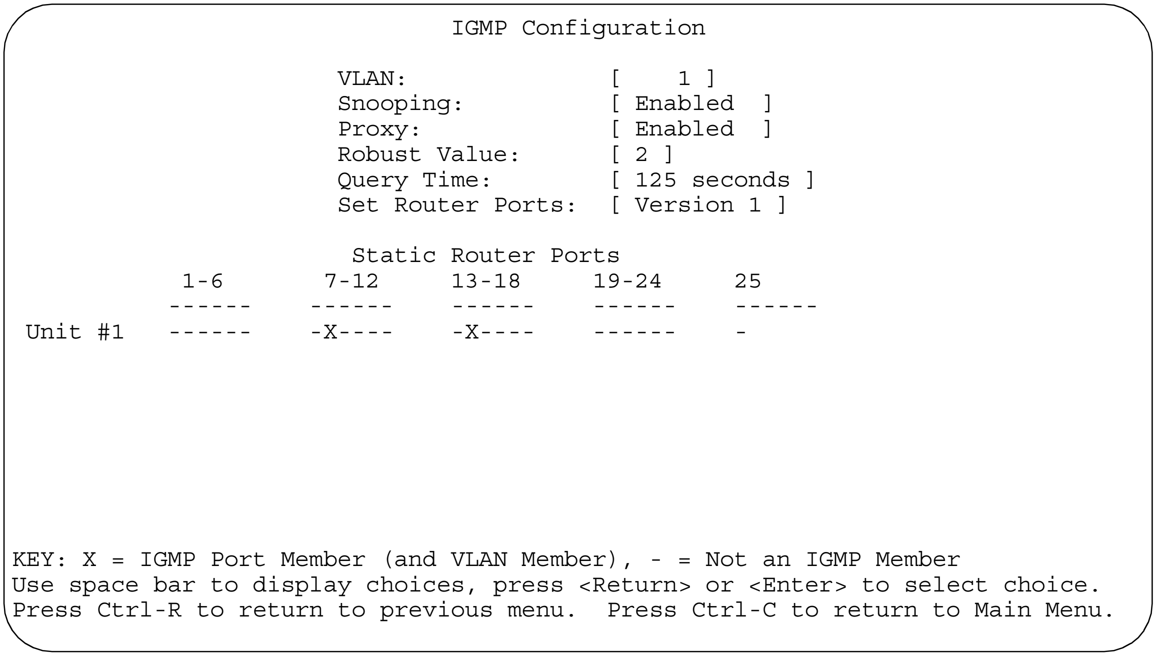
Option	Description
IGMP Configuration...	Displays the IGMP Configuration screen (see "IGMP Configuration" following this table). This screen allows you to set up IGMP configurations.
Display Multicast Group Membership...	Displays the Multicast Group Membership screen (see "Multicast Group Membership" on page 3-79). This screen allows you to view all IP multicast addresses that are active in the current LAN.
Return to Switch Configuration Menu	Exits the IGMP Configuration Menu and displays the Switch Configuration Menu.

IGMP Configuration

Figure 3-33 shows an example of the IGMP Configuration screen. In this example, switch ports 8 and 14 are set to receive all IP multicast-related traffic. The configured ports are VLAN port members of VLAN 5, and are called Static Router Ports.

➡ **Note:** Before configuring your switch for IGMP snooping, see "IGMP Snooping Configuration Rules" on page 1-55.

Choose IGMP Configuration (or press g) from the IGMP Configuration Menu to open the IGMP Configuration screen.



```
                               IGMP Configuration

                       VLAN:                  [    1 ]
                       Snooping:              [ Enabled  ]
                       Proxy:                 [ Enabled  ]
                       Robust Value:          [ 2 ]
                       Query Time:            [ 125 seconds ]
                       Set Router Ports:      [ Version 1 ]

                        Static Router Ports
            1-6       7-12     13-18     19-24     25
           ------    ------    ------    ------    ------
 Unit #1   ------    -X----    -X----    ------    -





KEY: X = IGMP Port Member (and VLAN Member), - = Not an IGMP Member
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Figure 3-33. IGMP Configuration Screen

Table 3-29 describes the IGMP Configuration screen fields.

Table 3-29. IGMP Configuration Screen Fields

Field	Description
VLAN	Allows you to set up or view IGMP configurations on specified VLANs. You can use the spacebar to toggle to any *existing* IGMP configurations (the maximum number of VLANs that can be displayed is 64). Default 1 Range 1 to 4094
Snooping	Allows you to enable or disable IGMP Snooping. This field affects all VLANs (for example, if you disable Snooping for the VLAN specified in the screen's VLAN field, Snooping is disabled for ALL VLANs). Default Enabled Range Enabled, Disabled

(continued)

Table 3-29. IGMP Configuration Screen Fields *(continued)*

Field	Description	
Proxy	Allows the switch to consolidate IGMP Host Membership Reports received on its downstream ports and to generate a consolidated proxy report for forwarding to its upstream neighbor. This field affects all VLANs (for example, if you disable Proxy for the VLAN specified in the screen's VLAN field, Proxy is disabled for all VLANs). You cannot set the Proxy field value to Disabled unless the Snooping field value is Enabled.	
	Default	Enabled
	Range	Enabled, Disabled
Robust Value	Allows you to set the switch to offset expected packet loss on a subnet. If packet losses on a subnet are unacceptably high, the Robust Value field can be increased to a higher value. This field affects only the VLAN specified in the screen's VLAN field (for example, if you change the robust value on the VLAN specified in the screen's VLAN field, other VLANs are not affected).	
	Default	2
	Range	1 to 64
Query Time	Allows you to control the number of IGMP messages allowed on the subnet by varying the *Query Interval* (the Query Interval is the interval between general queries sent by the IP multicast router). This field affects only the VLAN specified in the screen's VLAN field (for example, if you change the Query Time value field on the VLAN specified in the screen's VLAN field, other VLANs are not affected).	
	Default	125 seconds
	Range	1 to 512 seconds

(continued)

Table 3-29. IGMP Configuration Screen Fields *(continued)*

Field	Description	
Set Router Ports	Selects the IGMP version according to the IGMPv1 (Version 1) or IGMPv2 (Version 2) standard (see RFC 2236). Use this field in conjunction with the Static Router Ports field (see next field description) to select the IGMP version to set. You can also use this field to view which static router ports are set to Version 1 or to Version 2. Use the spacebar to toggle between the two versions and view the static router ports settings. This field affects all VLANs (for example, if you change the value of the Set Router Ports field on the VLAN specified in the screen’s VLAN field, all VLANs are affected).	
	Default	Version 1
	Range	Version 1, Version 2
Static Router Ports	Allows you to assign switch ports to receive all IP multicast-related traffic. The configured ports do not filter any IP multicast traffic. The Static Router Ports fields are displayed in six-port groups (for example, 1-6, 7-12, 13-18). The number of ports displayed depends on the switch model or type of optional MDA that is installed in the Uplink Module slot. This field affects all VLANs (for example, if you assign a port as a static router port in this screen, the port becomes a static router port for the VLAN specified in the screen’s VLAN field, and also for any other VLAN where this port is a member). See also “Configuring Ports as Static Router Ports” following this table.	
	Default	-
	Range	-, X

Configuring Ports as Static Router Ports

If you specify a port as a Static Router Port in the IGMP Configuration screen, that port will receive all the IP multicast-related information (such as, Host Membership Report, Host Membership Query, and IP multicast UDP data).

This feature is provided for certain legacy routers that are unable to periodically generate a Host Membership Query. If you configure a port as a static router port, the IP multicast traffic can still be forwarded to any dynamically detected IGMP routers.

If you are sure that it is required for your particular legacy router, configure only the switch ports that have the most direct path to the legacy router as the static router ports. This action will avoid misconfigurations that can prevent you from receiving IGMP multicast traffic.

Note: In most cases, configuring ports as Static Router Ports is not necessary and can prevent you from receiving IGMP multicast traffic. You should configure a static router port only if you are certain that it is required for your particular router. Most routers will be dynamically detected as IGMP routers, in which case no configuration is required.

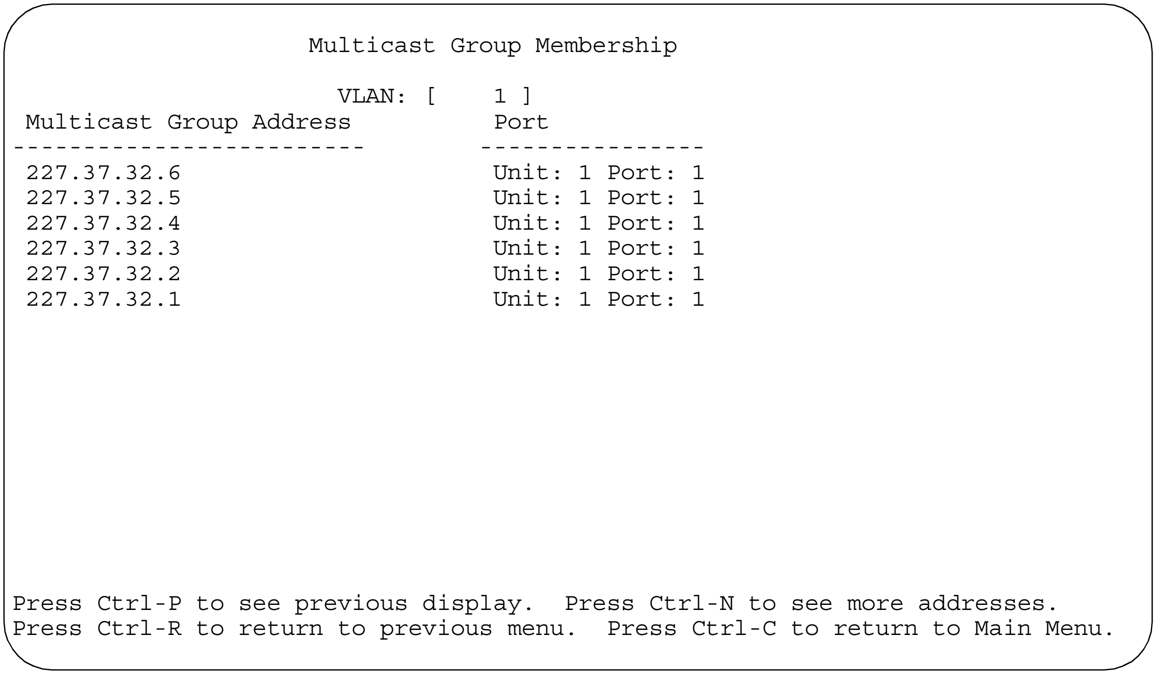
Multicast Group Membership

The Multicast Group Membership screen allows you to view configured IP multicast group addresses for specific VLANs. The screen displays the IP multicast group addresses associated with ports that are configured within a switch.

Note: The Multicast Group Membership screen will not display any entries if the Snooping field value is set to Disabled in the IGMP Configuration screen (see "IGMP Configuration" on page 3-75).

The displayed addresses are dynamic, and can change as clients join or leave the various IP multicast groups. You can view changes by refreshing the screen (press [Ctrl]-P to refresh the screen).

Choose Display Multicast Group Membership (or press d) from the IGMP Configuration Menu to open the Multicast Group Membership screen.



```
                     Multicast Group Membership

                       VLAN: [    1 ]
 Multicast Group Address          Port
-------------------------        ----------------
 227.37.32.6                      Unit: 1 Port: 1
 227.37.32.5                      Unit: 1 Port: 1
 227.37.32.4                      Unit: 1 Port: 1
 227.37.32.3                      Unit: 1 Port: 1
 227.37.32.2                      Unit: 1 Port: 1
 227.37.32.1                      Unit: 1 Port: 1











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

Figure 3-34. Multicast Group Membership Screen

Table 3-30 describes the Multicast Group Membership screen options.

Table 3-30. Multicast Group Membership Screen Options

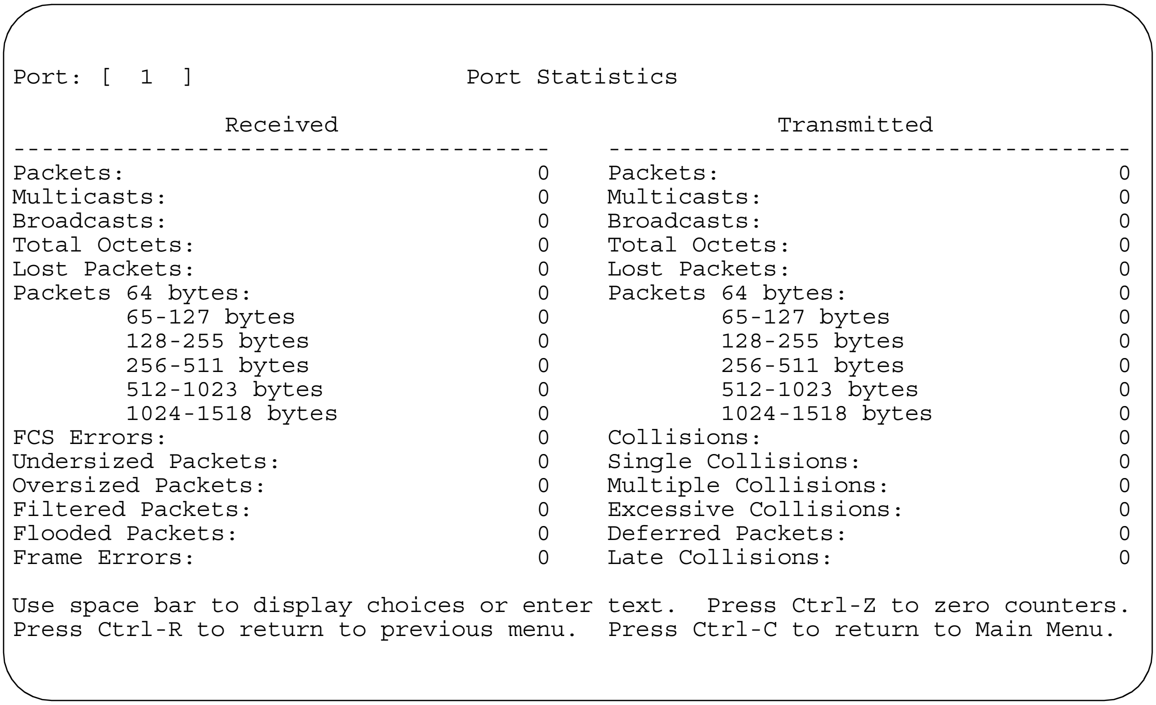
Option	Description
VLAN	Allows you to view IP multicast group addresses on specified VLANs. You can use the spacebar to view group addresses for any *existing* IGMP configurations (the maximum number of VLANs that can be displayed is 64).
Multicast Group Address	Displays all of the IP multicast group addresses that are currently active on the associated ports.
Port	Displays the port numbers that are associated with the IP multicast group addresses displayed in the IP multicast group address field.

Port Statistics

The Port Statistics screen (Figure 3-35) allows you to view detailed information about a switch port. 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 two seconds.

You can use the Port Statistics screen to clear (reset to zero) port counters for a specific port. Alternatively, you can use the Clear All Port Statistics option to clear port counters for all ports (see “Switch Configuration” on page 3-18).

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



```
Port: [  1  ]                   Port Statistics

               Received                               Transmitted
--------------------------------------    --------------------------------------
Packets:                             0    Packets:                             0
Multicasts:                          0    Multicasts:                          0
Broadcasts:                          0    Broadcasts:                          0
Total Octets:                        0    Total Octets:                        0
Lost Packets:                        0    Lost Packets:                        0
Packets 64 bytes:                    0    Packets 64 bytes:                    0
        65-127 bytes                 0            65-127 bytes                 0
        128-255 bytes                0            128-255 bytes                0
        256-511 bytes                0            256-511 bytes                0
        512-1023 bytes               0            512-1023 bytes               0
        1024-1518 bytes              0            1024-1518 bytes              0
FCS Errors:                          0    Collisions:                          0
Undersized Packets:                  0    Single Collisions:                   0
Oversized Packets:                   0    Multiple Collisions:                 0
Filtered Packets:                    0    Excessive Collisions:                0
Flooded Packets:                     0    Deferred Packets:                    0
Frame Errors:                        0    Late Collisions:                     0

Use space bar to display choices or enter text.  Press Ctrl-Z to zero counters.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to return to Main Menu.
```

Figure 3-35. Port Statistics Screen

Table 3-31 describes the Port Statistics screen fields.

Table 3-31. 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 IP multicast packets. Transmitted column: Indicates the total number of packets transmitted successfully on this port, including broadcast packets and IP multicast packets.
Multicasts	Received column: Indicates the total number of good IP multicast packets received on this port, excluding broadcast packets. Transmitted column: Indicates the total number of IP multicast packets transmitted successfully on this port, excluding broadcast packets.
Broadcasts	Received column: Indicates the total number of good broadcast packets received on this port. Transmitted column: Indicates the total number of broadcast packets transmitted successfully on this port.
Total Octets	Received column: Indicates the total number of octets of data (including data in bad packets) received on this port, excluding framing bits but including FCS octets. Transmitted column: Indicates the total number of octets of data transmitted successfully on this port, including FCS octets.
Lost Packets	Received column: Indicates the total number of packets lost (discarded) when the capacity of the port receive buffer was exceeded. Transmitted column: Indicates the total number of packets lost (discarded) when the capacity of the port transmit buffer was exceeded.
Packets 64 bytes	Received column: Indicates the total number of 64-byte packets received on this port. Transmitted column: Indicates the total number of 64-byte packets transmitted successfully on this port.
65-127 bytes	Received column: Indicates the total number of 65-byte to 127-byte packets received on this port. Transmitted column: Indicates the total number of 65-byte to 127-byte packets transmitted successfully on this port.

(continued)

Table 3-31. Port Statistics Screen Fields *(continued)*

Field	Description
128-255 bytes	Received column: Indicates the total number of 128-byte to 255-byte packets received on this port. Transmitted column: Indicates the total number of 128-byte to 255-byte packets transmitted successfully on this port.
256-511 bytes	Received column: Indicates the total number of 256-byte to 511-byte packets received on this port. Transmitted column: Indicates the total number of 256-byte to 511-byte packets transmitted successfully on this port.
512-1023 bytes	Received column: Indicates the total number of 512-byte to 1023-byte packets received on this port. Transmitted column: Indicates the total number of 512-byte to 1023-byte packets transmitted successfully on this port.
1024-1518 bytes	Received column: Indicates the total number of 1024-byte to 1518-byte packets received on this port. Transmitted column: Indicates the total number of 1024-byte to 1518-byte packets transmitted successfully on this port.
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.
Undersized Packets	Indicates the total number of packets received on this port with fewer than 64 bytes and with proper CRC and framing (also known as short frames or runts).
Oversized Packets	Indicates the total number of packets received on this port with more than 1518 bytes and with proper CRC and framing (also known as oversized frames).
Filtered Packets	Indicates the number of packets filtered (not forwarded) by this port.
Flooded Packets	Indicates the total number of packets flooded (forwarded) through this port because the destination address was not in the address database.
Frame Errors	Indicates the total number of valid-size packets that were received but discarded because of CRC errors and improper framing.
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.

(continued)

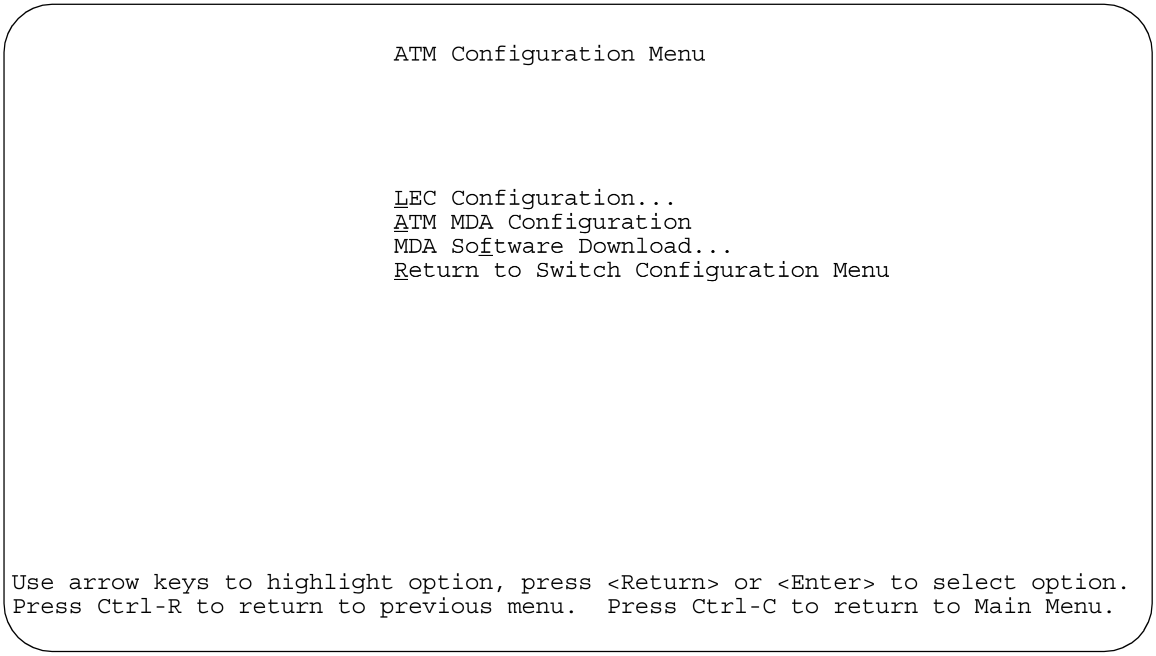
Table 3-31. Port Statistics Screen Fields *(continued)*

Field	Description
Deferred Packets	Indicates the total number of frames that were delayed on the first transmission attempt, but never incurred a collision.
Late Collisions	Indicates the total number of packet collisions that occurred after a total length of time that exceeded 512 bit-times of packet transmission.
The following field values appear only when the port selected in the Port field is configured with a gigabit MDA.	
Pause Frames	Transmitted column: Indicates the total number of pause frames transmitted on this port. Pause frames cause the transmitting port to temporarily suspend the transmission of packets when the receiving port's frame buffer is full (gigabit ports only). Received column: Indicates the total number of pause frames received on this port. Pause frames cause the transmitting port to temporarily suspend the transmission of packets when the receiving port's frame buffer is full (gigabit ports only).

ATM Configuration Menu

The ATM Configuration Menu (Figure 3-36) allows you to select the appropriate screen to configure or upgrade your BayStack 450-2M3/2S3 MDA.

Choose ATM Configuration (or press a) from the Switch Configuration Menu to open the ATM Configuration Menu.



```
                           ATM Configuration Menu





                           LEC Configuration...
                           ATM MDA Configuration
                           MDA Software Download...
                           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.
```

Figure 3-36. ATM Configuration Menu

Before Configuring Your ATM MDA

Your BayStack 450-2M3/2S3 MDA has two physical OC-3 ports (A1 and A2). Each of the physical ports are logically mapped to four LAN emulation clients (LECs) by default (LEC1 to LEC4).

The LECs can be thought of as *virtual* ports that perform data forwarding, address resolution, and other control functions over asynchronous transfer mode (ATM).

The default values for the four LECs are Disabled. You cannot enable the LECs without assigning them to a VLAN. After you assign the LECs to a VLAN, the LECs become virtual ports (VPorts) and show up in the appropriate CI screens as if they were a continuation of the switch's normal port population. For example, in a 24-port switch, the four VPorts appear in the CI screens as ports 25 to 28.

You can assign any of the four LECs to either one of the two physical ports to suit your network needs (for example, you can assign LEC2 and LEC3 to physical port A1 while LEC 1 and LEC 4 are assigned to physical port A2). The LECs must be assigned to a VLAN on the switch in order to function properly.

Note: When you configure your LECs using the following screen examples and tables, you will be instructed to use the VLAN Configuration screen to assign the appropriate LEC virtual port number to a VLAN.

See "VLAN Configuration" on page 3-43 for help in assigning VPorts to a VLAN.

See Appendix D, "ATM Overview," for an overview of ATM concepts and terminology that relate to the BayStack 450-2M3/2S3 MDA. That appendix also provides tips you can use when configuring your BayStack 450-2M3/2S3 MDA.

See Appendix E, "Quick Steps to Features," for flowcharts that detail the steps required to configure your BayStack 450-2M3/2S3 MDA.

Table 3-32 describes the ATM Configuration Menu options.

Table 3-32. ATM Configuration Menu Options

Option	Description
LEC Configuration...	Displays the LEC Configuration screen (see "LEC Configuration" on page 3-87). This screen allows you to specify parameters and port assignments for the LEC virtual ports.
ATM MDA Configuration...	Displays the ATM MDA Configuration screen (see "ATM MDA Configuration" on page 3-89). This screen allows you to set up and view ATM configuration parameters for the ATM MDA.
MDA Software Download...	Displays the MDA Software Download screen (see "ATM MDA Software Download" on page 3-92). This screen allows you to upgrade your ATM MDA with the latest firmware code.
Return to Switch Configuration Menu	Exits the ATM Configuration Menu and displays the Switch Configuration Menu.

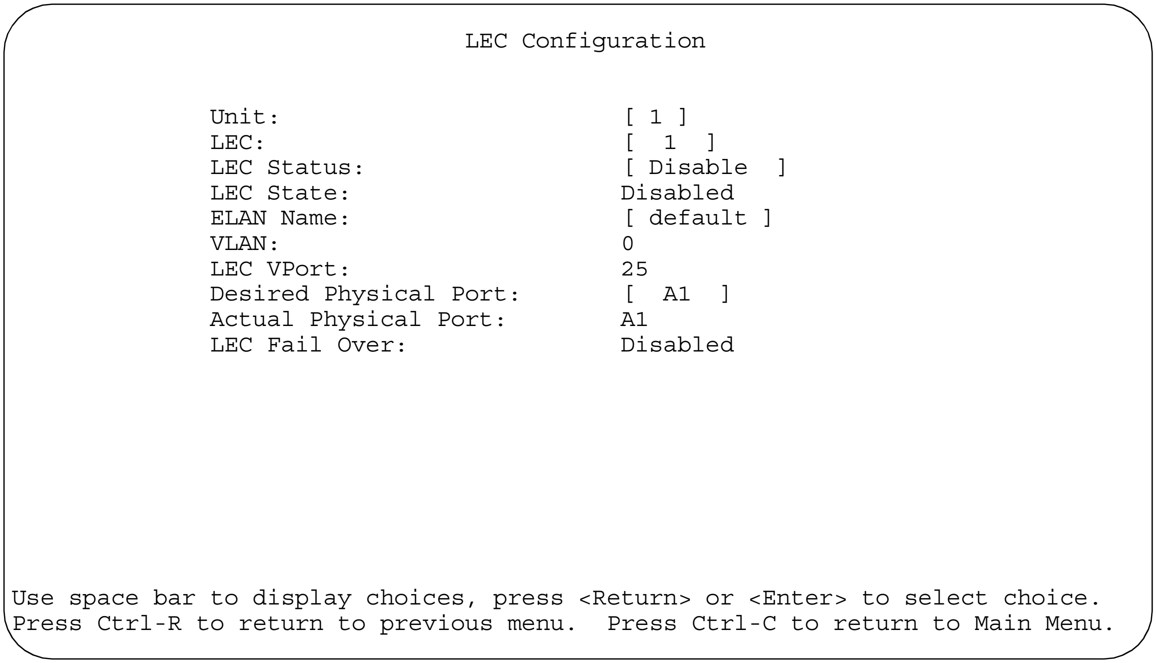
LEC Configuration

The LEC Configuration screen (Figure 3-37) allows you to specify parameters and port assignments for the LEC virtual ports.

When you configure your LEC virtual ports, you must also use the VLAN Configuration screen to assign the specified LEC to a current VLAN or to a new VLAN (see "VLAN Configuration" on page 3-43).

You can assign the LEC virtual ports to either one of the two physical ports (A1 or A2).

Choose LEC Configuration (or press l) from the ATM Configuration Menu to open the LEC Configuration screen.



```
                                LEC Configuration


              Unit:                         [ 1 ]
              LEC:                          [  1  ]
              LEC Status:                   [ Disable  ]
              LEC State:                    Disabled
              ELAN Name:                    [ default ]
              VLAN:                         0
              LEC VPort:                    25
              Desired Physical Port:        [  A1  ]
              Actual Physical Port:         A1
              LEC Fail Over:                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 3-37. LEC Configuration Screen

Table 3-33 describes the LEC Configuration screen fields.

Table 3-33. LEC Configuration Screen Fields

Field	Description	
Unit	This field appears only if the ATM MDA is installed in a switch that is part of a stack configuration. Allows you to select another stack unit that is configured with an ATM MDA. To view or configure another ATM MDA, type its unit number and press [Enter], or press the spacebar to toggle the unit numbers.	
LEC	Allows you to specify the LEC virtual port you want to configure.	
	Default	1
	Range	1, 2, 3, 4
LEC Status	Allows you to enable or disable the selected LEC.	
	Default	Disable
	Range	Disable, Enable
LEC State	This read-only field displays the current status of the selected LEC.	
	Default	Disabled
	Range	Disabled, Idle, Operational, Unknown
ELAN Name	Allows you to enter a name for the ELAN that is associated with the selected LEC. You should also verify that the ELAN you are connecting to exists on the target ATM switch.	
	Default	default
	Range	Any ASCII string of up to 20 printable characters
VLAN	This read-only field displays the current VLAN that is associated with the selected LEC. The default configuration for the LEC is 0 (no VLAN assigned). You can assign a LEC to any currently active port-based VLAN. Use the VLAN Configuration screen to assign the appropriate VPort number for the LEC to a VLAN. See Appendix D, “ATM Overview,” for more information about assigning LECs to a VLAN.	
	Default	0
	Range	1 to 4094
LEC VPort	This read-only field displays the LEC VPort (virtual port) number that is associated with the selected LEC. This VPort number is also shown on other CI screens (such as the VLAN Configuration screen or the Spanning Tree Configuration screen, as appropriate).	

(continued)

Table 3-33. LEC Configuration Screen Fields *(continued)*

Field	Description	
	Default	13 / 25 The four LECs are assigned VPort numbers that directly relate to the switch version (12 port or 24 port) where they are installed. For example, when installed in a 24-port switch, LECs 1, 2, 3, and 4 are assigned as VPorts 25, 26, 27, and 28 respectively.
	Range	(12-port models) = 13,14,15,16 / (24-port models) = 25,26,27,28
Desired Physical Port	Allows you to configure the physical port (A1 or A2) for the selected LEC.	
	Default	A1
	Range	A1, A2
Actual Physical Port	This read-only field displays the actual physical port for the selected LEC.	
	Default	A1
	Range	A1, A2
LEC Fail Over	This read-only field displays the LEC Fail Over setting for the ATM MDA. You can set the LEC Fail Over field using the ATM MDA Configuration screen (see "ATM MDA Configuration" on page 3-89).	

ATM MDA Configuration

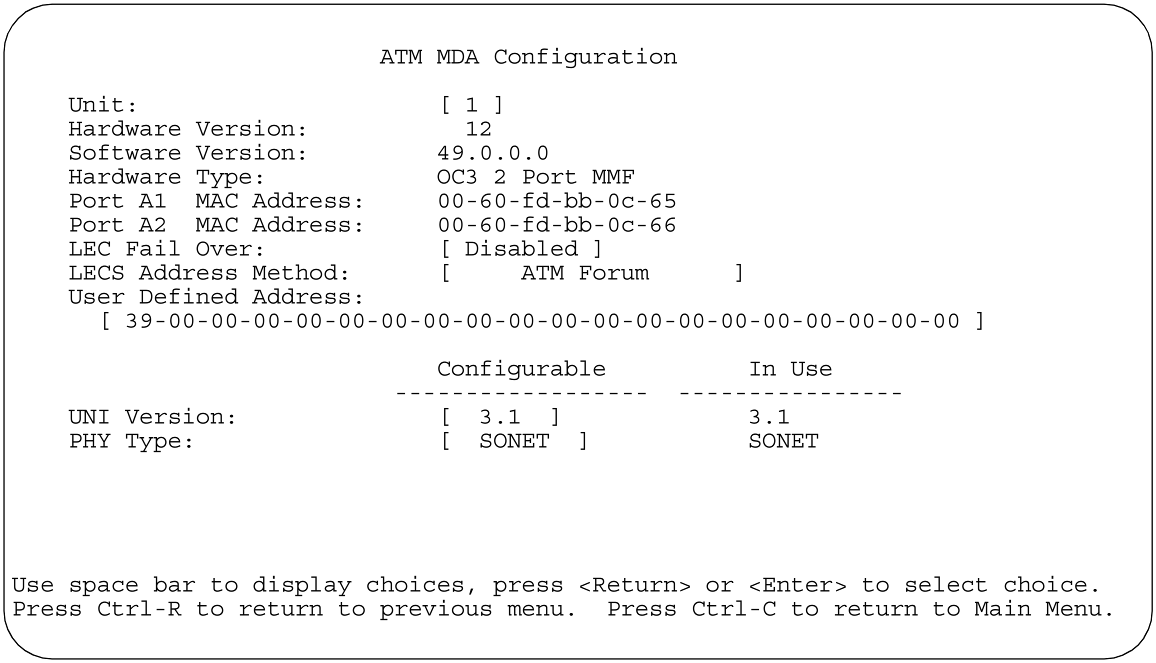
The ATM MDA Configuration screen (Figure 3-38) allows you to set up ATM configuration parameters for your BayStack 450-2M3/2S3 MDA.

Certain fields in this screen may require you to reset the switch if you change the current or default value for another value. The reset option is always preceded by a screen prompt. Enter Yes to reset the switch; enter No to abort the option.

You can also use this screen to view the current BayStack 450-2M3/2S3 MDA:

- Hardware version
- Software version
- Hardware type
- MAC addresses for physical ports A1 and A2

Choose ATM MDA Configuration (or press a) from the ATM Configuration Menu to open the ATM MDA Configuration screen.



```
                          ATM MDA Configuration

    Unit:                     [ 1 ]
    Hardware Version:           12
    Software Version:         49.0.0.0
    Hardware Type:            OC3 2 Port MMF
    Port A1  MAC Address:     00-60-fd-bb-0c-65
    Port A2  MAC Address:     00-60-fd-bb-0c-66
    LEC Fail Over:            [ Disabled ]
    LECS Address Method:      [     ATM Forum      ]
    User Defined Address:
      [ 39-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 ]

                              Configurable          In Use
                           ------------------  ----------------
    UNI Version:              [  3.1  ]             3.1
    PHY Type:                 [  SONET  ]           SONET




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 3-38. ATM MDA Configuration Screen

Table 3-34 describes the ATM MDA Configuration screen fields.

Table 3-34. ATM MDA Configuration Screen Fields

Field	Description
Unit	This field appears only if the ATM MDA is installed in a switch that is part of a stack configuration. Allows you to select another stack unit that is configured with an ATM MDA. To view or configure another ATM MDA, type its unit number and press [Enter], or press the spacebar to toggle the unit numbers.
Hardware Version	Read-only field that indicates the current hardware version of the selected ATM MDA.
Software Version	Read-only field that indicates the current software version of the selected ATM MDA.
Hardware Type	Read-only field that indicates the type of ATM MDA that is currently selected.

(continued)

Table 3-34. ATM MDA Configuration Screen Fields *(continued)*

Field	Description	
Port A1 MAC Address	Read-only field that indicates the port A1 MAC address of the ATM MDA that is currently selected.	
Port A2 MAC Address	Read-only field that indicates the port A2 MAC address of the ATM MDA that is currently selected.	
LEC Fail Over	Allows you to enable or disable the LEC Fail Over feature. **Note:** The BayStack 450-2M3/2S3 MDA has two physical ports (A1 and A2) that are available for LEC association. When the LEC Fail Over field value is set to Enabled, the LEC(s) associated with a failed physical port is automatically assigned to the remaining operational physical port. If the failed physical port recovers, the LEC(s) will be automatically assigned to the desired port.	
	Default	Disabled
	Range	Disabled, Enabled
LECS Address Method	Allows you to configure the selected LEC to obtain LANE services from a LAN emulation configuration server (LECS). You can choose one of three addressing methods that the LEC will use (see Range field). • ATM Forum -- The LEC will use an ATM Forum address. • User Defined -- The LEC will use the User Defined Address value (see next field) as the address of the LECS when attempting to set up the control direct to the LECS. • ILMI -- The switch will use the ILMI (interim local management interface) to obtain the address of the LECS.	
	Default	ATM Forum
	Range	ATM Forum, User Defined, ILMI
User Defined Address	Allows you to specify the ATM user-defined address to be used in the LECS Address Method field (see previous field). This field is a 20-byte ATM address	
	Default	39-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
	Range	Any 20-byte address field, where the first byte must be either 39, 45, or 47.
UNI Version	Allows you to select the user-to-network interface (UNI) the LEC will use. For more information about UNI 3.0 and UNI 3.1, refer to *ATM User-Network Interface (UNI) Specification, Version 3.0* and *ATM User-Network Interface (UNI) Specification, Version 3.1*.	
	Default	3.1
	Range	3.1, 3.0

(continued)

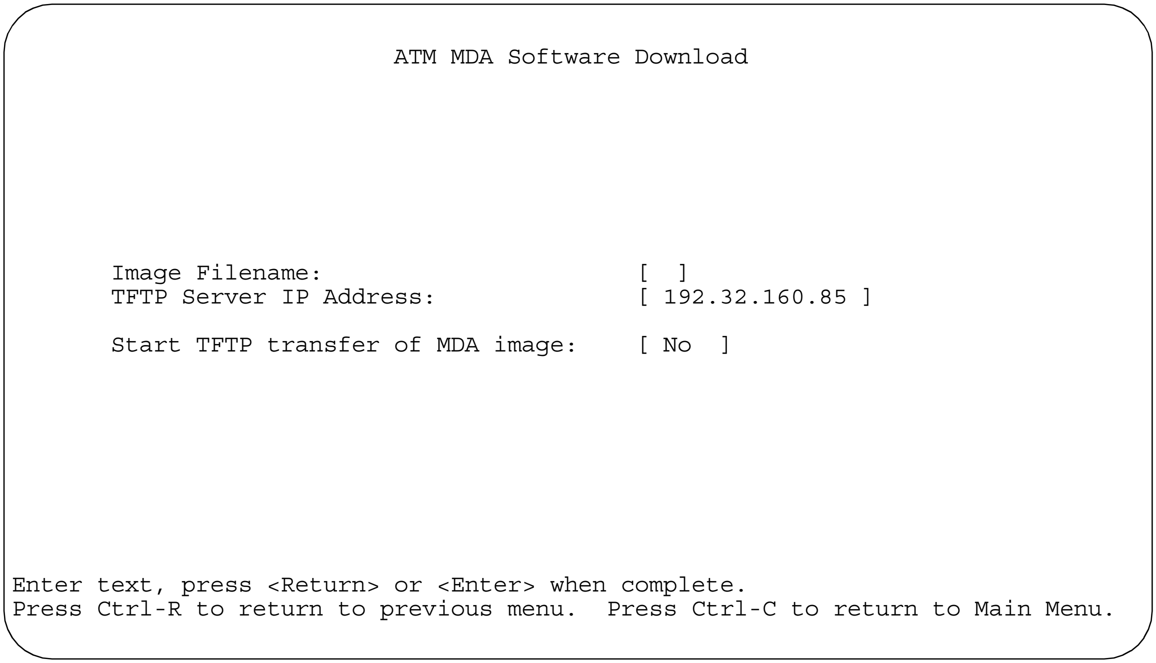
Table 3-34. ATM MDA Configuration Screen Fields *(continued)*

Field	Description
PHY Type	Allows you to choose the physical layer medium independent (PHY) component the LEC will use. You can choose between two versions of the following standard: • Synchronous Optical Network (SONET), a standard developed under ANSI and the Exchange Carriers Standards Association (ECSA) for digital optical transmission. • Synchronous Digital Hierarchy (SDH), a slightly different version of the SONET standard developed by the International Telegraph and Telephone Consultative Committee (CCITT). Default SONET Range SONET, SDH

ATM MDA Software Download

The ATM MDA Software Download screen (Figure 3-39) allows you to upgrade your BayStack 450-2M3/2S3 MDA with the latest firmware code.

Choose ATM MDA Software Download (or press f) from the ATM Configuration Menu to open the ATM MDA Software Download screen.



```
                          ATM MDA Software Download







      Image Filename:                    [  ]
      TFTP Server IP Address:            [ 192.32.160.85 ]

      Start TFTP transfer of MDA image:  [ No  ]









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

Figure 3-39. ATM MDA Software Download Screen

Table 3-35 describes the ATM MDA Software Download screen fields.

Table 3-35. ATM MDA Software Download Screen Fields

Field	Description	
Image Filename	The software image load file name.	
	Default	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	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

(continued)

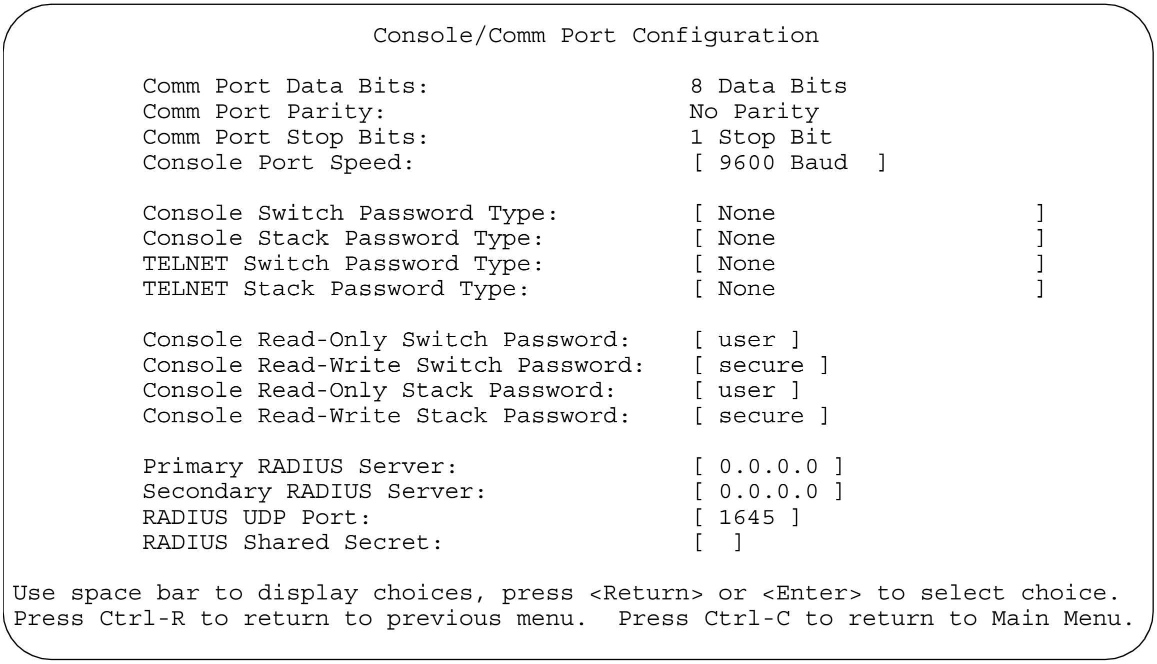
Table 3-35. ATM MDA Software Download Screen Fields *(continued)*

Field	Description	
Start TFTP transfer of MDA image	Specifies whether to start the download of the BayStack 450-2M3/2S3 MDA software image (default is No). Use the spacebar to toggle the selection to Yes. Press [Enter] to initiate the software download process. To ensure that the download process is not interrupted, do not power down the switch for approximately 10 minutes.	
	Default	No
	Range	Yes, No

Console/Comm Port Configuration

The Console/Comm Port Configuration screen (Figure 3-40) allows you to configure and modify the console/comm port parameters and security features.

Choose Console/Comm Port Configuration (or press o) from the main menu to open the 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 ]
         RADIUS UDP 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.
```

Figure 3-40. Console/Comm Port Configuration Screen

Table 3-36 describes the Console/Comm Port Configuration screen fields.

Table 3-36. 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.

(continued)

Table 3-36. Console/Comm Port Configuration Screen Fields *(continued)*

Field	Description	
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	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.

Achtung: Bei Auswahl einer Baudrate, 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.

(continued)

Table 3-36. Console/Comm Port Configuration Screen Fields *(continued)*

Field	Description
	注意: コンソール・ターミナルのボー・レートに合っていな 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 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 the 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 None Range None, Local Password, RADIUS Authentication
Console Stack Password Type	**Accessible with BayStack 450 and BayStack 410-24T switch models only:** Enables password protection for accessing the console interface (CI) of any participating stackable switch in a stack configuration, through a console terminal.
TELNET Switch Password Type	Enables password protection for accessing the console interface (CI) of a *standalone switch* through a TELNET session. If you set this field to Required, you can use the Logout option to restrict access to the CI. Thereafter, you will need to specify the correct password at the console-terminal prompt. See Console Read-Only Switch Password and Console Read-Write Switch Password for more information. Default None Range None, Local Password, RADIUS Authentication
TELNET Stack Password Type	**Accessible with BayStack 450 and BayStack 410-24T switch models only:** Enables password protection for accessing the console interface (CI) of any participating *stackable* switch in a stack configuration, through a TELNET session.

(continued)

Table 3-36. Console/Comm Port Configuration Screen Fields *(continued)*

Field	Description
Console Read-Only Switch Password	When the Console Switch Password field is set to Local Password (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: 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 Local Password (for TELNET, for Console, or for Both), this field allows read-write password access to the CI of a *standalone switch*. Users can log in to the CI using the correct password (see default), and can change any parameter, except the stack passwords. You can change the default passwords for read-only access and read-write access to a private password. Default: 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.

(continued)

Table 3-36. 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。
Console Read-Only Stack Password	**Accessible with BayStack 450 and BayStack 410-24T switch models only:** Allows read-only password access to the CI of any participating *stackable* switch in a stack configuration.
Console Read-Write Stack Password	**Accessible with BayStack 450 and BayStack 410-24T switch models only:** Allows read-write password access to the CI of any participating *stackable* switch in a stack configuration.
	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.

(continued)

Table 3-36. Console/Comm Port Configuration Screen Fields *(continued)*

Field	Description
	Achtung: Wenn Sie die für das System standardmäßig eingestellten Paßwörter ändern, notieren Sie sich die neuen Paßwörter, und bewahren Sie sie an einem sicheren Ort auf. Falls Sie die neuen Paßwörter vergessen, können Sie nicht mehr auf die Konsolenschnittstelle zugreifen. Wenden Sie sich in diesem Fall an Nortel Networks, um Unterstützung zu erhalten.
	Attention: Si vous changez les mots de passe par défaut du système, assurez-vous de bien noter vos nouveaux mots de passe et de les conserver dans un endroit sûr. Si vous perdez vos nouveaux mots de passe, vous ne pourrez plus accéder à votre interface. Le cas échéant, veuillez contacter Nortel Networks.
	Precaución: Si modifica las contraseñas predeterminadas asignadas por el sistema, asegúrese de anotar las nuevas contraseñas y guárdelas en un lugar seguro. Si olvida las nuevas contraseñas, no podrá acceder al interfaz de la consola. En ese caso, póngase en contacto con Nortel Networks para obtener ayuda al respecto.
	Attenzione: In caso di modifica delle password predefinite nel sistema, assicurarsi di annotare le nuove password e di conservarle in un luogo sicuro. Nel caso in cui le nuove password vengano dimenticate, non sarà possibile accedere all'interfaccia della console. In tal caso, contattare la Nortel Networks per avere assistenza.
	注意： システム装備したデフォルトのパスワードを変更する場合、必ず新しいパスワードを書き留めて安全な場所に保管してください。新しいパスワードを忘れてしまうと、 コンソール・インタフェイスにアクセスできません。 この場合は、Bay Networksまでご連絡ください。

(continued)

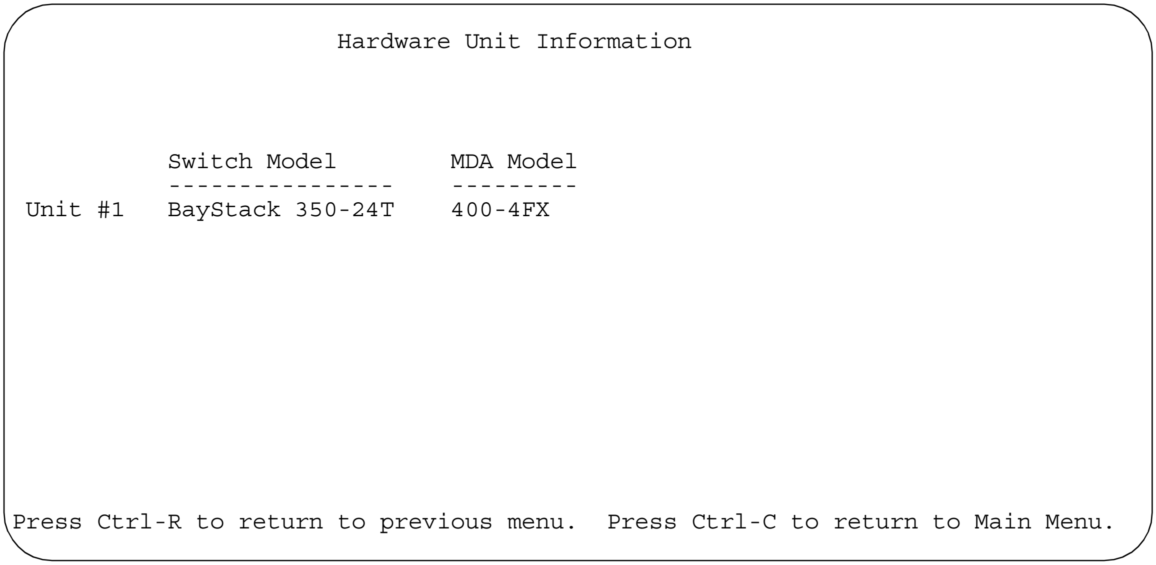
Table 3-36. Console/Comm Port Configuration Screen Fields *(continued)*

Field	Description	
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 UDP 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

The Hardware Unit Information screen (Figure 3-41) identifies your switch model, including any installed MDA.

Choose Display Hardware Units (or press h) from the main menu to open the Hardware Unit Information screen.



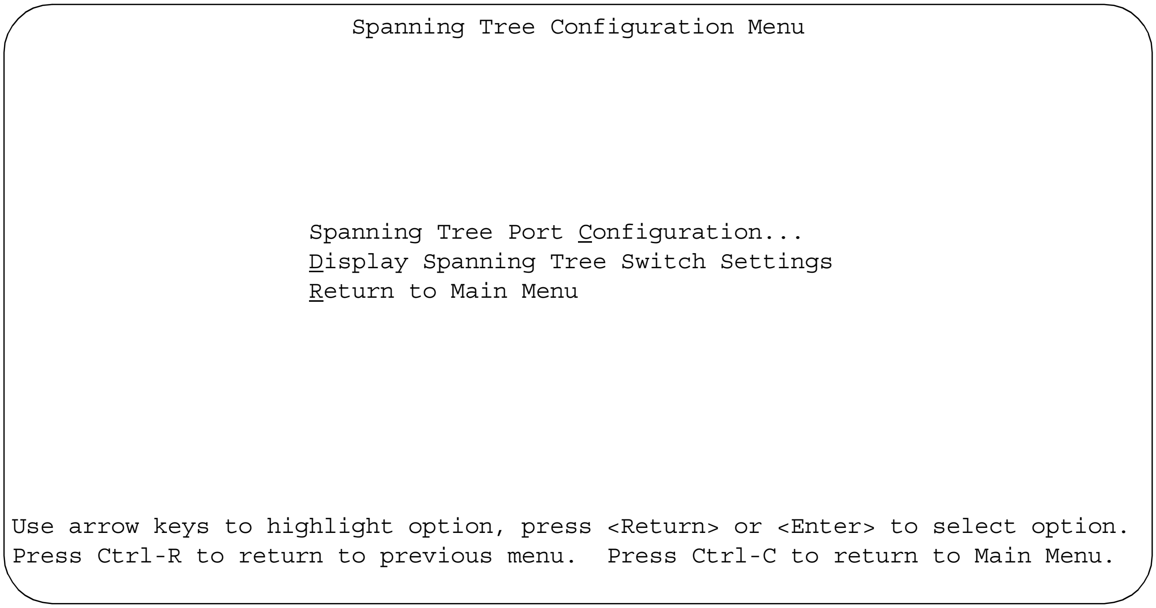
```
                       Hardware Unit Information



           Switch Model        MDA Model
           ----------------    ---------
 Unit #1   BayStack 350-24T    400-4FX










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

Figure 3-41. Hardware Unit Information Screen

Spanning Tree Configuration

The Spanning Tree Configuration Menu (Figure 3-42) 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.

Choose Spanning Tree Configuration (or press p) from the main menu to open the Spanning Tree Configuration Menu.



```
                        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.
```

Figure 3-42. Spanning Tree Configuration Menu

Table 3-37 describes the Spanning Tree Configuration Menu options.

Table 3-37. Spanning Tree Configuration Menu Options

Option	Description
Spanning Tree Port Configuration	Displays the Spanning Tree Port Configuration screen (see "Spanning Tree Port Configuration" on page 3-104).
Display Spanning Tree Switch Settings	Displays the Spanning Tree Switch Settings screen (see "Display Spanning Tree Switch Settings" on page 3-108).
Return to Main Menu	Exits the Spanning Tree Configuration Menu and displays the main menu.

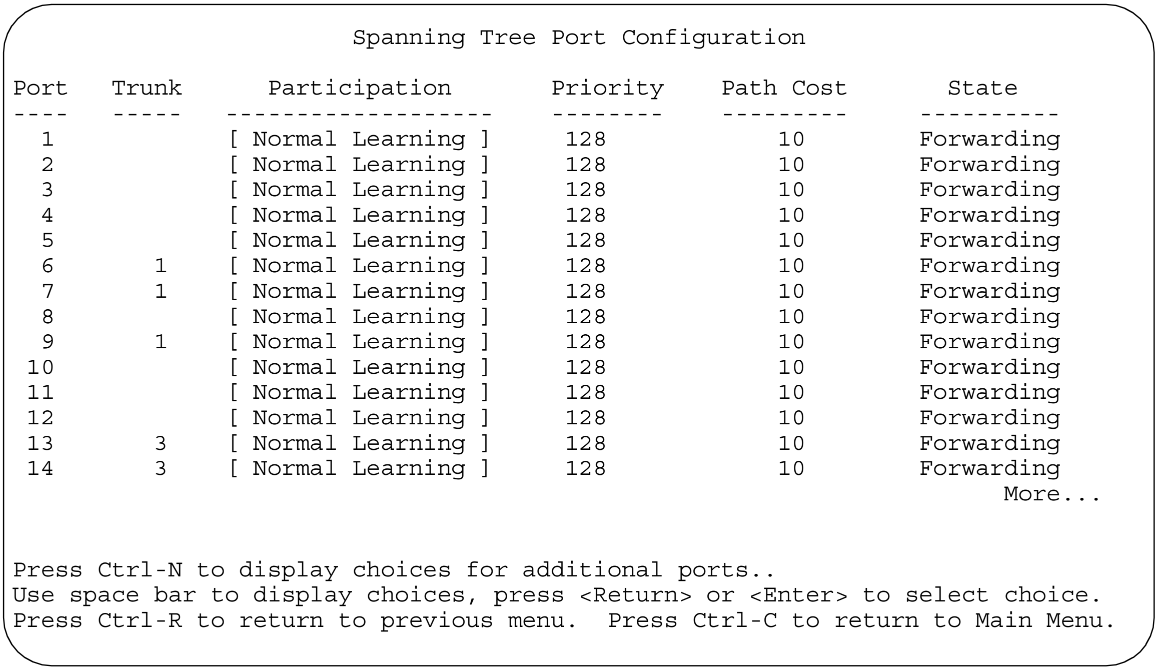
Spanning Tree Port Configuration

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.

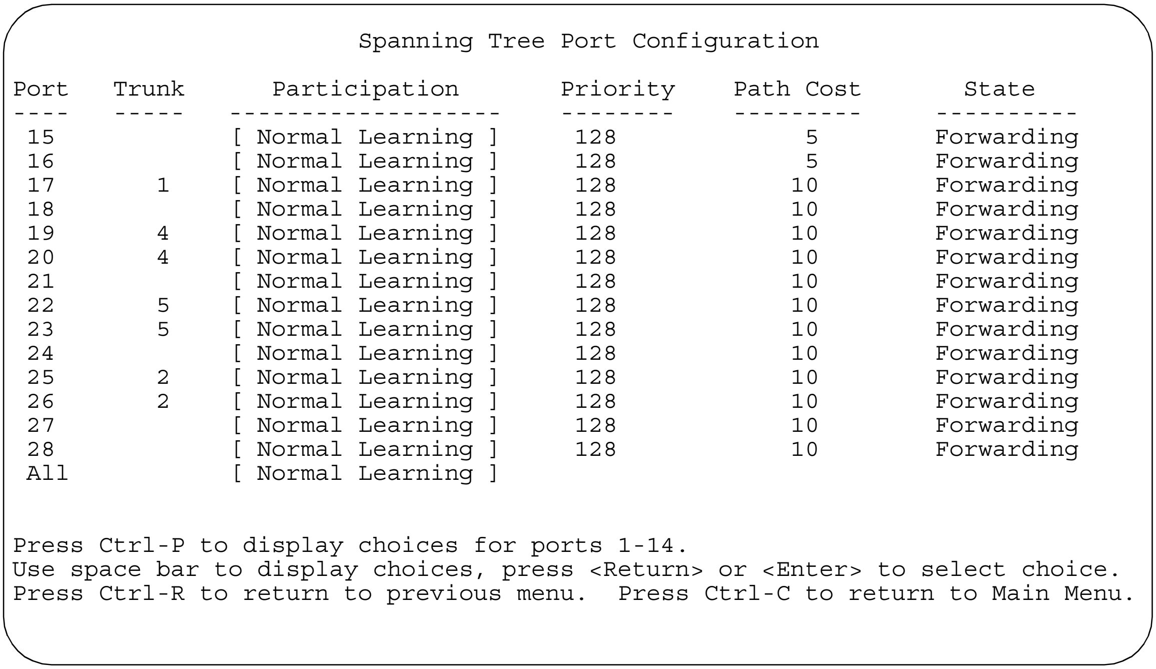
Figures 3-43 and 3-44 show sample port configurations for the two Spanning Tree Port Configuration screens.

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



```
                        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       1    [ Normal Learning ]     128             10       Forwarding
  7       1    [ Normal Learning ]     128             10       Forwarding
  8            [ Normal Learning ]     128             10       Forwarding
  9       1    [ Normal Learning ]     128             10       Forwarding
 10            [ Normal Learning ]     128             10       Forwarding
 11            [ Normal Learning ]     128             10       Forwarding
 12            [ Normal Learning ]     128             10       Forwarding
 13       3    [ Normal Learning ]     128             10       Forwarding
 14       3    [ 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 3-43. Spanning Tree Port Configuration Screen (1 of 2)



```
                        Spanning Tree Port Configuration

Port   Trunk      Participation       Priority    Path Cost       State
----   -----   -------------------    --------    ---------     ----------
 15            [ Normal Learning ]     128              5       Forwarding
 16            [ Normal Learning ]     128              5       Forwarding
 17       1    [ Normal Learning ]     128             10       Forwarding
 18            [ Normal Learning ]     128             10       Forwarding
 19       4    [ Normal Learning ]     128             10       Forwarding
 20       4    [ Normal Learning ]     128             10       Forwarding
 21            [ Normal Learning ]     128             10       Forwarding
 22       5    [ Normal Learning ]     128             10       Forwarding
 23       5    [ Normal Learning ]     128             10       Forwarding
 24            [ Normal Learning ]     128             10       Forwarding
 25       2    [ Normal Learning ]     128             10       Forwarding
 26       2    [ Normal Learning ]     128             10       Forwarding
 27            [ Normal Learning ]     128             10       Forwarding
 28            [ Normal Learning ]     128             10       Forwarding
 All           [ 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.
```

Figure 3-44. Spanning Tree Port Configuration Screen (2 of 2)

Table 3-38 describes the Spanning Tree Port Configuration screen fields.

Table 3-38. Spanning Tree Port Configuration Screen Fields

Field	Description
Port	Indicates the switch port numbers that correspond to the field settings in that row of the screen (for example, the field settings in row 2 apply to switch port 2). Note that the settings in the All row (bottom row) affect all switch ports.
Trunk	This read-only field indicates the trunks that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen (see "MultiLink Trunk Configuration" on page 3-61).

(continued)

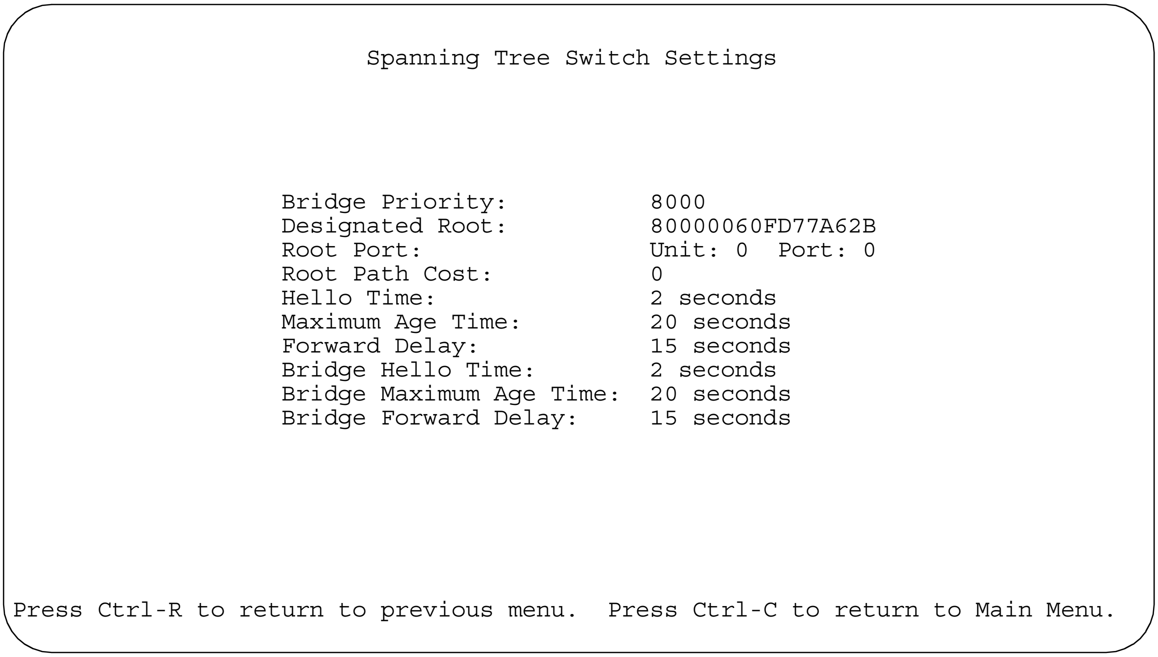
Table 3-38. Spanning Tree Port Configuration Screen Fields *(continued)*

Field	Description	
Participation	Allows you to configure any (or all) of the switch ports for spanning tree participation. When an individual port is a trunk member (see Trunk field), changing this setting for one of the trunk members changes the setting for all members of that trunk. You should consider how this can change your network topology before you change this setting (see “MultiLink Trunking Configuration Rules” on page 1-72). The Fast Learning parameter is the same as Normal Learning, except that the state transition timer is shortened to 2 seconds.	
	Default	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	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	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 Normal Learning or Fast Learning, the port transitions from the Disabled state through the Blocking, Listening, and Learning states before entering the Forwarding state.	
	Default	Topology dependent
	Range	Disabled, Blocking, Listening, Learning, Forwarding

Display Spanning Tree Switch Settings

The Spanning Tree Switch Settings screen (Figure 3-45) allows you to view spanning tree parameter settings for the BayStack 350 switch.

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



```
                         Spanning Tree Switch Settings




                   Bridge Priority:          8000
                   Designated Root:          80000060FD77A62B
                   Root Port:                Unit: 0  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.
```

Figure 3-45. Spanning Tree Switch Settings Screen

Table 3-39 describes the Spanning Tree Switch Settings parameters.

Table 3-39. 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	8000
	Range	0 to 65535
Designated Root	Indicates the bridge ID of the root bridge, as determined by the STA.	
	Default	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	0
	Range	0 to 16
Root Path Cost	Indicates the path cost from this switch port to the root bridge.	
	Default	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	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	20 seconds
	Range	6 to 40 seconds

(continued)

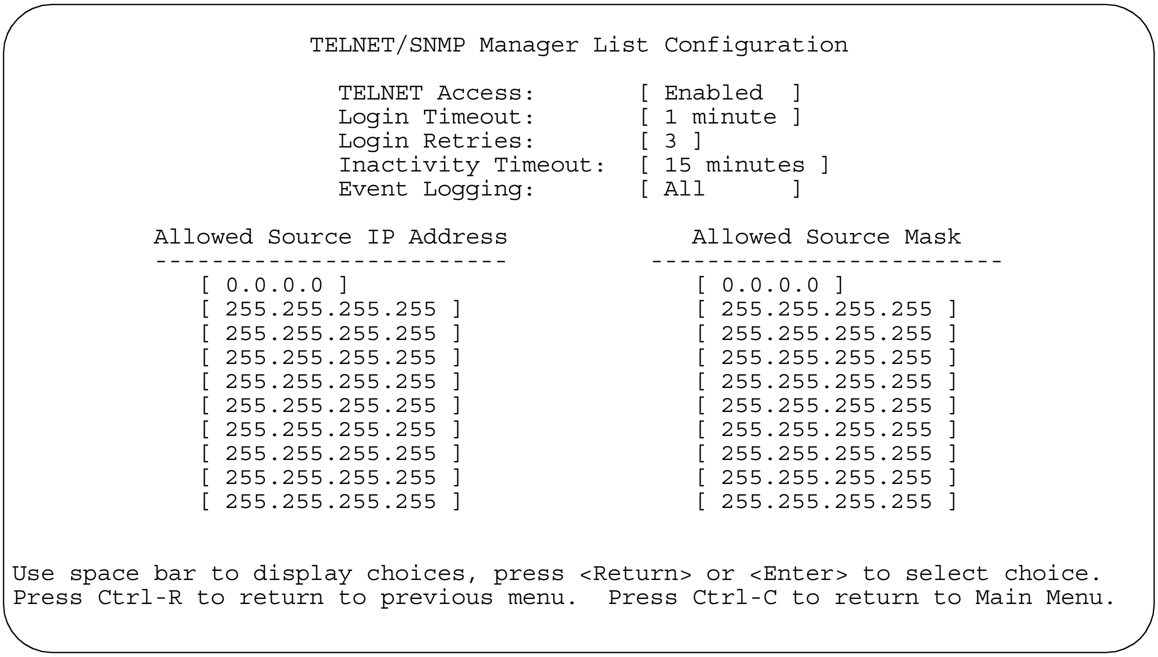
Table 3-39. Spanning Tree Switch Settings Parameters *(continued)*

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	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	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	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	15 seconds
	Range	4 to 30 seconds

TELNET/SNMP Manager List Configuration

The TELNET/SNMP Manager List Configuration screen (Figure 3-46) allows you to specify up to 10 user-assigned host IP addresses that are allowed TELNET and SNMP access to the switch. When you set the TELNET Access value to Enabled, you can communicate with the BayStack 350 switch from a remote console terminal and can have up to four active TELNET sessions at one time.

Choose TELNET/ SNMP Mgr List Configuration (or press t) from the main menu to open the TELNET/ SNMP Manager List Configuration screen.



```
                      TELNET/SNMP Manager List 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.
```

Figure 3-46. TELNET/SNMP Manager List Configuration Screen

Table 3-40 describes the TELNET/ SNMP Manager List Configuration screen fields.

Table 3-40. TELNET/SNMP Manager List Configuration Screen Fields

Field	Description
TELNET Access	Allows remote access to the CI through a TELNET session. Default Enabled Range Enabled, Disabled
Login Timeout	Specifies the amount of time you have to enter the correct password at the console-terminal prompt. Default 1 minute Range 0 to 10 minutes (0 indicates “no timeout”)
Login Retries	Specifies the number of times you can enter an incorrect password at the console-terminal prompt before the session is terminated. Default 3 Range 1 to 100
Inactivity Timeout	Specifies the amount of time the session can be inactive before it is terminated. Default 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 “Display Event Log” on page 3-120). Default All Range All, None, Accesses, Failures *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.

(continued)

Table 3-40. TELNET/SNMP Manager List Configuration Screen Fields *(continued)*

Field	Description	
Allowed Source IP Address	Specifies up to 10 user-assigned host IP addresses that are allowed TELNET and SNMP access to the switch.	
	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
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	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

The Software Download screen (Figure 3-47) allows you to revise the BayStack 350 switch software image that is located in nonvolatile flash memory.

To download the BayStack 350 switch software image, a properly configured Trivial File Transfer Protocol (TFTP) server must be present in your network, and the switch must have an IP address. (See “IP Configuration” on page 3-9 to learn how to configure the switch’s IP address.)

You can monitor the software download process by observing the BayStack 350 switch LEDs (see “LED Indications During the Download Process” on page 3-116).

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.

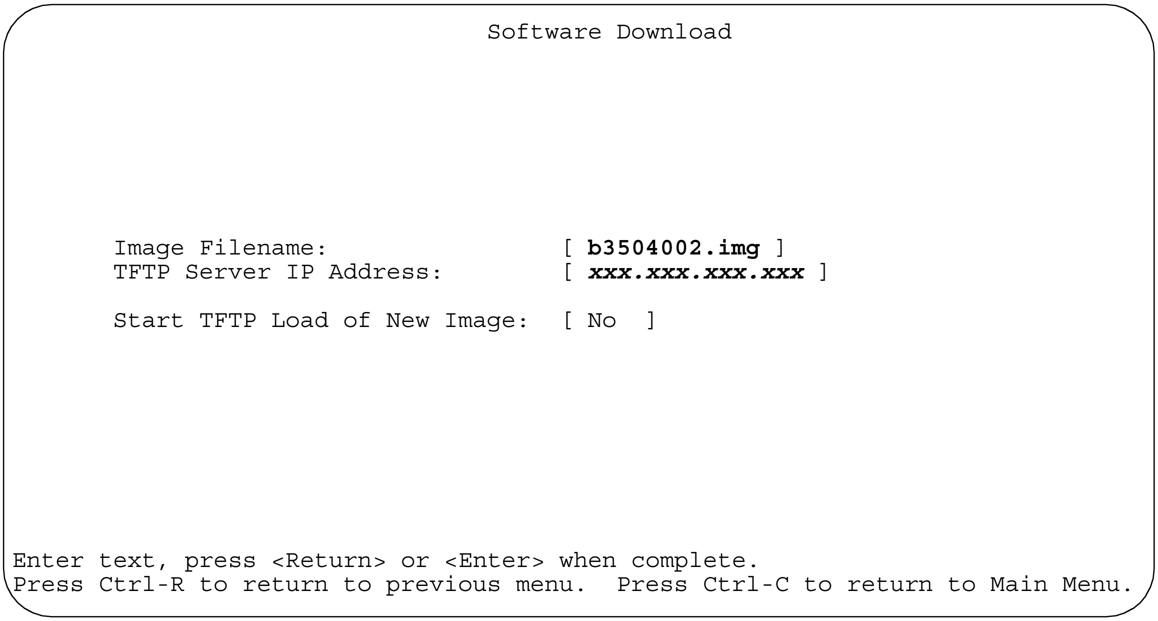
Attention: Ne pas couper l'alimentation de l'appareil pendant le chargement du logiciel. En cas d'interruption, le programme résident peut être endommagé.

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。

Choose Software Download (or press f) from the main menu to open the Software Download screen.



```
                              Software Download






      Image Filename:                        [ b3504002.img ]
      TFTP Server IP Address:                [ xxx.xxx.xxx.xxx ]

      Start TFTP Load of New Image:          [ No  ]







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

Figure 3-47. Software Download Screen

Table 3-41 describes the Software Download screen fields.

Table 3-41. Software Download Screen Fields

Field	Description
Image Filename	The software image load file name (Figure 3-47 shows an example image 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 Zero-length string Range An ASCII string of up to 30 printable characters

(continued)

Table 3-41. Software Download Screen Fields *(continued)*

Field	Description	
TFTP Server IP Address	The IP address of your TFTP load host.	
	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
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	No
	Range	Yes, No

LED Indications During the Download Process

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

Note: If problems occur during the software download process, the Software Download screen displays error codes that define the problem. The error codes are described in Chapter 4, “Troubleshooting.”

When the download process is complete, the switch automatically resets and the new software image initiates a self-test. The BayStack 350 switch Self-Test screen (see Figure 2-11 on page 2-15) briefly displays the results and is followed by the Nortel Networks logo screen. Press [Ctrl]-Y from the Nortel Networks logo screen to access the BayStack 350 switch main menu.

During the download process, the BayStack 350 switch is not operational. You can monitor the progress of the download process by observing the LED indications.

Table 3-42 describes the LED indications during the software download process.

➡ **Note:** The LED indications described in Table 3-42 apply to a 24-port switch model. Although a 12-port switch provides *similar* LED indications, the LED indication sequence is associated within the 12-port range.

Table 3-42. LED Indications During the Software Download Process

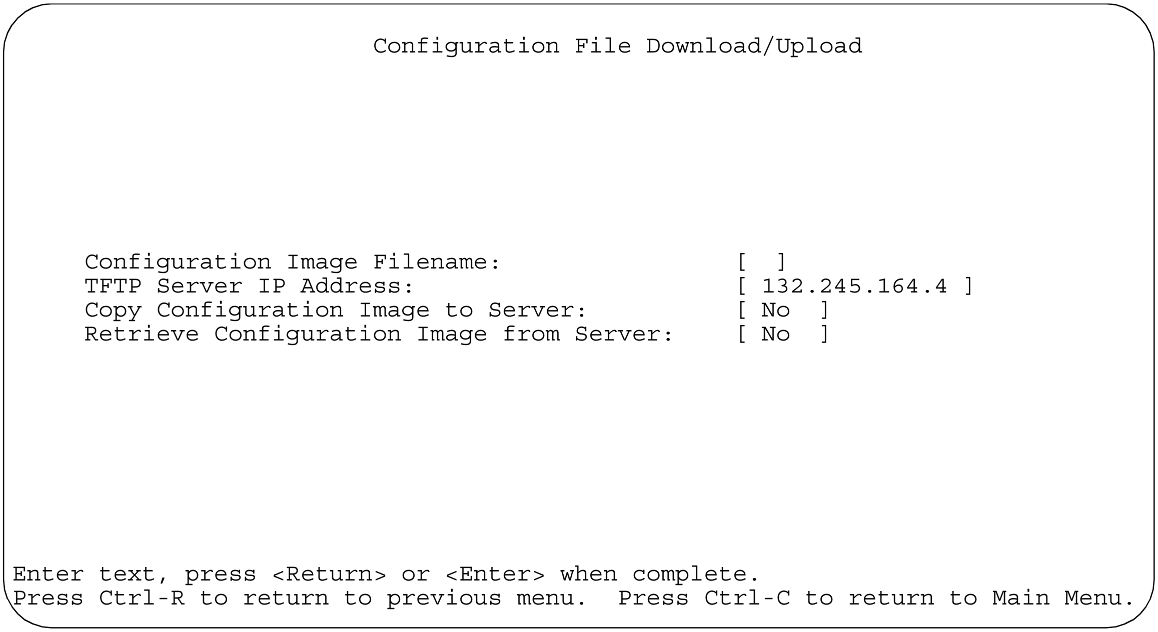
Phase	Description	LED Indications
1	The switch downloads the new software image.	**100 Mb/s port status LEDs (ports 18 to 24 only):** The LEDs begin to turn on in succession beginning with port 24, which indicates the progress of the download process. When LEDs 18 to 24 are all on, the switch has received the new software image successfully.
2	The switch erases the flash memory.	**100 Mb/s port status LEDs (ports 1 to 12 only):** The LEDs begin to turn on in succession beginning with port 1, which indicates that various sectors of the switch's flash memory are being erased. When LEDs 1 to 12 are all on, the switch's flash memory has been erased.
3	The switch programs the new software image into the flash memory.	**100 Mb/s port status LEDs (ports 1 to 8 only):** The LEDs begin to turn on in succession beginning with port 1, which indicates that the new software image is being programmed into the switch's flash memory. When LEDs 1 to 8 are all on, the new software image has been programmed successfully into the switch's flash memory.
4	The switch resets automatically.	After the reset completes, the new software image initiates the switch self-test, which comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress. The results of the self-test are displayed briefly in the Self-Test screen, after which the CI screens appear.

Configuration File

The Configuration File Download/Upload screen (Figure 3-48) allows you to store your switch configuration parameters on a TFTP server.

You can retrieve the configuration parameters and use the retrieved parameters to automatically configure a replacement switch or a group of switches if required. Certain requirements apply when automatically configuring a switch using this feature (see “Requirements” on page 3-119). You must set up the file on your TFTP server and set the file name read/write permission to Enabled before you can save the configuration parameters.

Choose Configuration File (or press g) from the main menu to open the Configuration File Download/Upload screen.



```
                           Configuration File Download/Upload







     Configuration Image Filename:                 [  ]
     TFTP Server IP Address:                       [ 132.245.164.4 ]
     Copy Configuration Image to Server:           [ No   ]
     Retrieve Configuration Image from Server:     [ No   ]









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

Figure 3-48. Configuration File Download/Upload Screen

Table 3-43 describes the Configuration File Download/Upload screen fields.

Table 3-43. 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	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	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	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	No
	Range	Yes, No

Requirements

- The Configuration File feature can be used only to copy *standalone switch configuration parameters to other standalone switches* or to copy *stack configuration parameters to other stack configurations*.

  For example, you cannot duplicate the configuration parameters of a unit in a *stack* configuration and use it to configure a *standalone* switch, such as the BayStack 350 switch.

- A configuration file obtained from a BayStack 350 switch can be used only to configure other BayStack 350 switches that have the same software revision and model type as the donor standalone switch.

  You can check your switch's current software revision using the System Characteristics screen (see "System Characteristics" on page 3-16).
- The configuration file also duplicates any settings that exist for any MDA that is installed in the donor switch.
- If you use the configuration file to configure another BayStack 350 switch that has the same MDA model installed, the configuration file settings will also apply to and override the existing MDA settings.

Although most configuration parameters are saved to the configuration file, certain parameters are not saved (Table 3-44).

Table 3-44. Parameters Not Saved to the Configuration File

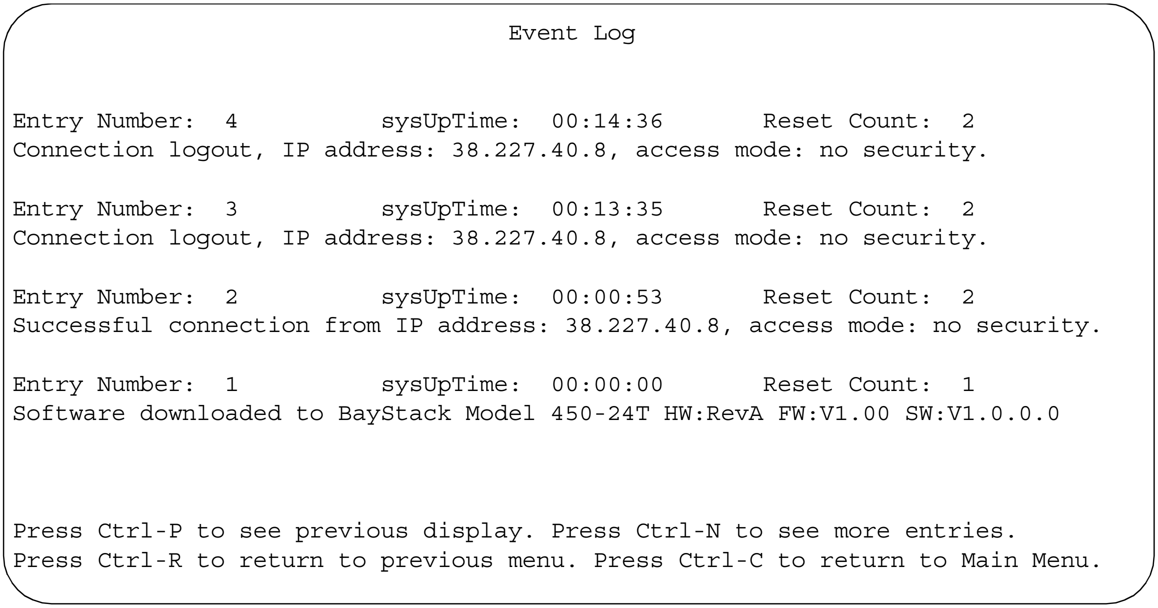
These parameters are not saved:	Used in this screen:	See page:
In-Band Switch IP Address In-Band Subnet Mask Default Gateway	IP Configuration/Setup	3-9
Console Read-Only Switch Password Console Read-Write Switch Password	Console/Comm Port Configuration	3-102
Configuration Image Filename TFTP Server IP Address	Configuration File Download/Upload	3-118

Display Event Log

This section describes the various functions of the Event Log screen (Figure 3-49).

➡ **Note:** This screen does not refresh dynamically to show new entries. To refresh the screen, press [Ctrl]-P.

Choose Display Event Log (or press e) from the main menu to open the Event Log screen.



```
                                   Event Log


Entry Number:  4          sysUpTime:  00:14:36       Reset Count:  2
Connection logout, IP address: 38.227.40.8, access mode: no security.

Entry Number:  3          sysUpTime:  00:13:35       Reset Count:  2
Connection logout, IP address: 38.227.40.8, access mode: no security.

Entry Number:  2          sysUpTime:  00:00:53       Reset Count:  2
Successful connection from IP address: 38.227.40.8, access mode: no security.

Entry Number:  1          sysUpTime:  00:00:00       Reset Count:  1
Software downloaded to BayStack Model 450-24T HW:RevA FW:V1.00 SW:V1.0.0.0



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

Figure 3-49. Event Log Screen

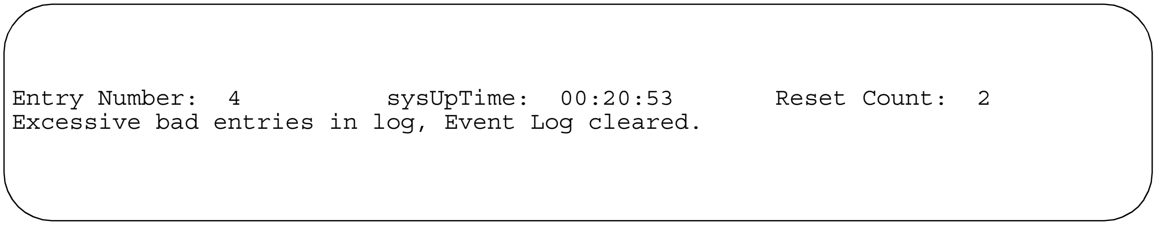
The Event Log screen provides the following information:

- **Software download:** Indicates the new software version.
- **Authentication failure:** Indicates any attempted SNMP **get** or **set** access that specified an invalid community string.
- **TELNET session status:** Indicates various TELNET events. (For details on configuring this feature, see "TELNET/SNMP Manager List Configuration" on page 3-111.)
- **Operational exception:** Indicates that the microprocessor has received an exception at the specified vector number and dumps stack registers.
- **Excessive bad entries:** Displays excessive bad entries detected by firmware.
- **Write threshold:** Displays event entries that exceeded the write threshold.
- **Flash update:** Displays status of flash updates.

Excessive Bad Entries

If the firmware detects excessive bad entries in the event log's flash memory (errors exceeding 75 percent of the memory buffer), the event log is cleared (all entries are discarded) and an event entry is displayed in the Event Log screen.

Figure 3-50 shows an example of the event log entry for this type of event.



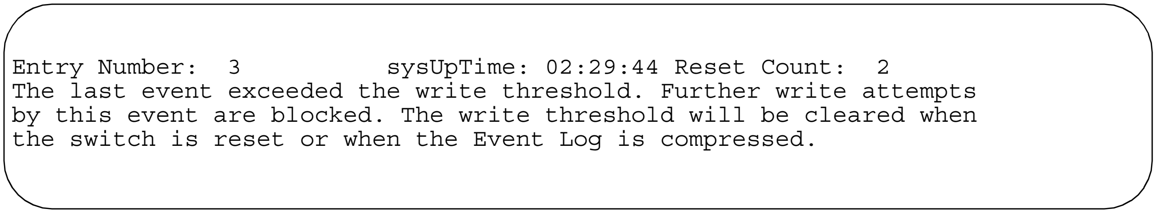
```
Entry Number:  4          sysUpTime:  00:20:53       Reset Count:  2
Excessive bad entries in log, Event Log cleared.
```

Figure 3-50. Sample Event Log Entry Showing Excessive Bad Entries

Write Threshold

To extend the lifetime of the event log's flash memory, a write threshold is set for each event entered in flash memory. The write threshold is 20 entries for each event. If any event exceeds the write threshold, an event entry is displayed in the Event Log screen.

Figure 3-51 shows an example of the event log entry for this type of event.



```
Entry Number:  3          sysUpTime: 02:29:44 Reset Count:  2
The last event exceeded the write threshold. Further write attempts
by this event are blocked. The write threshold will be cleared when
the switch is reset or when the Event Log is compressed.
```

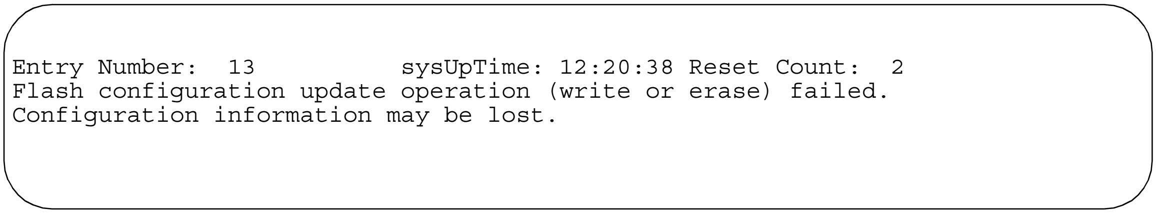
Figure 3-51. Sample Event Log Entry Exceeding the Write Threshold

The write threshold is reset when either of the following occurs:

- The BayStack 350 switch is reset.
- The firmware determines that compression is required for maintenance of the event log's flash memory.

Flash Update

Figure 3-52 shows an example of the event log entry for this type of event.



```
Entry Number:  13          sysUpTime: 12:20:38 Reset Count:  2
Flash configuration update operation (write or erase) failed.
Configuration information may be lost.
```

Figure 3-52. Sample Event Log Entry Showing Flash Update Status

Save Current Settings

The Save Current Settings option (accessed from the main menu) allows you to save your current configuration settings *without resetting your switch*.

This option is followed by a screen prompt to confirm the action. Enter Yes to save your configuration settings; enter No to abort the option.

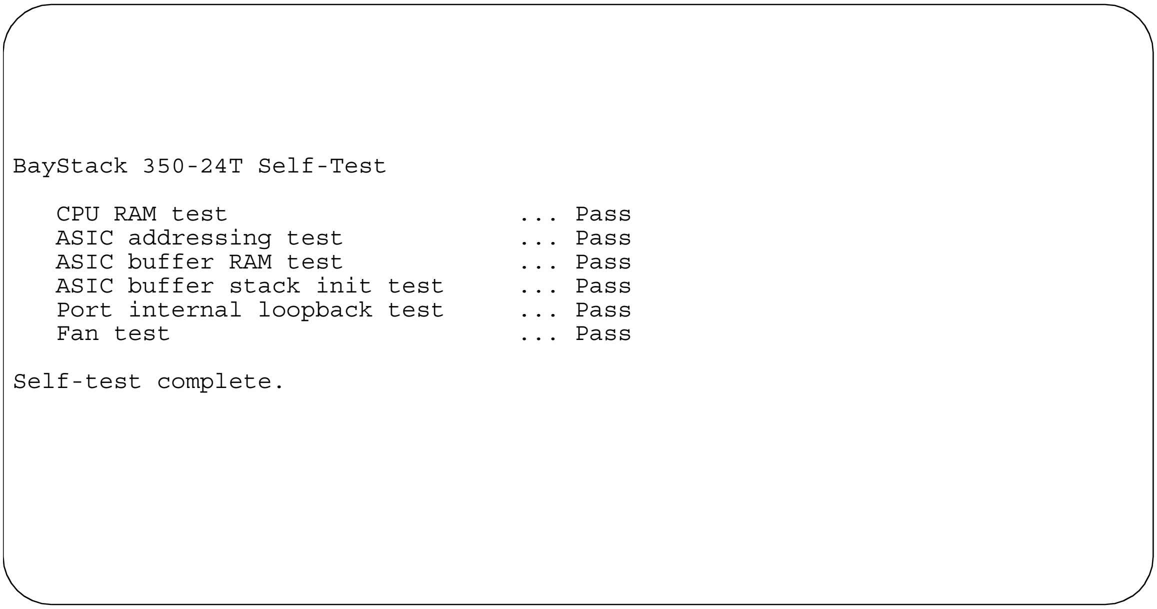
Reset

The Reset option (accessed from the main menu) allows you to reset your BayStack 350 switch without erasing any configured switch parameters.

Resetting your switch takes approximately 5 seconds to complete. During this time, your switch initiates a self-test that comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

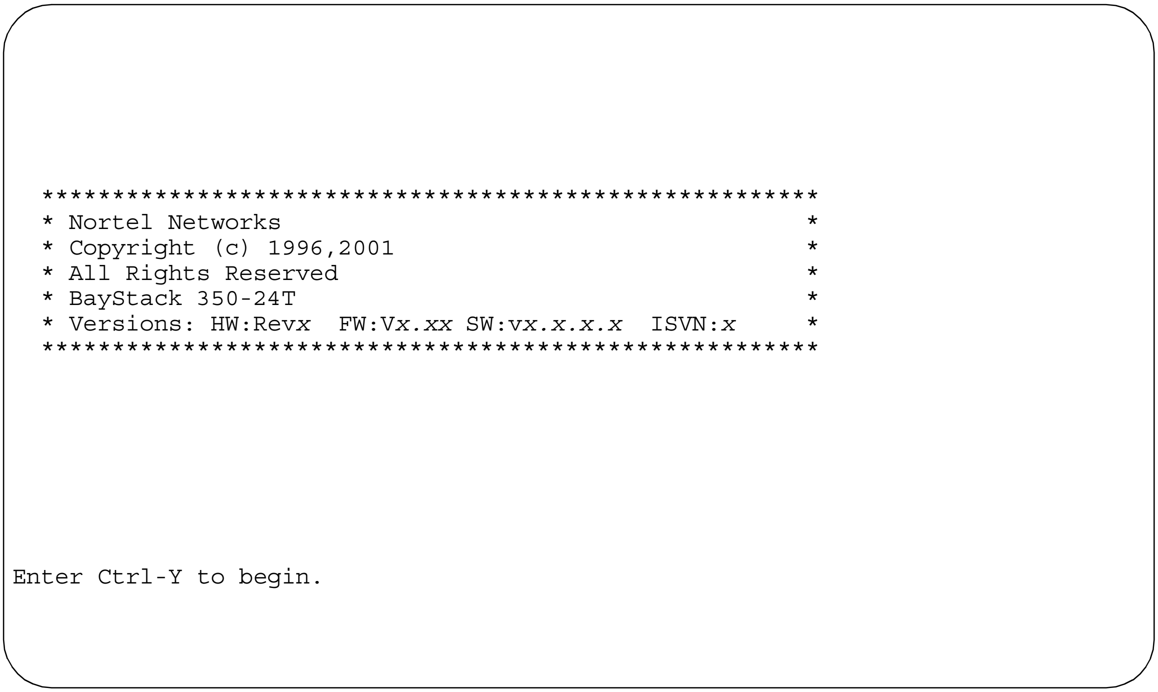
The results of the self-test are displayed briefly (5 or 10 seconds) in the Self-Test screen (Figure 3-53), which is followed by the Nortel Networks logo screen (Figure 3-54).

Note: The Self-Test screen remains displayed only if the self-test detects a fatal error.



```
BayStack 350-24T Self-Test

   CPU RAM test                       ... Pass
   ASIC addressing test               ... Pass
   ASIC buffer RAM test               ... Pass
   ASIC buffer stack init test        ... Pass
   Port internal loopback test        ... Pass
   Fan test                           ... Pass

Self-test complete.
```

Figure 3-53. Self-Test Screen After Resetting the Switch



```
  ******************************************************
  * Nortel Networks                                    *
  * Copyright (c) 1996,2001                            *
  * All Rights Reserved                                *
  * BayStack 350-24T                                   *
  * Versions: HW:Revx  FW:Vx.xx SW:vx.x.x.x  ISVN:x     *
  ******************************************************







Enter Ctrl-Y to begin.
```

Figure 3-54. Nortel Networks Logo Screen

Note: The Nortel Networks logo screen for your switch will display the correct model number and the current hardware, firmware, software, and ISVN versions.

Upon successful completion of the power-up self-tests, the switch is ready for normal operation.

To access the BayStack 350 Main Menu, press [Ctrl]-Y.

Reset to Default Settings

Caution: If you choose the Reset to Default Settings command, 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].

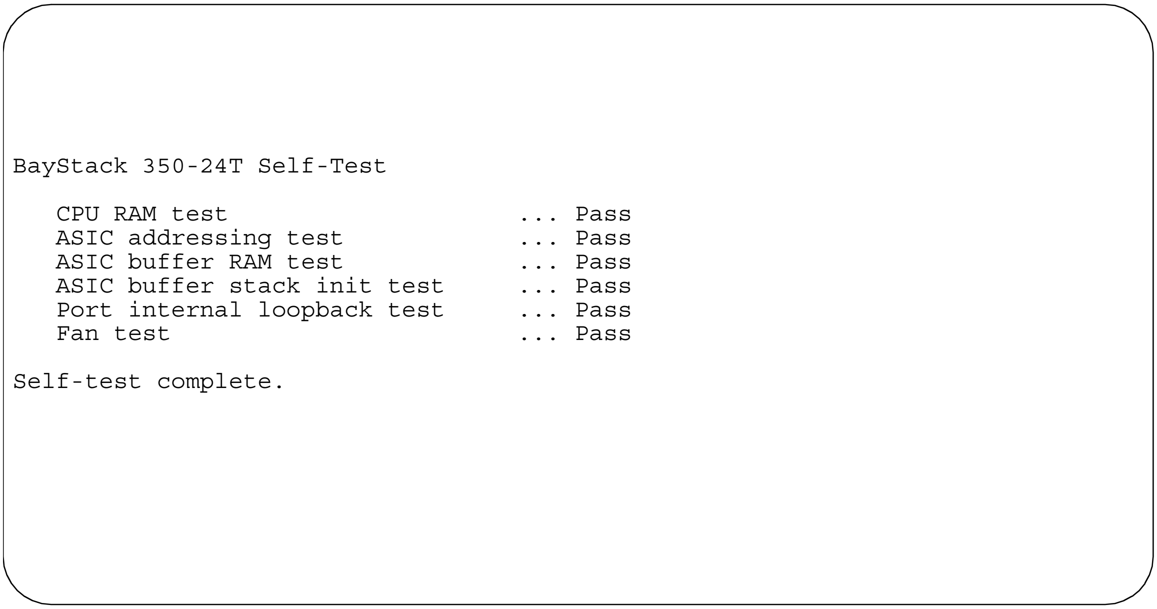
Attenzione: Nel caso in cui si selezioni la reimpostazione dei valori di default, tutte le impostazioni configurate verranno sostituite dai default di fabbrica premendo il tasto [Invio].

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。

The Reset to Default Settings option (accessed from the main menu) allows you to reset the BayStack 350 switch and replace all configured switch parameters with the factory default settings. For a list of the factory default settings, see Appendix G, “Default Settings.”

The Reset to Default Settings option takes approximately 5 seconds to complete. During this time, the switch initiates a self-test that comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

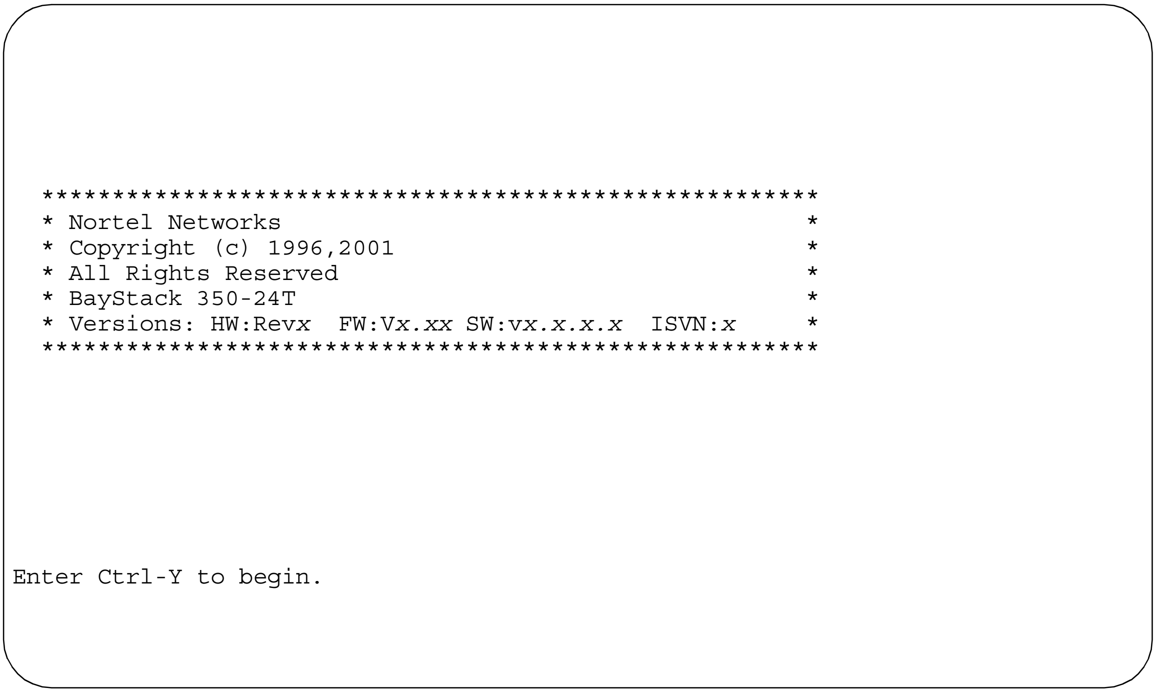
The results of the self-test are displayed briefly (5 or 10 seconds) in the Self-Test screen (Figure 3-55), which is followed by the Nortel Networks logo screen (Figure 3-56).



```
BayStack 350-24T Self-Test

   CPU RAM test                      ... Pass
   ASIC addressing test              ... Pass
   ASIC buffer RAM test              ... Pass
   ASIC buffer stack init test       ... Pass
   Port internal loopback test       ... Pass
   Fan test                          ... Pass

Self-test complete.
```

Figure 3-55. Self-Test Screen After Resetting to Default Settings

Note: The Self-Test screen remains displayed only if the self-test detects a fatal error.



```
  *******************************************************
  * Nortel Networks                                     *
  * Copyright (c) 1996,2001                             *
  * All Rights Reserved                                 *
  * BayStack 350-24T                                    *
  * Versions: HW:Revx  FW:Vx.xx SW:vx.x.x.x  ISVN:x     *
  *******************************************************









Enter Ctrl-Y to begin.
```

Figure 3-56. Nortel Networks Logo Screen After Resetting to Default Settings

> ➡ **Note:** The Nortel Networks logo screen for your switch will display the correct model number and the current hardware, firmware, software, and ISVN versions.

Upon successful completion of the power-up self-tests, the switch is ready for normal operation.

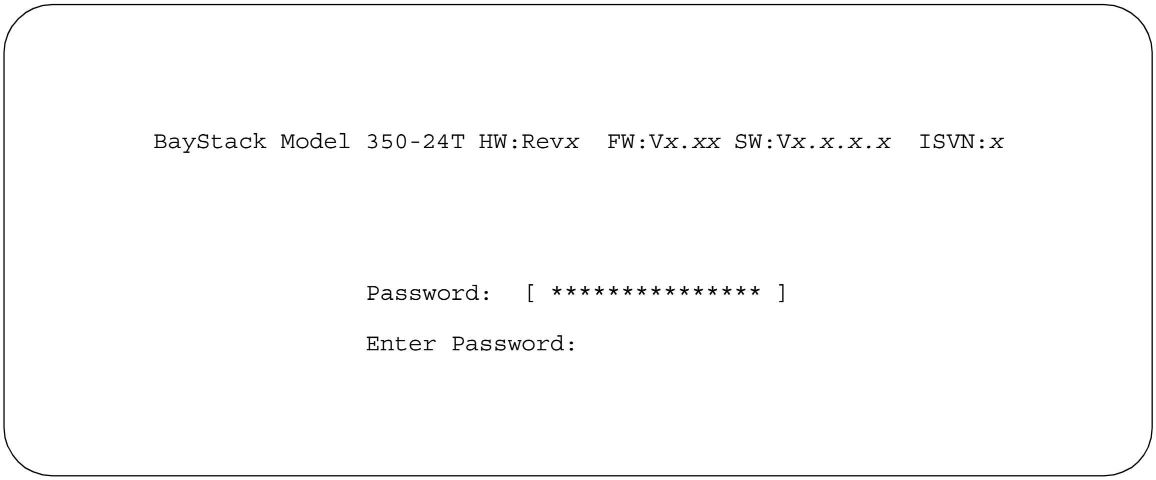
To access the BayStack 350 Main Menu, press [Ctrl]-Y.

Logout

The Logout option (accessed from the main menu) allows you to terminate the session from a password-protected console terminal or from an active TELNET session.

The Logout option works as follows:

- If you are accessing the BayStack 350 switch through a TELNET session, the Logout option terminates the TELNET session.
- If you are accessing the BayStack 350 switch through a password-protected console terminal (connected to the console/comm port on the switch), the Logout option displays the console-terminal password prompt (Figure 3-57). If RADIUS authentication is enabled, the Password field is preceded by a Username field. You must enter the correct password (and username, if applicable) to access the CI screens.



```
BayStack Model 350-24T HW:Revx  FW:Vx.xx SW:Vx.x.x.x  ISVN:x



               Password:  [ *************** ]

               Enter Password:
```

Figure 3-57. Password Prompt Screen

You can specify whether a password is required for the TELNET session or the console terminal using the Console/Comm Port Configuration screen (see "Hardware Unit Information" on page 3-102).

If the console terminal is not password protected, the system ignores the Logout option.

Chapter 4
Troubleshooting

This chapter explains how to isolate and diagnose problems with the BayStack 350 switch.

This chapter covers the following topics:

- "Interpreting the LEDs" (page 4-2)
- "Diagnosing and Correcting the Problem" (page 4-3)
- "Software Download Error Codes" (page 4-7)

The chapter topics lead you through a logical process for troubleshooting the BayStack 350 switch. For example, because LEDs provide visual indications of certain problems, refer to "Interpreting the LEDs" on page 4-2 to understand the various states (see Table 4-1) that your switch LEDs can exhibit during normal operation.

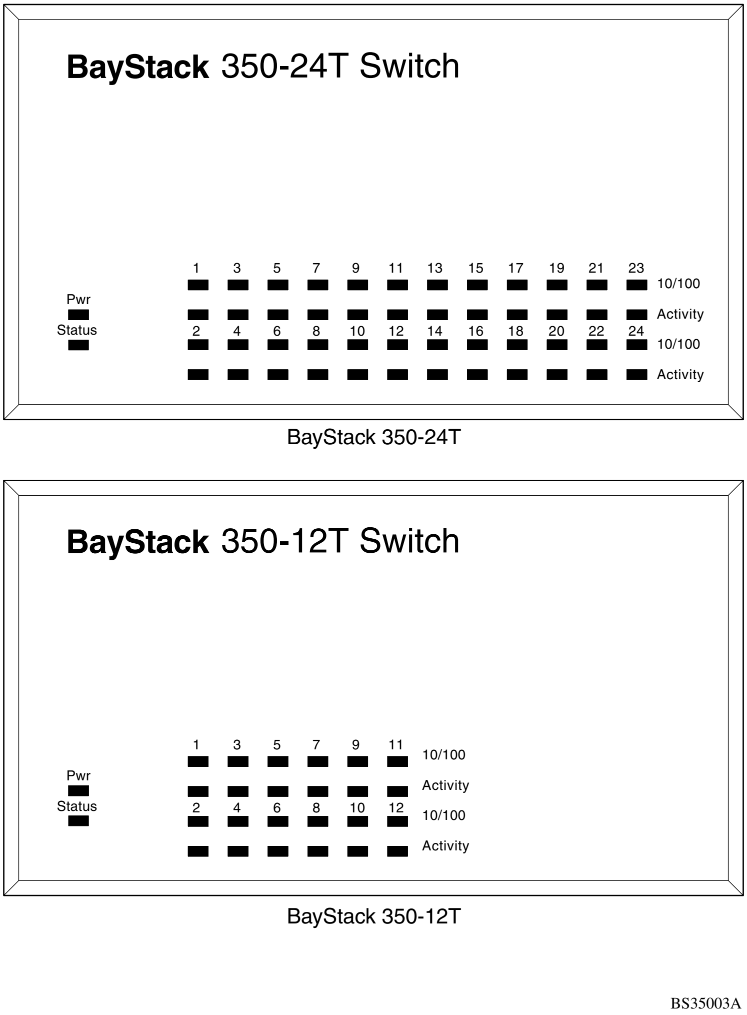
➡ **Note:** The LED Display panel configuration for your switch may be different than shown in Figure 4-1, depending on the date of manufacturing (see the note in "10BASE-T/100BASE-TX Port Connectors" on page 1-4).

For more help in determining the problem, "Diagnosing and Correcting the Problem" on page 4-3 describes symptoms and corrective actions (see Table 4-2) you can perform to resolve specific problems. Subsequent sections give step-by-step procedures to correct the problems.

Interpreting the LEDs

Figure 4-1 shows the BayStack 350-24T and BayStack 350-12T LED display panels.

Table 4-1 describes the LEDs.



BayStack 350-24T

BayStack 350-12T

Figure 4-1. BayStack 350 LED Display Panels

Table 4-1. LED Descriptions

Label	Type	Color	State	Meaning
Pwr	Power status	Green	On	DC power is available to the switch’s internal circuitry.
			Off	No AC power to switch, or power supply failed.
Status	System status	Green	On	Self-test passed successfully and switch is operational.
			Blinking	A nonfatal error occurred during the self-test.
			Off	The switch failed the self-test.
10/100	10/100 Mb/s port speed indicator	Green	On	The corresponding port is set to operate at 100 Mb/s and the link is good.
		Green	Blinking	The corresponding port has been disabled by software.
		Yellow	On	The corresponding port is set to operate at 10 Mb/s and the link is good.
		Yellow	Blinking	The corresponding 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.

Diagnosing and Correcting the Problem

Before you perform the problem-solving steps in this section, cycle the power to the BayStack 350 switch (disconnect and then reconnect the AC power cord); then, verify that the switch follows the normal power-up sequence.

⚠ **Warning:** To avoid bodily injury from hazardous electrical current, never remove the top cover of the device. There are no user-serviceable components inside.

⚠ **Vorsicht:** Um Verletzungsgefahr durch einen elektrischen Stromschlag auszuschließen, nehmen Sie niemals die obere Abdeckung vom Gerät ab. Im Geräteinnern befinden sich keine Komponenten, die vom Benutzer gewartet werden können.

Avertissement: Pour éviter tout risque d'électrocution, ne jamais retirer le capot de l'appareil. Cet appareil ne contient aucune pièce accessible par l'utilisateur.

Advertencia: A fin de evitar daños personales por corrientes eléctricas peligrosas, no desmonte nunca la cubierta superior de este dispositivo. Los componentes internos no son reparables por el usuario.

Avvertenza: Per evitare lesioni fisiche dovute a scariche pericolose di corrente, non rimuovere mai il coperchio superiore del dispositivo. I componenti interni non possono essere manipolati dall'utente.

警告：危険な電流から身体を保護するために、ディバイスの上部カバーを決して取り外さないでください。内部には、ユーザが扱うコンポーネントはありません。

Normal Power-Up Sequence

In a normal power-up sequence, the LEDs appear as follows:

1. After power is applied to the switch, the Pwr (Power) LED turns on within 5 seconds.
2. The switch initiates a self-test, during which the port LEDs display various patterns to indicate the progress of the self-test.
3. Upon successful completion of the self-test (within 10 seconds after power is applied), the Status LED turns on.
4. The remaining port LEDs indicate their operational status, as described in Table 4-2.

Table 4-2. Corrective Actions

Symptom	Probable cause	Corrective action
All LEDs are off.	The switch is not receiving AC power.	Verify that the AC power cord is fastened securely at both ends and that power is available at the AC power outlet.
	The fans are not operating or the airflow is blocked, causing the unit to overheat.	Verify that there is sufficient space for adequate airflow on both sides of the switch. **Note:** Operating temperature for the switch must not exceed 40°C (104°F). The switch should not be placed in the 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" on page 4-6.
The Status LED is off.	A fatal error was detected by the self-test.	Cycle the power to the switch (disconnect and then reconnect the AC power cord). If the problem persists, replace the switch.
The Status LED is blinking.	A nonfatal error occurred during the self-test.	Cycle the power to the switch (disconnect and then reconnect the AC power cord). If the problem persists, contact the Nortel Networks Technical Solutions Center.
When connecting a console/terminal to an operating switch through the switch's serial Comm Port, the console/terminal displays a blank screen.	This is a normal condition.	Press [Ctrl]-C to refresh the screen.

Port Connection Problems

Port connection problems can usually be traced to a poor cable connection or an improper connection of the port cables at either end of the link. These types of problems can be remedied by making sure that the cable connections are secure and that the cables are connected to the correct ports at both ends of the link.

Port connection problems can also be traced 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 350 switch negotiates port speeds according to the IEEE 802.3u autonegotiating standard. The switch adjusts (autonegotiates) its port speed and duplex mode to match the best service provided by the connected station, up to 100 Mb/s in full-duplex mode.

- If the connected station uses a form of autonegotiation that is not compatible with the IEEE 802.3u autonegotiating standard, the BayStack 350 switch cannot negotiate a compatible mode for correct operation.
- If the autonegotiation feature is not present or is not enabled at the connected station, the BayStack 350 switch may not be able to determine the correct duplex mode.

In both situations, the BayStack 350 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, follow these steps:

1. **Use the Port Configuration screen to disable autonegotiation for the suspect port (see “Port Configuration” on page 3-56).**
2. **Manually set the Speed/Duplex field to match the speed/duplex mode of the connected station (see Table 3-20 on page 3-57).**

   You may have to try several settings before you find the correct speed/duplex mode of the connected station.

If the problem persists, follow these additional steps:

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 350 switch port.**

Note: Nortel Networks recommends that you manually set the BayStack 350 switch port to the desired speed/duplex mode when connecting to any of the following Nortel Networks products:

- Nortel Networks 28000 product family
- Nortel Networks 58000 product family
- BayStack Model 302T switch (100 Mb/s port)

Port Interface

Ensure that the devices are connected using the appropriate crossover or straight-through cable (see Appendix F, “Connectors and Pin Assignments”).

Software Download Error Codes

Table 4-3 describes error codes that are associated with the software download process. The error codes appear only on the console screen of the switch that is connected to your TFTP load host during the software download process.

If an error code appears during the download process, perform the appropriate corrective action provided in Table 4-3.

If the suggested corrective action does not resolve the problem, contact your Nortel Networks Technical Solutions Center (see “How to Get Help” in the Preface section of this guide).

Table 4-3. Software Download Error Codes

Error code	Description	Corrective action
2002	TFTP load host failed to respond to ARP request.	Verify that your TFTP load host is operational and check that the connectivity between the switch/stack and the TFTP load host is valid.
2003	Received image failed CRC check.	Verify that the switch software image is valid (not corrupted) and repeat the software download process.
2004	The download process has lost synchronization with the TFTP load host.	Verify that your TFTP load host is operational, then repeat the software download process.
2005	TFTP timeout. The software download has timed out due to network congestion or the load host has stopped responding.	Verify that your TFTP load host is operational, then repeat the software download process.
2006	File access error.	Check that the file name of the software image is correct, and that the file protection is properly set for access.
2007	Non-data packet received from the TFTP load host.	Check that the file name of the software image is correct.
2008	Requested software image is too large.	Check that the file name of the software image is correct, and that you are accessing the appropriate software image for your switch.
2009	Received image failed CRC check.	Verify that the switch software image is valid (not corrupted) and repeat the software download process.
2010	No MAC address found in EEPROM.	Contact the Nortel Networks Technical Solutions Center.

Appendix A
Technical Specifications

This appendix lists the technical specifications for the BayStack 350 10/100/1000 Series Switches.

This appendix covers the following topics:

Environmental

Parameter	Operating Specification	Storage Specification
Temperature	0° to 40°C (32° to 104°F)	-25° to 70°C (-13° to 158°F)
Humidity	85% maximum relative humidity, noncondensing	95% maximum relative humidity, noncondensing
Altitude	3024 m (10,000 ft)	3024 m (10,000 ft)

Electrical

Parameter	Model 350-24T	Model 350-12T
Input Voltage	100 to 240 VAC @ 50 to 60 Hz	100 to 240 VAC @ 50 to 60 Hz
Input Power Consumption	150 W maximum	120 W maximum
Input Volt Amperes Rating	200 VA maximum	150 VA maximum
Input Current	2.0 A @ 100 VAC	1.5 A @ 100 VAC
Maximum Thermal Output	500 BTU/hr	400 BTU/hr

Physical Dimensions

Parameter	Specifications
Height	7.03 cm (2.77 in.)
Width	44.07 cm (17.55 in.)
Depth	38.1 cm (15.0 in.)
Weight	5.26 kg (11.60 lb)

Performance Specifications

Parameter	Specifications
Frame Forward Rate (64-byte packets)	Up to 3 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 • For ATM: 350,000 pps per port maximum (total bidirectional)
Address Database Size	16,000 entries at line rate (32,000 entries without flooding)
Addressing	48-bit MAC address
Frame Length	64 to 1518 bytes (IEEE 802.1Q Untagged) 64 to 1522 bytes (IEEE 802.1Q Tagged)

Network Protocol and Standards Compatibility

- IEEE 802.1p (Prioritizing)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.3 10BASE-T (ISO/IEC 8802-3, Clause 14)
- IEEE 802.3u 100BASE-FX (ISO/IEC 8802-3, Clause 26)
- IEEE 802.3u 100BASE-TX (ISO/IEC 8802-3, Clause 25)
- IEEE 802.3x (Full Duplex operation)
- IEEE 802.3z (Gigabit plus Flow Control)

Data Rate

- 10 Mb/s Manchester encoded or 100 Mb/s 4B/5B encoded

Interface Options

- 10BASE-T/100BASE-TX -- RJ-45 (8-pin modular) connectors for MDI-X interface
- 100BASE-FX Fiber -- SC and MT-RJ connectors for switched 100 Mb/s (100BASE-FX) connections over 50/125 and 62.5/125 micron multimode fiber optic cable (2 km/1.2 mi maximum distance)
- 1000BASE-SX (Shortwave Gigabit Fiber) MDA -- SC connectors for shortwave 850 nm fiber optic connections over multimode (550 m/1,805 ft) fiber optic cable
- 1000BASE-LX (Longwave Gigabit Fiber) MDA -- SC connectors for longwave 1300 nm fiber optic connections over single-mode (5 km/3.1 mi) or multimode (550 meter/1,805 ft) fiber optic cable
- ATM -- SC connectors for dual 155 Mb/s OC-3 connections over 8.5/125 µm single-mode (20 km/12.4 mi) or 62.5/125 µm multimode (2 km/1.24 mi) fiber optic cable

Safety Agency Certification

- UL Listed (UL 1950)
- IEC 950/EN60950
- C22.2 No. 950 (cUL)
- UL-94-V1 flammability requirements for PC board

Electromagnetic Emissions

- 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

- EN50082-1:1997

Declaration of Conformity

The Declaration of Conformity for the BayStack 350 switches complies with ISO/IEC Guide 22 and EN45014. The declaration identifies the product models, the Nortel Networks name and address, and the specifications recognized by the European community.

As stated in the Declaration of Conformity, the BayStack 350 switches comply with the provisions of Council Directives 89/336/EEC and 73/23/EEC.

Appendix B
Gigabit Fiber Optical Characteristics

The Uplink/Expansion Module on the BayStack 350 switch supports 1000BASE-X (Gigabit Ethernet) MDAs. This appendix describes the optical characteristics of the 1000BASE-X MDAs. See Appendix C, “Media Dependent Adapters,” for more information about MDAs.

This appendix covers the following topics:

- “1000BASE-SX Models” (page B-1)
- “1000BASE-LX Models” (page B-4)

1000BASE-SX Models

The 450-1SX and 450-1SR MDAs provide 1000BASE-SX (850 nanometers, short wavelength, Gigabit Ethernet) connectivity. The 450-1SX provides one 1000BASE-SX port. The 450-1SR provides one 1000BASE-SX port and one LinkSafe redundant port.

Operating Range

Table B-1 lists the operating range for the 1000BASE-SX models.

Table B-1. Operating Range for 1000BASE-SX

Fiber Type	Modal Bandwidth @ 850 Nanometers with Minimum Overfilled Launch (MHz · Km)	Minimum Range (Meters)
62.5 um MMF	160	2 to 220
62.5 um MMF	200	2 to 275

(continued)

Table B-1. Operating Range for 1000BASE-SX *(continued)*

Fiber Type	Modal Bandwidth @ 850 Nanometers with Minimum Overfilled Launch (MHz · Km)	Minimum Range (Meters)
50 um MMF	400	2 to 500
50 um MMF	500	2 to 550
10 um MMF	Not supported	Not supported

Transmit Characteristics

Table B-2 lists the transmit characteristics for the 1000BASE-SX models.

Table B-2. 1000BASE-SX Transmit Characteristics

Description	62.5 Micron Multimode Fiber	50 Micron Multimode Fiber	Units
Transmitter type	Shortwave Laser	Shortwave Laser	
Signaling speed	1.25 ± 100 ppm	1.25 ± 100 ppm	GBd
Wavelength (l, range)	770 to 860	770 to 860	nm
T rise/T fall (maximum; 20% - 80%; > 830 nm)	0.26	0.26	ns
T rise/T fall (maximum; 20% - 80%; < = 830 nm)	0.21	0.21	ns
RMS spectral width (maximum)	0.85	0.85	nm
Average launch power (maximum)[1]	See footnote 1	See footnote 1	dBm
Average launch power (minimum)	– 9.5	– 9.5	dBm
Average launch power of OFF transmitter (maximum)[2]	– 30	– 30	dBm
Extinction ratio (minimum)	9	9	dB
RIN (maximum)	– 117	– 117	dB/Hz
Coupled Power Ratio (CPR) minimum [3]	9 < CPR	9 < CPR	db

[1] The 1000BASE-SX launch power shall be the lesser of the class 1 safety limit, as defined by the IEEE 802.3z standard, Clause 38.7.2, or the average receive power (maximum), as defined in Table B-3.

[2] Examples of an OFF transmitter are: no power supplied to the PMD, laser shutdown for safety conditions, activation of a “transmit disable” or other optional laser shutdown conditions. During all conditions when the PMA is powered, the AC signal (data) into the transmit port will be valid encoded 8B/10B patterns (this is a requirement of the PCS layers), except for short durations during system power-on-reset or diagnostics when the PMA is placed in a loopback mode.

[3] Avoid radial overfilled launches even if the launch parameters are within the CPR range.

Receive Characteristics

Table B-3 lists the receive characteristics for the 1000BASE-SX models.

Table B-3. 1000BASE-SX Receive Characteristics

Description	62.5 Micron Multimode Fiber	50 Micron Multimode Fiber	Units
Signaling Speed (range)	1.25 ± 100 ppm	1.25 ± 100 ppm	GBd
Wavelength (range)	770 to 860	770 to 860	nm
Average receive power (maximum)	0	0	dBm
Receive sensitivity	– 17	– 17	dBm
Return loss (minimum)	12	12	dB
Stressed receive sensitivity [1], [2]	– 12.5	– 13.5	dBm
Receive electrical 3 dB upper cutoff frequency (maximum)	1500	1500	MHz
Vertical eye-closure penalty [3]	2.60	2.20	dB

[1] Measured with conformance test signal at TP3 for BER = 10^{-12} at the eye center.

[2] Measured with a transmit signal having a 9 dB extinction ratio. If you use another extinction ratio, correct the stressed receive sensitivity according to the extinction ratio penalty.

[3] Vertical eye-closure penalty is a test condition for measuring stressed receive sensitivity. It is not a required characteristic of the receiver.

Worst-Case Power Budget and Penalties

Table B-4 lists the worst-case power budget and penalties for the 1000BASE-SX models.

Note: The link power penalties (Table B-4) are used for link power budget calculations only. They are not requirements and are not meant to be tested.

Table B-4. Worst-Case 1000BASE-SX Power Budget and Penalties

	62.5 Micron		50 Micron		
Parameter	**Multimode Fiber**		**Multimode Fiber**		**Units**
Modal bandwidth as measured at 850 nm (minimum, overfilled launch)	160	200	400	500	MHz · km
Link power budget	7.5	7.5	7.5	7.5	dB
Operating distance	220	275	500	550	m
Channel insertion loss [1], [2]	2.38	2.60	3.37	3.56	dB
Link power penalties	4.27	4.29	4.07	3.57	dB
Unallocated margin in link power budget	0.84	0.60	0.05	0.37	dB

[1] Operating distances used to calculate the channel insertion loss are the maximum values specified in Table B-1 on page B-1.

[2] A wavelength of 830 nm is used to calculate channel insertion loss, link power penalties, and unallocated margin.

1000BASE-LX Models

The 450-1LX and 450-1LR MDAs provide 1000BASE-LX (1300 nanometers, long wavelength, Gigabit Ethernet) connectivity. The 450-1LX provides one 1000BASE-LX port. The 450-1LR provides one 1000BASE-LX port and one LinkSafe redundant port.

Operating Range

Table B-5 lists the operating range for the 1000BASE-LX models.

Table B-5. Operating Range for 1000BASE-LX

Fiber Type	Modal Bandwidth @ 1300 Nanometers with Minimum Overfilled Launch (MHz · km)	Minimum Range (Meters)
62.5 um MMF	500	2 to 550
50 um MMF	400	2 to 550
50 um MMF	500	2 to 550
10 um SMF	N/A	2 to 5000

Transmit Characteristics

Table B-6 lists the transmit characteristics for the 1000BASE-LX models.

Table B-6. 1000BASE-LX Transmit Characteristics

Description	62.5 Micron Multimode Fiber	50 Micron Multimode Fiber	10 Micron Single-Mode Fiber	Unit
Transmitter type	Longwave Laser	Longwave Laser	Longwave Laser	
Signaling speed (range)	1.25 ± 100 ppm	1.25 ± 100 ppm	1.25 ± 100 ppm	GBd
Wavelength (range)	1270 to 1355	1270 to 1355	1270 to 1355	nm
T rise /T fall (maximum 20-80% response time)	0.26	0.26	0.26	ns
RMS spectral width (maximum)	4	4	4	nm
Average launch power (maximum)	– 3	– 3	– 3	dBm
Average launch power (minimum)	– 11.5	– 11.5	– 11.0	dBm
Average launch power of OFF transmitter (maximum)	– 30	– 30	– 30	dBm
Extinction ratio (minimum)	9	9	9	dB
RIN (maximum)	– 120	– 120	– 120	dB/Hz
Coupled Power Ratio (CPR)[1]	28 < CPR < 40	12 < CPR < 20	N/A	dB

[1] Due to the dual media (single-mode and multimode) support of the LX transmitter, fulfillment of this specification requires a single-mode fiber offset-launch mode-conditioning patch cord described in IEEE 802.3, Clause 38.11.4 for MMF operation. This patch cord is not used for single-mode operation.

Receive Characteristics

Table B-7 lists the receive characteristics for the 1000BASE-LX models.

Table B-7. 1000BASE-LX Receive Characteristics

Description	Value	Units
Signaling speed (range)	1.25 ± 100 ppm	GBd
Wavelength (range)	1270 to 1355	nm
Average receive power (maximum)	– 3	dBm

(continued)

Table B-7. 1000BASE-LX Receive Characteristics *(continued)*

Description	Value	Units
Receive sensitivity	– 19	dBm
Return loss (minimum)	12	dB
Stressed receive sensitivity [1], [2]	– 14.4	dBm
Receive electrical 3 dB upper cutoff frequency (maximum)	1500	MHz
Vertical eye-closure penalty [3]	2.60	dB

[1] Measured with conformance test signal at TP3 (see IEEE 802.3, Clause 38.6.11) for BER = 10^{-12} at the eye center.

[2] Measured with a transmit signal having a 9 dB extinction ratio. If another extinction ratio is used, the stressed receive sensitivity should be corrected for the extinction ratio penalty.

[3] Vertical eye-closure penalty is a test condition for measuring stressed receive sensitivity. It is not a required characteristic of the receiver.

Worst-Case Power Budget and Penalties

Table B-8 lists the worst-case power budget and penalties for the 1000BASE-LX models.

Note: The link power penalties (Table B-8) are used for link power budget calculations only. They are not requirements and are not meant to be tested.

Table B-8. Worst-Case 1000BASE-LX Power Budget and Penalties

Parameter	62.5 um MMF	50 um MMF		10 um SMF	Unit
Modal bandwidth as measured at 1300 nm (minimum, overfilled launch)	500	400	500	N/A	MHz · km
Link power budget	7.5	7.5	7.5	8.0	dB
Operating distance	550	550	550	5000	m
Channel insertion loss	2.35	2.35	2.35	4.57	dB
Link power penalties	3.48	5.08	3.96	3.27	dB
Unallocated margin in link power budget	1.67	0.07	1.19	0.16	dB

Appendix C
Media Dependent Adapters

This appendix describes the optional media dependent adapters (MDAs) that are supported by your switch. The MDAs can support high-speed connections to servers, shared Fast Ethernet hubs, or backbone devices.

➡ **Note:** The MDAs are *not* hot-swappable. Power down the switch before installing or removing an MDA.

Your BayStack 350 switch supports the following MDAs:

Interface type:	Model:	Refer to:
10BASE-T/100BASE-TX (UTP)	400-4TX MDA	page C-2
100BASE-FX (Multimode fiber)	400-2FX MDA 400-4FX MDA	page C-3
1000BASE-SX (Shortwave gigabit fiber)	450-1SR MDA 450-1SX MDA	page C-6
1000BASE-LX (Longwave gigabit fiber)	450-1LR MDA 450-1LX MDA	page C-9
Asynchronous Transfer Mode (ATM)	450-2M3 MDA 450-2S3 MDA	page C-12
Gigabit Interface Converter (GBIC)	450-1GBIC MDA	page C-15

Nortel Networks is constantly adding new models and features to existing product lines. For a full range of MDAs that are available from Nortel Networks, see your Nortel Networks sales representative.

10BASE-T/100BASE-TX MDA

The 400-4TX MDA (Figure C-1) uses four 10BASE-T/100BASE-TX RJ-45 (8-pin modular) port connectors to attach Ethernet devices. Table C-1 describes the 400-4TX MDA components and LEDs.

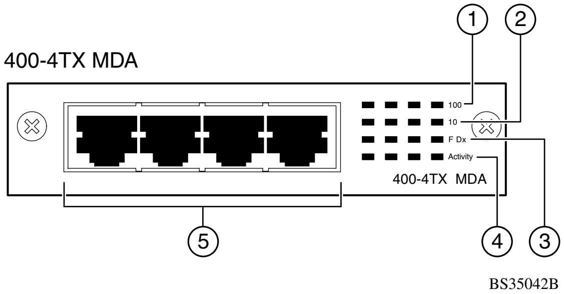


Figure C-1. 400-4TX MDA Front Panel

Table C-1. 400-4TX MDA Components

Item	Label	Description
1	100	100BASE-TX port status LEDs (green): On: The corresponding port is set to operate at 100 Mb/s. Off: The link connection is bad or there is no connection to this port. Blinking: The corresponding port is management disabled.
2	10	10BASE-T port status LEDs (green): On: The corresponding port is set to operate at 10 Mb/s. Off: The link connection is bad or there is no connection to this port. Blinking: The corresponding port is management disabled.
3	F Dx	Full-duplex port status LEDs (green): On: The corresponding port is in full-duplex mode. Off: The corresponding port is in half-duplex mode.
4	Activity	Port activity LEDs (green): Blinking: Indicates the network activity level for the corresponding port. A high level of network activity can cause LEDs to appear to be on continuously.
5		10BASE-T/100BASE-TX RJ-45 (8-pin modular) port connectors.

The RJ-45 ports are configured as media-dependent interface-crossover (MDI-X) connectors. These ports connect over straight cables to the network interface controller (NIC) card in a node or server, similar to a conventional Ethernet repeater hub. If you are connecting to another Ethernet hub or Ethernet switch, you need a crossover cable unless an MDI connection exists on the associated port of the attached device.

The 400-4TX MDA can operate at either 10 Mb/s or 100 Mb/s. The speed is determined through autonegotiation with its connecting device.

For installation instructions, see “Installing an MDA” on page C-17.

100BASE-FX MDAs

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.

警告：光ファイバ装置は目に有害なレーザー光や赤外線を放射することがあります。光ファイバやコネクタ・ポートを覗き込まないでください。光ファイバ・ケーブルは光源に接続されているものと思ってください。

There are two 100BASE-FX models (Figure C-2):

- 400-2FX MDA

  The 400-2FX MDA uses two longwave 1300 nm SC connectors to attach devices over 62.5/125- or 50/125-micron multimode fiber optic cable.

- 400-4FX MDA

  The 400-4FX MDA uses four longwave 1300 nm MT-RJ connectors to attach devices over 62.5/125- or 50/125-micron multimode fiber optic cable.

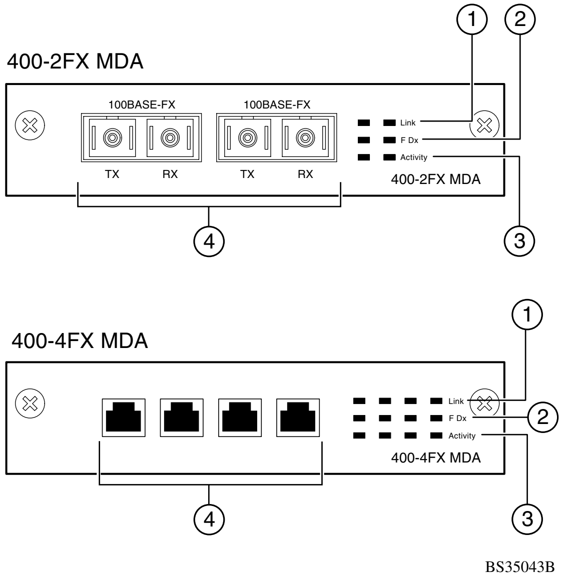


Figure C-2. 100BASE-FX MDA Front Panels

Both models conform to the IEEE 802.3u 100BASE-FX standard and can be used for fiber-based 100 Mb/s connections (2 km/1.2 mi maximum distance) to other compatible Fast Ethernet devices. Single-mode fiber cable is not supported.

Table C-2 describes the 100BASE-FX components and LEDs.

For installation instructions, see "Installing an MDA" on page C-17.

Table C-2. 100BASE-FX MDA Components

Item	Label	Description
1	Link	Communications link LEDs (green): On: Valid communications link established. Off: The communications link connection is bad or there is no connection to this port. Blinking: The corresponding port is management disabled.
2	F Dx	Full-duplex port status LEDs (green): On: The corresponding port is in full-duplex mode. Off: The corresponding port is in half-duplex mode.
3	Activity	Port activity LEDs (green): Blinking: Indicates the network activity level for the corresponding port. A high level of network activity can cause LEDs to appear to be on continuously.
4		100BASE-FX port connectors: • Model 400-2FX uses SC connectors. • Model 400-4FX uses MT-RJ connectors.

1000BASE-SX MDAs

Warning: This is a Class 1 Laser/LED product. It contains a laser light source that can injure your eyes. Never look into an optical fiber or connector port. Always assume that the fiber optic cable or connector is connected to a laser light source.

Vorsicht: Dieses Laser/LED-Produkt der Klasse 1 enthält eine Laserlichtquelle, die zu Augenverletzungen führen kann. Sehen Sie nie in einen Lichtwellenleiter oder Glasfaserstecker-Port. Gehen Sie immer davon aus, daß das Glasfaserkabel oder der Glasfaserstecker an eine Laserlichtquelle angeschlossen ist.

Avertissement: Ceci est un appareil Laser/DEL de Classe 1. Cet appareil contient une source lumineuse à rayons laser dangereuse pour les yeux. Ne regardez jamais directement une fibre optique ou un port de connexion. Agissez toujours comme si le câble de fibres optiques ou le connecteur était relié à une source lumineuse à rayons laser.

Advertencia: Éste es un producto láser/LED de Clase 1. Contiene una fuente de luz láser que puede causar lesiones en los ojos. Nunca mire dentro de un cable o de un puerto de conexión de fibra óptica. Asuma siempre que el cable o el connector de fibra óptica está conectado a una fuerte de luz láser.

Avvertenza: Questo è un produtto laser/LED di Classe 1 e contiene una sorgente luminosa a laser che può danneggiare gli occhi. Non guardare mai all’interno di una port a fibra ottica o di una porta connettore. Dare sempre per scontato che il cavo di fibra ottica o il connettore siano collegati ad una sorgente luminosa a laser.

警告:これはクラス1レーザー/LED製品です。目に障害を与える恐れのあるレーザー光源が含まれています。光ファイバおよびコネクタ・ポートは、のぞき込まないようにしてください。光ファイバ・ケーブルまたはコネクタは、常にレーザー光源に接続されているものと想定してください。

There are two 1000BASE-SX (shortwave gigabit) MDA models (Figure C-3):

- The 450-1SR MDA is a single MAC MDA with a separate redundant Phy (backup Phy port). Only one Phy port can be active at any time. If the active Phy port fails, the redundant Phy port automatically becomes the active port.
- The 450-1SX MDA is a single PHY MDA.

Both models conform to the IEEE 802.3z 1000BASE-SX standard and use shortwave 850 nm fiber optic connectors to connect devices over multimode (550 meter/1,805 ft) fiber optic cable.

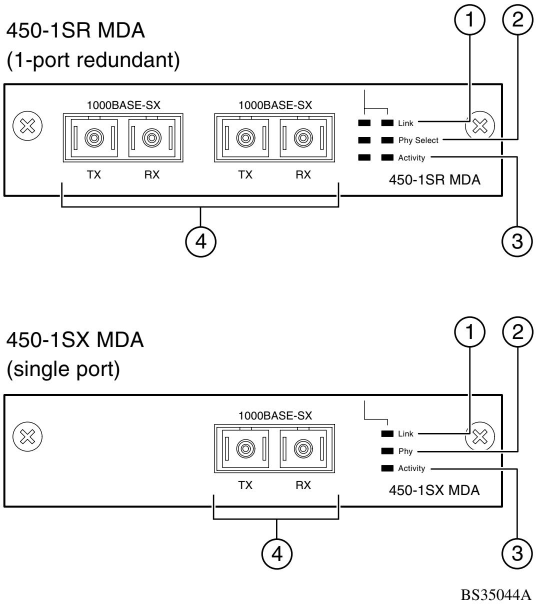


Figure C-3. 1000BASE-SX MDA Front Panels

Table C-3 describes the 1000BASE-SX components and LEDs.

For installation instructions, see "Installing an MDA" on page C-17.

Table C-3. 1000BASE-SX MDA Components

Item	Label	Description
1	Link	Communication link LEDs (green): On: Valid communications link. Off: The communications link connection is bad or there is no connection to this port. Blinking: The corresponding port is management disabled.
2	Phy or Phy Select	Phy status LEDs (green): On: The corresponding Phy port is active. Off: The corresponding Phy port is in backup mode or there is no connection to this port.
3	Activity	Port activity LEDs (green): Blinking: Indicates network activity level for the corresponding port. A high level of network activity can cause LEDs to appear to be on continuously.
4		1000BASE-X SC port connectors.

1000BASE-LX MDAs

Warning: This is a Class 1 Laser/LED product. It contains a laser light source that can injure your eyes. Never look into an optical fiber or connector port. Always assume that the fiber optic cable or connector is connected to a laser light source.

Vorsicht: Dieses Laser/LED-Produkt der Klasse 1 enthält eine Laserlichtquelle, die zu Augenverletzungen führen kann. Sehen Sie nie in einen Lichtwellenleiter oder Glasfaserstecker-Port. Gehen Sie immer davon aus, daß das Glasfaserkabel oder der Glasfaserstecker an eine Laserlichtquelle angeschlossen ist.

Avertissement: Ceci est un appareil Laser/DEL de Classe 1. Cet appareil contient une source lumineuse à rayons laser dangereuse pour les yeux. Ne regardez jamais directement une fibre optique ou un port de connexion. Agissez toujours comme si le câble de fibres optiques ou le connecteur était relié à une source lumineuse à rayons laser.

Advertencia: Éste es un producto láser/LED de Clase 1. Contiene una fuente de luz láser que puede causar lesiones en los ojos. Nunca mire dentro de un cable o de un puerto de conexión de fibra óptica. Asuma siempre que el cable o el connector de fibra óptica está conectado a una fuerte de luz láser.

Avvertenza: Questo è un produtto laser/LED di Classe 1 e contiene una sorgente luminosa a laser che può danneggiare gli occhi. Non guardare mai all'interno di una port a fibra ottica o di una porta connettore. Dare sempre per scontato che il cavo di fibra ottica o il connettore siano collegati ad una sorgente luminosa a laser.

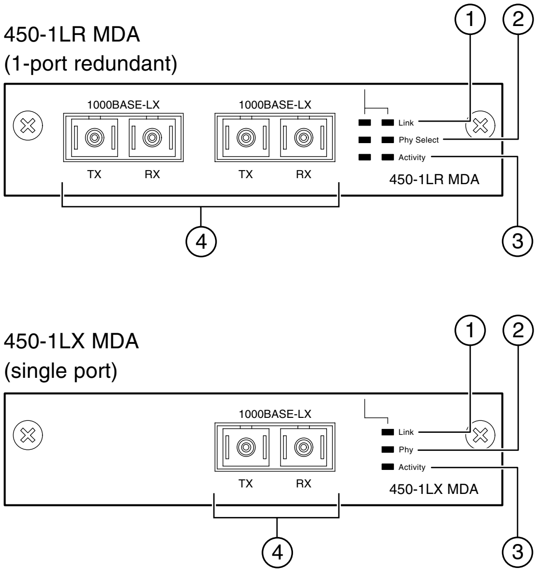
警告:これはクラス1レーザー/LED製品です。目に障害を与える恐れのあるレーザー光源が含まれています。光ファイバおよびコネクタ・ポートは、のぞき込まないようにしてください。光ファイバ・ケーブルまたはコネクタは、常にレーザー光源に接続されているものと想定してください。

There are two 1000BASE-LX (longwave gigabit) MDA models (Figure C-4):

- The 450-1LR MDA is a single MAC MDA with a separate redundant Phy (backup Phy port). Only one Phy port can be active at any time. If the active Phy port fails, the redundant Phy port automatically becomes the active port.
- The 450-1LX MDA is a single Phy MDA.

Both models conform to the IEEE 802.3z 1000BASE-LX standard and use longwave 1300 nm fiber optic connectors to connect devices over single mode (5 kilometer/16,405 ft) or multimode (550 meter/1,805 ft) fiber optic cable.

Note: The optical performance of this transceiver cannot be guaranteed when connected to a multimode fiber plant without the use of the special offset SMF/MMF mode conditioning patch cord (see "1000BASE-LX Multimode Applications" on C-22).



BS35045A

Figure C-4. 1000BASE-LX MDA Front Panels

Table C-4 describes the 1000BASE-LX MDA components and LEDs.

For installation instructions, see "Installing an MDA" on page C-17.

Table C-4. 1000BASE-LX MDA Components

Item	Label	Description
1	Link	Communication link LEDs (green): On: Valid communications link. Off: The communications link connection is bad or there is no connection to this port. Blinking: The corresponding port is management disabled.
2	Phy or Phy Select	Phy status LEDs (green): On: The corresponding Phy port is active. Off: The corresponding Phy port is in backup mode or there is no connection to this port.
3	Activity	Port activity LEDs (green): Blinking: Indicates network activity level for the corresponding port. A high level of network activity can cause LEDs to appear to be on continuously.
4		1000BASE-X SC port connectors (see "1000BASE-LX Multimode Applications" on page C-22 for special requirements).

Asynchronous Transfer Mode (ATM) MDAs

Warning: This is a Class 1 Laser/LED product. It contains a laser light source that can injure your eyes. Never look into an optical fiber or connector port. Always assume that the fiber optic cable or connector is connected to a laser light source.

Vorsicht: Dieses Laser/LED-Produkt der Klasse 1 enthält eine Laserlichtquelle, die zu Augenverletzungen führen kann. Sehen Sie nie in einen Lichtwellenleiter oder Glasfaserstecker-Port. Gehen Sie immer davon aus, daß das Glasfaserkabel oder der Glasfaserstecker an eine Laserlichtquelle angeschlossen ist.

Avertissement: Ceci est un appareil Laser/DEL de Classe 1. Cet appareil contient une source lumineuse à rayons laser dangereuse pour les yeux. Ne regardez jamais directement une fibre optique ou un port de connexion. Agissez toujours comme si le câble de fibres optiques ou le connecteur était relié à une source lumineuse à rayons laser.

Advertencia: Éste es un producto láser/LED de Clase 1. Contiene una fuente de luz láser que puede causar lesiones en los ojos. Nunca mire dentro de un cable o de un puerto de conexión de fibra óptica. Asuma siempre que el cable o el connector de fibra óptica está conectado a una fuerte de luz láser.

Avvertenza: Questo è un produtto laser/LED di Classe 1 e contiene una sorgente luminosa a laser che può danneggiare gli occhi. Non guardare mai all’interno di una port a fibra ottica o di una porta connettore. Dare sempre per scontato che il cavo di fibra ottica o il connettore siano collegati ad una sorgente luminosa a laser.

警告:これはクラス1レーザー/LED製品です。目に障害を与える恐れのあるレーザー光源が含まれています。光ファイバおよびコネクタ・ポートは、のぞき込まないようにしてください。光ファイバ・ケーブルまたはコネクタは、常にレーザー光源に接続されているものと想定してください。

There are two ATM MDA models (Figure C-5):

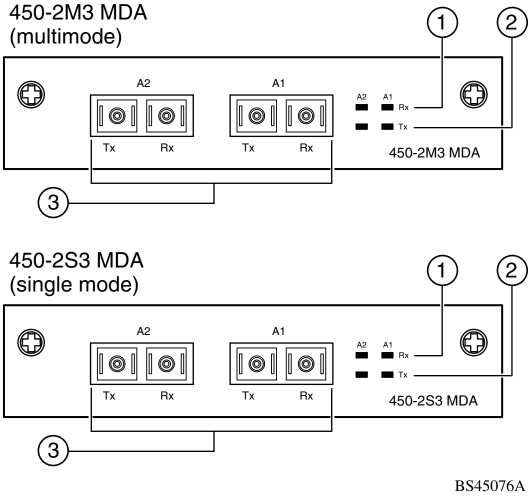


Figure C-5.   ATM MDA Front Panels

- The 450-2M3 MDA uses two SC duplex fiber optic connectors for connections over 62.5/125-micron multimode fiber optic cable.
- The 450-2S3 MDA uses two SC duplex fiber optic connectors for connections over 8.5/125-micron single-mode fiber optic cable.

Both ports can be active at the same time. If a port fails, traffic destined for the failed port can be set to automatically route to the remaining operational port (see “ATM Configuration Menu” on page 3-85).

Both models use longwave 1300 nm fiber optic connectors to connect devices over single mode (10 km/6.2 mi) or multimode (2 km/1.2 mi) fiber optic cable.

Table C-5 describes the 450-2M3 MDA and 450-2S3 MDA front-panel components.

Table C-5. 450-2M3 and 450-2S3 MDA Description

Item	Label	Description
1	Rx	Receive Status: On steady (green): Valid communications link; no activity. On steady (yellow): No valid communications link. Off: The MDA is broken (or not fully seated in the slot). Blinking (green): Valid communications link; receive activity.
2	Tx	Transmit Status: On steady (green): Valid communications link; no activity. On steady (yellow): No valid communications link. Off: The MDA is broken (or not fully seated in the slot). Blinking (green): Valid communications link; transmit activity.
3		SC port connectors.

For installation instructions, see "Installing an MDA" on page C-17.

Gigabit Interface Converter (GBIC) MDA

Warning: This is a Class 1 Laser/LED product. It contains a laser light source that can injure your eyes. Never look into an optical fiber or connector port. Always assume that the fiber optic cable or connector is connected to a laser light source.

Vorsicht: Dieses Laser/LED-Produkt der Klasse 1 enthält eine Laserlichtquelle, die zu Augenverletzungen führen kann. Sehen Sie nie in einen Lichtwellenleiter oder Glasfaserstecker-Port. Gehen Sie immer davon aus, daß das Glasfaserkabel oder der Glasfaserstecker an eine Laserlichtquelle angeschlossen ist.

Avertissement: Ceci est un appareil Laser/DEL de Classe 1. Cet appareil contient une source lumineuse à rayons laser dangereuse pour les yeux. Ne regardez jamais directement une fibre optique ou un port de connexion. Agissez toujours comme si le câble de fibres optiques ou le connecteur était relié à une source lumineuse à rayons laser.

Advertencia: Éste es un producto láser/LED de Clase 1. Contiene una fuente de luz láser que puede causar lesiones en los ojos. Nunca mire dentro de un cable o de un puerto de conexión de fibra óptica. Asuma siempre que el cable o el connector de fibra óptica está conectado a una fuerte de luz láser.

Avvertenza: Questo è un produtto laser/LED di Classe 1 e contiene una sorgente luminosa a laser che può danneggiare gli occhi. Non guardare mai all’interno di una port a fibra ottica o di una porta connettore. Dare sempre per scontato che il cavo di fibra ottica o il connettore siano collegati ad una sorgente luminosa a laser.

警告:これはクラス1レーザー/LED製品です。目に障害を与える恐れのあるレーザー光源が含まれています。光ファイバおよびコネクタ・ポートは、のぞき込まないようにしてください。光ファイバ・ケーブルまたはコネクタは、常にレーザー光源に接続されているものと想定してください。

The 450-1GBIC MDA (see Figure C-6) provides a single host port for supported Gigabit Interface Converters (GBICs).

The GBICs are hot-swappable input/output enhancement components that are designed for use with your BayStack 350 switch to allow Gigabit Ethernet ports to link with fiber optic networks.

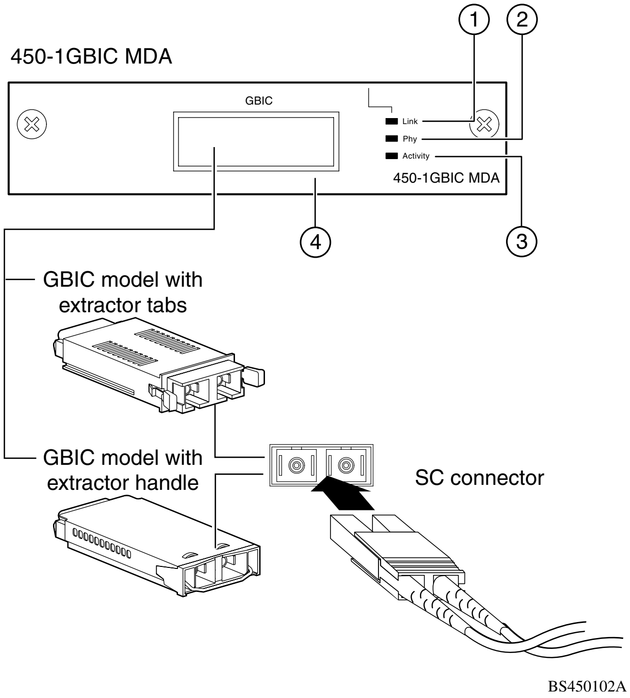


Figure C-6. 450-1GBIC MDA Front Panel

Table C-6 describes the 450-1GBIC MDA front-panel components.

Table C-6. 450-1GBIC MDA Components

Item	Label	Description
1	Link	Communication link LEDs (green): On: Valid communications link. Off: The communications link connection is bad or there is no connection to this port. Blinking: The corresponding port is management disabled.
2	Phy	Phy status LEDs (green): On: The corresponding Phy port is active. Off: The corresponding Phy port is in backup mode or there is no connection to this port.
3	Activity	Port activity LEDs (green): Blinking: Indicates network activity level for the corresponding port. A high level of network activity can cause LEDs to appear to be on continuously.
4		GBIC Host port.

For instructions on installing your 450-1GBIC MDA on your BayStack 350 switch, see “Installing an MDA” following this section.

For instructions on installing GBICs on your 450-1GBIC MDA, see “Installing GBICs” on page C-19.

Installing an MDA

The Uplink Module slot on the BayStack 350 switch accommodates a single MDA. The connection can be either an RJ-45 10/100BASE-TX MDA or a fiber (100BASE-FX, 1000BASE-SX/LX, or ATM) MDA with an SC or MT-RJ connector.

Note: The MDAs are *not* hot-swappable. Power down the switch before installing or removing an MDA.

To install an MDA into the Uplink Module slot:

1. **Unplug the AC power cord from the back of the switch.**
2. **Loosen the thumb screws and remove the filler panel (or previously installed MDA) from the Uplink Module slot.**
3. **Insert the MDA into the Uplink Module card guides (Figure C-7).**

   Make sure the MDA slides in on the card guides. Failure to align the MDA to the card guides could damage the pins.

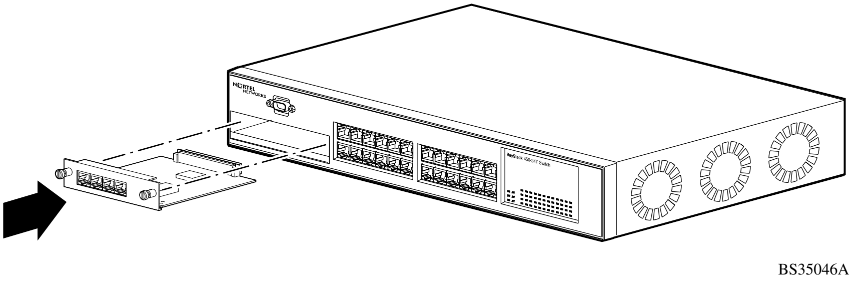


Figure C-7. Installing an MDA

4. **Press the MDA *firmly* into the Uplink Module slot.**

   Be sure that the MDA is fully seated into the mating connector.

5. **Secure the MDA by tightening the thumb screws on the MDA front panel.**
6. **Attach devices to the MDA ports (see “Attaching Devices to the BayStack 350 Switch” on page 2-7).**

   After connecting the port cables, continue to follow the instructions in Chapter 2 to connect power and verify the installation.

➡ **Note:** The IEEE 802.3u specification requires that all ports operating at 100 Mb/s use only Category 5 unshielded twisted pair (UTP) cabling.

Replacing an MDA

When replacing an installed MDA:

1. **Power down the switch.**

Remove the AC power cord from the power source.

2. **Remove the installed MDA.**

   Loosen the thumbscrews and remove the MDA.

3. **Install the replacement MDA.**

   Be sure to *firmly* tighten the two thumbscrews on the MDA front panel.

4. **Power up the switch.**

Installing GBICs

This section describes how to install gigabit interface converters (GBICs) on your 450-1GBIC MDA's Host port.

➡ **Note:** For more information about supported GBICs and for details about cabling specifications, refer to the *Gigabit Interface Converter (GBIC) Installation Guide* (part number 208723-A).

Refer to Table C-7 for a list of supported GBIC models that you can order from Nortel Networks.

Table C-7. Available GBIC Models

Model number	Description	Part number
1000BASE-SX	Uses shortwave 850 nm fiber optic connectors to connect devices over multimode (550 m/1805 ft) fiber optic cable.	AA1419001
1000BASE-LX	Uses longwave 1300 nm fiber optic connectors to connect devices over single mode (5 km/3.1 mi) or multimode (550 m/ 1805 ft) fiber optic cable.	AA1419002
1000BASE-XD	Uses single mode fiber to connect devices over distances up to 50 km (31 mi), depending on the quality of the cable.	AA1419003
1000BASE-ZX	Uses single mode fiber to connect devices over distances up to 70 km (43 mi), depending on the quality of the cable. The ports operate in full-duplex mode only.	AA1419004

The GBICs are available in different case styles (Figure C-8). One type has two spring tabs at the front of the GBIC; the other type has an extractor handle on the front.

GBICs are shipped with a protective rubber plug in the connectors. Leave the plug in place when no cables are connected to the GBIC.

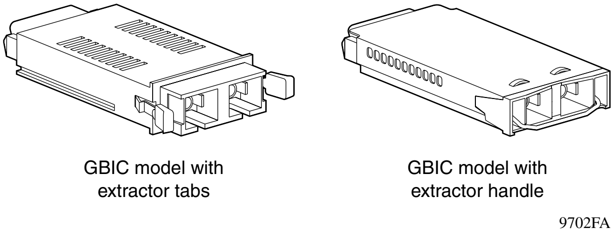

GBIC model with extractor tabs
GBIC model with extractor handle
9702FA

Figure C-8. GBIC Case Styles

Installation

The 450-1GBIC MDA Host port is covered with a spring-loaded filler panel that rotates out of the way as you push the GBIC into place.

You can install or replace a GBIC in an operating 450-1GBIC MDA without turning off power to the switch.

Note: The MDAs are *not* hot-swappable. Power down the switch before installing or removing an MDA.

To install a GBIC:

1. **Remove the GBIC from its protective packaging.**
2. **Insert the GBIC into the Host port on the MDA (Figure C-9).**

   GBICs are keyed to prevent improper insertion. If the GBIC resists pressure, do not force it. Remove it, turn it over, and reinsert it.

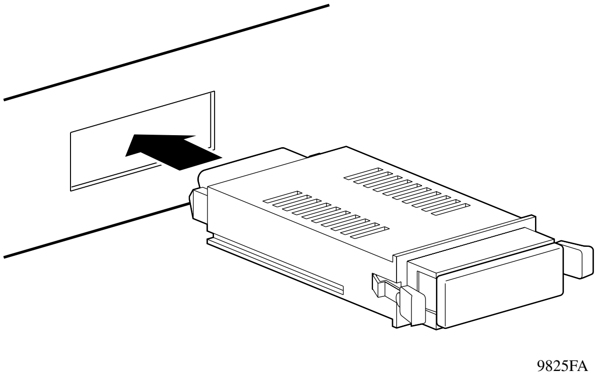


Figure C-9. Installing A GBIC

3. **Press on the front of the GBIC until it snaps into place.**
4. **Remove the rubber plug from the connectors to connect cables.**

Removing an Installed GBIC

To remove an installed GBIC:

1. **If the GBIC has spring tabs, press in on the tabs on each side of the GBIC as you pull the GBIC out of the MDA's Host port (Figure C-10).**

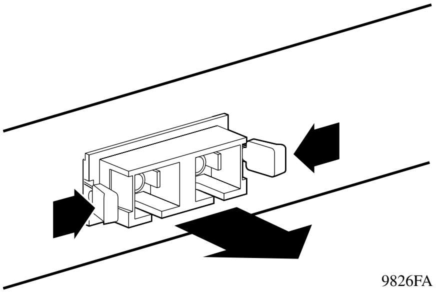


Figure C-10. Removing a GBIC

2. **If the GBIC has an extractor handle, grasp the handle and pull firmly to remove the GBIC from the MDA's Host port.**

1000BASE-LX Multimode Applications

For 1000BASE-LX multimode applications, the longwave gigabit transceivers must be mode conditioned *externally* via a special offset SMF/MMF patch cord. The offset SMF/MMF patch cord allows the same transceiver to be used for both multimode and single-mode fiber. See your Nortel Networks sales representative for more information about the SMF/MMF patch cord.

The 1000BASE-LX transceiver is designed to mechanically accomodate the *single-mode ferrules* used on one end of the special offset SMF/MMF patch cord. *Multimode ferrules* must not be used because they can bind and cause damage to the transceiver. Do not connect multimode cables *directly* into the 1000BASE-LX MDA transceiver. Instead, connect a special offset SMF/MMF patch cord into the transceiver, and then connect the multimode cable into the SMF/MMF patch cord.

For more information about gigabit transmission over fiber optic cable and mode conditioning, refer to the following publication:

Reference Note: Gigabit Ethernet Physical Layer Considerations (Part number 201540-B).

The publication is available on the World Wide Web at:

www25.nortelnetworks.com/library/tpubs/

At the Web site, click on Accelar under the Routing Switches heading.

Appendix D
ATM Overview

This appendix describes asynchronous transfer mode (ATM) terminology, as well as concepts and examples of how your BayStack 450-2M3/2S3 MDAs operate within a network. The following topics are discussed in this appendix:

- "ATM Terminology" (page D-1)
- "ATM Data Transmission" (page D-5)
- "Configuration Concepts" (page D-6)
- "Configuration Rules" (page D-13)

ATM Terminology

This section defines the ATM-related terms used in this manual. You should review and understand the ATM terminology before you review the concepts described in this appendix. Figure D-1 provides a graphical representation of the terms described in this section.

LAN Emulation (LANE)

LAN emulation (LANE) refers to the services and protocols defined in the ATM Forum Technical Committee's *LAN Emulation Over ATM Version 1.0* specification. The LANE protocol allows token ring and Ethernet clients on LAN-to-ATM bridge/switch devices to communicate transparently across ATM networks with direct-attached ATM servers and with other LAN clients on other LAN-to-ATM bridges/switches.

The clients create token ring- or Ethernet-emulated LANs (ELANs) in the ATM network, and then configure the ATM servers and LAN-to-ATM bridges/switches to connect to them (see "Emulated LAN (ELAN)" on page D-3).

Figure D-1 shows two BayStack switches that are configured with BayStack 450-2M3/2S3 MDAs. The MDAs are physically connected to the ATM switch with two physical ports (not shown). Each MDA can support up to four LAN emulation client (LEC) virtual ports to the ELANs. PC1 uses the services provided by the BayStack 450-2M3/2S3 MDA to communicate with PC2 through the ATM switch.

In this example, LEC1 queries the LAN emulation configuration server (LECS) for the ATM address of the LAN emulation server (LES) that is providing services for the specified ELAN. The LES sets up the broadcast and unknown server (BUS) for LEC1, and establishes the ELAN.

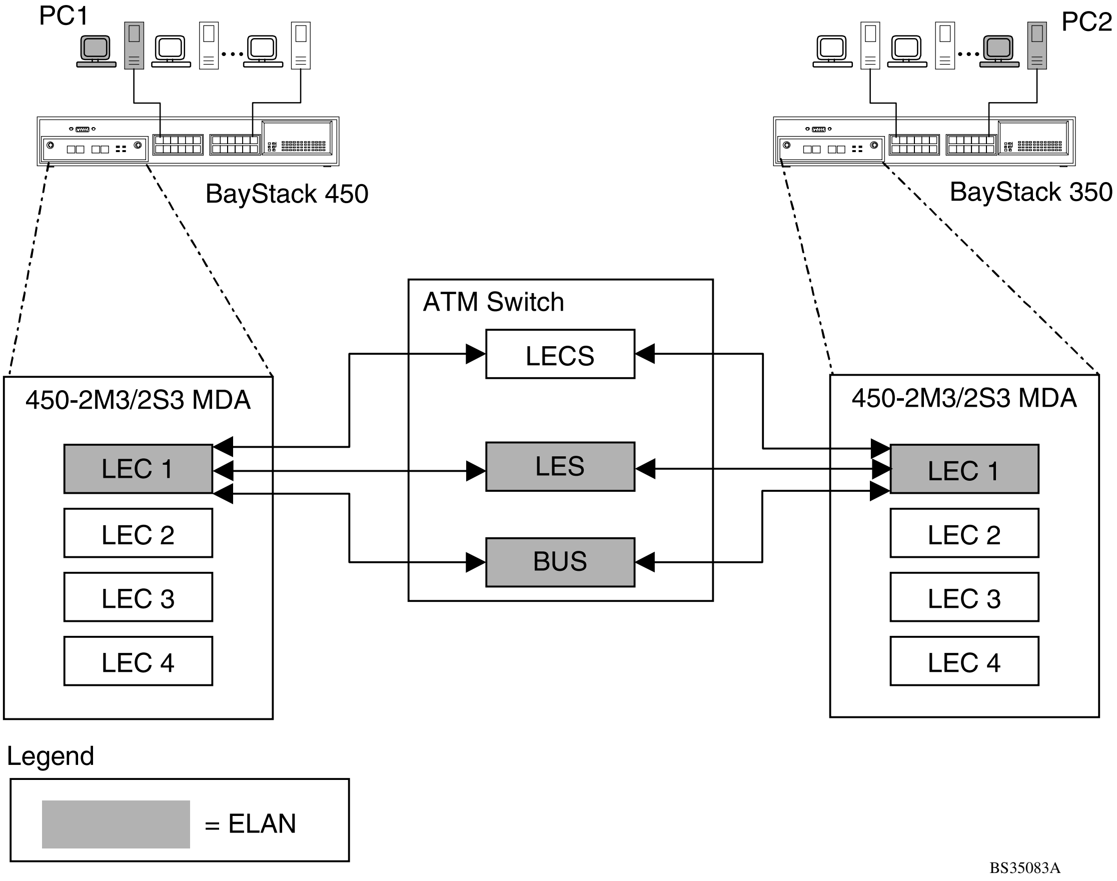


Figure D-1. ATM LAN Emulation Model

For more information about LANE, refer to the ATM Forum Technical Committee *LAN Emulation Over ATM Version 1.0* specification.

Emulated LAN (ELAN)

An emulated LAN (ELAN) is an implementation of a virtual LAN (VLAN) that is using the ATM Forum's LAN emulation (LANE) specification. The ELAN comprises a group of ATM-attached devices that are logically analogous to a group of LAN stations attached to an IEEE 802.3 or IEEE 802.5 segment.

Multiple ELANs can be configured within an ATM network, and membership in an ELAN is independent of where the end system is physically connected. The end system can be associated with multiple ELANs.

Because multiple ELANs over a single ATM network are logically independent, a broadcast frame that originates from a member of a particular ELAN is distributed only to the members of that ELAN.

The shaded blocks in Figure D-1 on page D-2, represent a single ELAN that was created by a user on PC1 wanting to communicate with a user on PC2.

For more information about ELANs, refer to the ATM Forum Technical Committee *LAN Emulation Over ATM Version 1.0* specification.

LAN Emulation Client (LEC)

A LAN emulation client (LEC) is a type of virtual port that performs data forwarding, address resolution, and other control functions over ATM when attached to a bridge group on the switch. The LEC provides a MAC-level emulated Ethernet IEEE 802.3 or IEEE 802.5 service interface to higher-level software. The LEC implements an ATM Forum LANE standards-compliant user network interface (UNI) when communicating with other LECs within an ELAN (see "User-to-Network Interface (UNI) on page D-5).

The BayStack 450-2M3/2S3 MDA implements the ATM Forum's LEC as a *proxy* for all of the MAC addresses listed in the BayStack 350 switch's address database. The LECs shown in the example in Figure D-1 on page D-2 are proxy LECs.

For more information about LECs, refer to the ATM Forum Technical Committee *LAN Emulation Over ATM Version 1.0* specification.

LAN Emulation Configuration Server (LECS)

A LAN emulation configuration server (LECS) assigns individual LECs to different ELANs based upon the LECS' policies, configuration database, and the information that is provided by the LEC.

The LECS assigns the LEC to an ELAN by giving the LEC the ATM address of the LAN emulation server (LES) that is providing services for that specific ELAN (see "LAN Emulation Server (LES)" on page D-4).

In Figure D-1 on page D-2, the LECS assigns LEC1 to the ELAN (shaded blocks) by providing LEC1 with the ATM address of the LES that is providing the service for that ELAN.

For more information about LECS, refer to the ATM Forum Technical Committee *LAN Emulation Over ATM Version 1.0* specification.

LAN Emulation Server (LES)

A LAN emulation server (LES) implements the control coordination function for the ELAN. The LES registers and resolves MAC addresses and route descriptors to ATM addresses, and may register its LAN destinations with the LECS.

A LEC also queries the LES when it wants to resolve a MAC address or route descriptor to an ATM address. The LES either responds directly to the LEC or forwards the query to other LECs so that they may respond.

For more information about LES, refer to the ATM Forum Technical Committee *LAN Emulation Over ATM Version 1.0* specification.

Broadcast and Unknown Server (BUS)

The broadcast and unknown server (BUS) handles data sent by a LEC to the broadcast MAC address, all multicast traffic, and initial unicast frames that are sent by a LEC before the data direct target ATM address has been resolved (before a data direct VCC has been established).

This BUS must always exist in the ELAN and all LECs must join its distribution group.

For more information about BUS, refer to the ATM Forum Technical Committee *LAN Emulation Over ATM Version 1.0* specification.

User-to-Network Interface (UNI)

The user-to-network interface (UNI) represents the interface between an end point of an ATM network and the switch (the user connection).

The UNI can also be the interface between an end point of an ATM network and a switch or between a switch and a router.

There are two types of UNI interfaces:

- Private UNI -- interface between an end point device and a private network switch
- Public UNI -- interface between an end point device and the public switched network

For more information about UNI 3.0 and UNI 3.1, refer to *ATM User-Network Interface (UNI) Specification, Version 3.0* and *ATM User-Network Interface Interface (UNI) Specification, Version 3.1*.

ATM Data Transmission

Data transmission (also called *cell switching*) through the ATM network relies on the establishment of logical connections between ATM entities. ATM is a *connection-oriented* service. This means that an ATM entity cannot transmit information until it establishes a connection with a receiving entity. These connections consist of *virtual channels, virtual paths,* and *transmission paths* (Figure D-2).

A *virtual channel* is a logical connection between two communicating ATM entities. Each virtual channel may carry a different protocol or traffic type. The virtual channel transports cells that have a common identifier. The identifier is called the virtual identifier (VCI) and is part of the cell header. You can establish permanent virtual channels or you can set them up as dynamic virtual channels, which allows the network to adjust to the traffic demand.

A *virtual path* is a set of virtual channels between a common source and destination. The virtual channels in a virtual path logically associate to a common identifier. This identifier is called the virtual path identifier (VPI) and is part of the cell header. You can base cells on either the VPI alone, or on a combination of the VPI and the VCI.

Virtual paths enable you to separate network transport functions into types that are related to an individual logical connection (virtual channel) and types that are related to a group of logical connections (virtual path).

A *transmission path* is a physical connection that comprises several virtual paths, each virtual path containing several virtual channels. The transmission path may support multiple virtual paths across a single connection to the network.

Figure D-2 shows the relationships between the virtual channel, the virtual path, and the transmission path.

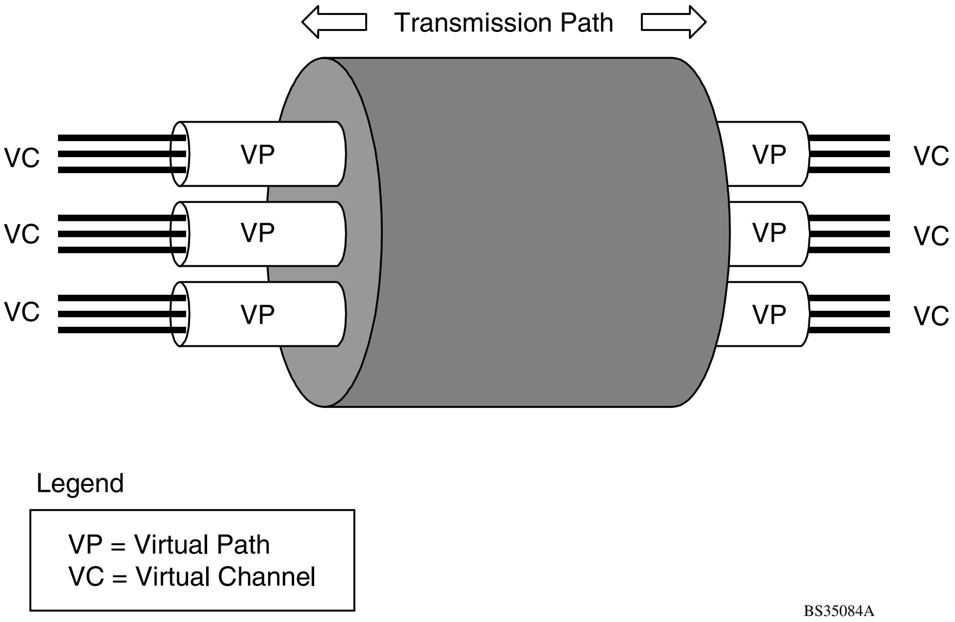


Figure D-2. ATM Transmission Components

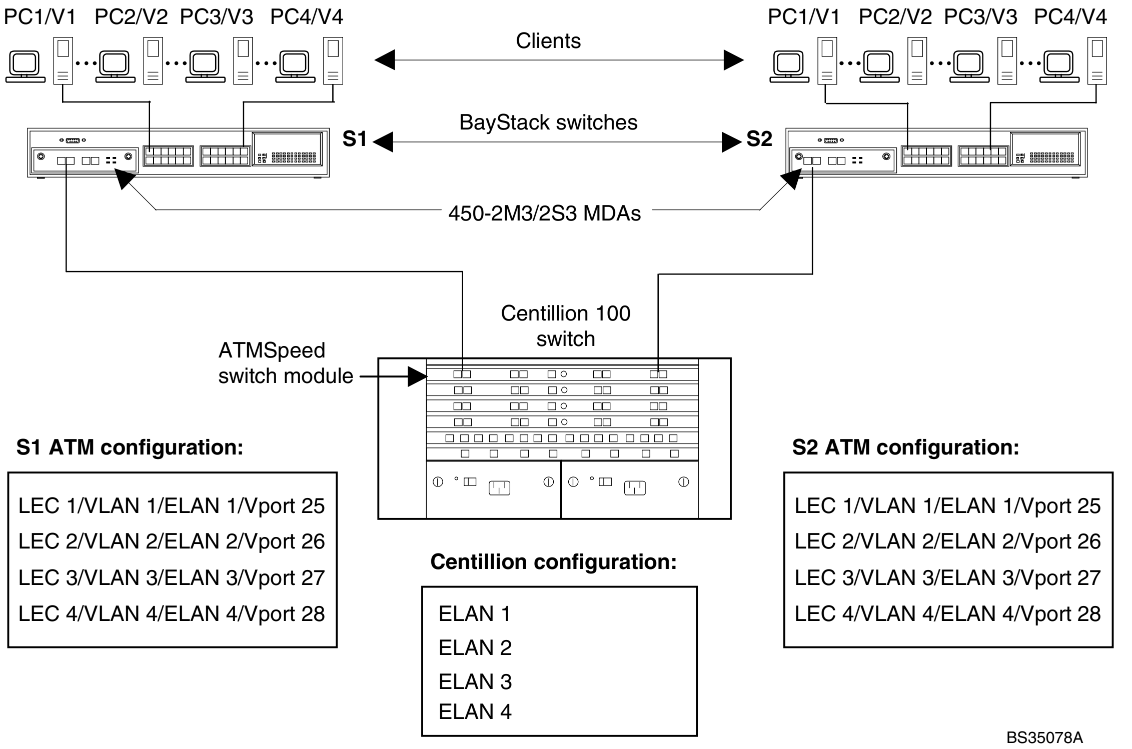
Configuration Concepts

This section describes the configuration concepts related to the operation of the BayStack 450-2M3/2S3 MDA in a standalone or stack configuration.

ELAN VLAN Mapping

Figure D-3 shows how your BayStack 450-2M3/2S3 MDAs can provide ATM connections to a Nortel Networks Centillion™ 100 switch. Clients (PCs) that are connected to S1 can communicate with clients connected to S2, provided that the VLANs (with their respective client members) are mapped onto the same ELANs as shown.

Although this example shows standalone switches, you can apply the same example to a stack of up to eight switches, with 32 VLANs and 32 ELANs.



S1 ATM configuration:

LEC 1/VLAN 1/ELAN 1/Vport 25
LEC 2/VLAN 2/ELAN 2/Vport 26
LEC 3/VLAN 3/ELAN 3/Vport 27
LEC 4/VLAN 4/ELAN 4/Vport 28

Centillion configuration:

ELAN 1
ELAN 2
ELAN 3
ELAN 4

S2 ATM configuration:

LEC 1/VLAN 1/ELAN 1/Vport 25
LEC 2/VLAN 2/ELAN 2/Vport 26
LEC 3/VLAN 3/ELAN 3/Vport 27
LEC 4/VLAN 4/ELAN 4/Vport 28

Figure D-3. ELAN VLAN Mapping

Available Services

This section describes the services that are available to support your BayStack 450-2M3/2S3 MDA.

LANE

BayStack 450 software version V3.1 supports the ATM Forum’s LAN Emulation (LANE) specification V1.0 (IEEE 802.3). This version of the LANE software is compatible with Nortel Networks Centillion switches (models C100, C1000, and 5000BH) implementation of LANE. The BayStack 450-2M3/2S3 MDA operates only as a LAN Emulation Client (LEC). This type of operation requires the BayStack 450-2M3/2S3 MDA to rely on the LANE services offered with Nortel Networks Centillion switches (models C100, C1000, and 5000BH) or other industry-standard equipment for LES, LECS, and BUS functionality.

UNI Support

Your BayStack 450-2M3/2S3 MDA supports UNI 3.0 and 3.1

For more information about UNI 3.0 and UNI 3.1, refer to *ATM User-Network Interface (UNI) Specification, Version 3.0* and *ATM User-Network Interface Interface (UNI) Specification, Version 3.1*.

LECS Address Methods

Three types of LECS address location methods are available:

- The ATM Forum (default)

  4700790000000000000000000000A03E00000100
- User Defined

  Any 20-byte address that begins with either 37, 39, or 45.
- ILMI

  Address determined by the interim local management interface (ILMI).

PHY

Your BayStack 450-2M3/2S3 MDA provides a dual-channel ATM PHY. The ATM PHY chip implements SDH and SONET encapsulation using the ATM transmission convergence (TC) sublayer, as specified by the ATM Forum specification using the SONET/SDH 155.25 Mb/s STS-3c/STM-1 and the SONET 51.84 Mb/s STS-1 formats.

This method allows ATM terminals to link to ATM switching systems that use SONET/SDH- compatible transport mechanisms.

Virtual Ports

Your BayStack 450-2M3/2S3 MDA has two physical OC-3 ports (A1 and A2) that are used to connect to an ATM switch. As shown in Figure D-4, both physical ports are logically mapped to four LEC *virtual ports* (VPorts), LEC1 to LEC4.

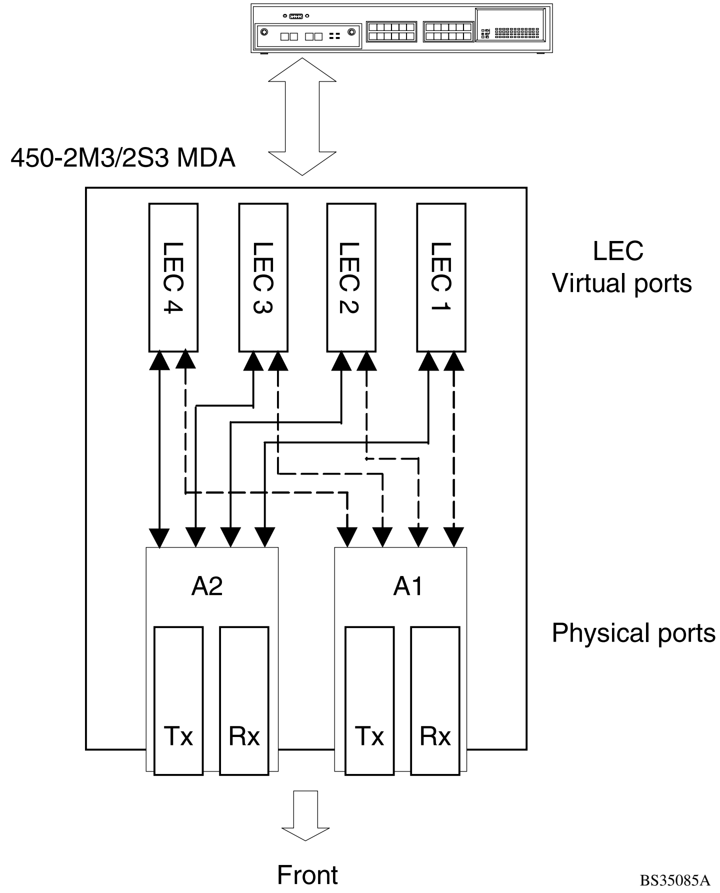


Figure D-4. Virtual and Physical Ports

During initial powerup, your switch assigns the VPorts as a continuation of the default port numbering within the CI menus and screens. For example, if you have a 12-port switch, VPorts LEC1 to LEC4 are assigned port 13 to port 16. For 24-port models, the VPorts are assigned port 25 to port 28.

You can assign any of the four VPorts to either one of the two physical ports (for example, you can assign LEC2 and LEC3 to physical port A1, and assign LEC 1 and LEC 4 to physical port A2).

LEC Failover

The BayStack 450-2M3/2S3 MDA has two front-panel physical ports (A1 and A2) that are available for LEC association. Both physical ports can be active at the same time.

If either of the two physical ports fails, the LEC Failover feature (when enabled) allows all LECs that are associated with the failed physical port to be automatically assigned to the remaining operational physical port. If the failed physical port recovers, all associated LECs are automatically assigned to the original desired port.

You can enable LEC Failover protection for your BayStack 450-2M3/2S3 MDA by setting the LEC Fail Over field value in the ATM MDA Configuration screen to Enabled (see "ATM MDA Configuration" on page 3-89).

➡ **Note:** LEC Failover protection is limited to either of the two physical ports within the same MDA only.

Spanning Tree on LEC Ports

The default STP setting for your BayStack 450-2M3/2S3 MDA's LECs Vports is Normal Learning. Because BayStack 350 switches (software version V3.1, and earlier) do not support multiple STPs, you may have to disable STP on all LEC VPorts. Figure D-5 shows possible consequences of not disabling the STP when using the BayStack 450-2M3/2S3 MDA.

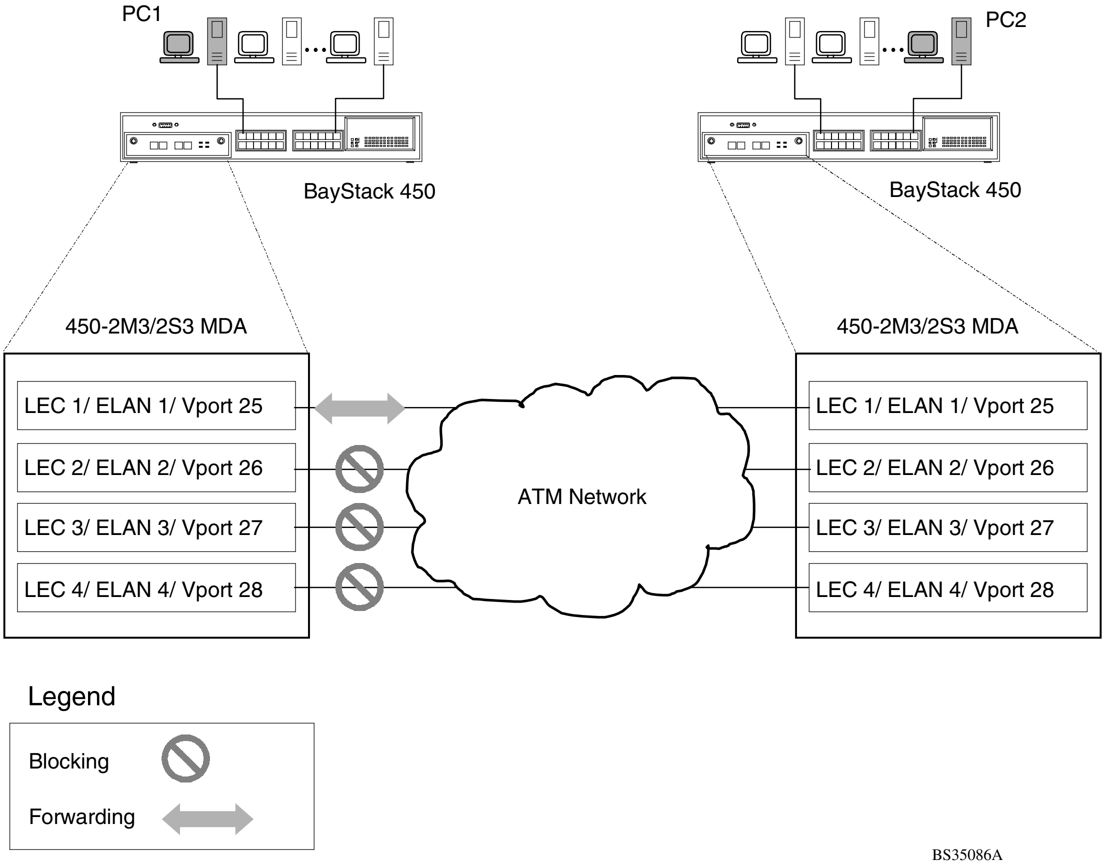


Figure D-5. LEC VPorts with Spanning Tree Enabled (1 of 2)

As shown in Figure D-5, there are four virtual parallel links between the two BayStack 450-2M3/2S3 MDAs. Each link consists of a LEC VPort on each side on the same ELAN. Because STP is enabled for the four LEC VPorts, three of the LEC VPorts are in the Blocking state (based on the spanning tree algorithm).

You can disable STP on the LEC VPorts with the risk of creating loops within the network. If you are sure of a loop-free topology beyond the ATM uplink, then you can disable the STP on the uplink ports to ensure connectivity on all four ELANs/ VLANs (Figure D-6).

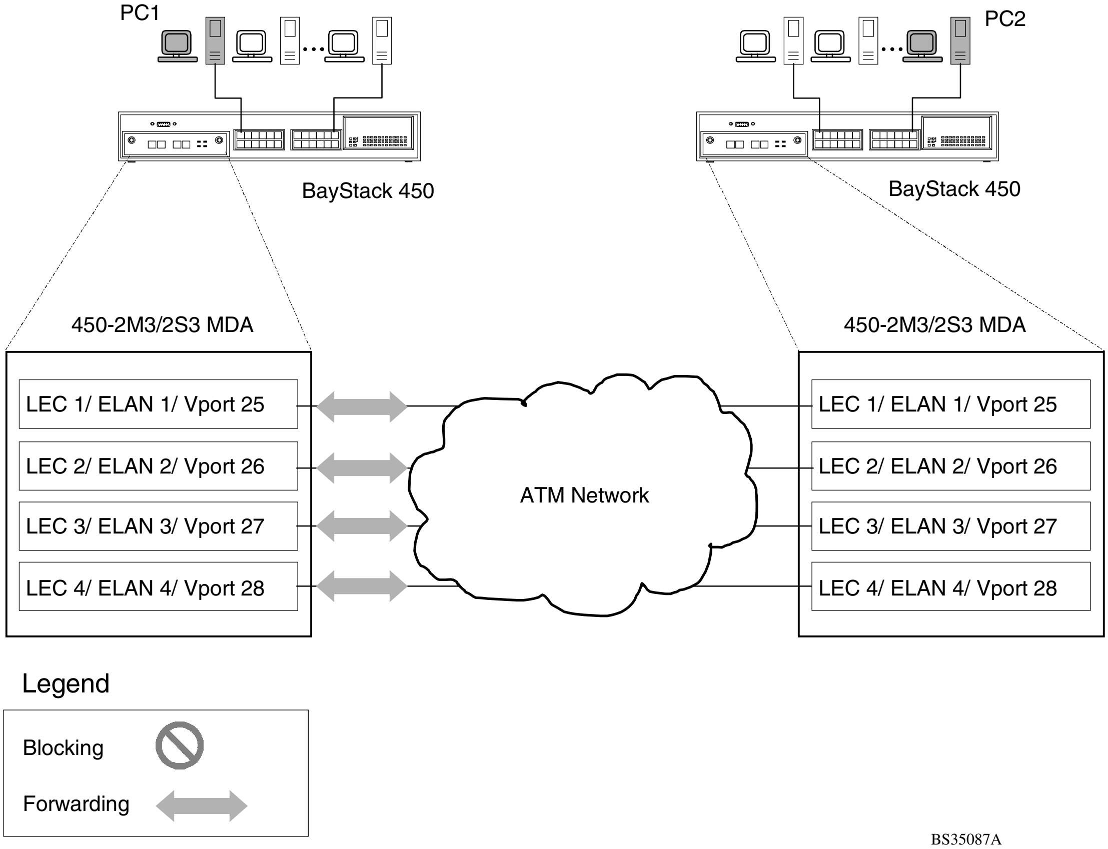


Figure D-6. LEC VPorts with Spanning Tree Disabled (2 of 2)

Note: Because there is only one BayStack 450-2M3/2S3 MDA LEC VPort on one VLAN/ELAN, a loop-free network topology is ensured to some extent; however, it may not be sufficient to ensure a loop-free topology for the entire network.

Configuration Rules

This section summarizes important configuration rules for the BayStack 450-2M3/2S3 MDA.

Initial Configuration

During the initial configuration of the BayStack 450-2M3/2S3 MDA, you must perform the following steps:

1. **Configure the VLAN memberships for the four LECs in the VLAN Configuration screen.**
2. **Set the LEC State field to Enabled in the LEC Configuration screen.**

See “Configuring the BayStack 450-2M3/2S3 MDAs” on page E-15 for flowcharts that detail the configuration steps required for your BayStack 450-2M3/2S3 MDA.

Enabling a LEC

Every LEC requires the following:

- A unique ELAN name

  The ELAN name default value is: default

- An Actual Physical Port number (A1 or A2)

  The physical port number default value is: A1

- A port-based VLAN.

  You must assign the LEC to a new or existing port-based VLAN (using the VLAN Configuration screen) the first time a LEC is assigned, or whenever you issue the Reset to Default Settings command.

  In all other cases, a LEC’s VLAN membership is saved and restored following subsequent switch power cycles.

LECs and VLAN Membership

The following configuration rules apply:

- You cannot assign a LEC as a tagged VLAN member.
- The PVID value for a LEC is read-only and must always equal its VLAN ID.
- LEC VLAN members do not support priority.
- A LEC can only be a member of one VLAN.
- A VLAN can only have one LEC member.
- LECs can be configured as members of port-based VLANs only; LECs cannot be configured as members of protocol-based VLANs.

Console Differences

Many of the features that are available to your BayStack 350 switch Ethernet-based ports cannot be supported by ATM. In those cases the VPorts that represent the ATM LECs will either be hidden or displayed as read-only fields.

The following BayStack 350 switch features are not supported by the BayStack 450-2M3/2S3 MDA:

- MultiLink Trunking
- Port Mirroring
- Filtering of untagged/tagged frames
- VLAN Traffic Class Priority
- Change of PVID
- Protocol-based VLANs
- VLAN tagging
- Rate Limiting

The following are ATM-related screen differences:

- In the Port Statistics screen, the ATM VPort statistics support only a subset of the field values that are displayed for standard switch ports.
- The ATM submenu appears on the Switch Configuration Menu if any unit in a stack configuration contains an ATM MDA.
- In the VLAN Port Configuration screen, the ATM VPorts are not assigned to a default VLAN following a Reset command, as with normal switch ports.
- In the VLAN Port Configuration screen, the ELAN name is substituted for the VLAN name PID.

Appendix E
Quick Steps to Features

If you are a system administrator with experience configuring BayStack 350 switch VLANs, ATM MDAs, MultiLink Trunking, Port Mirroring, and IGMP Snooping, use the flowcharts on the following pages as quick configuration guides. The flowcharts refer you to the "configuration rules" appropriate for each feature.

The flowcharts cover the following topics:

- "Configuring 802.1Q VLANs" (page E-2)
- "Configuring Security Settings" (page E-5)
- "Configuring the BayStack 450-2M3/2S3 MDAs" (page E-15)
- "Configuring MultiLink Trunks" (page E-18)
- "Configuring Port Mirroring" (page E-19)
- "Configuring IGMP Snooping" (page E-21)

To learn more about:	See this section:
802.1Q VLANs	"IEEE 802.1Q VLAN Workgroups" on page 1-34.
Switch and Network Security	"Security" on page 1-12.
BayStack 450-2M3/2S3 MDAs	Appendix D, "ATM Overview."
MultiLink Trunks	"MultiLink Trunks" on page 1-60.
Port Mirroring	"Port Mirroring (Conversation Steering)" on page 1-78.
IGMP Snooping	"IGMP Snooping" on page 1-51.

Configuring 802.1Q VLANs

To create or modify an 802.1Q VLAN, follow the flowcharts in Figures E-1 to E-3.

Choose VLAN Configuration (or press v) from the VLAN Configuration Menu screen to open the VLAN Configuration screen.

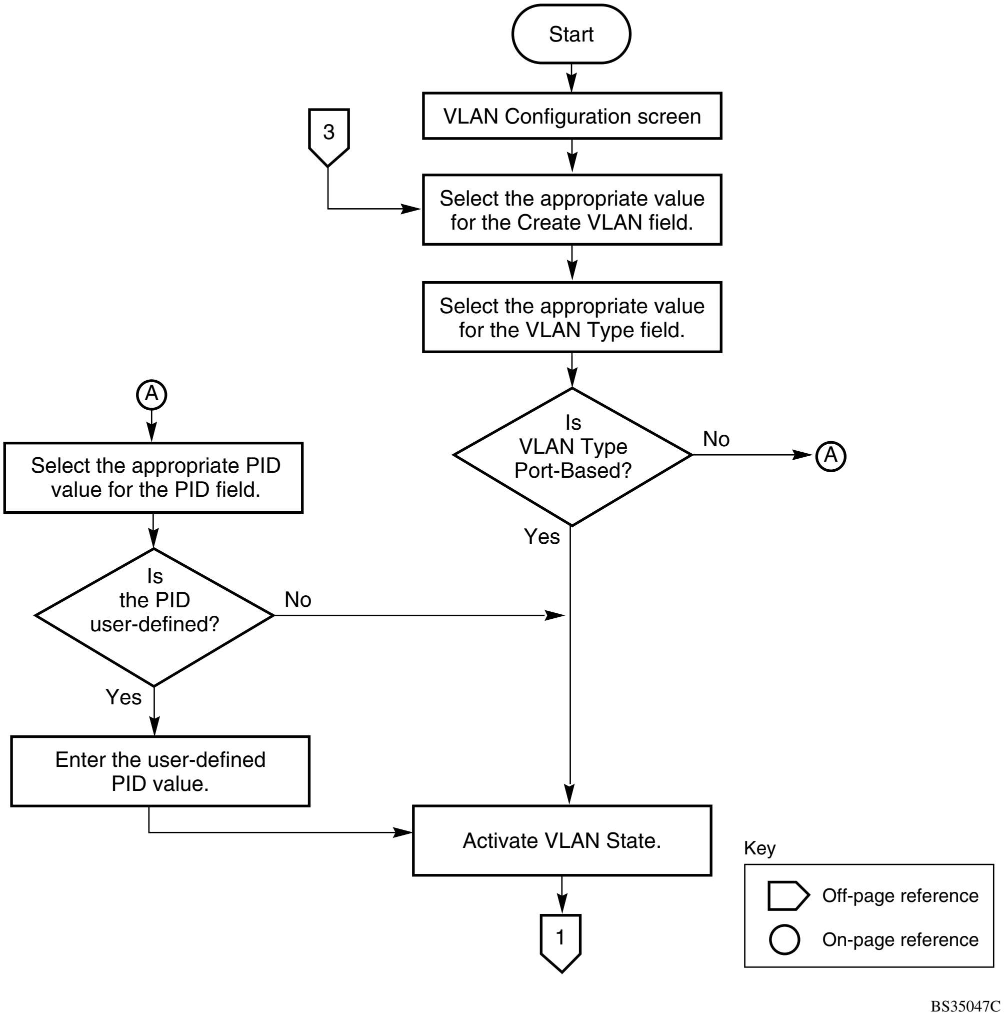

Start
VLAN Configuration screen
3
Select the appropriate value for the Create VLAN field.
Select the appropriate value for the VLAN Type field.
A
Is VLAN Type Port-Based?
No
A
Yes
Select the appropriate PID value for the PID field.
Is the PID user-defined?
No
Yes
Enter the user-defined PID value.
Activate VLAN State.
1
Key
Off-page reference
On-page reference
BS35047C

Figure E-1. Configuring 802.1Q VLANs (1 of 3)

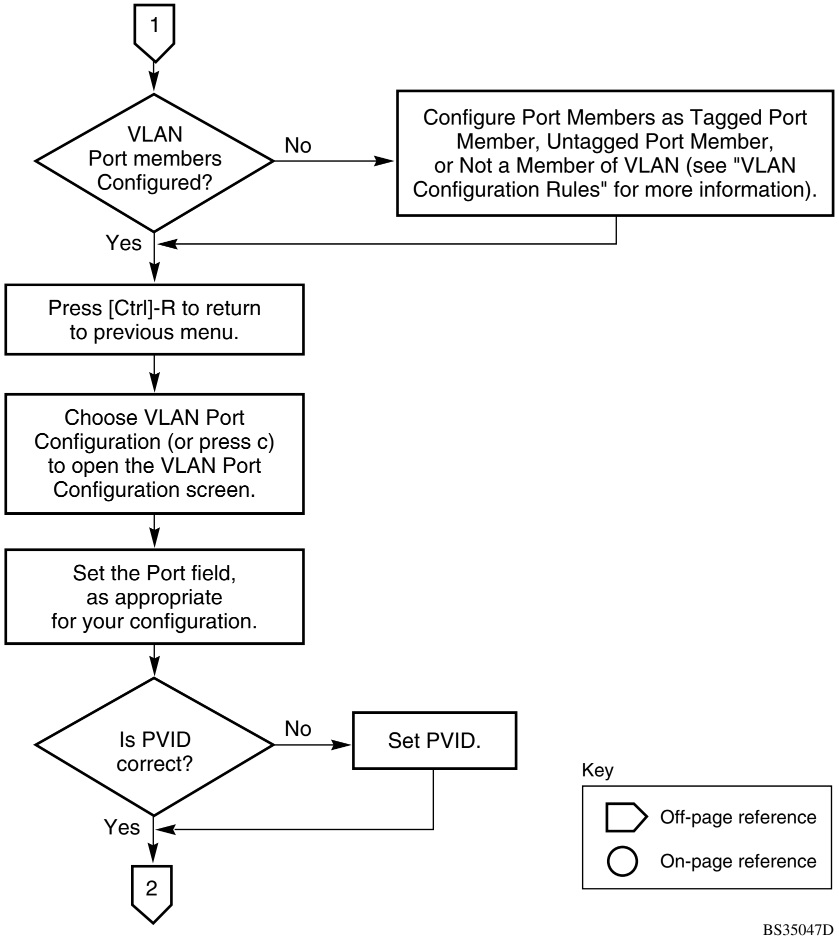

1
VLAN Port members Configured?
No
Configure Port Members as Tagged Port Member, Untagged Port Member, or Not a Member of VLAN (see "VLAN Configuration Rules" for more information).
Yes
Press [Ctrl]-R to return to previous menu.
Choose VLAN Port Configuration (or press c) to open the VLAN Port Configuration screen.
Set the Port field, as appropriate for your configuration.
Is PVID correct?
No
Set PVID.
Yes
2
Key
Off-page reference
On-page reference
BS35047D

Figure E-2. Configuring 802.1Q VLANs (2 of 3)

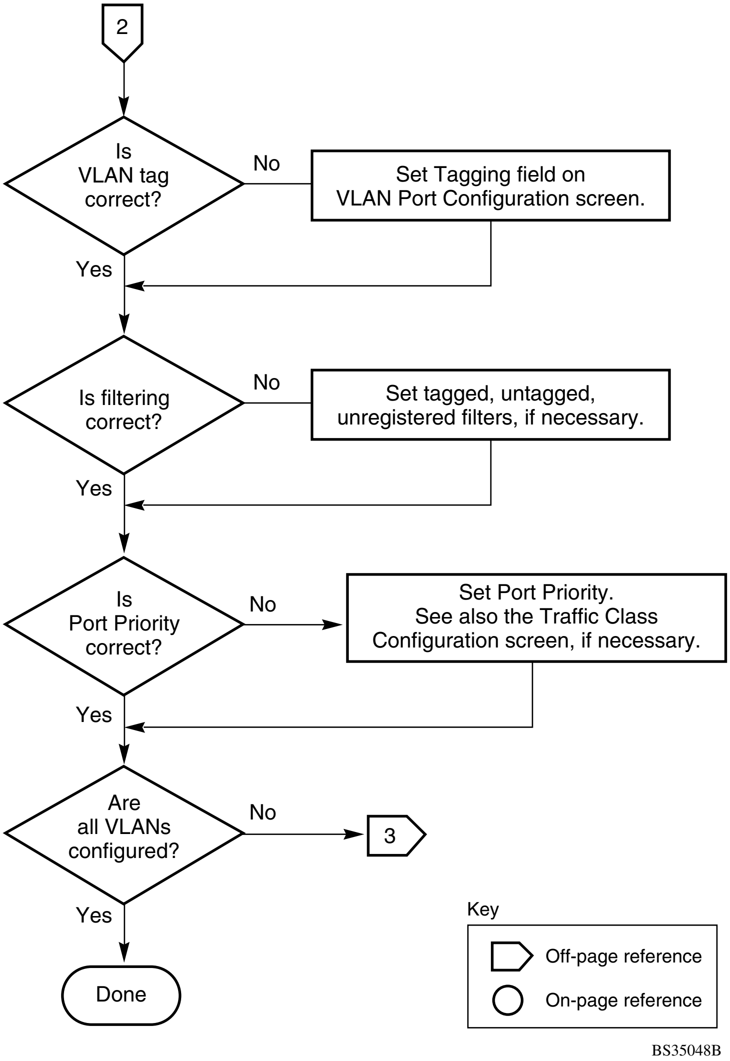

2
Is VLAN tag correct?
No
Set Tagging field on VLAN Port Configuration screen.
Yes
Is filtering correct?
No
Set tagged, untagged, unregistered filters, if necessary.
Yes
Is Port Priority correct?
No
Set Port Priority. See also the Traffic Class Configuration screen, if necessary.
Yes
Are all VLANs configured?
No
3
Yes
Done
Key
Off-page reference
On-page reference
BS35048B

Figure E-3. Configuring 802.1Q VLANs (3 of 3)

Configuring Security Settings

To configure or modify your security settings, follow the flowcharts in Figures E-4 to E-13.

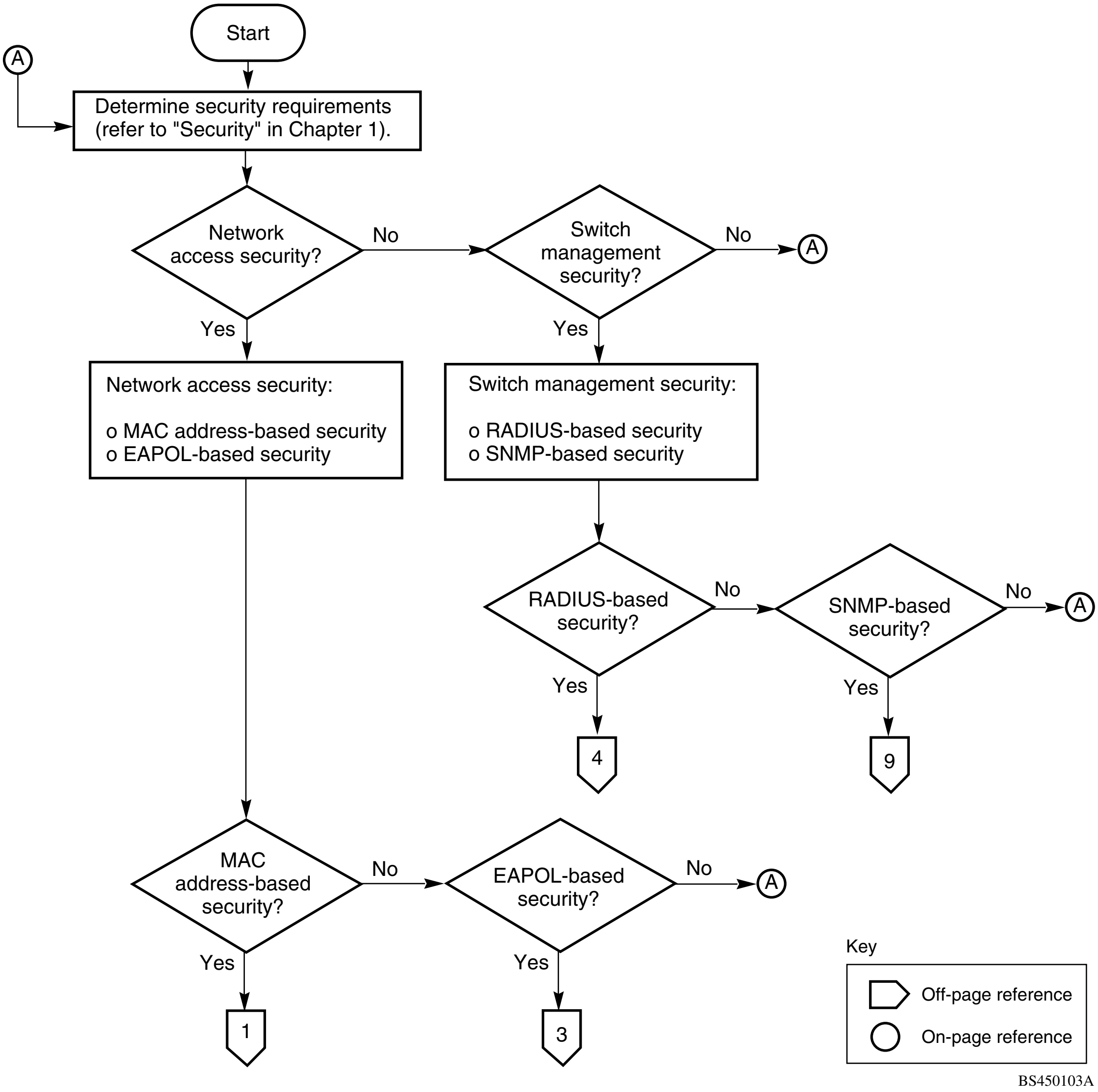


Figure E-4. Security Configurations

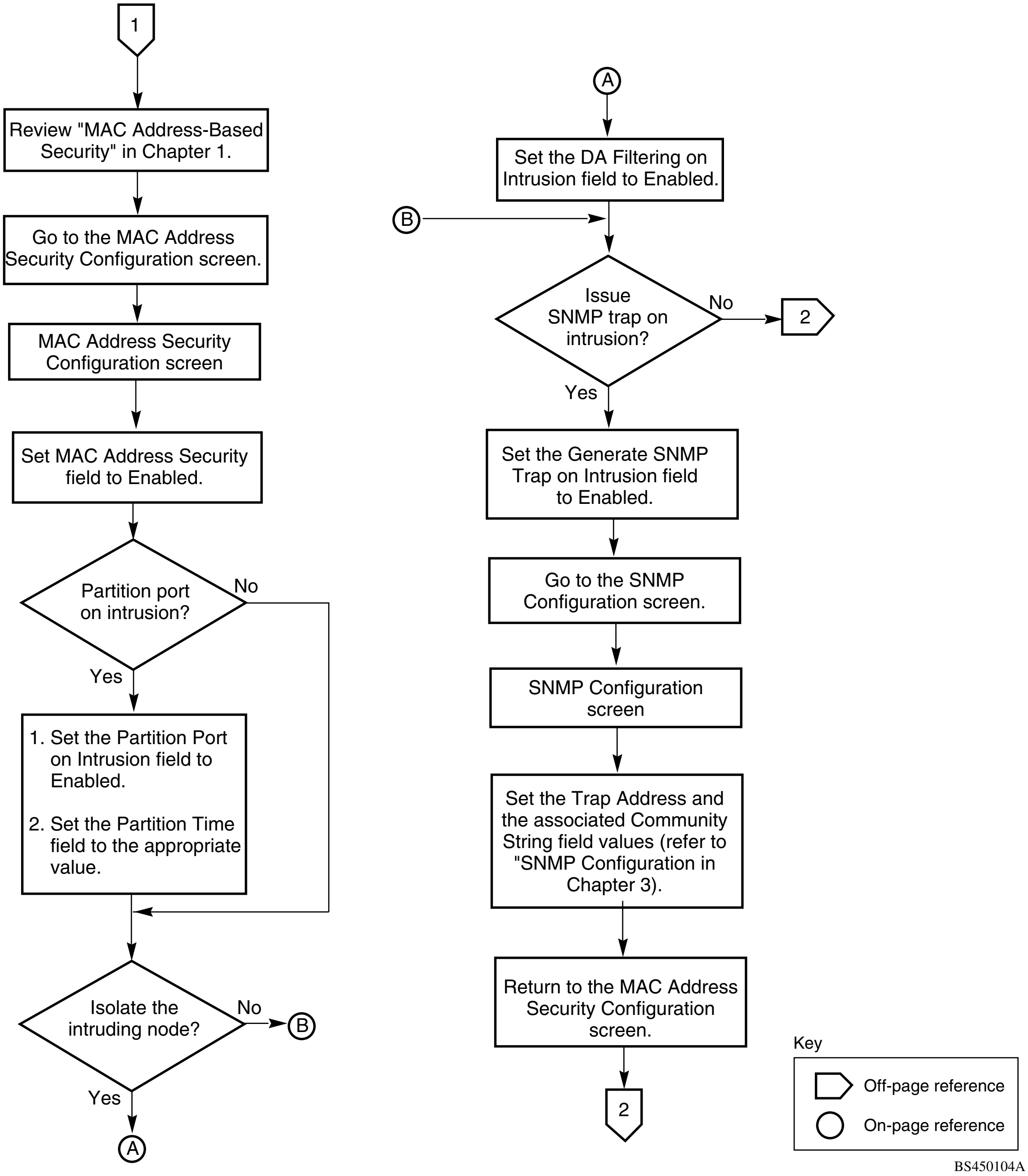

1
Review "MAC Address-Based Security" in Chapter 1.
Go to the MAC Address Security Configuration screen.
MAC Address Security Configuration screen
Set MAC Address Security field to Enabled.
Partition port on intrusion?
No
Yes
1. Set the Partition Port on Intrusion field to Enabled.
2. Set the Partition Time field to the appropriate value.
Isolate the intruding node?
No
B
Yes
A
A
Set the DA Filtering on Intrusion field to Enabled.
B
Issue SNMP trap on intrusion?
No
2
Yes
Set the Generate SNMP Trap on Intrusion field to Enabled.
Go to the SNMP Configuration screen.
SNMP Configuration screen
Set the Trap Address and the associated Community String field values (refer to "SNMP Configuration in Chapter 3).
Return to the MAC Address Security Configuration screen.
2
Key
Off-page reference
On-page reference
BS450104A

Figure E-5. MAC Address-Based Security (1 of 2)

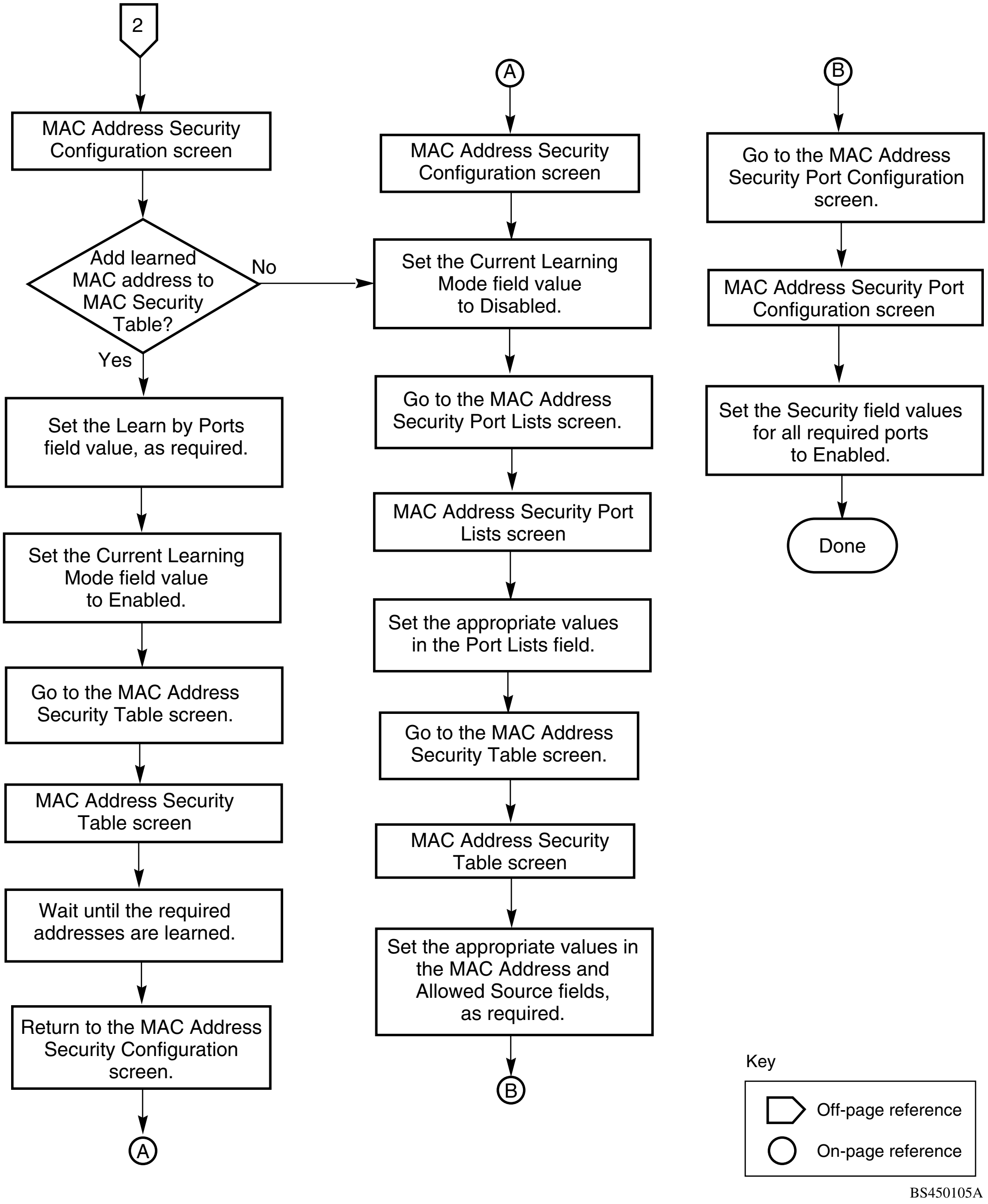

2
MAC Address Security Configuration screen
Add learned MAC address to MAC Security Table?
No
Yes
Set the Learn by Ports field value, as required.
Set the Current Learning Mode field value to Enabled.
Go to the MAC Address Security Table screen.
MAC Address Security Table screen
Wait until the required addresses are learned.
Return to the MAC Address Security Configuration screen.
A
A
MAC Address Security Configuration screen
Set the Current Learning Mode field value to Disabled.
Go to the MAC Address Security Port Lists screen.
MAC Address Security Port Lists screen
Set the appropriate values in the Port Lists field.
Go to the MAC Address Security Table screen.
MAC Address Security Table screen
Set the appropriate values in the MAC Address and Allowed Source fields, as required.
B
B
Go to the MAC Address Security Port Configuration screen.
MAC Address Security Port Configuration screen
Set the Security field values for all required ports to Enabled.
Done
Key
Off-page reference
On-page reference
BS450105A

Figure E-6. MAC Address-Based Security (2 of 2)

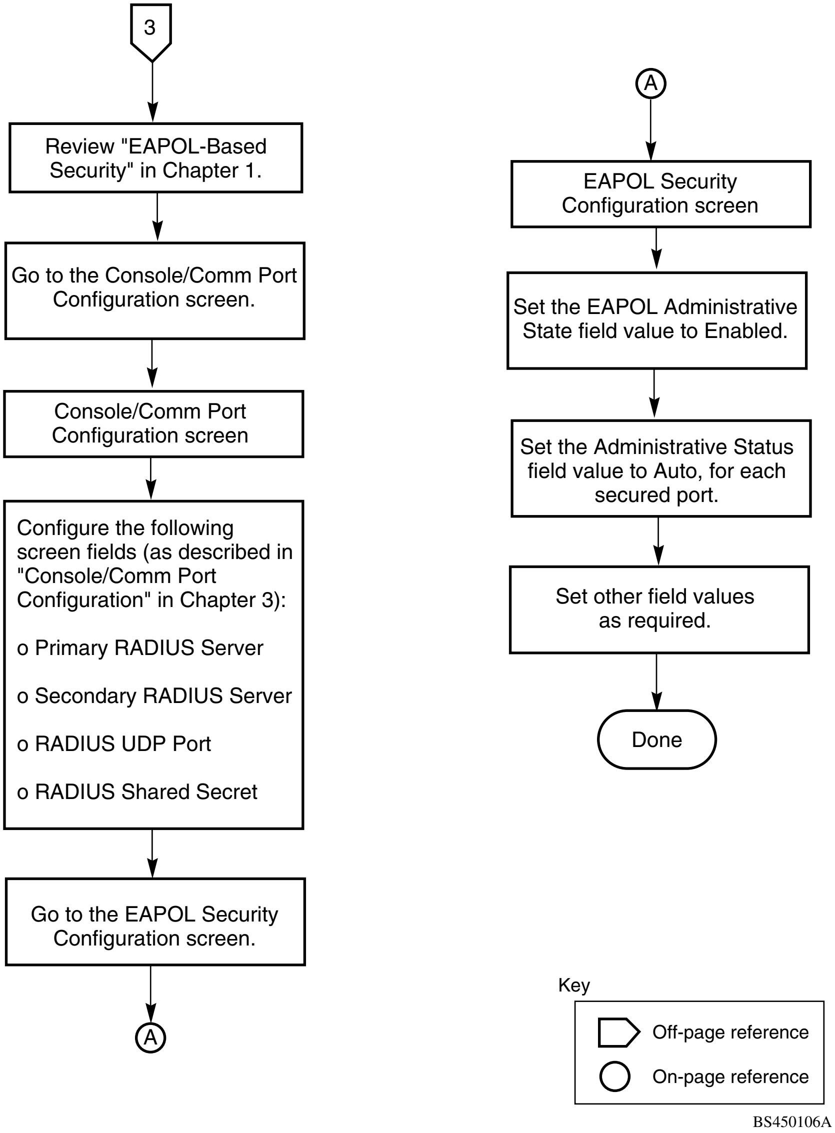

3
Review "EAPOL-Based Security" in Chapter 1.
Go to the Console/Comm Port Configuration screen.
Console/Comm Port Configuration screen
Configure the following screen fields (as described in "Console/Comm Port Configuration" in Chapter 3):
o Primary RADIUS Server
o Secondary RADIUS Server
o RADIUS UDP Port
o RADIUS Shared Secret
Go to the EAPOL Security Configuration screen.
A
A
EAPOL Security Configuration screen
Set the EAPOL Administrative State field value to Enabled.
Set the Administrative Status field value to Auto, for each secured port.
Set other field values as required.
Done
Key
Off-page reference
On-page reference
BS450106A

Figure E-7. EAPOL-Based Security

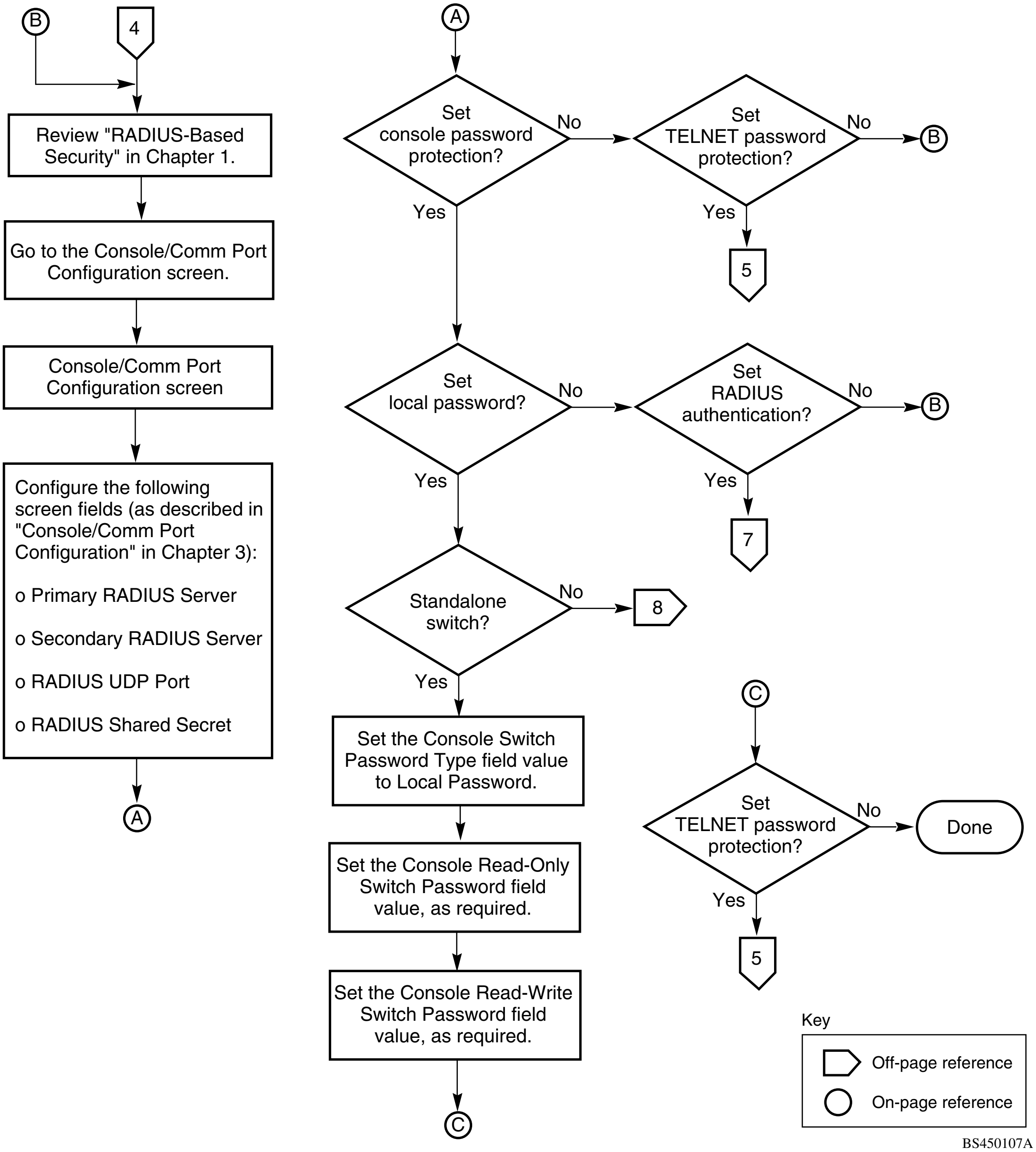

B
4
Review "RADIUS-Based Security" in Chapter 1.
Go to the Console/Comm Port Configuration screen.
Console/Comm Port Configuration screen
Configure the following screen fields (as described in "Console/Comm Port Configuration" in Chapter 3):
o Primary RADIUS Server
o Secondary RADIUS Server
o RADIUS UDP Port
o RADIUS Shared Secret
A
A
Set console password protection?
No
Yes
Set TELNET password protection?
No
B
Yes
5
Set local password?
No
Yes
Set RADIUS authentication?
No
B
Yes
7
Standalone switch?
No
8
Yes
Set the Console Switch Password Type field value to Local Password.
Set the Console Read-Only Switch Password field value, as required.
Set the Console Read-Write Switch Password field value, as required.
C
C
Set TELNET password protection?
No
Done
Yes
5
Key
Off-page reference
On-page reference
BS450107A

Figure E-8. RADIUS-Based Security (1 of 5)

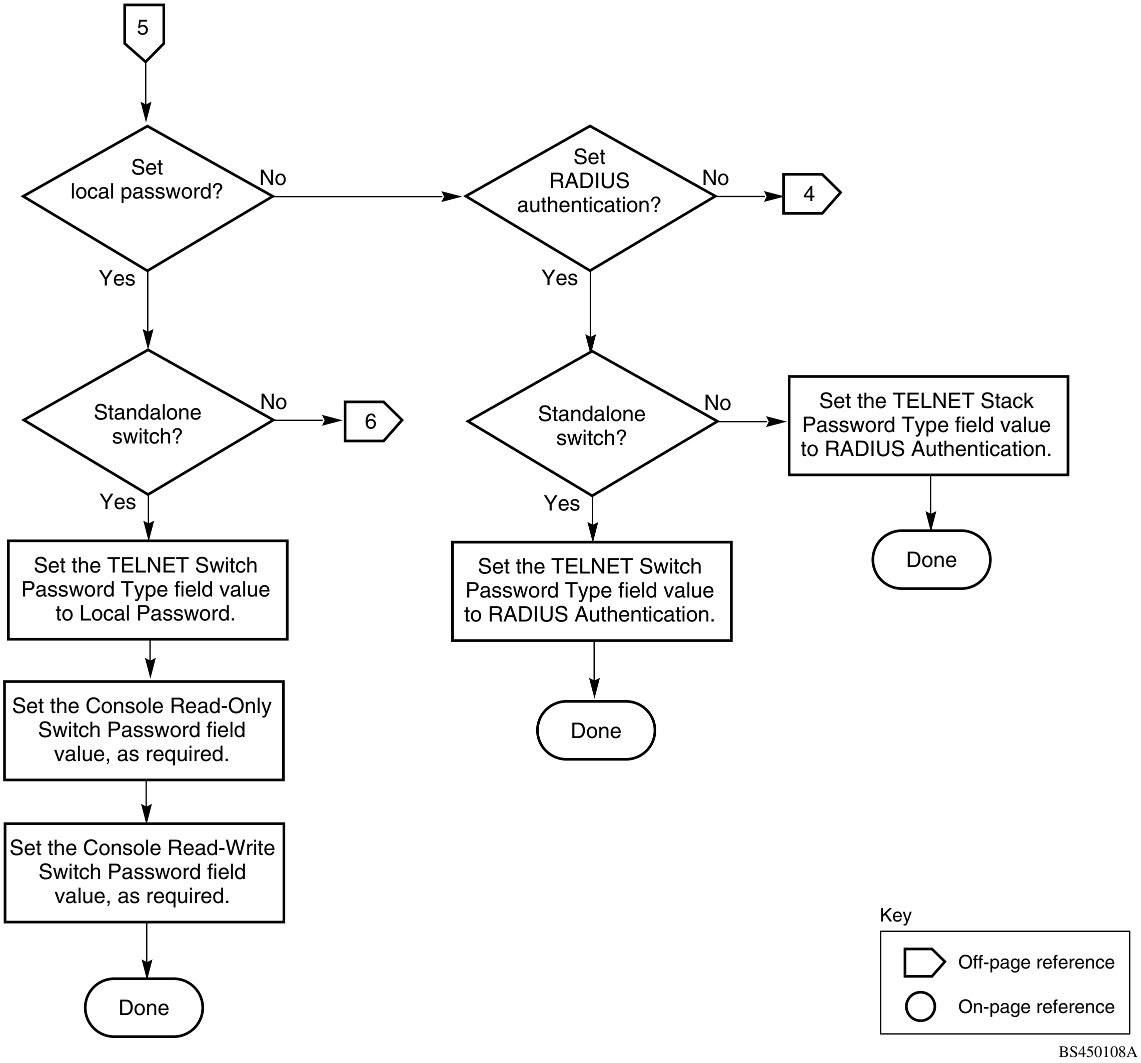

5
Set local password?
No
Set RADIUS authentication?
No
4
Yes
Yes
Standalone switch?
No
6
Standalone switch?
No
Set the TELNET Stack Password Type field value to RADIUS Authentication.
Yes
Yes
Done
Set the TELNET Switch Password Type field value to Local Password.
Set the TELNET Switch Password Type field value to RADIUS Authentication.
Set the Console Read-Only Switch Password field value, as required.
Done
Set the Console Read-Write Switch Password field value, as required.
Key
Off-page reference
On-page reference
Done
BS450108A

Figure E-9. RADIUS-Based Security (2 of 5)

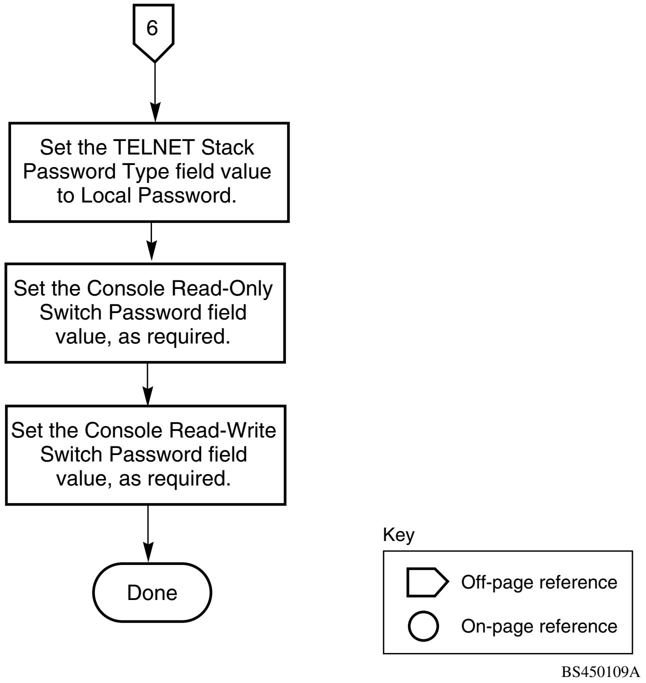

6
Set the TELNET Stack Password Type field value to Local Password.
Set the Console Read-Only Switch Password field value, as required.
Set the Console Read-Write Switch Password field value, as required.
Done
Key
Off-page reference
On-page reference
BS450109A

Figure E-10. RADIUS-Based Security (3 of 5)

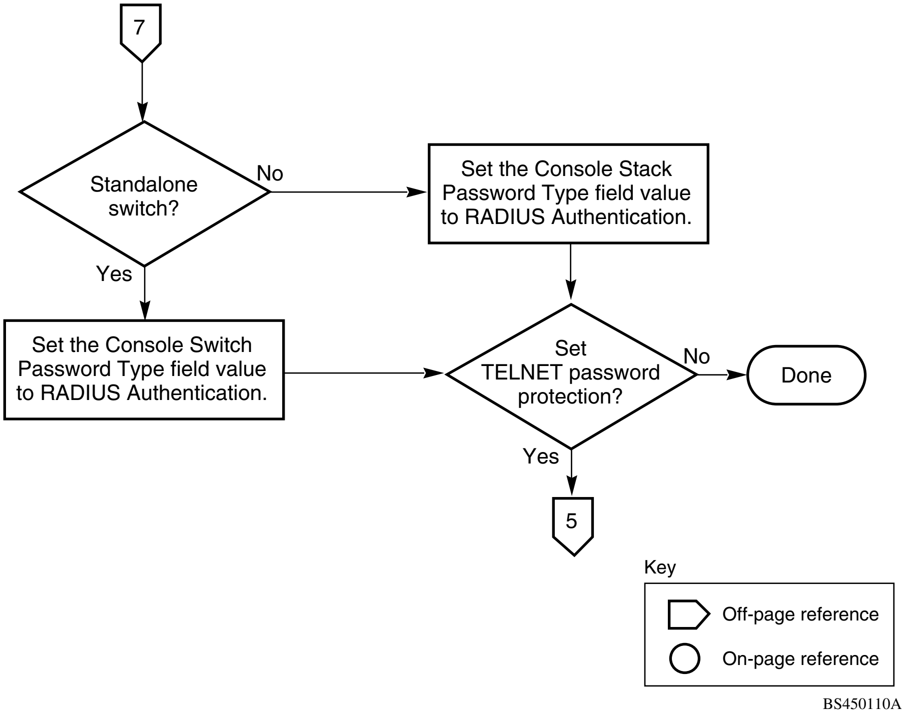

7
Standalone switch?
No
Set the Console Stack Password Type field value to RADIUS Authentication.
Yes
Set the Console Switch Password Type field value to RADIUS Authentication.
Set TELNET password protection?
No
Done
Yes
5
Key
Off-page reference
On-page reference
BS450110A

Figure E-11. RADIUS-Based Security (4 of 5)

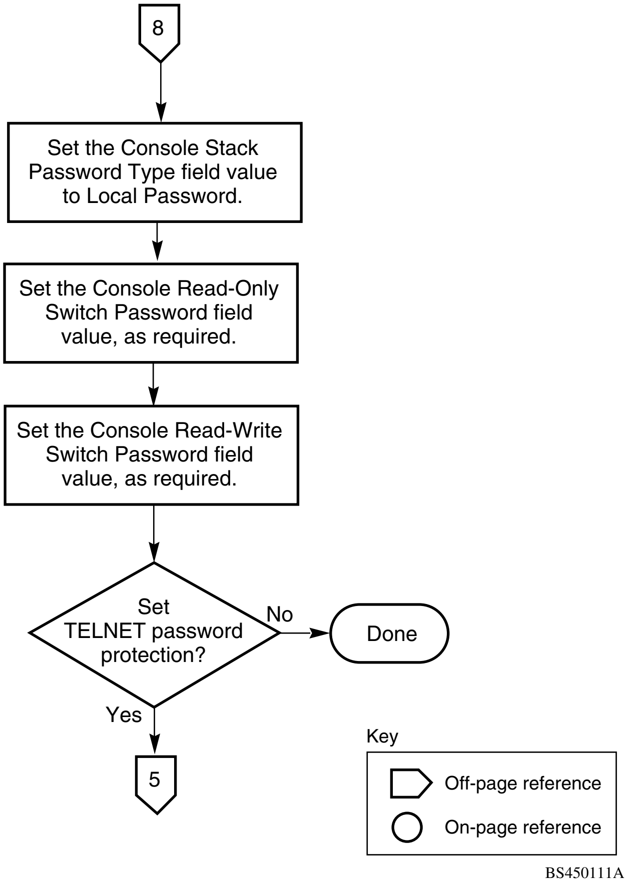

8
Set the Console Stack Password Type field value to Local Password.
Set the Console Read-Only Switch Password field value, as required.
Set the Console Read-Write Switch Password field value, as required.
Set TELNET password protection?
No
Done
Yes
5
Key
Off-page reference
On-page reference
BS450111A

Figure E-12. RADIUS-Based Security (5 of 5)

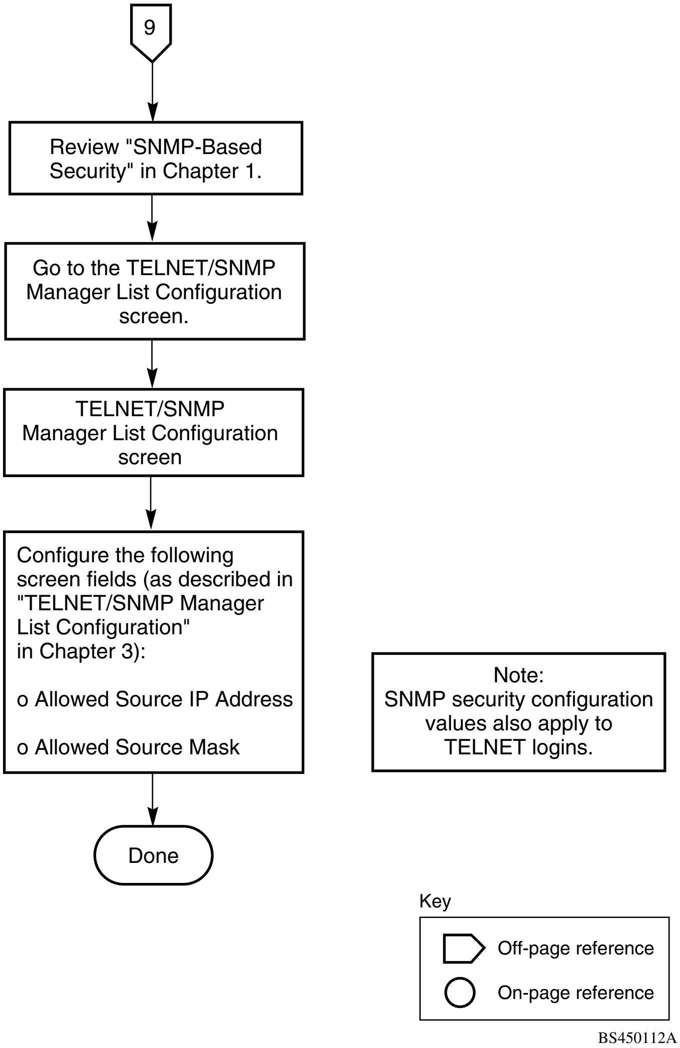
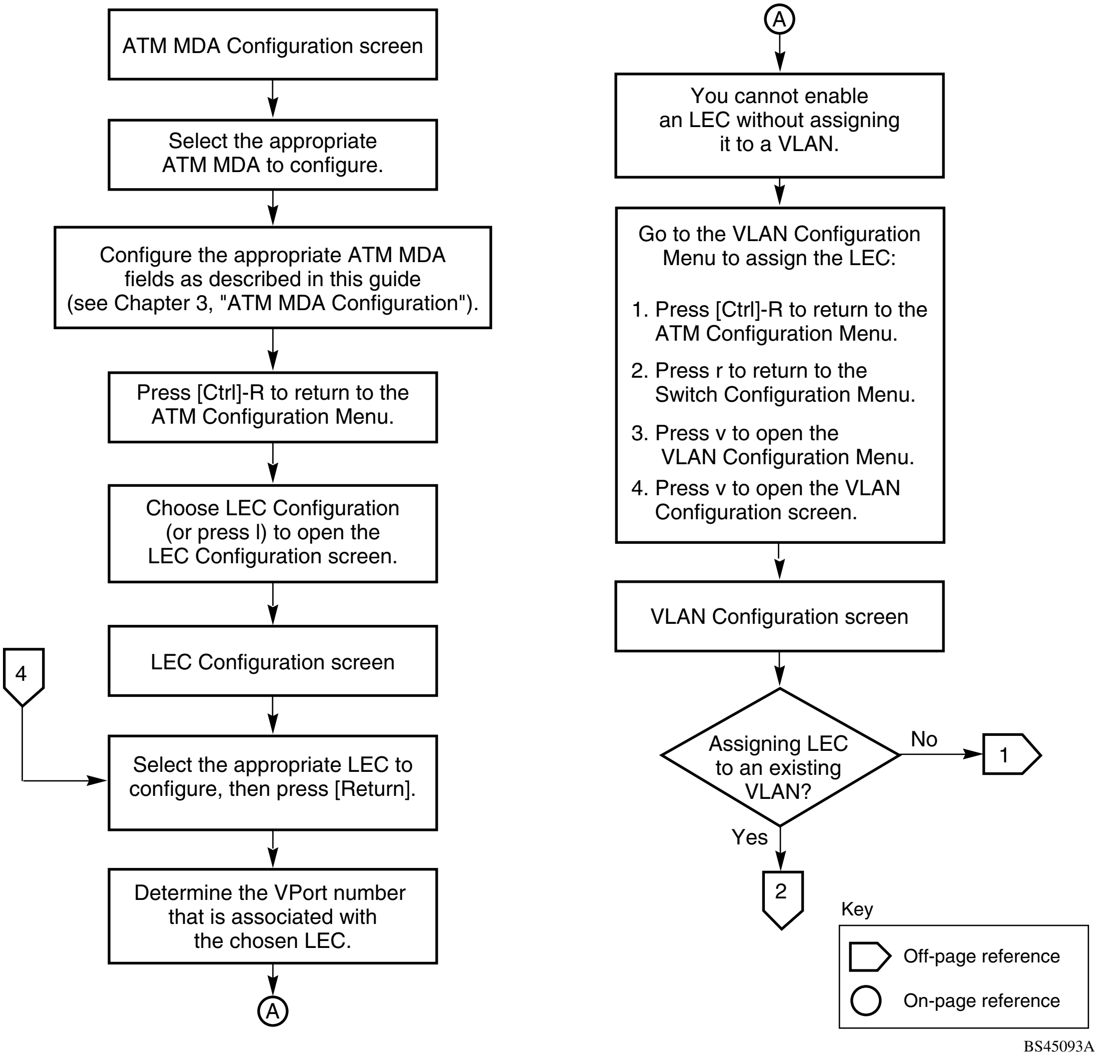

9
Review "SNMP-Based Security" in Chapter 1.
Go to the TELNET/SNMP Manager List Configuration screen.
TELNET/SNMP Manager List Configuration screen
Configure the following screen fields (as described in "TELNET/SNMP Manager List Configuration" in Chapter 3):
o Allowed Source IP Address
o Allowed Source Mask
Done
Note: SNMP security configuration values also apply to TELNET logins.
Key
Off-page reference
On-page reference
BS450112A

Figure E-13. SNMP-Based Security

Configuring the BayStack 450-2M3/2S3 MDAs

To configure or modify the BayStack 450-2M3/2S3 MDA, follow the flowcharts in Figures E-14 to E-16.

Choose ATM MDA Configuration (or press a) from the ATM Configuration Menu to open the ATM MDA Configuration screen.


ATM MDA Configuration screen

Select the appropriate ATM MDA to configure.

Configure the appropriate ATM MDA fields as described in this guide (see Chapter 3, "ATM MDA Configuration").

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

Choose LEC Configuration (or press l) to open the LEC Configuration screen.

LEC Configuration screen

Select the appropriate LEC to configure, then press [Return].

Determine the VPort number that is associated with the chosen LEC.

You cannot enable an LEC without assigning it to a VLAN.

Go to the VLAN Configuration Menu to assign the LEC:

1. Press [Ctrl]-R to return to the ATM Configuration Menu.
2. Press r to return to the Switch Configuration Menu.
3. Press v to open the VLAN Configuration Menu.
4. Press v to open the VLAN Configuration screen.

VLAN Configuration screen

Assigning LEC to an existing VLAN?

Figure E-14. Configuring the BayStack 450-2M3/2S3 MDA (1 of 3)

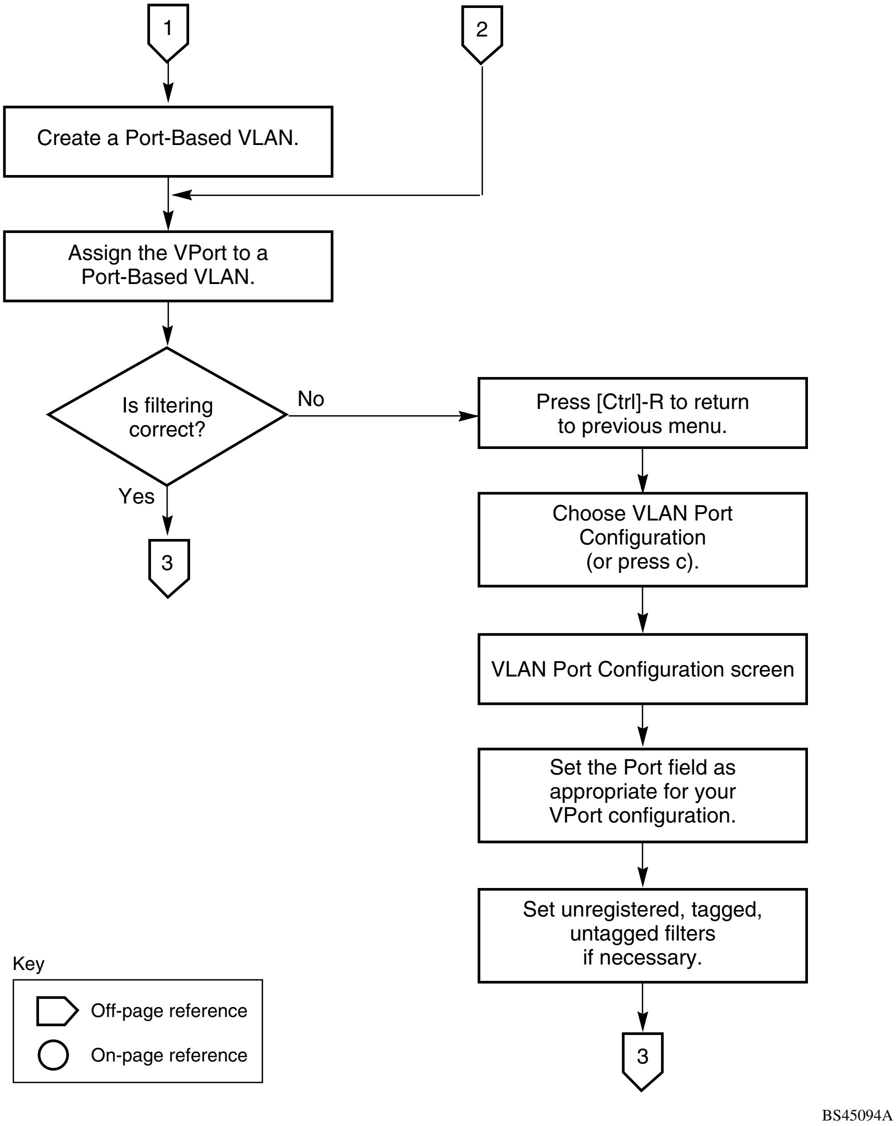

1
2
Create a Port-Based VLAN.
Assign the VPort to a Port-Based VLAN.
Is filtering correct?
No
Yes
3
Press [Ctrl]-R to return to previous menu.
Choose VLAN Port Configuration (or press c).
VLAN Port Configuration screen
Set the Port field as appropriate for your VPort configuration.
Set unregistered, tagged, untagged filters if necessary.
3
Key
Off-page reference
On-page reference
BS45094A

Figure E-15. Configuring the BayStack 450-2M3/2S3 MDA (2 of 3)

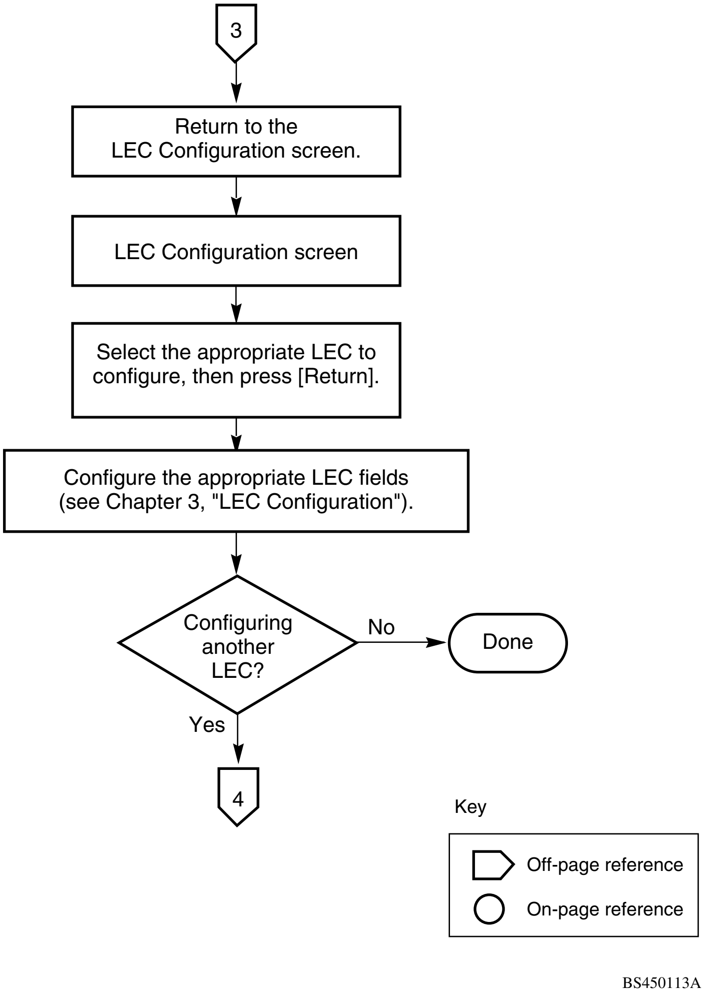

3
Return to the LEC Configuration screen.
LEC Configuration screen
Select the appropriate LEC to configure, then press [Return].
Configure the appropriate LEC fields (see Chapter 3, "LEC Configuration").
Configuring another LEC?
No
Done
Yes
4
Key
Off-page reference
On-page reference
BS450113A

Figure E-16. Configuring the BayStack 450-2M3/2S3 MDA (3 of 3)

For detailed information about the the BayStack 450-2M3/2S3 MDA configuration screens, see “ATM Configuration Menu” on page 3-85.

For conceptual information about the BayStack 450-2M3/2S3 MDA and configuration tips, see Appendix D, “ATM Overview.”

Configuring MultiLink Trunks

To create or modify a MultiLink trunk, follow the flowchart in Figure E-17.

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

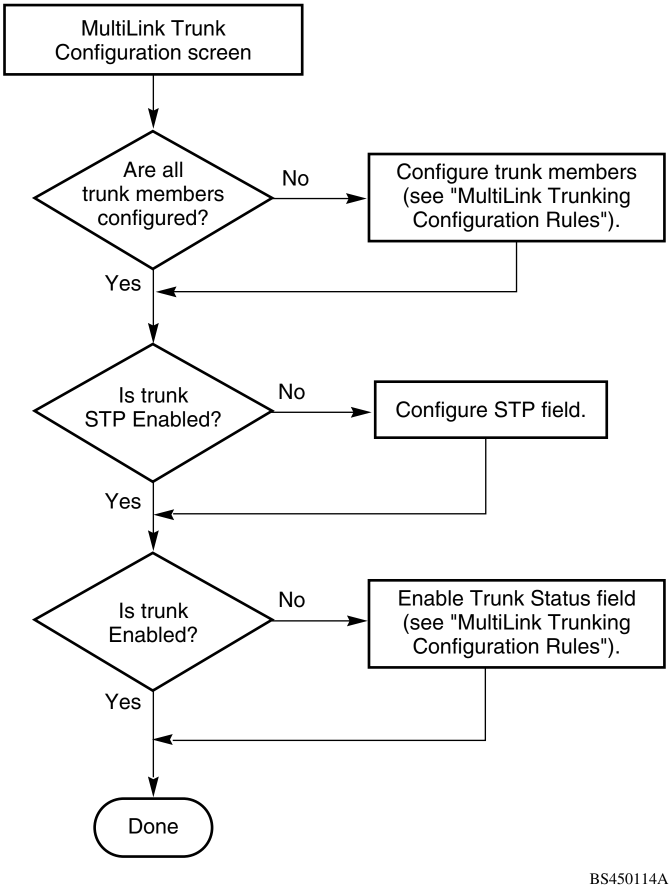

MultiLink Trunk Configuration screen
Are all trunk members configured?
No
Configure trunk members (see "MultiLink Trunking Configuration Rules").
Yes
Is trunk STP Enabled?
No
Configure STP field.
Yes
Is trunk Enabled?
No
Enable Trunk Status field (see "MultiLink Trunking Configuration Rules").
Yes
Done
BS450114A

Figure E-17. Configuring MultiLink Trunks

Configuring Port Mirroring

To create or modify port-mirroring ports, follow the flowcharts in Figures E-18 and E-19.

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

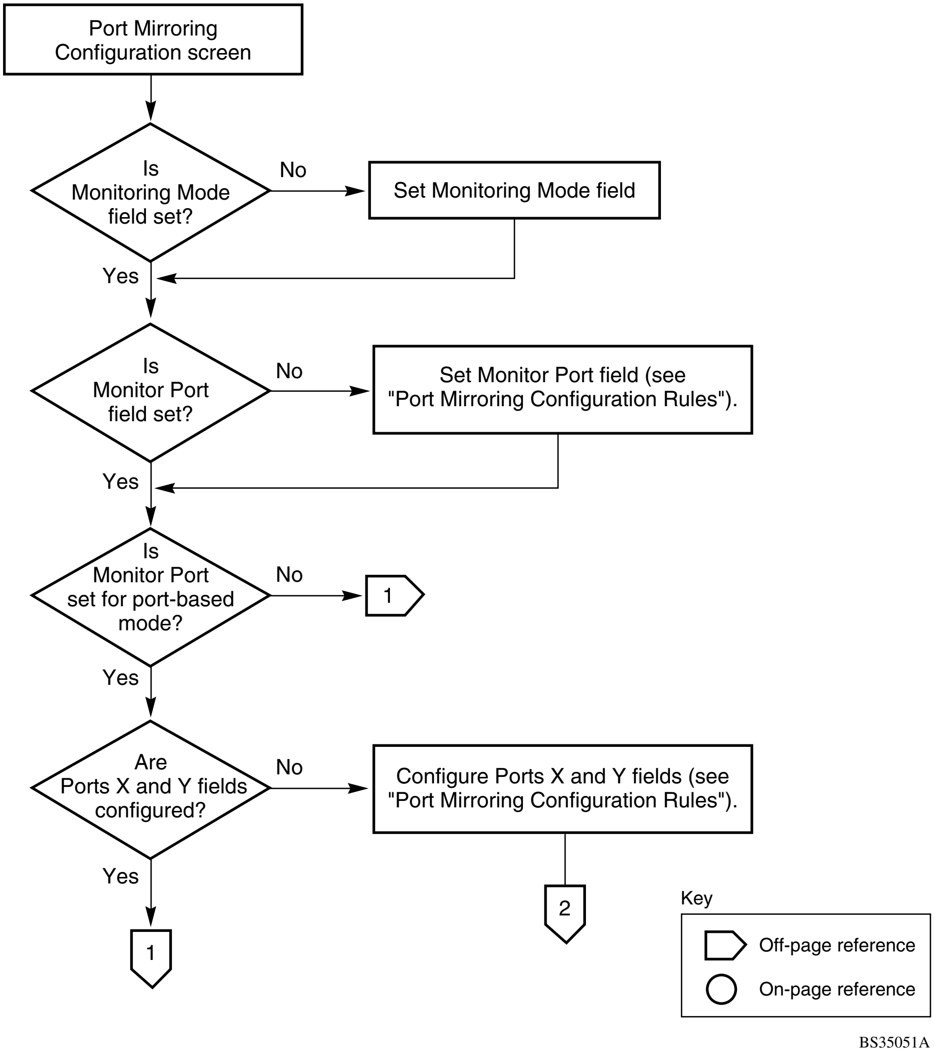

Port Mirroring Configuration screen
Is Monitoring Mode field set?
No
Set Monitoring Mode field
Yes
Is Monitor Port field set?
No
Set Monitor Port field (see "Port Mirroring Configuration Rules").
Yes
Is Monitor Port set for port-based mode?
No
1
Yes
Are Ports X and Y fields configured?
No
Configure Ports X and Y fields (see "Port Mirroring Configuration Rules").
Yes
1
2
Key
Off-page reference
On-page reference
BS35051A

Figure E-18. Configuring Port Mirroring (1 of 2)

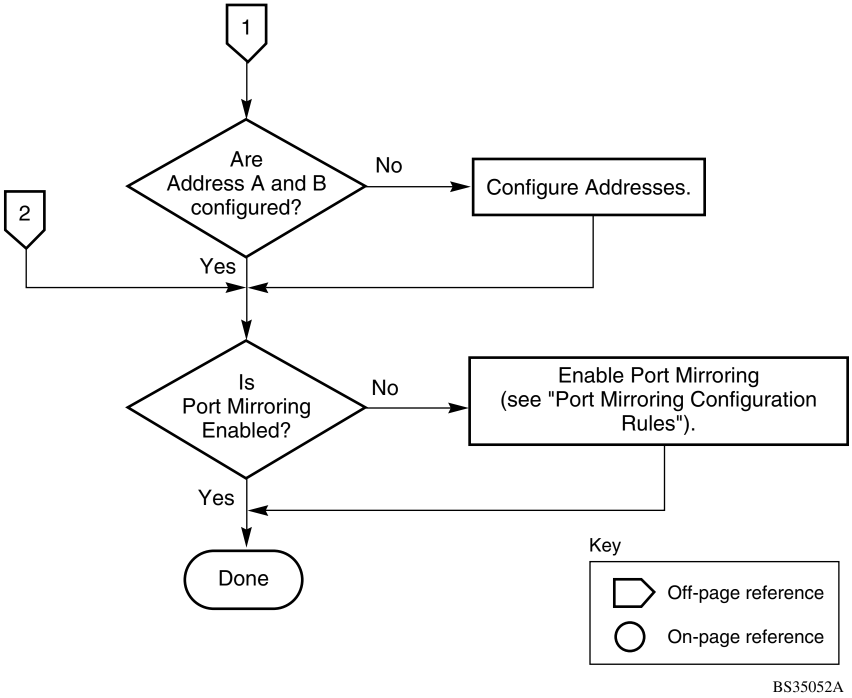

1
Are Address A and B configured?
No
Configure Addresses.
2
Yes
Is Port Mirroring Enabled?
No
Enable Port Mirroring (see "Port Mirroring Configuration Rules").
Yes
Done
Key
Off-page reference
On-page reference
BS35052A

Figure E-19. Configuring Port Mirroring (2 of 2)

Configuring IGMP Snooping

To create or modify IGMP Snooping ports, follow the flowcharts in Figures E-20 to E-22.

Choose IGMP Configuration (or press g) from the Switch Configuration Menu screen to open the IGMP Configuration screen.

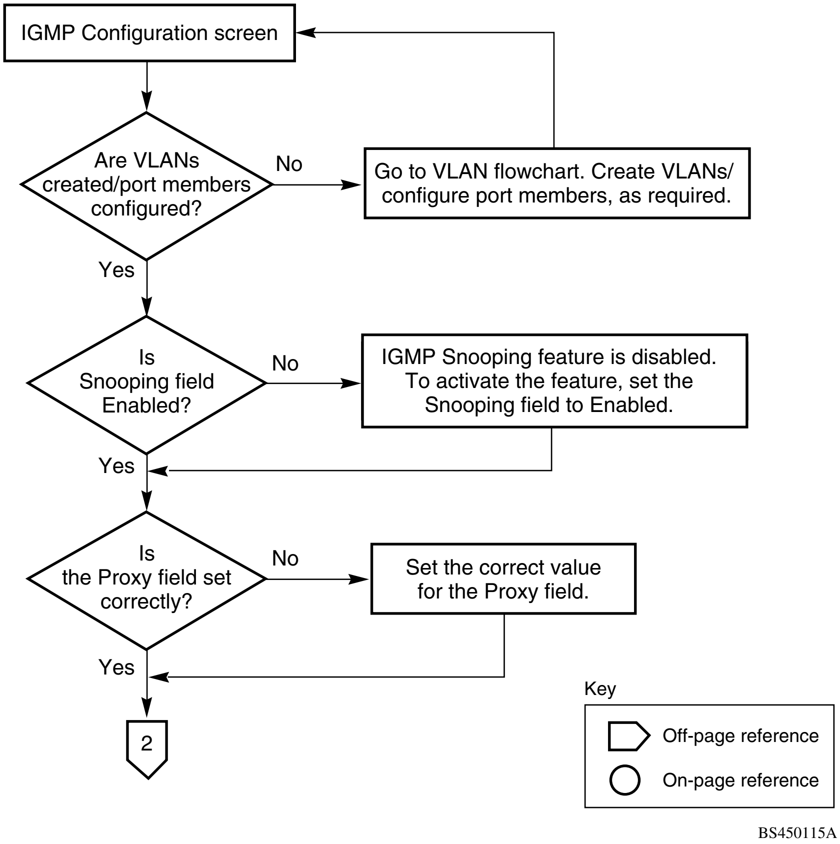

IGMP Configuration screen
Are VLANs created/port members configured?
No
Go to VLAN flowchart. Create VLANs/ configure port members, as required.
Yes
Is Snooping field Enabled?
No
IGMP Snooping feature is disabled. To activate the feature, set the Snooping field to Enabled.
Yes
Is the Proxy field set correctly?
No
Set the correct value for the Proxy field.
Yes
2
Key
Off-page reference
On-page reference
BS450115A

Figure E-20. Configuring IGMP Snooping (1 of 3)

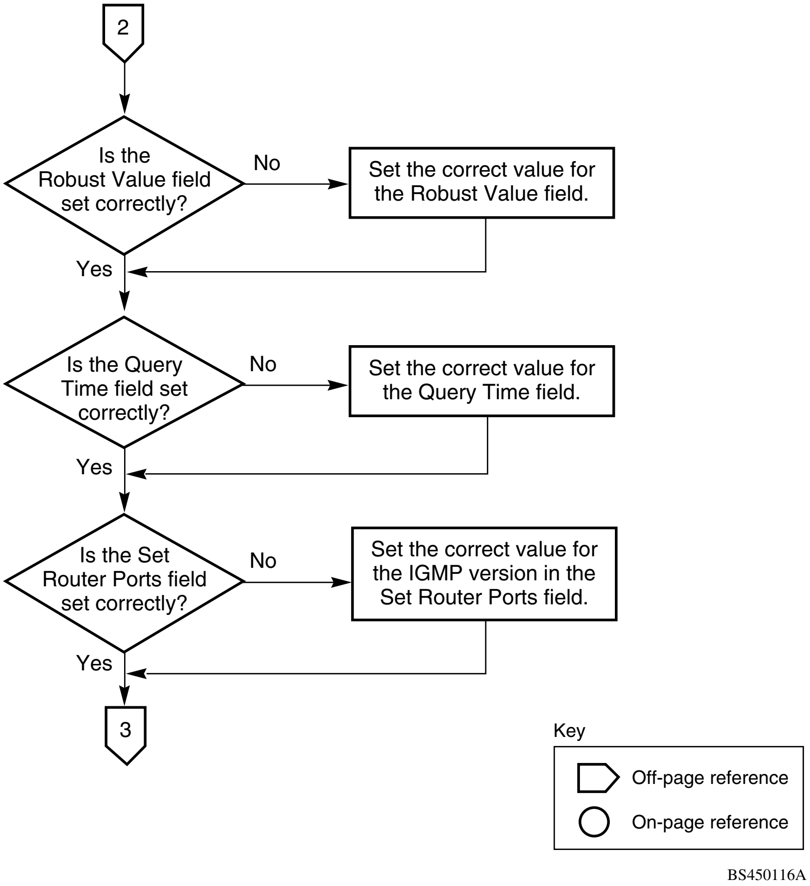

2
Is the Robust Value field set correctly?
No
Set the correct value for the Robust Value field.
Yes
Is the Query Time field set correctly?
No
Set the correct value for the Query Time field.
Yes
Is the Set Router Ports field set correctly?
No
Set the correct value for the IGMP version in the Set Router Ports field.
Yes
3
Key
Off-page reference
On-page reference
BS450116A

Figure E-21. Configuring IGMP Snooping (2 of 3)

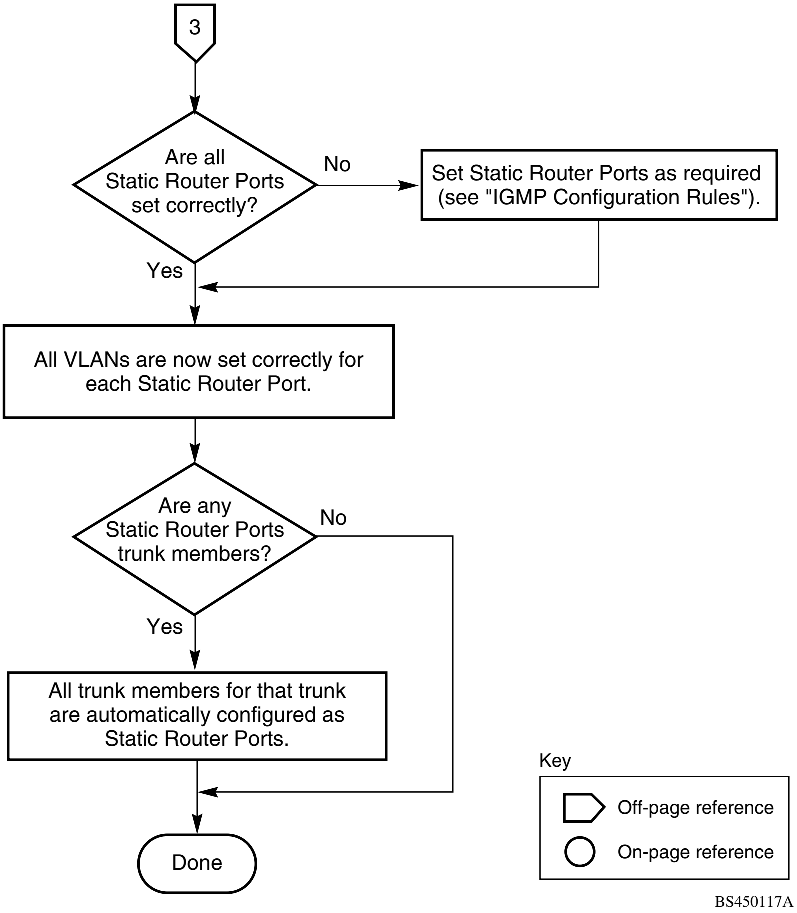

3
Are all Static Router Ports set correctly?
No
Set Static Router Ports as required (see "IGMP Configuration Rules").
Yes
All VLANs are now set correctly for each Static Router Port.
Are any Static Router Ports trunk members?
No
Yes
All trunk members for that trunk are automatically configured as Static Router Ports.
Done
Key
Off-page reference
On-page reference
BS450117A

Figure E-22. Configuring IGMP Snooping (3 of 3)

Appendix F
Connectors and Pin Assignments

This appendix describes the BayStack 350 switch port connectors and pin assignments.

This appendix covers the following topics:

- “RJ-45 (10BASE-T/100BASE-TX) Port Connectors) (page F-1)
- “MDI and MDI-X Devices” (page F-2)
- “DB-9 (RS-232-D) Console/Comm Port Connector” (page F-5)

RJ-45 (10BASE-T/100BASE-TX) Port Connectors

The RJ-45 port connectors (Figure F-1) are wired as MDI-X ports to connect end stations without using crossover cables. (See “MDI and MDI-X Devices” on page F-2 for information about MDI-X ports.) For 10BASE-T connections, use Category 3 (or higher) UTP cable. For 100BASE-TX connections, use only Category 5 UTP cable.

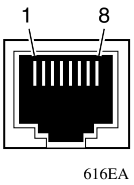


Figure F-1. RJ-45 (8-Pin Modular) Port Connector

Table F-1 lists the RJ-45 (8-pin modular) port connector pin assignments.

Table F-1. RJ-45 Port Connector Pin Assignments

Pin	Signal	Description
1	RX+	Receive Data +
2	RX-	Receive Data -
3	TX+	Transmit Data +
4	Not applicable	Not applicable
5	Not applicable	Not applicable
6	TX-	Transmit Data -
7	Not applicable	Not applicable
8	Not applicable	Not applicable

MDI and MDI-X Devices

Media dependent interface (MDI) is the IEEE standard for the interface to unshielded twisted pair (UTP) cable.

For two devices to communicate, the transmitter of one device must connect to the receiver of the other device. The connection is established through a crossover function, which can be a crossover cable or a port that implements the crossover function internally.

Ports that implement the crossover function internally are known as MDI-X ports, where X refers to the crossover function.

Note: For the transmitter of one device to connect to the receiver of another device, the total number of crossovers must always be an odd number.

The following sections describe the use of straight-through and crossover cables for connecting MDI and MDI-X devices.

MDI-X to MDI Cable Connections

BayStack 350 switches use MDI-X ports that allow you to connect directly to end stations without using crossover cables (Figure F-2).

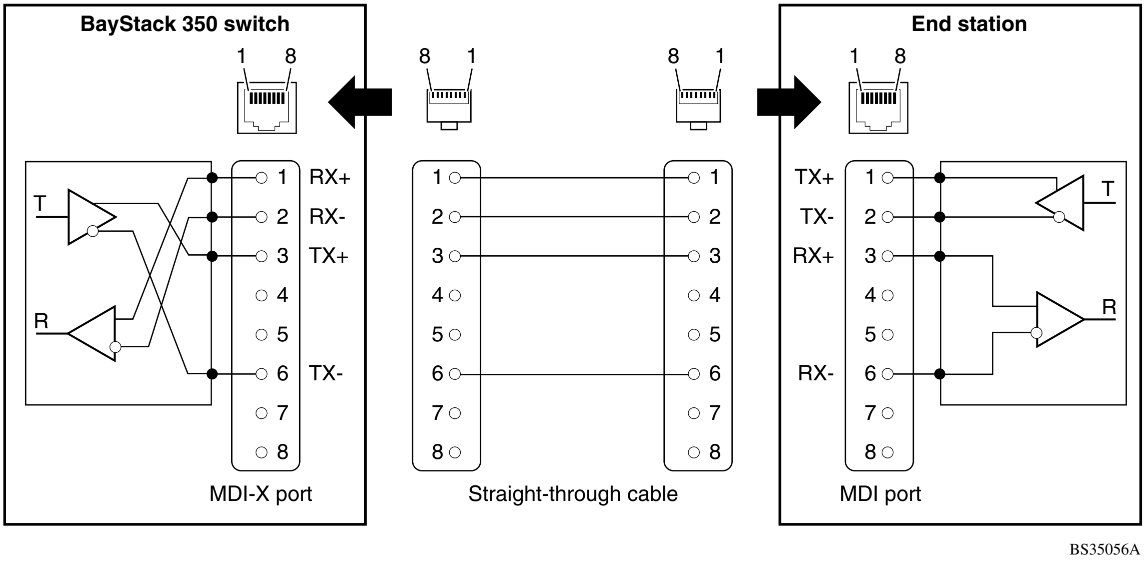


Figure F-2. MDI-X to MDI Cable Connections

MDI-X to MDI-X Cable Connections

If you are connecting the BayStack 350 switch to a device that also implements MDI-X ports, use a crossover cable (Figure F-3).

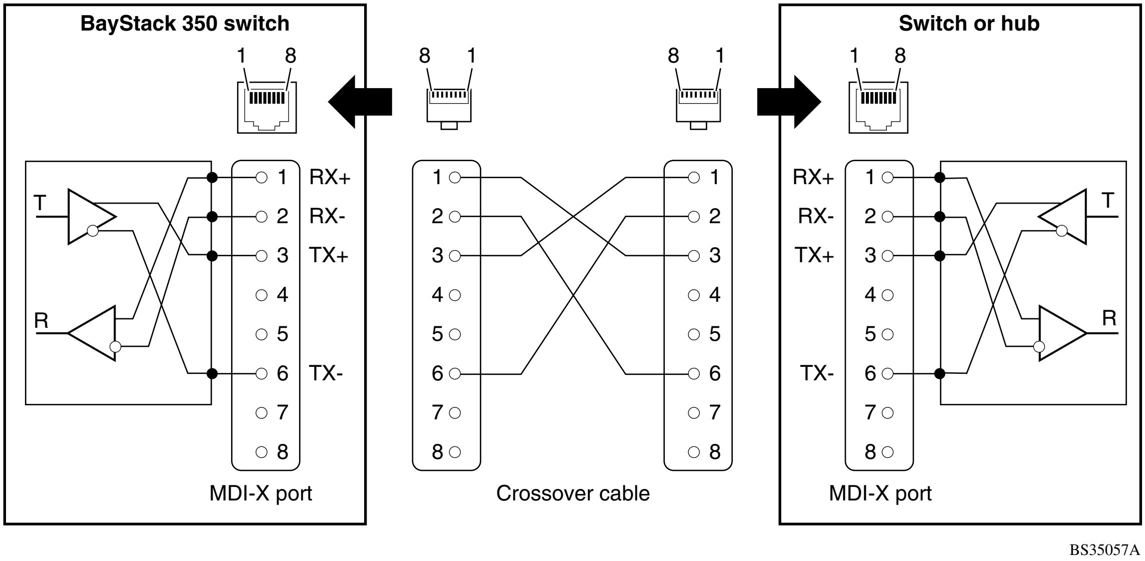


Figure F-3. MDI-X to MDI-X Cable Connections

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

The DB-9 Console/Comm Port connector (Figure F-4) 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.

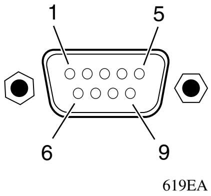


Figure F-4. DB-9 Console/Comm Port Connector

Table F-2 lists the DB-9 Console/Comm Port connector pin assignments.

Table F-2. DB-9 Console/Comm Port Connector Pin Assignments

Pin	Signal	Description
1	CD	Carrier detect (not used)
2	TXD	Transmit data (output)
3	RXD	Receive data (input)
4	DTR	Data terminal ready (not used)
5	GND	Signal ground
6	DSR	Data set ready (output always asserted)
7	RTS	Request to send (not used)
8	CTS	Clear to send (output always asserted)
9	RI	Ring indicator (not used)
Shell		Chassis ground

Appendix G
Default Settings

Table G-1 lists the factory default settings for the BayStack 350 switch.

Table G-1. Factory Default Settings for the BayStack 350 Switch

CI screen	Field	Default setting
IP Configuration/Setup (page 3-9)	BootP Request Mode	BootP Disabled
	In-Band Stack IP Address	0.0.0.0 (Not Used)
	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)
	IP Address to Ping	0.0.0.0 (no IP address assigned)
	Start Ping	No
SNMP Configuration (page 3-14)	Read-Only Community String	public
	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

(continued)

Table G-1. Factory Default Settings for the BayStack 350 Switch *(continued)*

CI screen	Field	Default setting
System Characteristics (page 3-16)	Reset Count	1
	Last Reset Type	Power Cycle
	Power Status	Primary Power
	sysContact	Zero-length string
	sysName	Zero-length string
	sysLocation	Zero-length string
MAC Address Table (page 3-20)	Aging Time	300 seconds
	Find an Address	00-00-00-00-00-00 (no MAC address assigned)
	Port Mirroring Address A:	00-00-00-00-00-00 (no MAC address assigned)
	Port Mirroring Address B:	00-00-00-00-00-00 (no MAC address assigned)
MAC Address Security Configuration (page 3-24)	MAC Address Security	Disabled
	MAC Address Security SNMP_Locked	Disabled
	Partition Port on Intrusion	Disabled
	Partition Time	1 second
	DA Filtering on Intrusion	Disabled
	Generate SNMP Trap on Intrusion	Disabled
	Clear by Ports	NONE
	Learn by Ports	NONE
	Current Learning Mode	Disabled
MAC Address Security Port Configuration (page 3-28)	Security	Disabled
MAC Address Security Port Lists (page 3-30)	Port List	Blank field

(continued)

Table G-1. Factory Default Settings for the BayStack 350 Switch *(continued)*

CI screen	Field	Default setting
MAC Address Security Table (page 3-34)	Find an Address	00-00-00-00-00-00 (no MAC address assigned)
	MAC Address	- - - - - (no MAC address assigned)
	Allowed Source	- (Blank field)
EAPOL Security Configuration (page 3-37)	Unit	1
	Port	1
	Initialize	No
	Administrative Status	Force Authorized
	Operational Status	Authorized
	Administrative Traffic Control	Incoming and Outgoing (read-only)
	Operational Traffic Control	Incoming and Outgoing (read-only)
	Re-authenticate Now	No
	Re-authentication	Enabled
	Re-authentication Period	3600 seconds
	Quiet Period	60 seconds
	Transmit Period	30 seconds
	Supplicant Timeout	30 seconds
	Server Timeout	30 seconds
	Maximum Requests	2 attempts
VLAN Configuration (page 3-43)	Create VLAN	1
	Delete VLAN	blank field
	VLAN Name	VLAN # (*VLAN number*)
	Management VLAN	Yes
	VLAN Type	Port-Based
	Protocol Id (PID)	None
	User-defined PID	0x0000
	VLAN State	Inactive

(continued)

Table G-1. Factory Default Settings for the BayStack 350 Switch *(continued)*

CI screen	Field	Default setting
	Port Membership	U (all ports assigned as untagged members of VLAN 1)
VLAN Port Configuration (page 3-49)	Port	1
	Filter Tagged Frames	No
	Filter Untagged Frames	No
	Filter Unregistered Frames	No
	Port Name	Port 1
	PVID	1
	Port Priority	0
	Tagging	Untagged Access
	AutoPVID (all ports)	Disabled
VLAN Display by Port (page 3-52)	Port	1
	PVID	1 (read only)
	Port Name	Port 1 (read only)
Traffic Class Configuration (page 3-54)	Traffic Class	Low
Port Configuration (page 3-56)	Status	Enabled (for all ports)
	LnkTrap	On
	Autonegotiation	Enabled (for all ports)
	Speed/Duplex	100Mbs/Half (when Autonegotiation is Disabled)
High Speed Flow Control Configuration (page 3-58)	Autonegotiation	Enabled
	Flow Control	Disabled
	Note: The following two fields only appear when a single Phy MDA with a separate redundant Phy port is installed.	
	Preferred Phy	Right
	Active Phy	Read-only field indicating the operational Phy port (Right, Left, or None)

(continued)

Table G-1. Factory Default Settings for the BayStack 350 Switch *(continued)*

CI screen	Field	Default setting
MultiLink Trunk Configuration (page 3-61)	Trunk Members	Zero-length string
	STP	Normal
	Trunk Mode	Basic
	Trunk Status	Enabled
	Trunk Name	Trunk #1 to Trunk #6
MultiLink Trunk Utilization (page 3-65)	Traffic Type	Rx and Tx
Port Mirroring Configuration (page 3-67)	Monitoring Mode	Disabled
	Monitor Port	Zero-length string
	Port X	Zero-length string
	Port Y	Zero-length string
	Address A	00-00-00-00-00-00 (no MAC address assigned)
	Address B	00-00-00-00-00-00 (no MAC address assigned)
Rate Limiting Configuration (page 3-71)	Packet Type	Both
	Limit	None
IGMP Configuration (page 3-75)	VLAN	1
	Snooping	Enabled
	Proxy	Enabled
	Robust Value	2
	Query Time	125 seconds
	Set Router Ports	Version 1
	Static Router Ports	- (for all ports)
Multicast Group Membership (page 3-79)	VLAN	1
Port Statistics (page 3-81)	Port	1
LEC Configuration (page 3-87)	LEC	1
	LEC Status	Disable
	LEC State	Disabled
	ELAN Name	default
	VLAN	0 (no VLAN assigned)

(continued)

Table G-1. Factory Default Settings for the BayStack 350 Switch *(continued)*

CI screen	Field	Default setting
	LEC Vport	13 (12-port models) 25 (24-port models)
	Desired Physical Port	A1
	Actual Physical Port	A1
ATM MDA Configuration (page 3-89)	LEC Fail Over	Disabled
	LECS Address Method	ATM Forum
	User Defined Address	39-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
	UNI Version	3.1
	PHY Type	SONET
ATM MDA Software Download (page 3-92)	Image Filename	Zero-length string
	TFTP Server IP Address	0.0.0.0 (no IP address assigned)
	Start TFTP Transfer of MDA Image	No
Console/Comm Port Configuration (page 3-95)	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

(continued)

Table G-1. Factory Default Settings for the BayStack 350 Switch *(continued)*

CI screen	Field	Default setting
	RADIUS UDP Port	1645
	RADIUS Shared Secret	Blank field
Spanning Tree Port Configuration (page 3-104)	Participation	Normal Learning
	Priority	128
	Path Cost	10 or 100
Spanning Tree Switch Settings (page 3-108)	Bridge Priority	8000 (read only)
	Designated Root	8000 (bridge_id) (read only)
	Root Port	Unit: 0 / 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/SNMP Manager List Configuration (page 3-111)	TELNET Access	Enabled
	Login Timeout	1 minute
	Login Retries	3
	Inactivity Timeout	15 minutes
	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)

(continued)

Table G-1. Factory Default Settings for the BayStack 350 Switch *(continued)*

CI screen	Field	Default setting
	(For details about this field, see Table 3-40 on page 3-112.)	Remaining nine fields: 255.255.255.255 (any address is allowed)
Software Download (page 3-114)	Image Filename	Zero-length string
	TFTP Server IP Address	0.0.0.0 (no IP address assigned)
	Start TFTP Load of New Image	No
Configuration File (page 3-118)	Configuration Image Filename	Zero-length string
	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 H
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 Bay 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=b350_100.img

# Where:
#    host name:                    bay1
#    hardware type:                Ethernet
#    MAC address:                  00-60-FD-00-00-00
#    IP address:                   192.0.0.1
#    home directory of boot file:  c:\ezlan\images
#    boot file:                    b350_100.img
```

Index