Using the BayStack 350 10/100/1000 Series Switch

Part No. 304376-B Rev 00
January 1999

Bay Networks Where Information Flows.™

Bay Networks *Where Information Flows.*™

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Statement of Conditions

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

Bay 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 Bay Networks BayStack 350 10/100 Autosense 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.

EC Declaration of Conformity

This product conforms to the provisions of Council Directive 89/336/EEC and 73/23/EEC. The Declaration of Conformity is available on the Bay Networks World Wide Web site at www.baynetworks.com.

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.

Canada Requirements Only

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (BayStack 350 10/100 Autosense 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 10/100 Autosense 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.

Bay 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 BAY 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. Bay Networks, Inc. (“Bay 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 Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay 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. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay 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 Bay 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 Bay 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. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay 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 Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay 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. Bay Networks will replace defective media at no charge if it is returned to Bay 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. Bay 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. Bay 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 Bay 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 BAY 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 BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY 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 Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay 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 Bay Networks the Software, user manuals, and all copies. Bay 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 Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY 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 BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Chapter 3
Using the Console Interface

Figures

Tables

Preface

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

There are two versions of the BayStack 350 10/100/1000 Series Switches: the BayStack 350-24T switch and the BayStack 350-12T switch. 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 Module slot for attaching optional media dependent adapters (MDAs) that support a range of media types, including gigabit Ethernet. Installation instructions are included with each MDA (see your Bay Networks sales representative for ordering information).

For more information about the MDAs, refer to Appendix B, “Media Dependent Adapters.”

Before You Begin

This guide is intended for network installers and system administrators who are responsible for installing, configuring, or maintaining networks.

This guide assumes that you have the following background:

- Understanding of the transmission and management protocols used on your network

Organization

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

If you want to:	Go to:
Learn about the BayStack 350 switch and its key features	Chapter 1
Install the BayStack 350 switch on a flat surface or in a 19-inch equipment rack, and verify its operation	Chapter 2
Connect to the BayStack 350 switch Console/Comm Port and learn how to use the console interface (CI) menus to configure and manage the switch	Chapter 3
Troubleshoot and diagnose problems with the BayStack 350 switch	Chapter 4
View operational and environmental specifications that apply to the BayStack 350 switch	Appendix A
Learn about optional media dependent adapters (MDAs) you can use with the BayStack 350 switch	Appendix B
Learn about Quick-Step flowcharts for using the BayStack 350 switch features	Appendix C
Learn more about the BayStack 350 switch connectors (ports) and pin assignments	Appendix D
View a listing of the factory default settings for the BayStack 350 switch	Appendix E
View a sample BootP configuration file	Appendix F
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 Bay Networks 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:

AUI	attachment unit interface
BootP	Bootstrap Protocol

(continued)

CSMA/CD	carrier sense multiple access/collision detection
IP	Internet Protocol
MAC	media access control
MDI-X	medium dependent interface crossover
PPP	Point-to-Point Protocol
SNMP	Simple Network Management Protocol

Related Publications

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

- *Installing Media Dependent Adapters (MDA)s* (Bay Networks part number 302403-B)

  Describes how to install optional media dependent adapters (MDA)s to your BayStack 350 switch.

You can now print Bay Networks technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs/*. Find the Bay Networks product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

You can purchase Bay Networks documentation sets, CDs, and selected technical publications through the Bay Networks Collateral Catalog. The catalog is located on the World Wide Web at *support.baynetworks.com/catalog.html* and is divided into sections arranged alphabetically:

- The “CD ROMs” section lists available CDs.
- The “Guides/Books” section lists books on technical topics.
- The “Technical Manuals” section lists available printed documentation sets.

Make a note of the part numbers and prices of the items that you want to order. Use the “Marketing Collateral Catalog description” link to place an order and to print the order form.

How to Get Help

For product assistance, support contracts, information about educational services, and the telephone numbers of our global support offices, go to the following URL:

http://www.baynetworks.com/corporate/contacts/

In the United States and Canada, you can dial 800-2LANWAN for assistance.

Chapter 1
BayStack 350 10/100/1000 Series Switches

This chapter introduces the BayStack 350 10/100/1000 Series Switches and covers the following topics:

- Physical description
- Summary of features
- Network configuration examples
- Overview of main features

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).

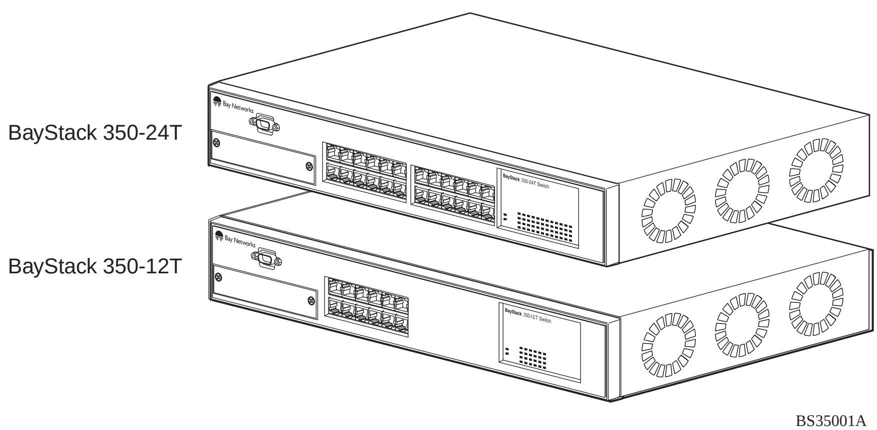
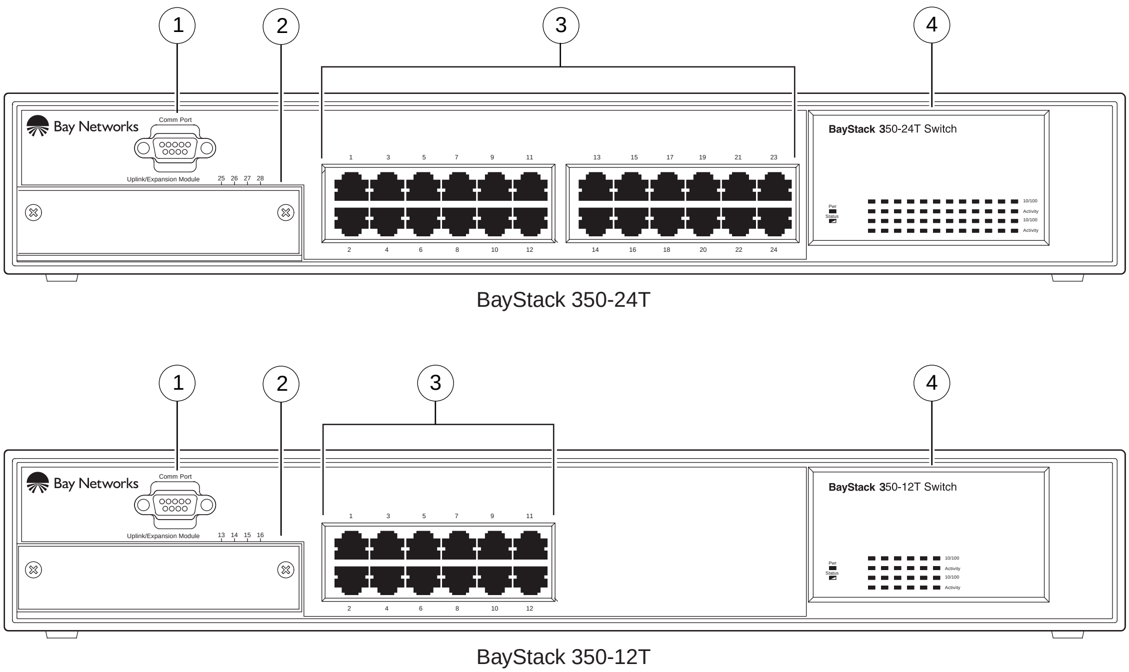


Figure 1-1. BayStack 350 10/100/1000 Series Switches

Front-Panel

Figure 1-2 shows the front-panel of the BayStack 350-24T switch and the BayStack 350-12T switch. 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 1-6.



1 = Comm Port

2 = Uplink/Expansion slot

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

4 = LED display panel

BS35002A

Figure 1-2. Front-Panel Components

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 “Connecting the 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 D-5).

The console port runs at 9600 baud and uses eight data bits, one stop bit, and no parity as the communications format, with flow control set to disabled.

Uplink/Expansion Slot

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

10BASE-T/100BASE-TX Port Connectors

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

Note: The RJ-45 port connectors on BayStack 450 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 1-2). Port-specific examples in this guide show the appropriate port connections when required; other examples apply to both versions.

All BayStack 350 switches are shipped with port connectors 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 D-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 of operation.

The switch ports also support half- and full-duplex mode operation (see “Connecting the 10BASE-T/100BASE-TX Ports” on page 2-9).

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 D, “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 1-3).

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

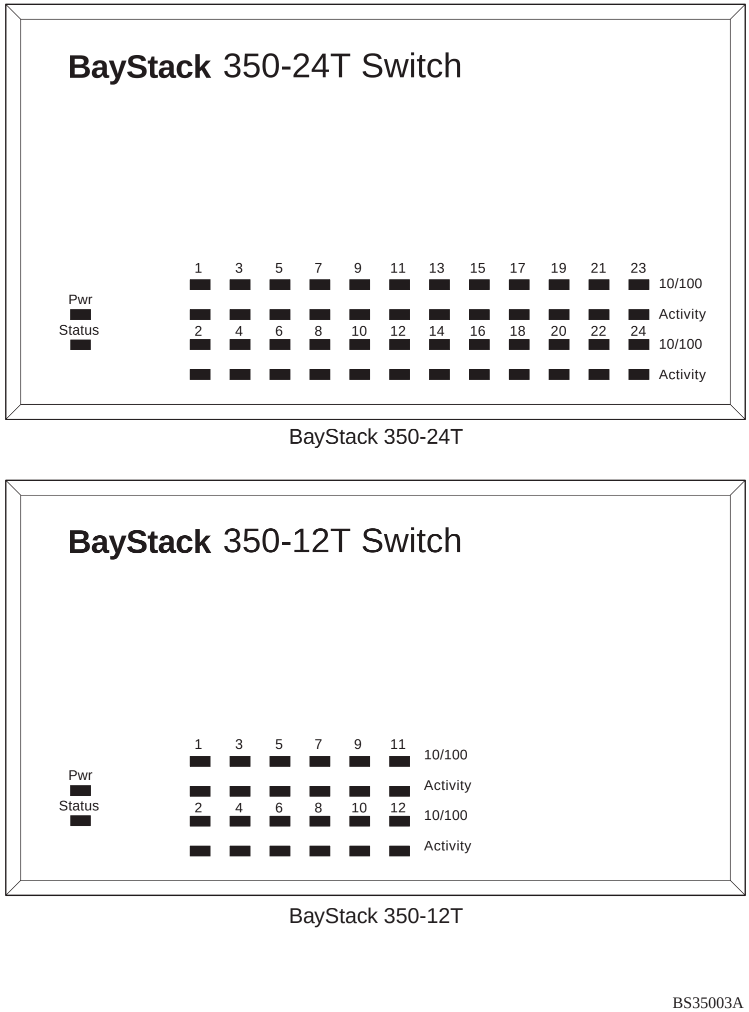


Figure 1-3. LED Display Panel

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.

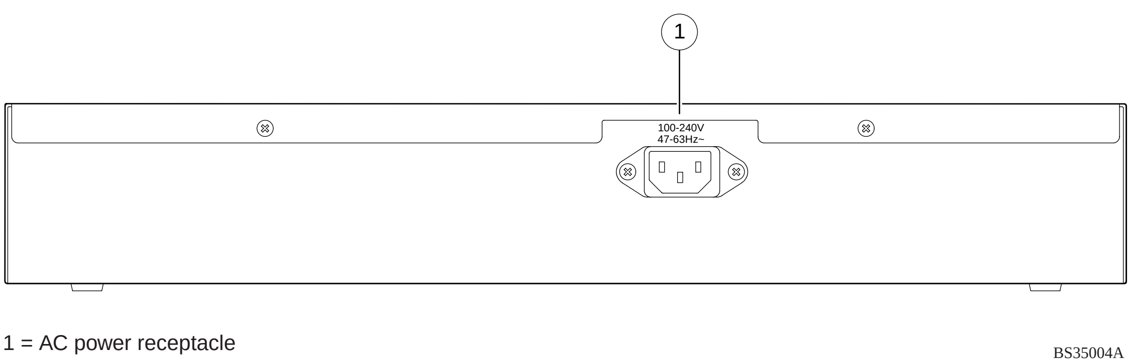
(continued)

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.
		Amber	On	The corresponding port is set to operate at 10 Mb/s and the link is good.
		Amber	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

This section describes the BayStack 350 switch back-panel components (Figure 1-4). Descriptions of the back-panel components follow the figure.



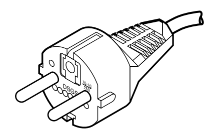
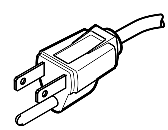
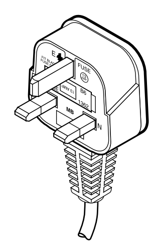
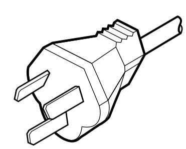
1 = AC power receptacle

Figure 1-4. Back-Panel Components

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 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, utilizing a 2.56 Gigabit/second switch fabric
- Learning rate: 3 million addresses per second (peak)
- 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 users to configure and manage the switch locally or remotely.

- SNMP agent support for the following Management Information Bases (MIBs):

  - Bridge MIB (RFC 1493)

  - Ethernet MIB (RFC 1643)

  - RMON MIB (RFC 1757)

  - MIB-II (RFC 1213)

  - Interface MIB (RFC 1573)

  - Bay Networks proprietary MIBs:

    s5Chass MIB

    s5Agent MIB

    s5ECM MIB (Ethernet Common)

    s5emt MIB (multi-segment topology)

    Rapid City MIB

- 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

- 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

- 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

- Upgradeable device firmware in nonvolatile flash memory using the Trivial File Transfer Protocol (TFTP)

IEEE 802.1Q VLANs

BayStack 350 switches support up to 64 port-based VLANs with IEEE 802.1Q tagging available per port. When a switch port is configured to be a member of a VLAN, it is added to a group of ports (workgroup) that belong to one broadcast domain. You can assign different ports (and therefore the devices attached to these ports) to different broadcast domains. This feature allows network flexibility because you can reassign VLANs to accommodate network moves, additions, and changes, eliminating the need to change physical cabling.

For more information about 802.1Q VLANs, see “IEEE 802.1Q VLAN Workgroups” on page 1-18.

IGMP Snooping Feature

For conserving bandwidth and controlling IP Multicast, the IGMP Snooping feature can provide the same benefit as IP Multicast routers, but in the local area.

For more information about the IGMP Snooping feature, see "IGMP Snooping" on page 1-34.

IEEE 802.1p Prioritizing

BayStack 350 switches can prioritize the order in which packets are forwarded, on a per-port basis.

For more information about the 802.1p prioritizing feature, see "IEEE 802.1p Prioritizing" on page 1-39.

MultiLink Trunking

The MultiLink Trunking feature allows a user to group multiple ports (up to four) together when forming a link to another switch or server, thus increasing aggregate throughput of the interconnection between two devices, up to 800 Mb/s in full-duplex mode. BayStack 350 switches can be configured with up to six MultiLink Trunks.

For more information about the MultiLink Trunking feature, see "MultiLink Trunks" on page 1-43.

Port Mirroring

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

For more information about the port mirroring feature, see "Port Mirroring (Conversation Steering)" on page 1-61.

Flash Memory Storage

The BayStack 350 switch uses flash memory to store the switch software image. Flash memory allows you to update the software image with a newer version without changing the switch hardware.

An in-band connection between the switch and the TFTP load host is required to download the software image (see “Software Download” on page 3-70).

For information about connecting a console terminal for this procedure, see “Connecting the Console/Comm Port” on page 2-10.

Note: 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.

Certain configuration parameters, including the system characteristics strings, some VLAN parameters, the IGMP configuration parameters, and the MultiLink trunk names are stored in flash memory. These parameters are updated every 10 minutes or whenever a Reset command is executed. Powering off the switch within 10 minutes of changing these configuration parameters can cause the configuration parameters to be lost.

BootP Automatic IP Configuration

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 F, “Sample BootP Configuration File.”

SNMP MIB Support

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 MIB-II (RFC 1213) and the RMON MIB (RFC 1757), which provide access to detailed management statistics. With SNMP management, you can configure SNMP traps (on individual ports) to be generated automatically for conditions such as an unauthorized access attempt or changes in a port's operating status.

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 a supported speed and duplex mode is acknowledged by the attached device.

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 any generic SNMP-based network management software; however, you must assign an IP address to the switch. You can set the switch's IP address by using the Console/Comm Port or BootP, which resides on the switch.

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

Network Configuration

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 three network configuration examples using BayStack 350 10/100/1000 Series Switches:

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

Note: All models of the BayStack 350 10/100/1000 Series Switches can be used interchangeably in the following network configuration examples.

Desktop Switch Application

Figure 1-5 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).

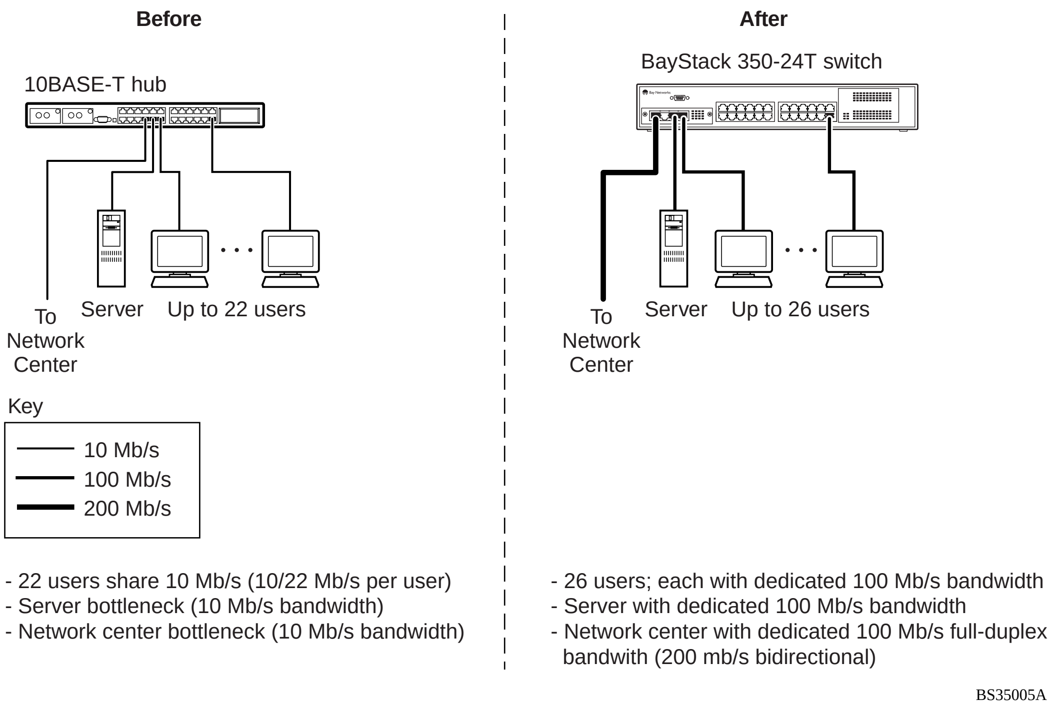


Figure 1-5. BayStack 350-24T Used as a Desktop Switch

Segment Switch Application

Figure 1-6 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.

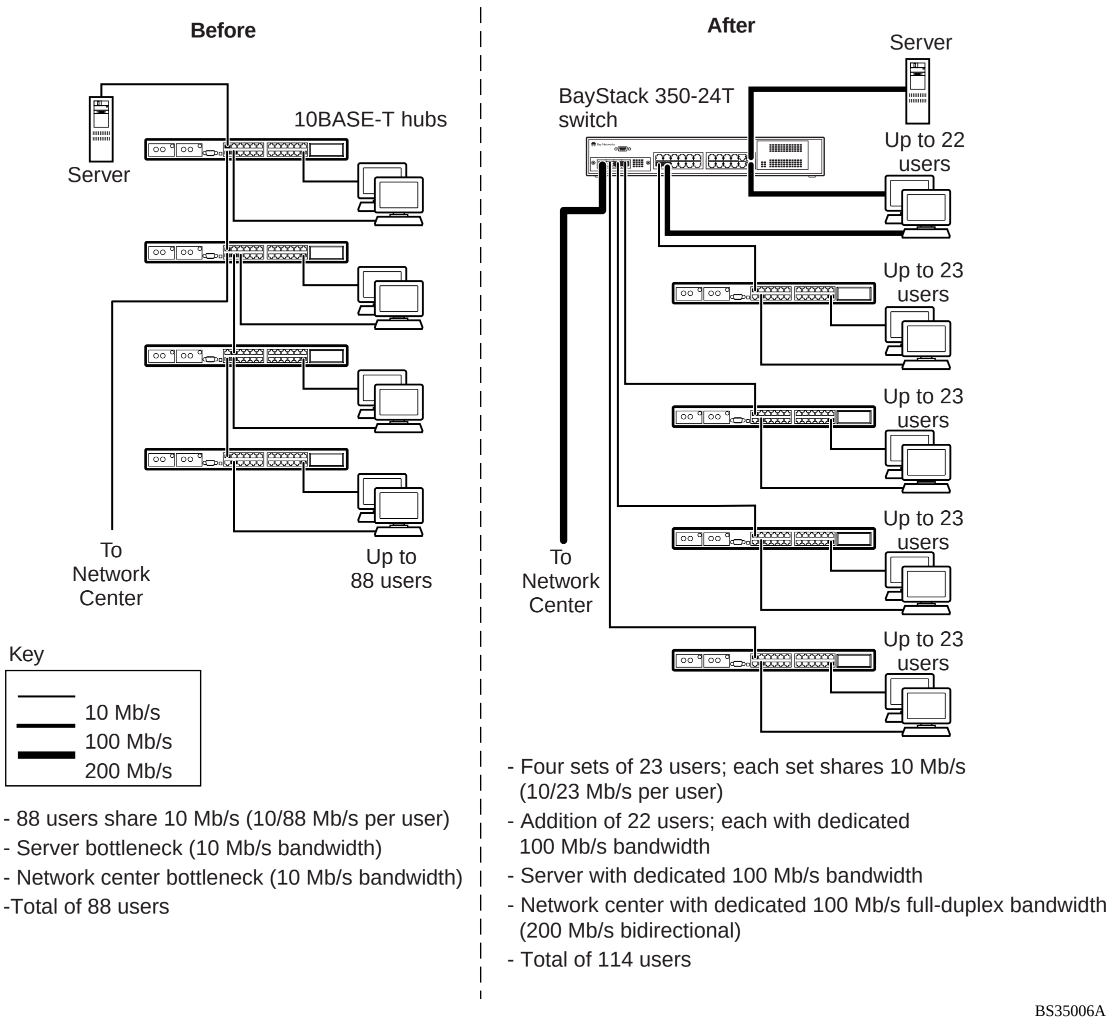


Figure 1-6. BayStack 350-24T Used as a Segment Switch

High-Density Switched Workgroup Application

Figure 1-7 shows a BayStack 350-24T switch with a high-speed (gigabit) connection to a Bay 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 1-7, 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 Bay Networks library Web page: *support.baynetworks.com/library/* for online documentation about the Bay Networks Accelar 1100 switch and the BayStack 303 and 304 switches.

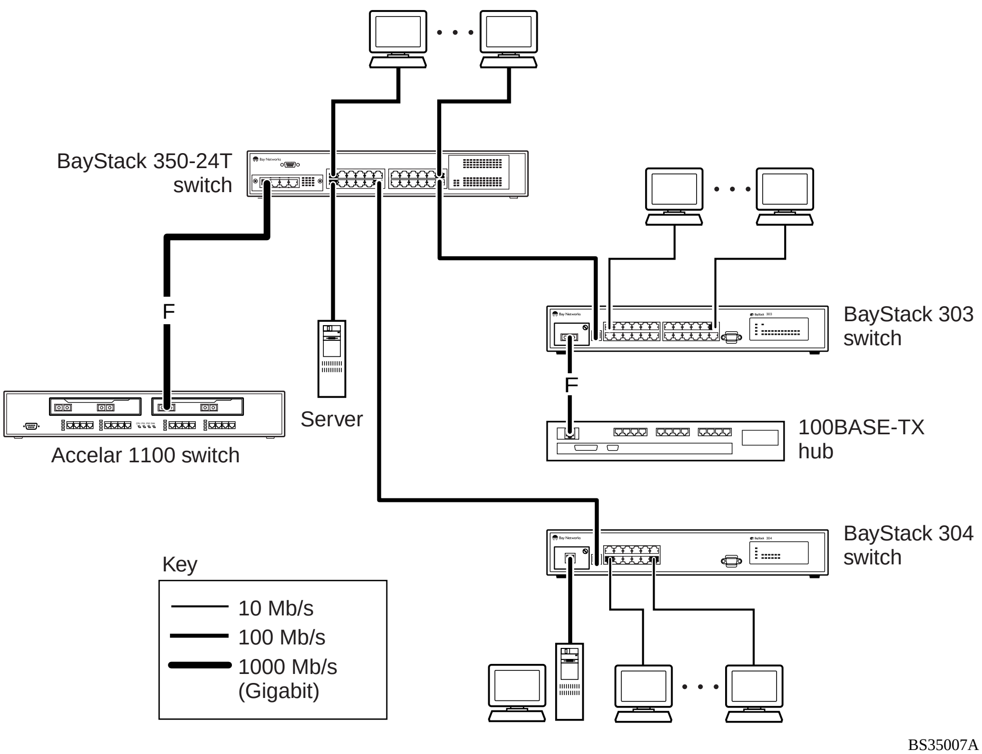


Figure 1-7. Configuring Power Workgroups and a Shared Media Hub

IEEE 802.1Q VLAN Workgroups

BayStack 350 switches support up to 64 port-based 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 1-8). 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 or TELNET; VLAN assignment is not currently available through SNMP. 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.

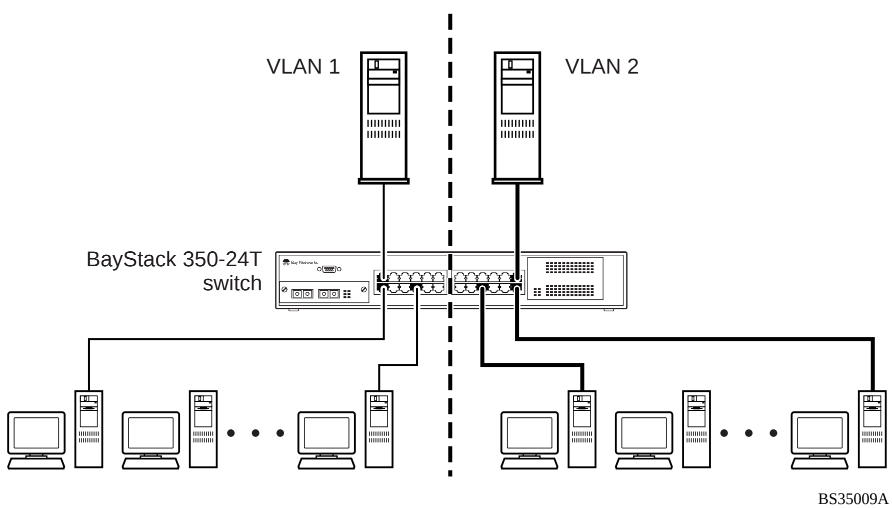


Figure 1-8. **Port-Based VLAN Example**

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. For example, a port with a PVID of 3 (PVID =3) assigns all untagged frames received on this port to VLAN 3.
- Tagged frame --- the 32-bit field (VLAN tag) in the frame header that identifies the frame as belonging to a specific VLAN. Untagged frames are marked (tagged) with this classification as they leave the switch through a port that is configured as a tagged port.
- Untagged frame --- a frame that does not carry any VLAN tagging information in the frame header.
- VLAN port members --- a set of ports that form a broadcast domain for a specific VLAN. A port can be a member of one or more VLANs.
- Untagged member --- a port that has been configured as an untagged member of a specific VLAN. When an untagged frame exits the switch through an untagged member port, the frame header remains unchanged. When a tagged frame exits the switch through an untagged member port, the tag is stripped and the tagged frame is changed to an untagged frame.
- Tagged member --- a port that has been configured as a member of a specific VLAN. When an untagged frame exits the switch through a tagged member port, the frame header is modified to include the 32-bit tag associated with the PVID. When a tagged frame exits the switch through a tagged member port, the frame header remains unchanged (original VID remains).
- User_priority --- a three-bit field in the header of a tagged frame. The field is interpreted as a binary number, therefore has a value of 0 to 7. This field allows the tagged frame to carry the user-priority across bridged LANs where the individual LAN segments may be unable to signal priority information.
- Port priority --- the priority level assigned to *untagged* frames received on a port. This value becomes the user_priority for the frame. *Tagged* packets get their user_priority from the value contained in the 802.1Q frame header.
- Unregistered packet --- a tagged frame that contains a VID where the receiving port is not a member of that VLAN.

- Filtering Database Identifier (FID) --- the specific filtering/forwarding database within the 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) which distinguishes it from all other VLANs. In the default configuration example shown in Figure 1-9, all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID =1). Untagged packets enter and leave the switch unchanged.

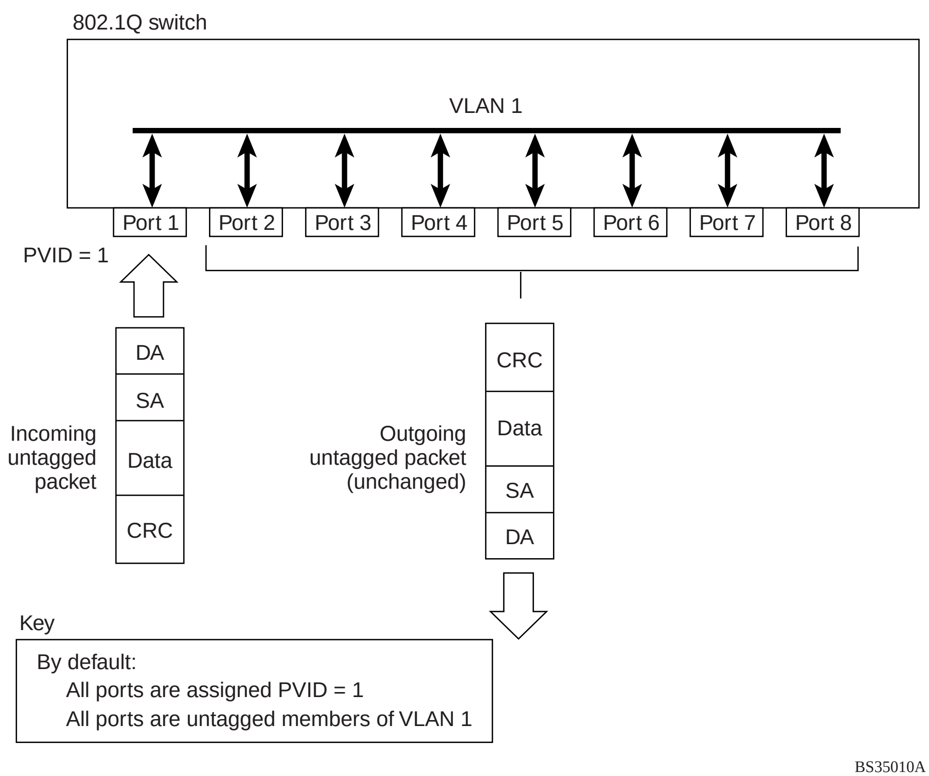


Figure 1-9. Default VLAN Settings

To configure VLANs, a user can reconfigure the switch ports as *tagged* or *untagged* members of specific VLANs (see Figure 1-10 through Figure 1-13).

In Figure 1-10, 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.

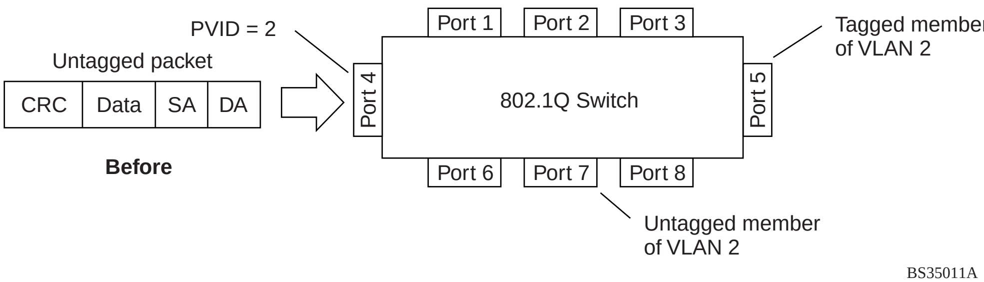


Figure 1-10. 802.1Q Tagging (1 of 4)

As shown in Figure 1-11, 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.

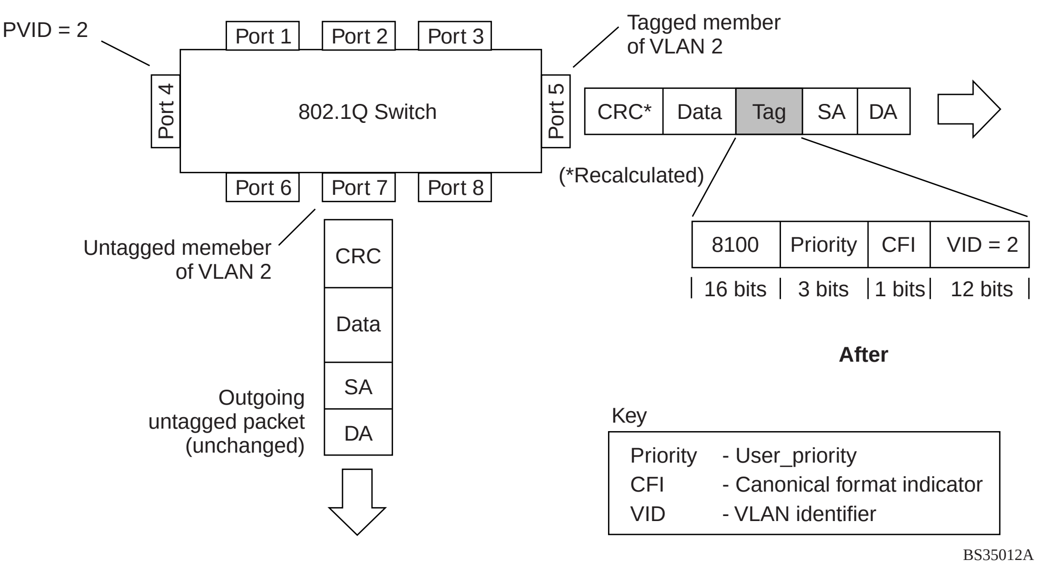


Figure 1-11. 802.1Q Tagging (2 of 4)

In Figure 1-12, 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.

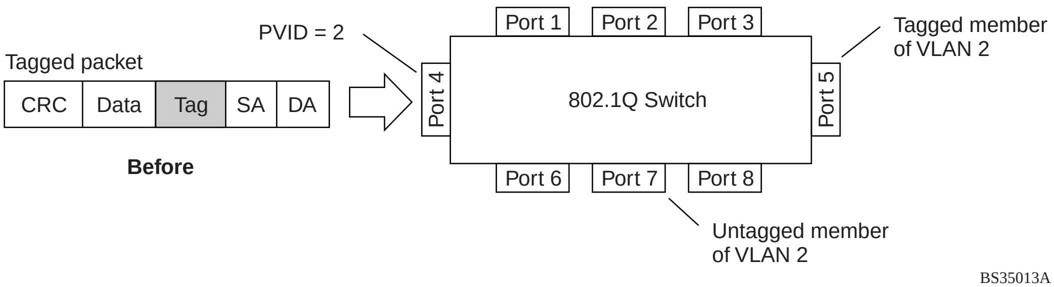


Figure 1-12. 802.1Q Tagging (3 of 4)

As shown in Figure 1-13, 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.

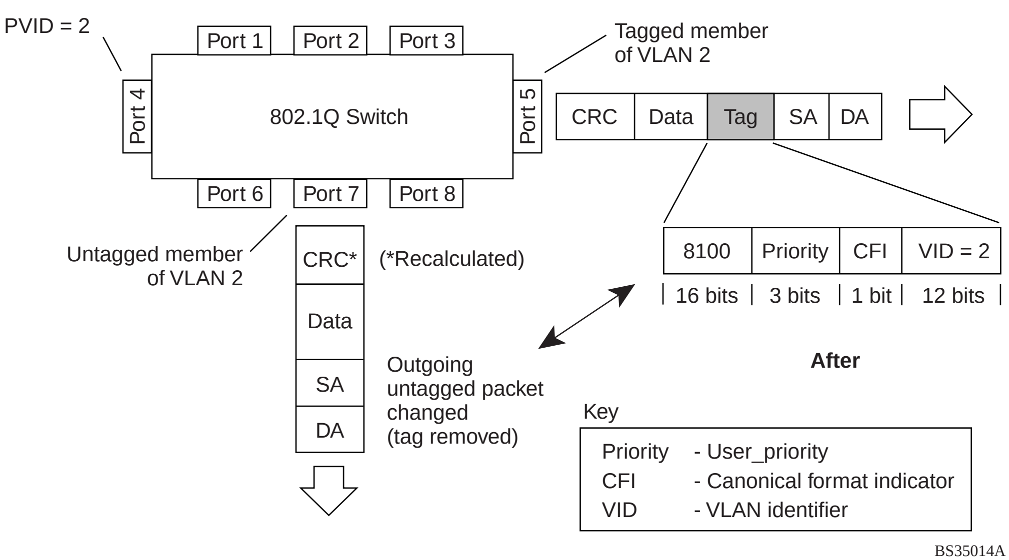


Figure 1-13. 802.1Q Tagging (4 of 4)

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 1-14 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.

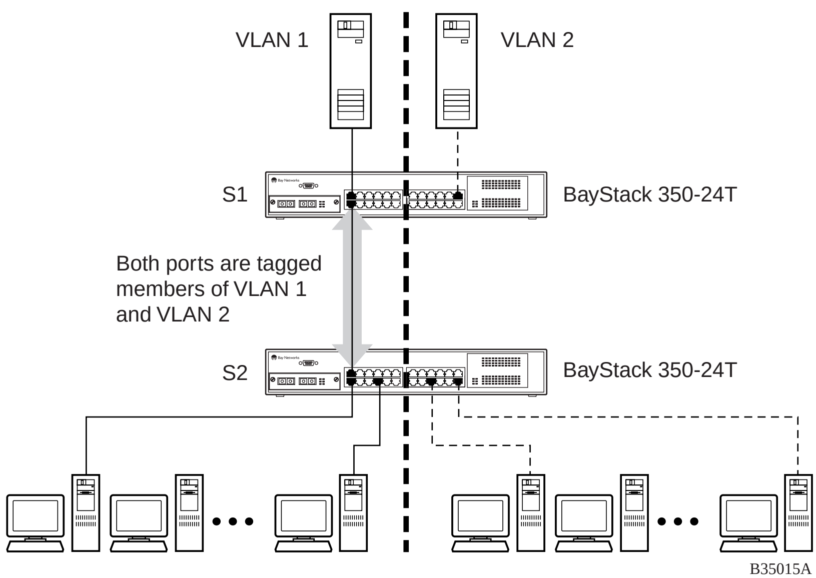


Figure 1-14. VLANs Spanning Multiple 802.1Q Tagged Switches

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 1-15 shows VLANs spanning multiple untagged switches. In this configuration switch S2 does not support 802.1Q tagging and a single switch port on each switch must be used for each VLAN.

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

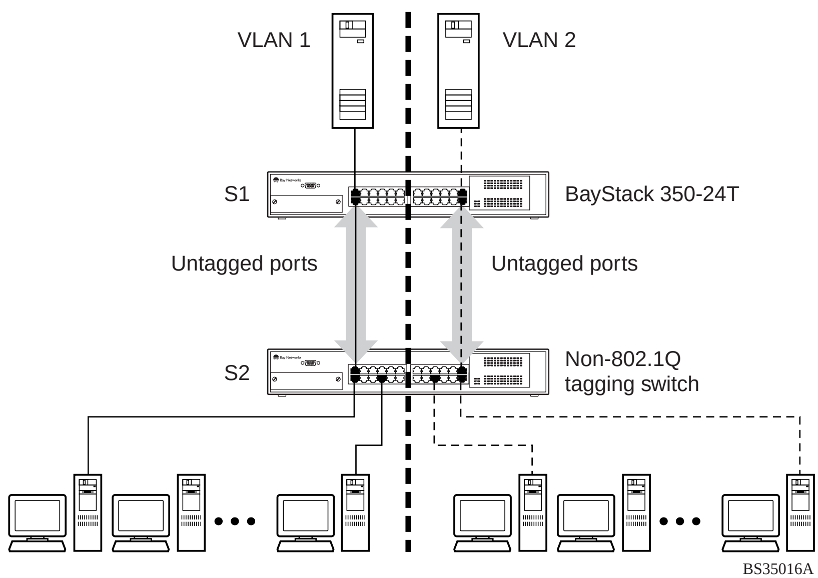


Figure 1-15. VLANs Spanning Multiple Untagged Switches

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 will be 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 1-16 shows possible consequences of enabling the STP when using VLANs between untagged (non-802.1Q tagged) switches.

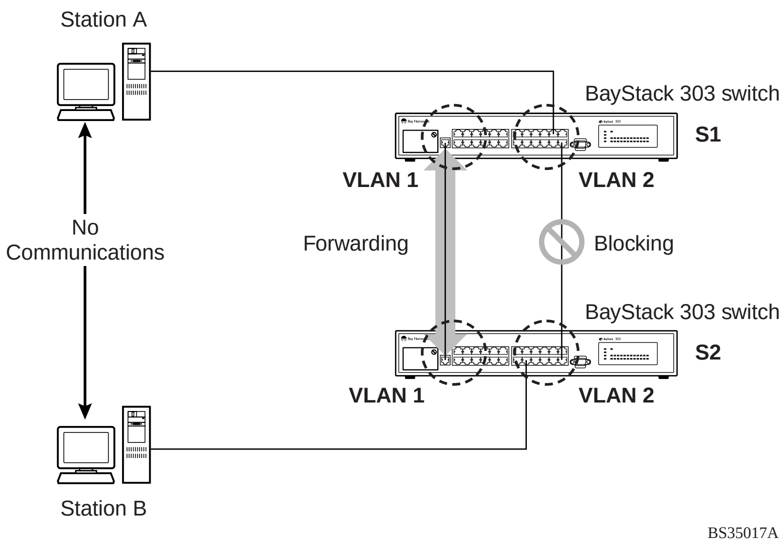


Figure 1-16. Possible Problems with VLANs and Spanning Tree Protocol

As shown in Figure 1-16, with STP enabled, only one connection between switch 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 1-17.

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.

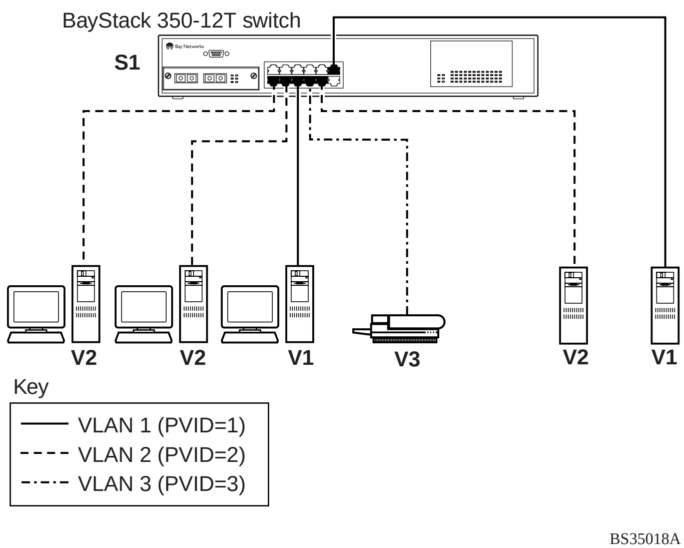


Figure 1-17. Multiple VLANs Sharing Resources

In order for the above configuration to operate as described, the ports have to be set to participate as VLAN port members. When this is done, the switch establishes the appropriate broadcast domains within the switch (see Figure 1-18).

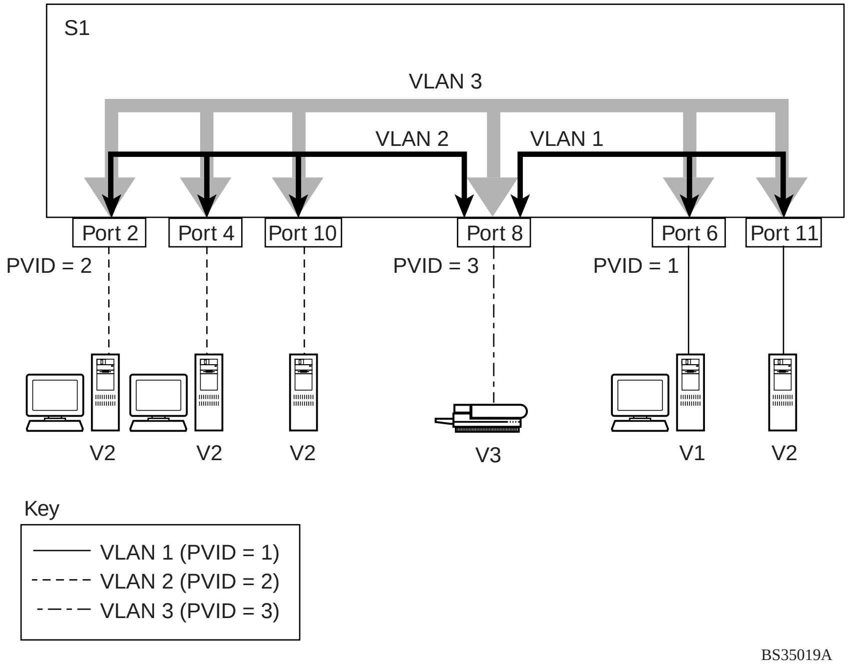


Figure 1-18. VLAN Broadcast Domains Within the Switch

The broadcast domain for each of the VLANs shown in Figure 1-18 are created by configuring VLAN port memberships for each VLAN and then configuring each of the ports 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 1-18.

To configure the VLAN port membership for VLAN 1, follow these steps:

1. **Select Switch Configuration from the BayStack 450-12T 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 1-19):

```
                                    VLAN Configuration


                 Create a VLAN:       [  1  ]
                 Delete a VLAN:       [     ]
                 VLAN Name:           [ VLAN #1 ]


                 Port Numbers
            1-5     6-10     11-12
           -----    -----    -----
           UUUUU    UUUUU    UU






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 1-19. Default VLAN Configuration Screen Example

The VLAN Configuration screen settings shown in Figure 1-19 are default settings with all switch ports classified as *untagged* members of VLAN 1.

Figure 1-20 shows the VLAN Configuration screen after it is configured to support the VLAN 3 broadcast domain shown in Figure 1-18 on page 1-27 (the VLAN Name field is optional).

Ports 2, 4, 6, 8, 10, and 11 are now untagged members of VLAN 3 as shown in Figure 1-18 on page 1-27.

```
                                 VLAN Configuration



                 Create a VLAN:        [  3  ]
                 Delete a VLAN:        [     ]
                 VLAN Name:            [ Michele's VLAN ]


                 Port Numbers
            1-5     6-10     11-12
           -----    -----    -----
           -U-U-    U-U-U    U-









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 1-20. VLAN Configuration Screen Example

To configure the PVID (port VLAN identifier) for Port 8, follow these steps:

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 1-21).

The VLAN Port Configuration screen settings shown in Figure 1-21 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  ]










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 1-21. Default VLAN Port Configuration Screen Example

Figure 1-22 shows the VLAN Port Configuration screen after it is configured to support the PVID assignment for port 8, as shown in Figure 1-18 (the Port Name field is optional).

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:                        [ Library Sharing ]
          PVID:                             [  3  ]
          Port Priority:                    [  0  ]













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 1-22. VLAN Port Configuration Screen Example

VLAN Workgroup Summary

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

As shown in Figure 1-23, switch S1 (a BayStack 350-12T switch) is configured with multiple VLANs:

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

Because S4 (a non-802.1Q switch) does not support 802.1Q tagging, a single switch port on each switch must be utilized for each VLAN (see “VLANS Spanning Multiple Untagged Switches” on page 1-24).

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 1-23).

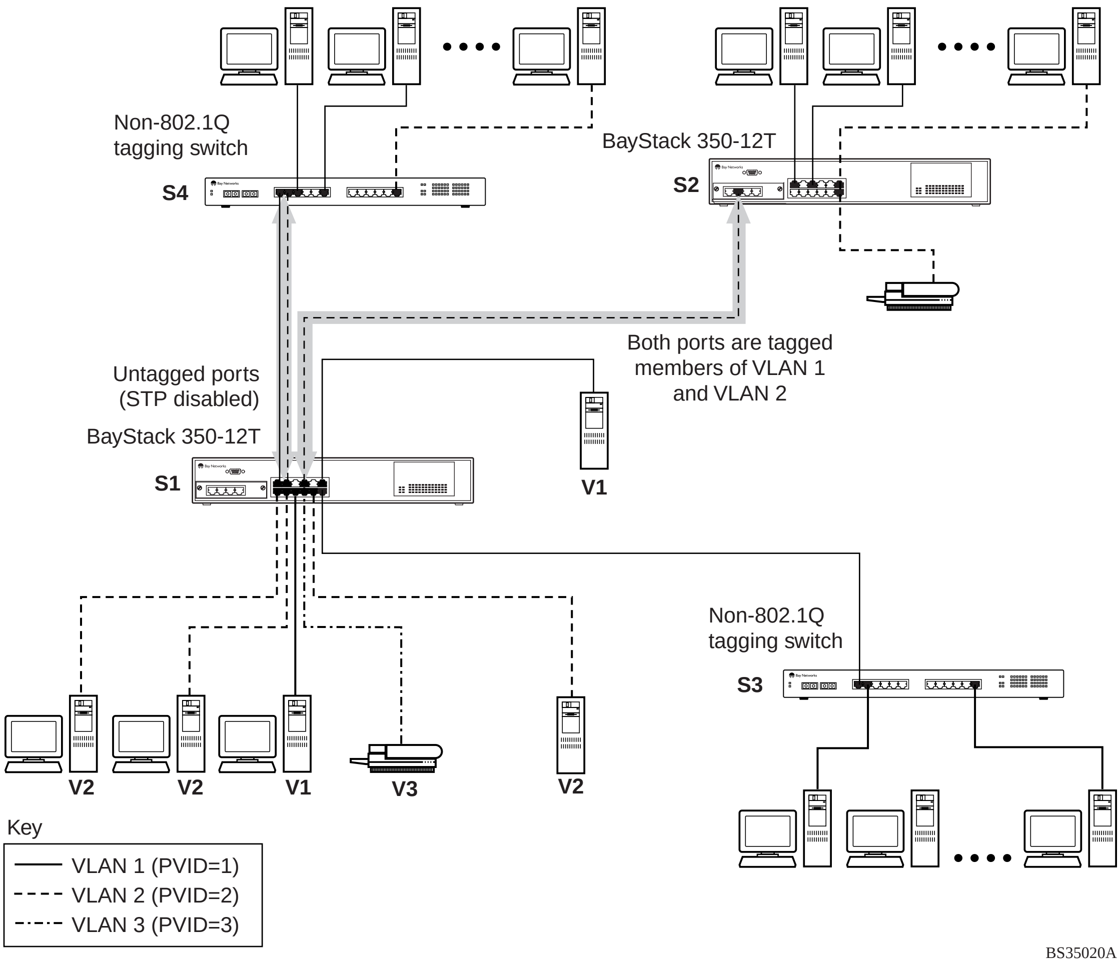


Figure 1-23. VLAN Configuration Spanning Multiple Switches

VLAN Configuration Rules

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

- All ports that are involved in port mirroring must have memberships in the same VLANs. If a port is configured for port mirroring, the port's VLAN membership cannot be changed.
- If a port is a trunk group member, all trunk members are added or deleted from the VLAN.
- All ports involved in trunking and port mirroring must have the same VLAN configuration. If a port is on a trunk with a mirroring port, the VLAN configuration cannot be changed.
- 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.
- The following gigabit MDA restriction applies for VLAN configurations: tagging is restricted on secondary VLANS to either *all* tagged or *all* untagged.

For more information about configuring VLANs, see "VLAN Configuration Menu" on page 3-20.

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

IGMP Snooping

BayStack 350 switches can sense IGMP Host Membership Reports from attached stations and can use this information to set up a dedicated path between the requesting station and a local IP Multicast router. Once 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 describes how BayStack 350 switches provide the same benefit as IP Multicast routers, but in the local area:

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

Figure 1-24 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 which only forward the IP Multicast stream on their local network 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 non-participating endstations on that subnet, receive the IP Multicast stream.

Note: Although the non-participating endstations 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 10/100/1000 Series Switches.

As shown in Figure 1-24, a non-IP Multicast filtering switch causes IP Multicast traffic to be sent to all segments on the local subnet.

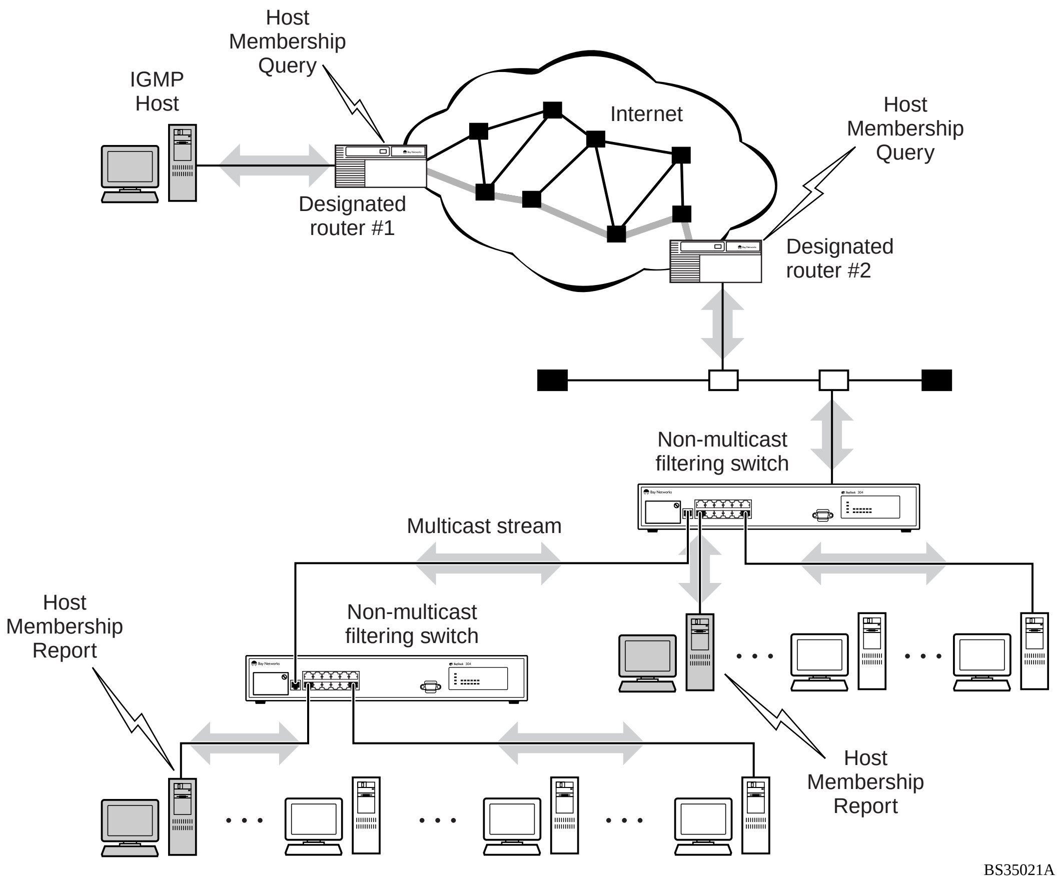


Figure 1-24. IP Multicast Propagation with IGMP Routing

The BayStack 350 10/100/1000 Series Switches can automatically set up IP Multicast filters so the IP Multicast traffic is only directed to the participating end nodes (see Figure 1-25).

In Figure 1-25, 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.

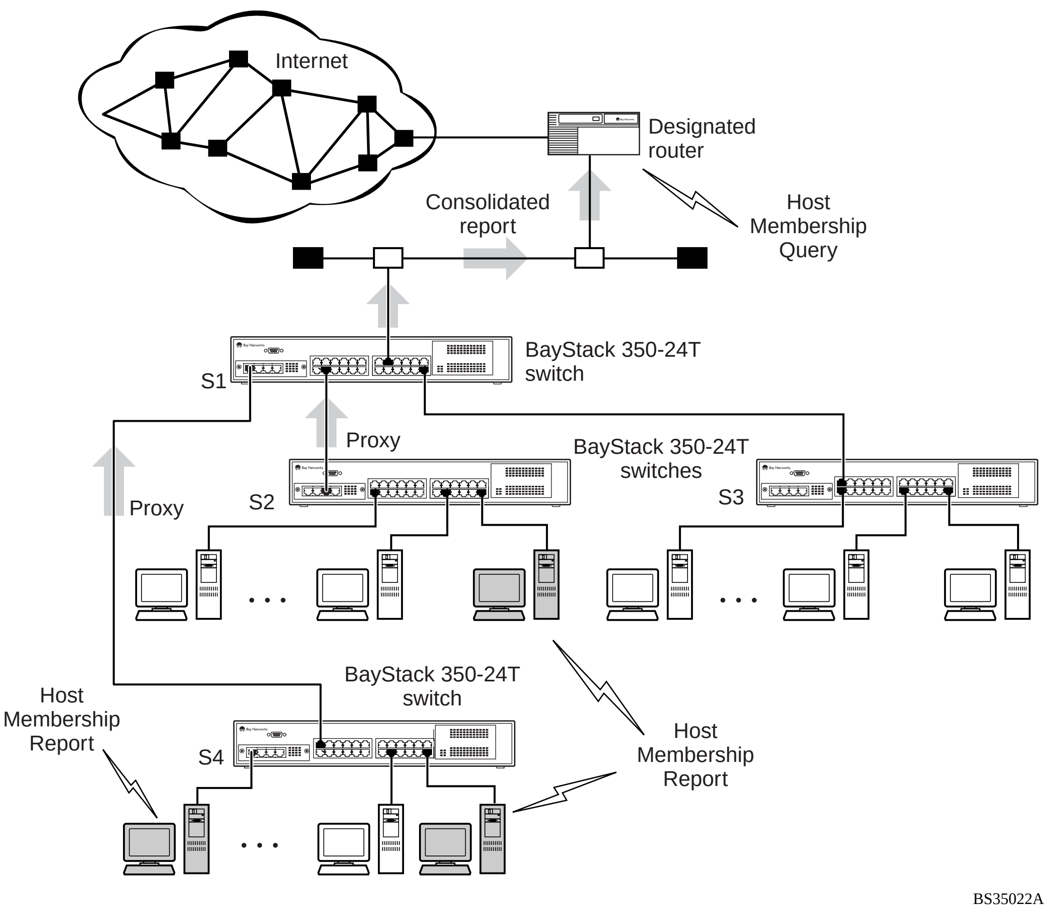


Figure 1-25. BayStack 350-24T Filtering IP Multicast Streams (1 of 2)

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 1-26).

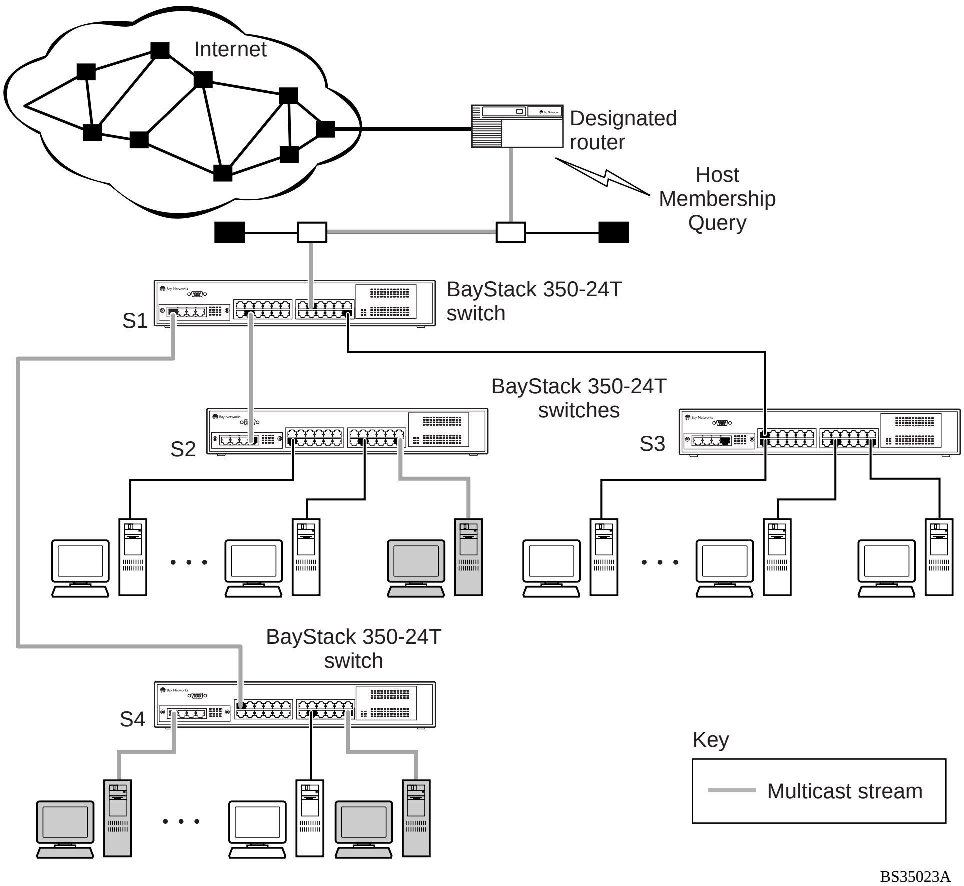


Figure 1-26. BayStack 350-24T switches Filtering IP Multicast Stream (2 of 2)

IGMP Snooping Configuration Rules

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

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

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

For more information about using the IGMP Snooping feature, see “IGMP Configuration” on page 3-48.

See also Appendix C, “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). Untagged packets received by the switch on that port are tagged according to the priority level you assign to the port (see Figure 1-27).

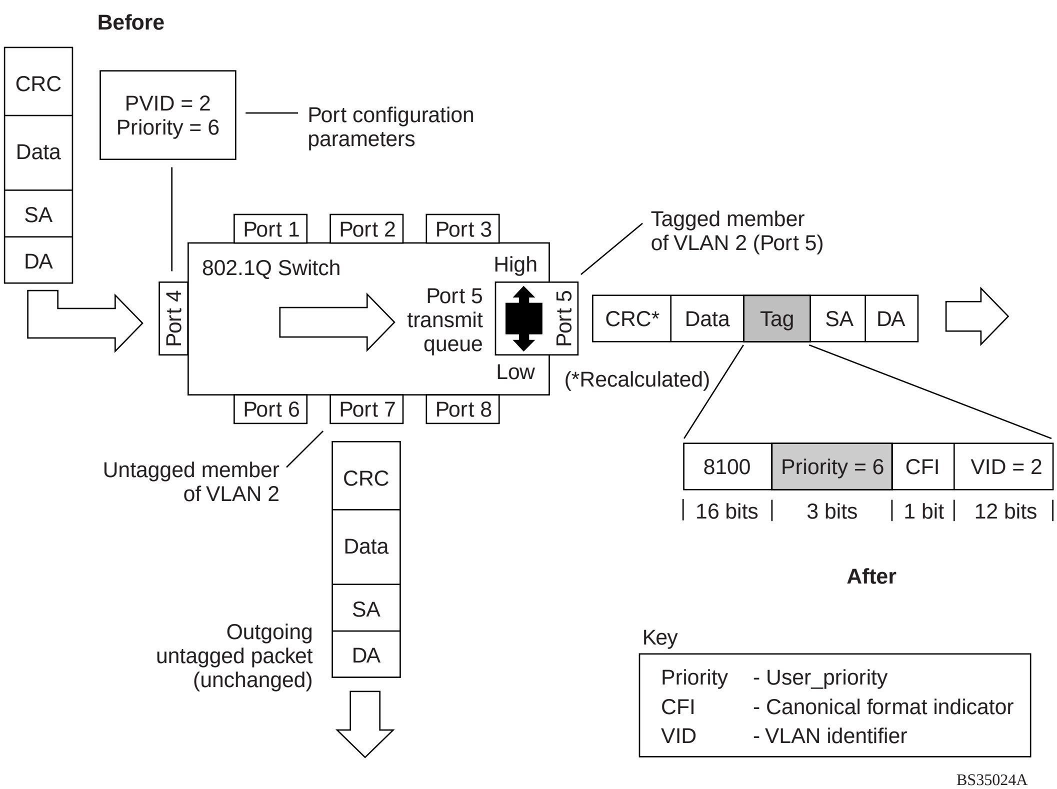


Figure 1-27. Prioritizing Packets

The newly tagged frame is read within the switch and sent to the port's high or low transmit queue for disposition (see Figure 1-28). The port transmit queue example shown in Figure 1-28 applies to all ports on the BayStack 350 switch.

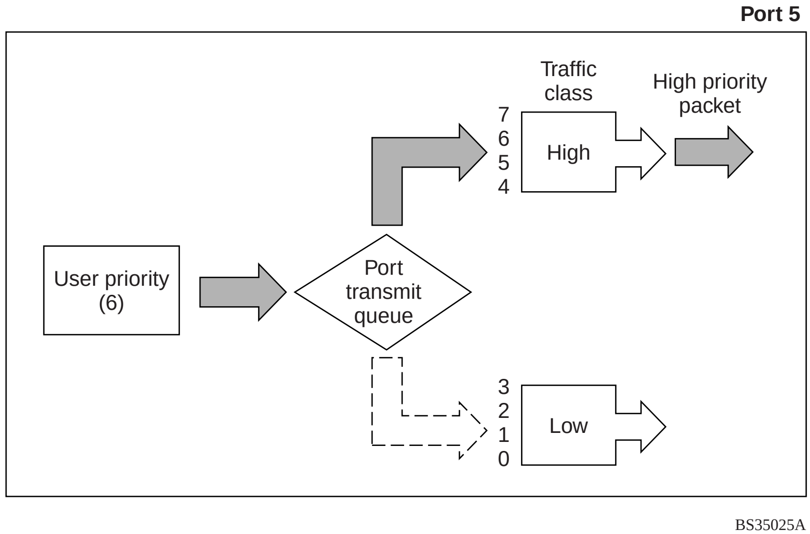


Figure 1-28. Port Transmit Queue

As shown in Figure 1-28, the switch provides two transmission queues, a High transmission queue and a Low transmission queue, for any given port. Frames are assigned to one of these queues on the basis of user_priority using a *traffic class table*. This table is managed by using the Traffic Class Configuration screen (Figure 1-29). 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 1-27.

For more information about using the Traffic Class Configuration screen, see “VLAN Configuration” on page 3-22.

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 450-12T 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 1-29).

```
                        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 1-29. 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 1-30).

Figure 1-30 shows the VLAN Port Configuration screen setup for port 4 in Figure 1-27 on page 1-39.

```
                        VLAN Port Configuration


               Port:                             [  4  ]
               Filter Tagged Frames:             [ No  ]
               Filter Untagged Frames:           [ No  ]
               Filter Unregistered Frames:       [ No  ]
               Port Name:                        [ Principal's port ]
               PVID:                             [  2  ]
               Port Priority:                    [  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 1-30. Setting Port Priority Example

For more information about using this feature, see “VLAN Configuration Menu” on page 3-20.

MultiLink Trunks

MultiLink trunks allow you to group up to four switch ports together to form a link to another switch or server, thus increasing aggregate throughput of the interconnection between the devices (up to 800 Mb/s in full-duplex mode). BayStack 350 switches can be configured with up to six MultiLink trunks. MultiLink Trunking software detects misconfigured (or broken) trunk links and redirects traffic on the misconfigured or broken trunk link to other trunk members within that trunk.

You can use the Trunk Configuration screen to create switch-to-switch and switch-to-server MultiLink trunk links (see Figure 1-31 and Figure 1-32).

Figure 1-31 shows two trunks (T1 and T2) connecting switch S1 to switches S2 and S3.

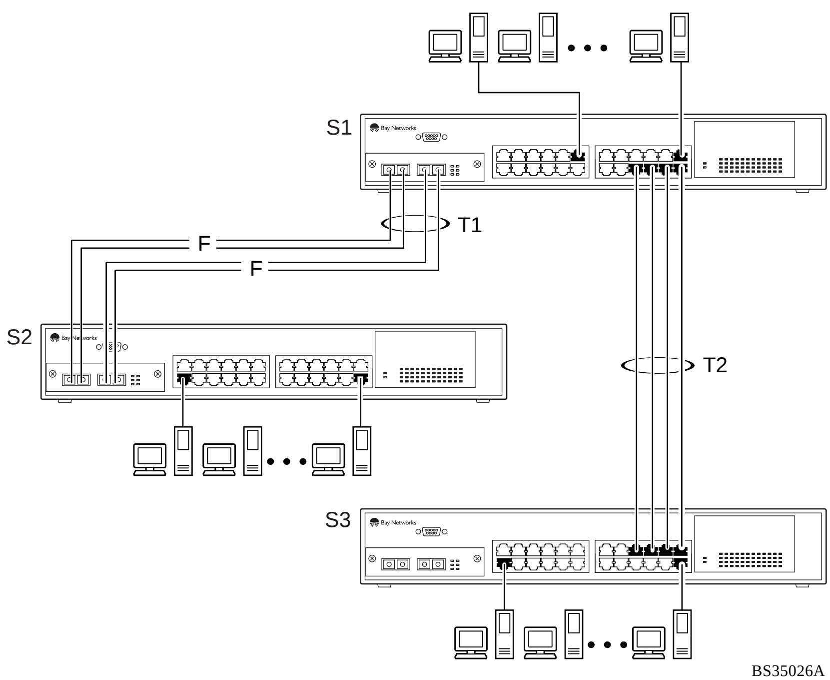


Figure 1-31. Switch-to-Switch Trunk Configuration Example

Each of the trunks shown in Figure 1-31 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 1-32 shows a typical switch-to-server trunk configuration. In this example, file server FS1 utilizes 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.

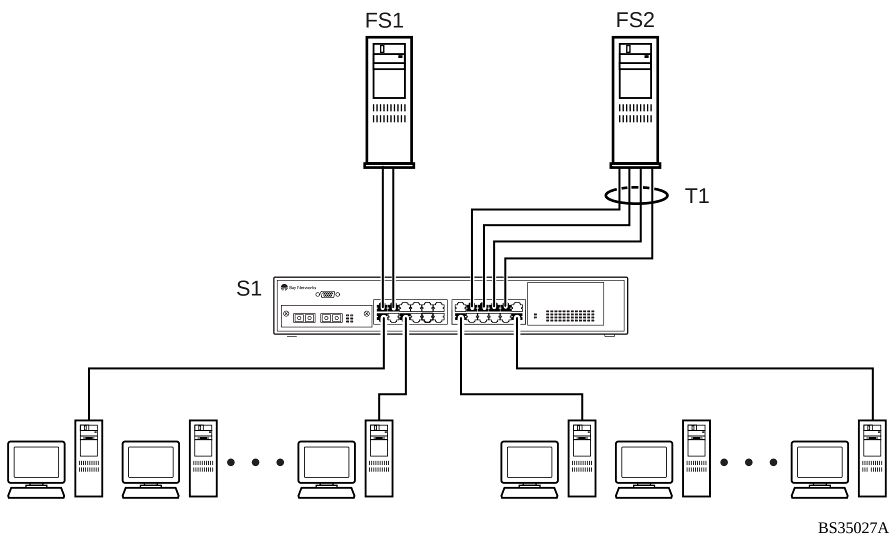


Figure 1-32. Switch-to-Server Trunk Configuration Example

Client/Server Configuration Utilizing MultiLink Trunks

Figure 1-33 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; they can be selected 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*, trunks T2 and T3 must be configured into separate VLANs for this configuration to function properly (see "IEEE 802.1Q VLAN Workgroups" on page 1-18).

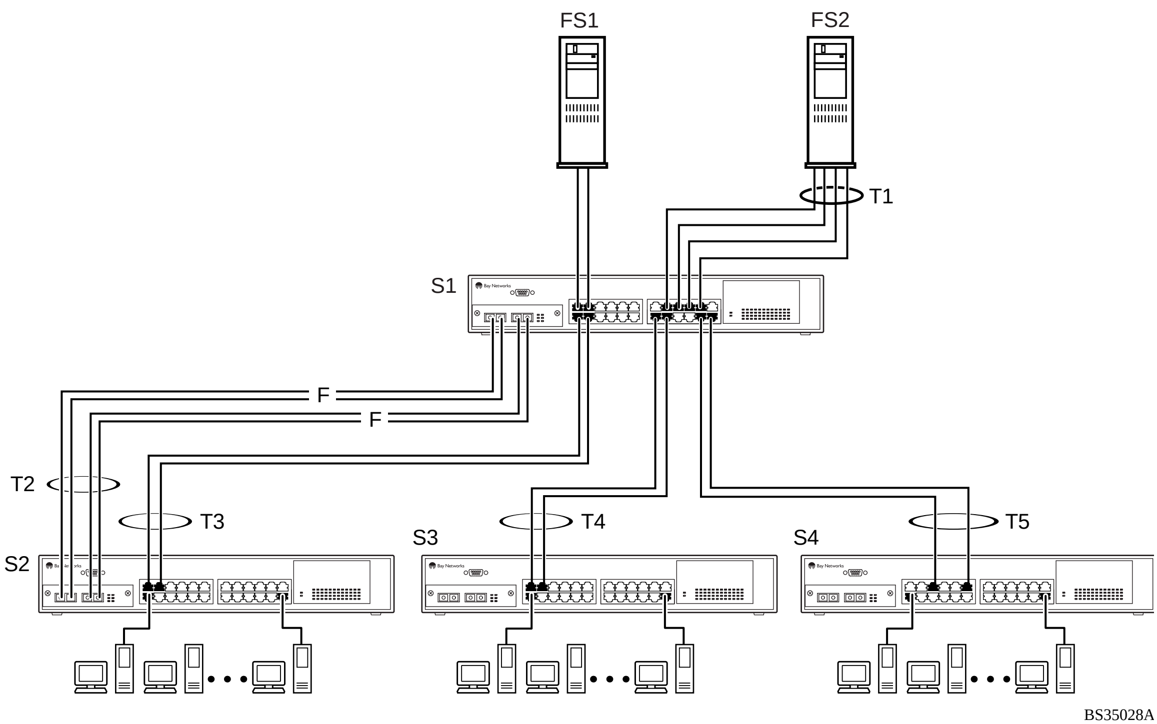


Figure 1-33. Client/Server Configuration Example

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 3-35.

Trunk Configuration Screen Examples

This section shows examples of the MultiLink Trunk Configuration screens for the client/server configuration example shown in Figure 1-33 on page 1-45. The screens show how you could set up the trunk configuration screens for switches S1 to S4. For more information, see “Spanning Tree Considerations” on page 1-57, and “MultiLink Trunk Configuration” on page 3-35.

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 screen (Figure 1-34).

```
                        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 1-34. Choosing the MultiLink Trunk Configuration Screen

The MultiLink Trunk Configuration screen opens (Figure 1-35).

```
                          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 1-35. MultiLink Trunk Configuration Screen for Switch S1

The MultiLink Trunk Configuration screen for 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 statically assigned to specific trunk members for flooding and forwarding. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.

- **Trunk 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 1-33 on page 1-45, switch S2 is set up with two trunk configurations (T2 and T3). Both trunks connect directly to switch S1.

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

Figure 1-36 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 1-36. MultiLink Trunk Configuration Screen for Switch S2

The MultiLink Trunk Configuration screen for switch S2 is configured as follows:

- **Trunk (read only)** indicates the trunks (1 to 6) that corresponds to the switch ports specified in the Trunk Members fields.
- **Trunk Members** indicates the ports that can be configured, in each row, to create the corresponding trunk:

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

- **Trunk 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 1-33 on page 1-45, 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 screen.

Figure 1-37 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 1-37. MultiLink Trunk Configuration Screen for Switch S3

The MultiLink Trunk Configuration screen for 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 statically assigned to specific trunk members for flooding and forwarding. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.

- **Trunk 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** 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 1-33, switch S4 is set up with one trunk configuration (T5). This trunk connects directly to switch S1.

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

Figure 1-38 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 1-38. MultiLink Trunk Configuration Screen for Switch S4

The MultiLink Trunk Configuration screen for switch S4 is configured as follows:

- **Trunk (read only)** indicates the trunk (1 to 6) that corresponds to the switch ports specified in the Trunk Members fields.
- **Trunk Members (Unit/Port)** 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 statically assigned to specific trunk members for flooding and forwarding. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.
- **Trunk 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** 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. These settings, along with specific configuration rules, must be considered before configuring your MultiLink trunk.

Before configuring any MultiLink trunk, follow these steps:

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. **A minimum of two ports are required for each trunk.**
   b. **Ensure that the chosen switch ports are set to Enabled, using the Port Configuration screen (see "Port Configuration" on page 3-30) or through network management.**
   c. **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" on page 1-57).**
5. **Consider how existing VLANs will be affected by the addition of a trunk.**
6. **After completing the above steps, see "MultiLink Trunk Configuration" on page 3-35 for screen examples and field descriptions that will help you configure your MultiLink trunks.**

MultiLink Trunking Configuration Rules

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

- Any port that participates in MultiLink Trunking must be an active port (set to Enabled via the Port Configuration screen or through network management).

- All trunk members must be configured into the same VLAN before the Trunk Configuration screen's Trunk Status field can be set to Enabled (See "VLAN Configuration" on page 3-22).
- When an active port is configured in a trunk, the port becomes a *trunk member* as soon as the Trunk Status field is set to Enabled. After the Trunk Status field is set to Enabled, the spanning tree parameters for the port will change to reflect the new trunk settings.
- 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 (see "Spanning Tree Considerations" on page 1-57.
- When a trunk is enabled, the trunk spanning tree participation setting takes precedence over that of any trunk member. When a trunk is active, the trunk STP setting can be changed from either the Trunk Configuration screen or the Spanning Tree Configuration screen.
- If the VLAN settings of any trunk member are changed, the VLAN settings of all members of that trunk are changed similarly.
- When any trunk member is set 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 has to be reconfigured through the Trunk Configuration screen to rejoin the trunk. A screen prompt precedes this action. A trunk member cannot be disabled if there are only two trunk members on the trunk.
- A trunk member cannot be configured as a monitor port (see "Port Mirroring Configuration" on page 3-41).
- Trunks cannot be monitored by a monitor port; however, trunk members can be monitored (see "Port-Based Mirroring Configuration" on page 1-62).
- All trunk members must have identical IGMP Snooping configurations.
- If the IGMP Snooping configuration for any trunk member is changed, the IGMP Snooping settings for all trunk members are changed.

Spanning Tree Considerations

The spanning tree Path Cost parameter is recalculated based on the aggregate bandwidth of the trunk. For example, Figure 1-39 shows a four port trunk (T1) with two port members operating at 100 Mb/s and the other two port members operating 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). If a second three port trunk (T2) is configured with an aggregate bandwidth of 210 Mb/s, with a comparable Path Cost of 4, the switch software chooses the trunk with the larger bandwidth (T1) to determine the most efficient path.

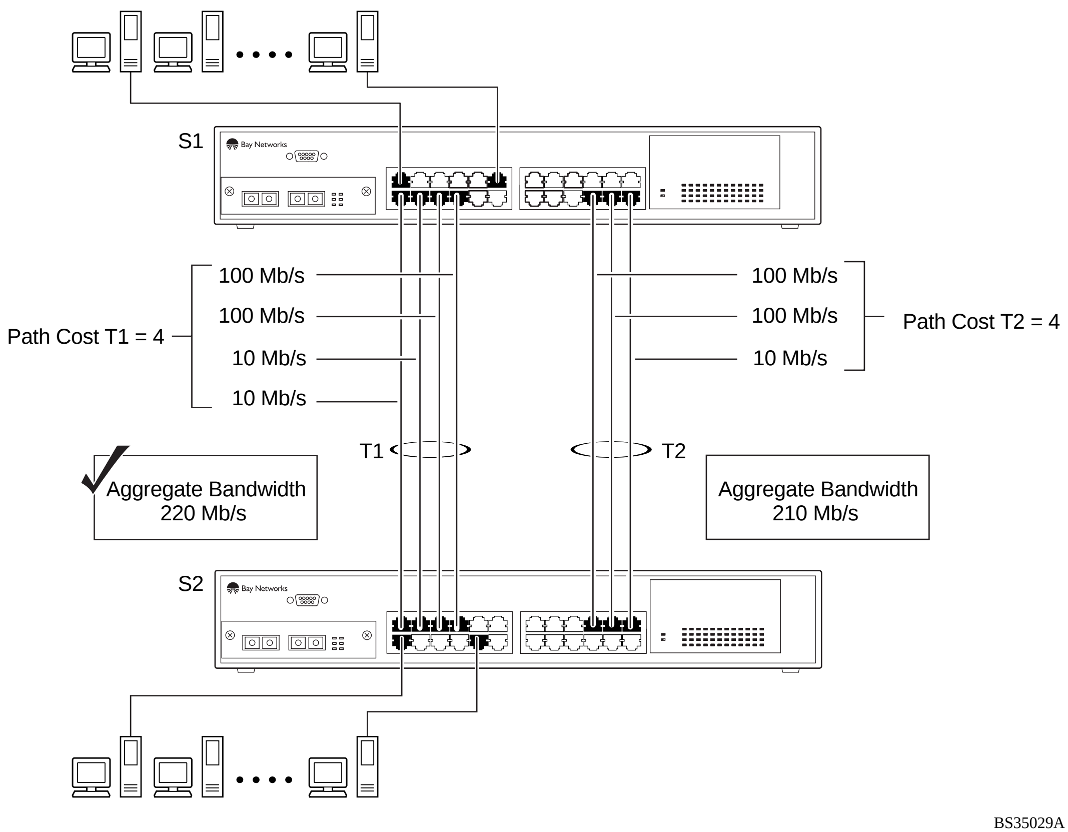


Figure 1-39. Path Cost Arbitration Example

The switch can also detect trunk member ports that are physically misconfigured. For example, in Figure 1-40, trunk member ports 2, 4, and 6 of switch S1 are configured *correctly* to trunk member ports 7, 9, and 11 of switch S2. The Spanning Tree Port Configuration screen for each switch shows the port State field for each port in the Forwarding state.

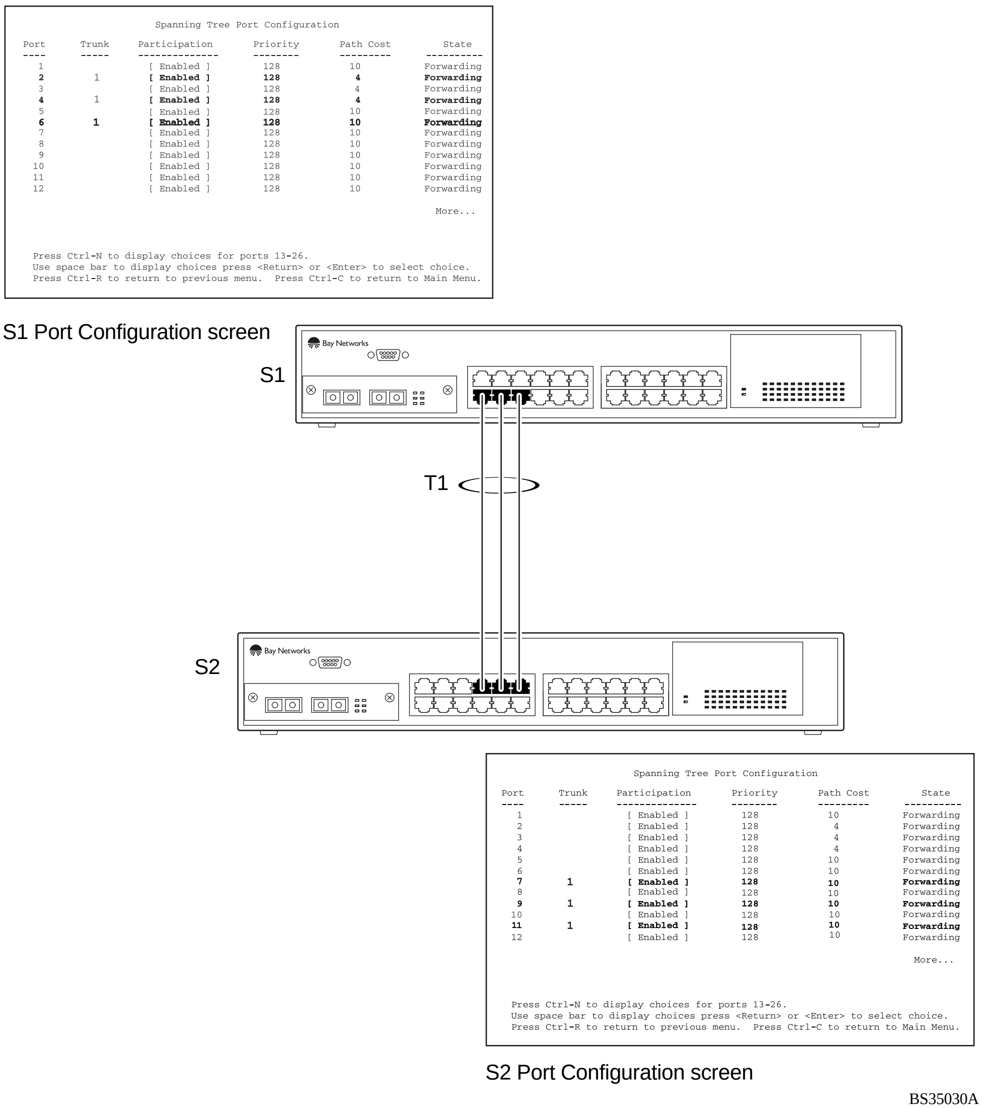


Figure 1-40. Example 1: Correctly Configured Trunk

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 1-41).

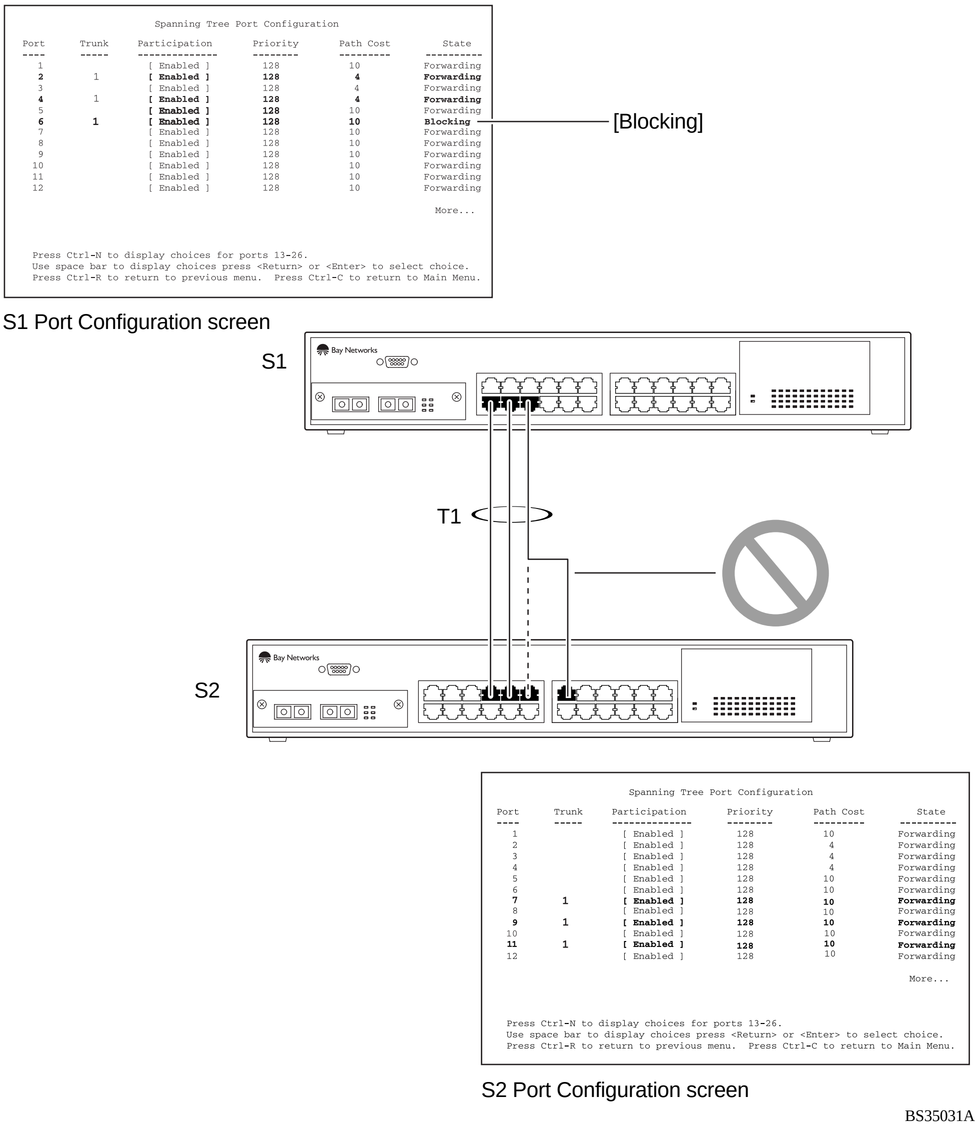


Figure 1-41. Example 2: Detecting a Misconfigured Port

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) are logically connected 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 are changed.

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 3-35.

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

Port Mirroring (Conversation Steering)

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 Bay Networks StackProbe™ or equivalent, must be connected to the designated monitor port to use this feature (contact your Bay 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 of the Port Mirroring Configuration screen is provided with each of the examples to support the network configuration example.

Note that in the following examples, 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 1-42 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 1-55).

Figure 1-43 shows the Port Mirroring Configuration screen setup for this example.

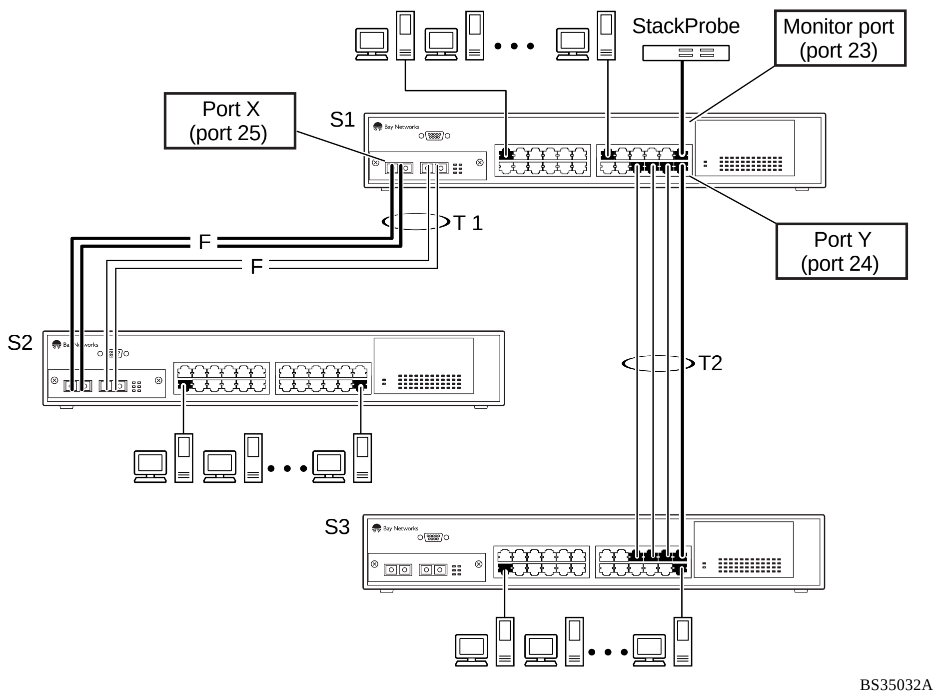


Figure 1-42. Port-Based Mirroring Configuration Example

In the configuration example shown in Figure 1-42 on page 1-62, the designated monitor port (port 23) can be set to monitor traffic in any of the following modes:

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

As shown in the Port Mirroring Configuration screen example (Figure 1-43), 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 1-43. Port Mirroring Port-Based Screen Example

Address-Based Mirroring Configuration

Figure 1-44 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.

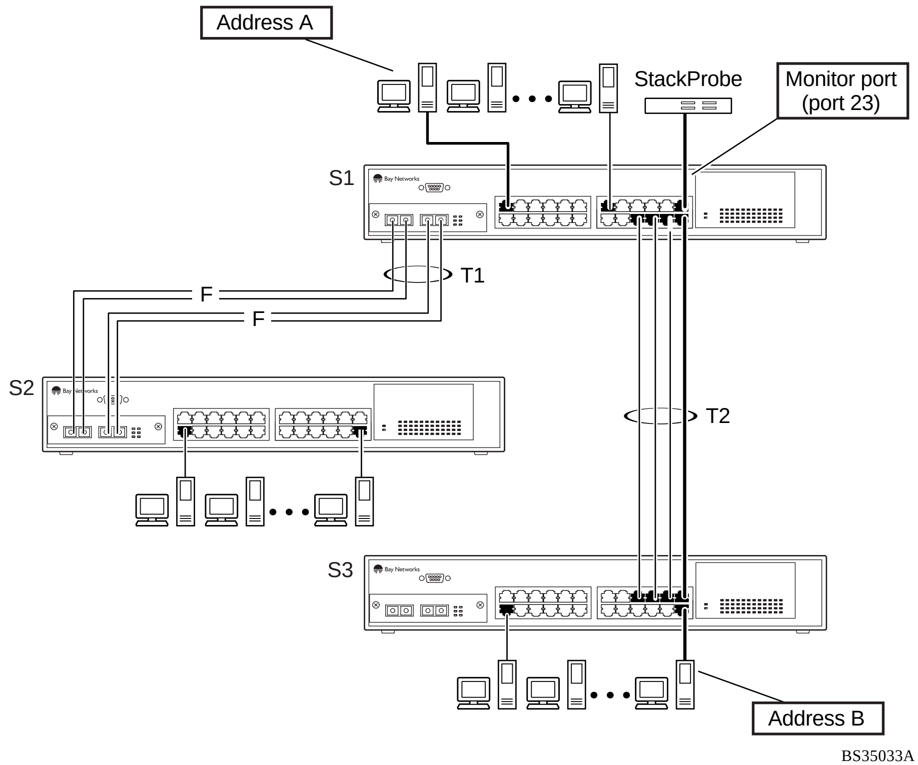


Figure 1-44. Address-Based Mirroring Configuration Example

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

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

Figure 1-45 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. The screen data displayed at the bottom of the screen will change to show the *new* currently active port mirroring configuration when you press Return.

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 3-18).

```
                        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 1-45. Port Mirroring Address-Based Screen Example

Port Mirroring Configuration Rules

The following configuration rules must be applied to any port mirroring configuration:

- A monitor port cannot be configured as a trunk member or IGMP member, and cannot be used for normal switch functions.
- When a port is configured and enabled as a monitor port, the port is automatically disabled from participating in the spanning tree. When the port is reconfigured as a standard switch port (no longer a monitor port), the port becomes enabled for spanning tree participation.
- When creating 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” on page 3-22).
- VLAN configuration settings for any ports configured for port-based mirroring cannot be changed. Use the Port Mirroring Configuration screen to disable port mirroring (or reconfigure the port mirroring ports), then change the VLAN configuration settings.
- For port-based monitoring of traffic, use one of the following modes for monitoring broadcast, IP Multicast, or unknown DA frames:

  Monitor all traffic received by port X.

  Monitor all traffic transmitted by port X.

  Monitor all traffic received and transmitted by port X.

  Monitor all traffic received by port X or transmitted by port Y.

For more information about using the Port Mirroring feature, see “Port Mirroring Configuration” on page 3-41.

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

Chapter 2
Installing the BayStack 350 Switch

This chapter provides the following information about the BayStack 350 switch:

- Installation requirements
- Installation procedure
- Instructions for connecting power
- Instructions for verifying the installation
- Instructions for the initial switch setup

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 1-7.

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.

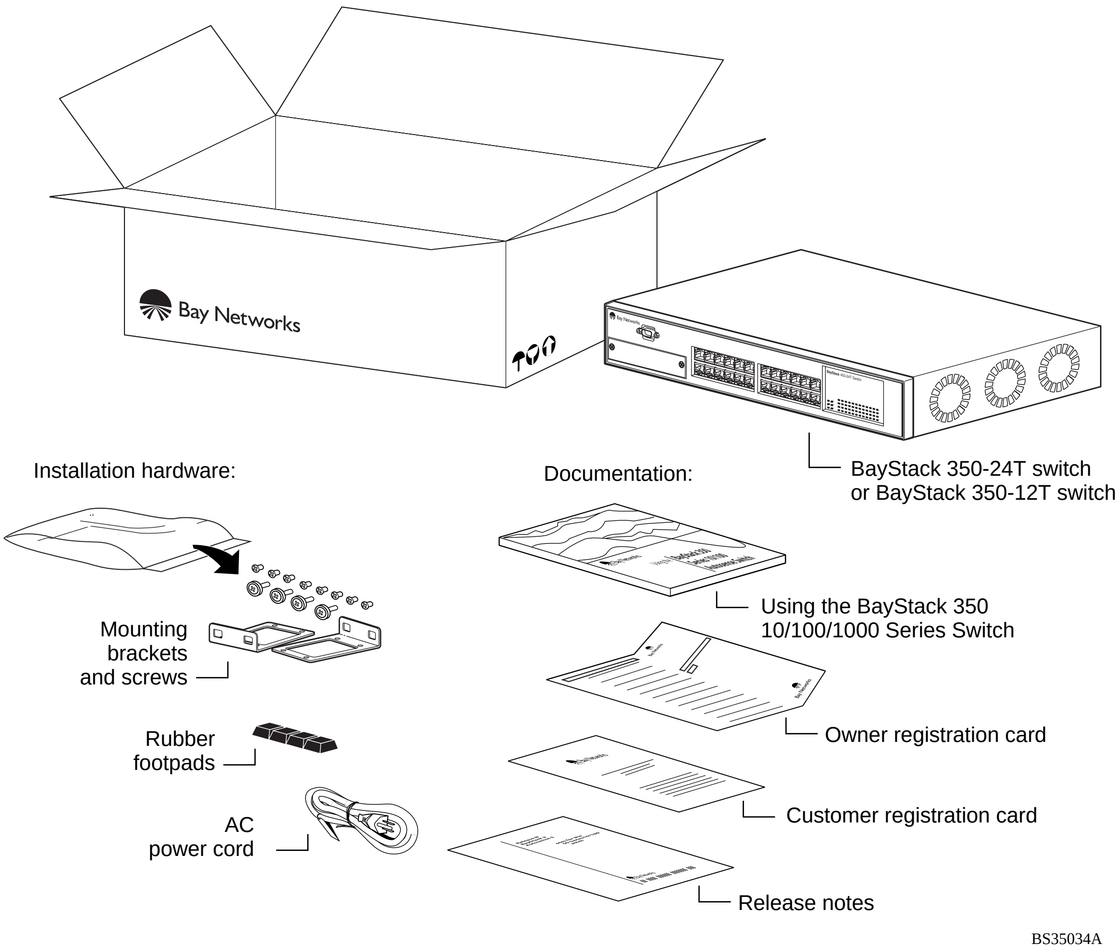


Figure 2-1. Package Contents

Note: Your shipping box may be configured differently than shown in the above example; 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. See your Bay Networks sales representative for part number and ordering information. Installation instructions are provided with the wall mount kit.

Installing the BayStack 350 Switch on a Flat Surface

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.

Caution: When this device is installed in a stack 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。

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 2-8.

Installing the BayStack 350 Switch in a Rack

The BayStack 350 switch occupies a 1.6-unit (1.6u) rack space and can be installed in most standard 19-inch racks. The rack must be grounded 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.

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。

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.**

   You can install the switch flush to the rack or extended from the rack, depending on the orientation of the mounting brackets (see Figure 2-2).

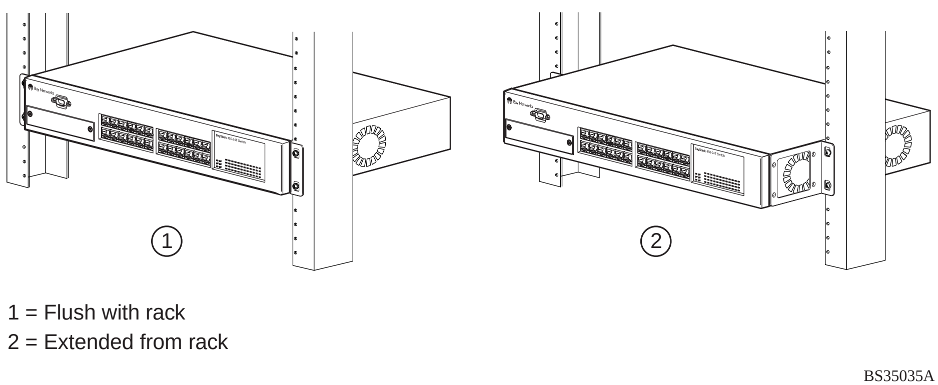


Figure 2-2. Positioning the Chassis in the Rack

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

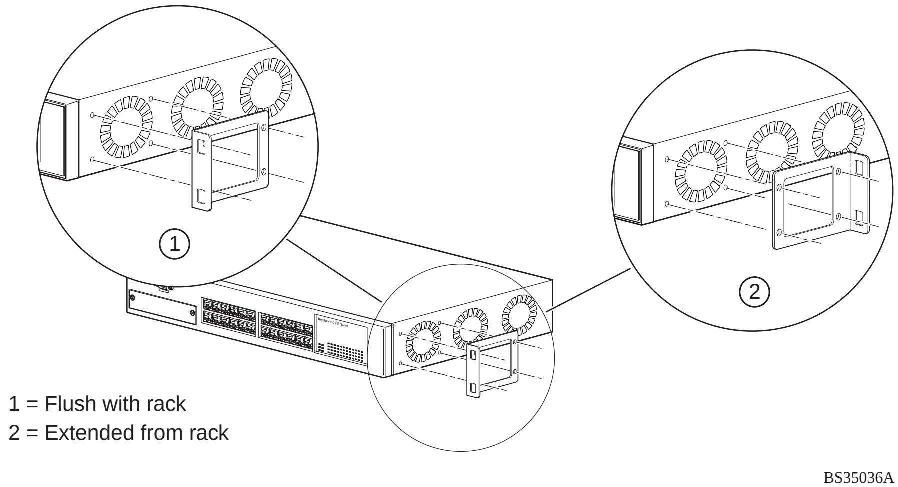


Figure 2-3. Attaching Mounting Brackets

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).**
4. **Insert two screws, appropriate for your 19-inch rack, into each of the mounting brackets and tighten.**

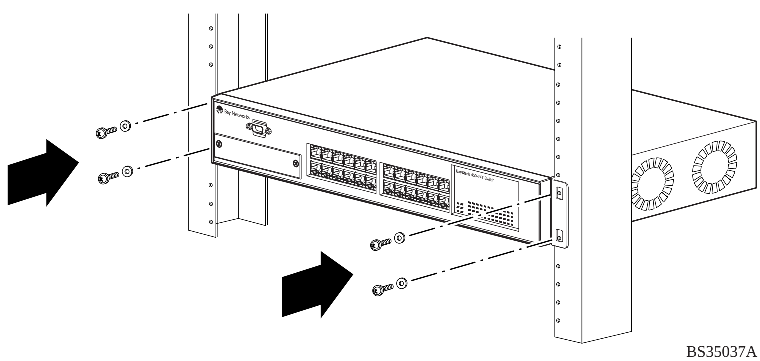


Figure 2-4. Installing the BayStack 350 Switch in an Equipment Rack

5. **After the switch is secured in the rack, proceed to the next section, "Attaching Devices to the BayStack 350 Switch" on page 2-8.**

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 setup 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 B, “Media Dependent Adapters” for more information about MDA types available from Bay 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, proceed to “Connecting Power” on page 2-11 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

For information about autonegotiation, see “Autosensing and Autonegotiation” on page 1-13. For troubleshooting possible related problems, see “Autonegotiation Modes” on page 4-6.

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

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 D, "Connectors and Pin Assignments," for more information.

Note: By default, all BayStack 350 switch 10BASE-T/100BASE-TX switch ports are set with the autonegotiation feature 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.

A standard RJ-45 connection is provided to connect devices to the switch through the 10BASE-T/100BASE-TX ports.

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).

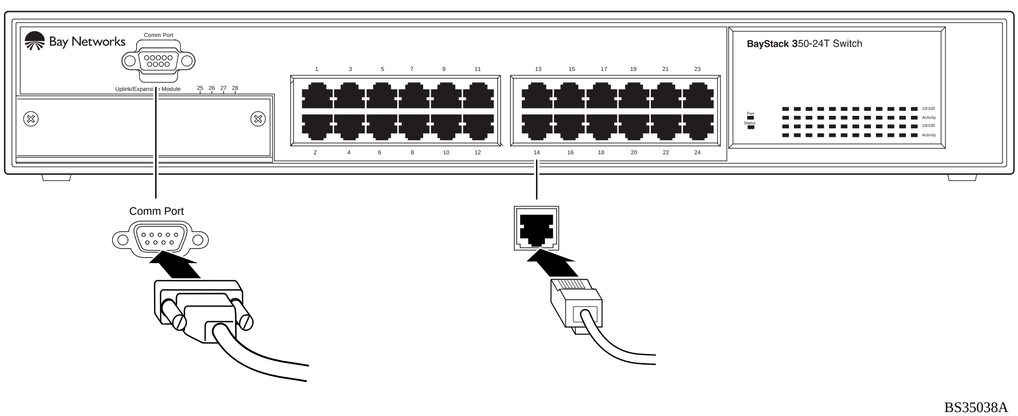


Figure 2-5. 10/100 Mb/s Port Connections

Connecting the 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 D-1 for a description of the pin assignments.

To connect a terminal to the console port, follow these steps:

1. **Set the terminal protocol as described previously.**
2. **Connect the terminal (or a computer in terminal-emulation mode) to the console port using the RS-232 cable.**

3. **Connect the female connector of the RS-232 cable directly to the Console/Comm Port on the switch, and tighten the captive retaining screws (see Figure 2-6).**

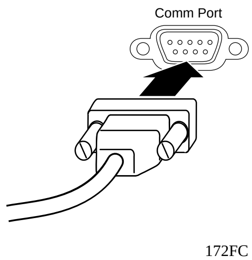


Figure 2-6. Connecting to the Console/Comm Port

4. **Connect the other end of the cable to a terminal or the serial connector of a personal computer running communications software.**

5. **Proceed to 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 2-7).**

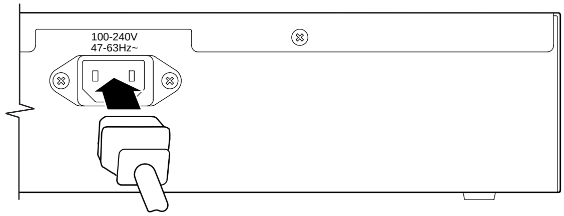


Figure 2-7. BayStack 350 Switch AC Power Receptacle

2. **Plug the other end of the AC power cord into the grounded AC power outlet (Figure 2-8).**

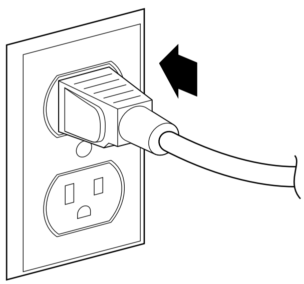


Figure 2-8. Grounded AC Power Outlet

3. **Proceed to 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 2-9). 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 subroutines are initiated by the self-test, the port status LEDs flash various patterns. When the switch passes the self-test (within 10 seconds), the Status LED turns on (Figure 2-9). If a nonfatal error occurs during the 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.

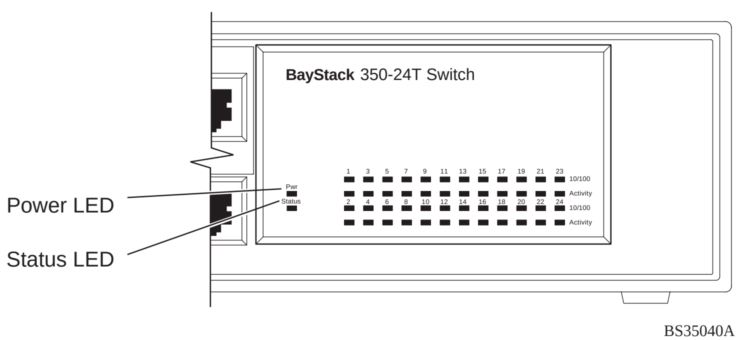


Figure 2-9. Observing LEDs to Verify Proper Operation

Verifying the Installation Using the Self-Test Screen

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

The results of the self-test are displayed briefly (5 or 10 seconds) in the Self-Test screen, which is followed by the Bay Networks logo screen (Figure 2-11).

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

```
BayStack 350 Self-Test

   CPU RAM test                ... Pass
   ASIC addressing test        ... Pass
   ASIC buffer RAM test        ... Pass
   Port internal loopback test ... Pass

Self-test complete.
```

Figure 2-10. BayStack 350 Switch Self-Test Screen

```
***********************************************
* Bay Networks,Inc.                           *
* Copyright (c) 1996,1998,1999                *
* All Rights Reserved                         *
* BayStack 350-XX T                           *
* Versions: HW:Revx  FW:Vx.xx SW:Vx.x.x.x     *
***********************************************







Enter Ctrl-Y to begin.
```

Figure 2-11. Bay Networks Logo Screen

➡ **Note:** The Bay Networks logo screen for your switch will display the correct model number and the current hardware, firmware, and software 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 of the BayStack 350 Switch

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

The BayStack 350 switch is designed for plug-and-play operation; however, 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 (refer to Chapter 3, “Using the Console Interface” for more information about configuring your BayStack 350 switch).

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 Self-Test screen displays, press [Ctrl]-Y.**

The Main Menu is displayed (Figure 2-12). 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...
                   Spanning Tree Configuration...
                   TELNET Configuration...
                   Software Download...
                   Display Event Log
                   Reset
                   Reset to Default Settings
                   Logout



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

Figure 2-12. Main Menu

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

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

Note: The IP interface of the BayStack 350 switch is *only* on VLAN 1. You can manage the switch *only* from VLAN 1 (or via routers that connect VLAN 1 to the network management station).

Note: IP addresses are written as four decimal numbers (for example, 123.123.123.123). Each decimal number represents an 8-bit octet. When strung together, the four octets form the 32-bit Internet address. This is called dotted-decimal notation. The largest possible value of a field in a dotted-decimal number is 255, which represents an octet of all ones.

```
                                IP Configuration/Setup



                 BootP Request Mode:  [ BootP When Needed     ]

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





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.
```

IP Configuration/Setup Screen

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

5. **Enter the IP subnet mask address in the In-Band Subnet Mask field, then press [Return].**
6. **Enter the default gateway address in the Default Gateway field, then press [Return].**

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 includes the following information:

- Accessing the CI menus and screens
- Using the CI menus and screens
- Description of options available from the Main Menu

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 “Connecting the Console/Comm Port” on page 2-10).

You can also manage the BayStack 350 switch using any generic SNMP-based management software; however, certain parameters (such as the switch IP address) must be configured for the switch management function to become fully operational (see “Initial Setup of the BayStack 350 Switch” on page page 2-16).

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 S<u>w</u>itch 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.

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

Screen Fields and Descriptions

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.

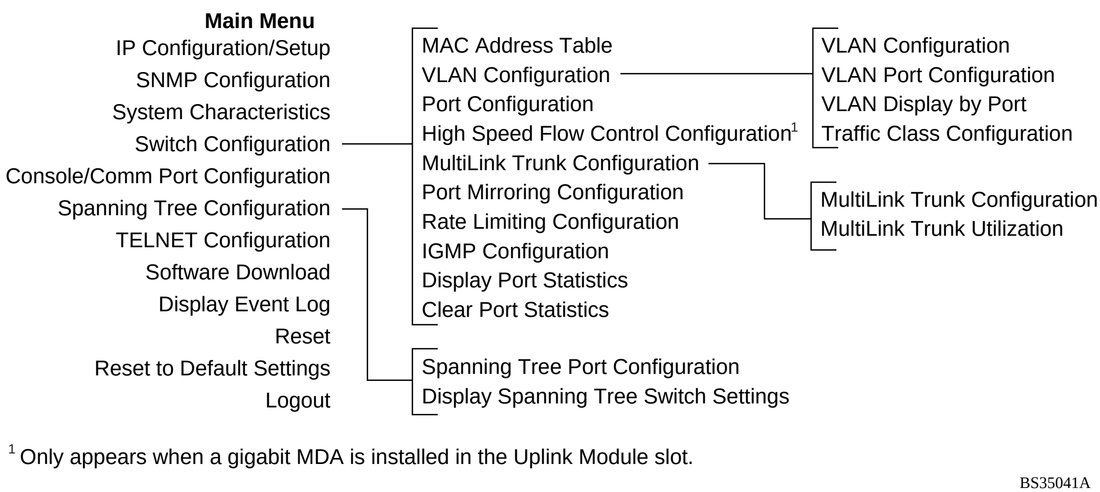


Figure 3-1. Map of Console Interface Screens

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.

```
                      BayStack 350-24T Main Menu


                    IP Configuration/Setup...
                    SNMP Configuration...
                    System Characteristics...
                    Switch Configuration...
                    Console/Comm Port Configuration...
                    Spanning Tree Configuration...
                    TELNET Configuration...
                    Software Download...
                    Display Event Log
                    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 3-7). This screen allows you to set or modify IP configuration parameters.
SNMP Configuration	Displays the SNMP Configuration screen (see "SNMP Configuration" on page 3-12). 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, and set the trap community strings.

(continued)

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

Option	Description
System Characteristics	Displays the System Characteristics screen (see "System Characteristics" on page 3-14). This screen allows you to view switch characteristics, including number of resets, power status, hardware and firmware version, and MAC address. . This screen also contains three user-configurable fields: sysContact, sysName, and sysLocation.
Switch Configuration	Displays the Switch Configuration Menu screen (see "Switch Configuration" on page 3-16). This menu provides the following configuration options: MAC Address Table, VLAN Configuration, Port Configuration, High Speed Flow Control Configuration (only when a gigabit MDA is installed), MultiLink Trunk Configuration, Port Mirroring Configuration, Rate Limiting Configuration, IGMP Configuration, Display Port Statistics, and Clear All Port Statistics.
Console/Comm Port Configuration	Displays the Console/Comm Port Configuration screen (see "Console/Comm Port Configuration" on page 3-54). This screen allows you to configure and modify the console/Comm port parameters, including the console port speed and password settings.
Spanning Tree Configuration	Displays the Spanning Tree Configuration Menu (see "Spanning Tree Configuration" on page 3-59). This menu provides the following configuration options: Spanning Tree Port Configuration, Display Spanning Tree Switch Settings.
TELNET Configuration	Displays the TELNET Configuration screen (see "TELNET Configuration" on page 3-67). This screen allows you to 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.
Software Download	Displays the Software Download screen (see "Software Download" on page 3-70). This screen allows you to revise the BayStack 350 switch software image that is located in nonvolatile flash memory.
Display Event Log	Displays the Event Log screen (see "Display Event Log" on page 3-74).
Reset	Resets the switch with the current configuration settings. This option is followed by a screen prompt that precedes the action. Enter Yes to reset the switch; enter No to abort the option. When you select this option, the switch resets, runs a self-test, then displays the Bay Networks logo screen. Press [Ctrl]-Y to access the BayStack 350 Main Menu.

(continued)

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

Option	Description
Reset to Default Settings	Resets the switch to the factory default configuration settings. This option is followed by a screen prompt that precedes the action. Enter Yes to reset the switch to the factory default configuration settings; enter No to abort the option. **Caution:** If you choose the Reset to Default Settings option, all of your configured settings will be replaced with factory default settings when you press Enter. **Achtung:** Bei Auswahl des Befehls zur Rücksetzung auf die Standardeinstellungen werden alle von Ihnen konfigurierten Einstellungen durch die werkseitigen Standardeinstellungen ersetzt, wenn Sie die Eingabetaste drücken. **Attention:** Si vous restaurez la configuration usine, votre configuration courante sera remplacée par la configuration usine dès que vous appuierez sur [Entrée]. **Precaución:** Si selecciona el comando Restaurar valores predeterminados, todos los valores de configuración se sustituirán por las valores predeterminados en fábrica al pulsar [Intro]. **Attenzione:** Nel caso in cui si selezioni la reimpostazione dei valori di default, tutte le impostazioni configurate verranno sostituite dai default di fabbrica premendo il tasto [Invio]. 注意：「デフォルトの設定にリセット」コマンドを選択すると、現在のコンフィグレーションされた設定は、[Enter]を押したとき、工場出荷時の設定に変更されます。

(continued)

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

Option	Description
	When you select this option, the switch resets, runs a self-test, then displays the Bay 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 3-82).

IP Configuration/Setup

The IP Configuration/Setup screen (Figure 3-3) allows you to set or modify the BayStack 350 switch IP configuration parameters. Data that you enter in the user-configurable fields takes effect as soon as you press Enter.

To open the IP Configuration/Setup screen, choose IP Configuration/Setup (or press i) from the main menu.

Note: The read-only fields in this screen are updated based on the BootP mode specified in the BootP Request Mode field. (See "Choosing a BootP Request Mode" on page 3-9 for more information.)

```
                          IP Configuration/Setup



          BootP Request Mode:  [ BootP When Needed     ]

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





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

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 "Choosing a BootP Request Mode" on page 3-9 for details about the four modes.)	
	Default Value:	BootP Disabled
	Range:	BootP When Needed, BootP Always, BootP Disabled, BootP or Last Address
Configurable	Column header for the user-configurable fields in this screen.	
In Use	Column header for the read-only fields in this screen. The read-only data displayed in this column represents data that is currently in use.	

(continued)

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

Field	Description
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 IP Address	The in-band IP address of the BayStack 350 switch. Default Value: 0.0.0.0 (no IP address assigned) Range: Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point. **Note:** When the IP address is entered in the In-Band IP Address field, and the In-Band Subnet Mask field value is not present, the software provides an *in-use* default value for the In-Band Subnet Mask field that is based on the class of the IP address entered in the In-Band IP Address field.
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 Value: 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.
Default Gateway	The IP address of the default gateway. Default Value: 0.0.0.0 (no IP address assigned) Range: Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point.

Choosing a BootP Request Mode

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

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

Note: Whenever the switch is broadcasting BootP requests, the BootP process will time out if a reply is not received within (approximately) seven 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 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.

BootP Disabled

Allows the switch to be managed only by using the IP address set from the console terminal.

When selected, this mode operates as follows:

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

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

BootP or Last Address

Allows the switch to be managed even if a BootP server is not reachable.

When selected, this mode operates as follows:

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

If an IP address is *not* currently in use, these actions take effect immediately.

If an IP address *is* currently in use, these actions take effect only after the switch is reset or power cycled.

SNMP Configuration

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  ]
      Link Up/Down Trap:            [ 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 Value:	public
	Range:	Any ASCII string of up to 32 printable characters
Read-Write Community String	The community string used for in-band read-write SNMP operations.	
	Default Value:	private
	Range:	Any ASCII string of up to 32 printable characters
Trap #1 IP Address*	Number one of four trap IP addresses. Successive trap IP address fields are numbered 2, 3, and 4. Each trap address has an associated community string (see Community String).	
	Default Value:	0.0.0.0 (no IP address assigned)
	Range:	Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
Community String	The community string associated with one of the four trap IP addresses (see Trap #1 IP Address).	
	Default Value:	Zero-length string
	Range:	Any ASCII string of up to 32 printable characters
Authentication Trap	Determines whether a trap will be sent when there is an SNMP authentication failure.	
	Default Value:	Enabled
	Range:	Enabled, Disabled
Link Up/Down Trap	Determines whether *Link Up* or *Link Down* traps will be sent from the switch.	
	Default Value	Enabled
	Range	Enabled, Disabled

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

System Characteristics

The System Characteristics screen (Figure 3-5) allows you to view system characteristics and 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



MAC Address:          00-60-FD-77-A1-AC

Reset Count:          9
Last Reset Type:      Software Download
Power Status:         Primary Power

sysDescr:             BayStack 350-24T HW:Revx  FW:Vx.xx SW:Vx.x.x.x
sysObjectID:          1.3.6.1.4.1.45.3.35.2
sysUpTime:            02:29:44
sysServices:          3
sysContact:           [ Mario Lento ]
sysName:              [ Documentation ]
sysLocation:          [ Building 20, Floor 28 ]



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	
MAC Address	The MAC address of the BayStack 350 switch.	
Reset Count	A read-only field that indicates the number of resets since the operational firmware was first loaded on the switch.	
	Default Value:	1
	Range:	0 to 2^{32} -1
Last Reset Type	A read-only field that indicates the last type of reset.	
	Default Value:	Power Cycle
	Range:	Power Cycle, Software Download, Management Reset, Management Factory Reset
Power Status	A read-only field that indicates the current power source.	
	Default Value:	Primary Power
sysDescr	A read-only field that specifies the hardware and software version.	
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 Value::	Zero-length string
	Range:	Any ASCII string of up to 56 printable characters*
sysName	A name that uniquely identifies the switch.	
	Default Value::	Zero-length string
	Range:	Any ASCII string of up to 56 printable characters*
sysLocation	The physical location of the switch.	
	Default Value:	Zero-length string
	Range:	Any ASCII string of up to 56 printable characters

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

Switch Configuration

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

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

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

```
                        Switch Configuration Menu



                          MAC Address Table
                          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
                          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 screen 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 3-18). 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).
VLAN Configuration	Displays the VLAN Configuration Menu (see "VLAN Configuration Menu" on page 3-20). This menu provides the following options: VLAN Configuration, VLAN Port Configuration, VLAN Display by Port, Traffic Class Configuration, and Return to Switch Configuration Menu screen. This menu allows you to create and modify VLANs.
Port Configuration	Displays the Port Configuration screen (see "Port Configuration" on page 3-30). This screen allows you to configure a specific switch port or all switch ports.
High Speed Flow Control Configuration	This menu selection only appears when an optional gigabit MDA is installed in the Uplink Module slot. When the gigabit MDA is installed, selecting this option displays the High Speed Flow Control Configuration screen (see "High Speed Flow Control Configuration" on page 3-32).
MultiLink Trunk Configuration	Displays the MultiLink Trunk Configuration Menu (see "MultiLink Trunk Configuration" on page 3-35). This menu provides the following options: MultiLink Trunk Configuration, MultiLink Trunk Utilization, and Return to Switch Configuration Menu screen. This menu allows you to create and modify trunks, and to monitor the bandwidth utilization of configured trunks.
Port Mirroring Configuration	Displays the Port Mirroring Configuration screen (see "Port Mirroring Configuration" on page 3-41). This screen allows you to designate a single switch port as a traffic monitor for up to two specified ports or addresses.
Rate Limiting Configuration	Displays the Rate Limiting Configuration screen (see "Rate Limiting Configuration" on page 3-45). This screen allows you to limit the forwarding rate of broadcast and multicast packets.
IGMP Configuration	Displays the IGMP Configuration screen (see "IGMP Configuration" on page 3-48). This screen allows you to optimize multicast traffic by setting up IGMP port memberships that filter multicast on a per port basis (see "IGMP Snooping" on page 1-34 for more information about this feature).

(continued)

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

Option	Description
Display Port Statistics	Displays the Port Statistics screen (see "Port Statistics" on page 3-51). 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.
Return to Main Menu	Exits the Switch Configuration Menu screen and displays the main menu.

MAC Address Table

The MAC Address Table screen (Figure 3-7) allows you to view MAC addresses that the switch has learned 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 3-41).

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

Note: This screen does not refresh dynamically to show new entries. To refresh the screen, press [Ctrl]-P or [Ctrl]-N.

```
                              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-FD-00-02-30
00-00-A2-85-BB-26     Port: 1
00-60-FD-12-02-15     Port: 1
00-08-C7-1D-4F-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 Value: 300 seconds
	Range: 10 to 1,000,000 seconds
Find an Address	Allows the user to search for a specific MAC address.
	Default Value: 00-00-00-00-00-00 (no MAC address assigned)
	Range: 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF

(continued)

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

Field	Description
Port Mirroring Address A	This field only appears when any of the five *address-based* monitoring modes are selected 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 displays in this screen. See "Port Mirroring Configuration" on page 3-41 for more information. Default Value: 00-00-00-00-00-00 (no MAC address assigned) Range: 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF
Port Mirroring Address B	This field only appears when any of the two *address-based* monitoring modes that use Address B are selected 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 displays in this screen. See "Port Mirroring Configuration" on page 3-41 for more information. Default Value: 00-00-00-00-00-00 (no MAC address assigned) Range: 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF

VLAN Configuration Menu

The VLAN Configuration Menu screen (Figure 3-8) allows you to select the appropriate screen to configure up to 64 port-based VLANs. When you create VLANs, you can assign various ports (and therefore the devices attached to these ports) to different broadcast domains. Creating VLANs increases network flexibility by allowing you to reassign devices to accommodate network moves, additions, and changes, eliminating the need to change physical cabling.

See "IEEE 802.1Q VLAN Workgroups" on page 1-18, for detailed information about configuring VLANs.

Choose VLAN Configuration (or press v) from the Switch Configuration Menu screen 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 3-8. VLAN Configuration Menu Screen

Table 3-7 describes the VLAN Configuration Menu screen options.

Table 3-7. VLAN Configuration Menu Screen Options

Option	Description
VLAN Configuration	Displays the VLAN Configuration screen (see "VLAN Configuration" on page 3-22). This screen allows you to set up VLAN workgroups.
VLAN Port Configuration	Displays the VLAN Port Configuration screen (see "VLAN Port Configuration" on page 3-24). This screen allows you to set up a specific switch port or all switch ports.
VLAN Display by Port	Displays the VLAN Display by Port screen (see "VLAN Display by Port" on page 3-27).
Traffic Class Configuration	Displays the Traffic Class Configuration screen (see "Traffic Class Configuration" on page 3-28).
Return to Switch Configuration Menu	Exits the VLAN Configuration Menu screen and displays the Switch Configuration Menu screen.

VLAN Configuration

The VLAN Configuration screen (Figure 3-9) allows you to assign switch ports as *VLAN port members*. Ports that are configured as VLAN port members become part of a set of ports that form a broadcast domain for a specific VLAN. Switch ports can be assigned as VLAN port members of one or more VLANs.

VLAN port members can be assigned attributes that allow the individual ports to operate in accordance with the IEEE 802.1Q tagging rules. You can assign each VLAN port member as *tagged* or *untagged* port members (see "IEEE 802.1Q Tagging" on page 1-19, for a description of important terms used with 802.1Q VLANs).

You can also use this screen to create and to delete specific VLANs and to assign VLAN names.

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

```
                        VLAN Configuration

            Create VLAN:              [   1  ]
            Delete VLAN:              [      ]
            VLAN Name:                [ VLAN #1 ]

                           Port Membership
      1-6        7-12      13-18      19-24      25-28
     ------     ------     ------     ------     ------
     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 3-9. VLAN Configuration Screen

Table 3-8 describes the VLAN Configuration screen fields.

Table 3-8. VLAN Configuration Screen Fields

Field	Description
Create VLAN	Allows you to set up or view configured VLAN workgroups. Enter the number of the new VLAN you want to create or view, then press [Return]. The Port Membership fields indicate the corresponding VLAN workgroup configuration, if configured, or all dashes (-), indicating no VLAN Members configured. Alternatively, you can use the spacebar to toggle through the various configured VLAN workgroups. You can only create up to 64 different VLANs. Default 1 Range: 2 to 4094
Delete VLAN	Allows you to delete specified VLANs. Enter the number of the VLAN you want to delete, then press [Return], or use the spacebar to toggle through the selection until you reach the VLAN you want to delete, then press [Return]. The selected VLAN is deleted as soon as you press [Return]. The software does not prompt you to reconsider this action. 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 1-18 for more information. Default blank field Range: 2 to 4094
VLAN Name	Allows you to assign a name field to configured VLANs. Default VLAN # (*VLAN number*) Range: Any ASCII string of up to 16 printable characters
Port Membership	Allows you to assign switch ports as a tagged port member (T), untagged port member (U), or as a non-VLAN port member (-). Switch ports can be configured in one or more VLANs. An exception to this rule applies to the gigabit MDAs (see note). **Note:** The gigabit MDAs restrict the configuration of VLAN tagging. The gigabit MDA ports can be set up as tagged VLAN members or as untagged VLAN members for a VLAN that has a VID which is equal to the port’s PVID. For all other VLANs configured on that port the VLAN port membership will be *all* tagged or *all* untagged (see “VLAN Port Configuration” on page 3-24). 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 Value: U (All ports are assigned as untagged members of VLAN 1.) Range: U, T, and -

VLAN Port Configuration

The VLAN Port Configuration screen (Figure 3-10) allows you to configure specified switch ports with the appropriate PVID/VLAN association that enables the creation of broadcast domains (see “Shared Servers” on page 1-26 for more information about setting up 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 1-19). You can also prioritize the order in which the switch forwards packets, on a per-port basis (see “IEEE 802.1p Prioritizing” on page 1-39).

Figure 3-9 shows an example of the VLAN Port Configuration screen with a gigabit MDA installed in switch port 25. The gigabit MDA restricts the configuration of VLAN tagging (see “Port Membership” field in Table 3-8, on page 3-23).

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

```
                        VLAN Port Configuration



              Port:                             [ 25  ]
              Filter Tagged Frames:             [ No  ]
              Filter Untagged Frames:           [ No  ]
              Filter Unregistered Frames:       [ No  ]
              Port Name:                        [ Port #25 ]
              PVID:                             [   1  ]
              Port Priority:                    [  0  ]

The following parameters specify egress rules for the Gigabit port only:

Primary VLAN Tagging (with VLAN equal to PVID):        [ Untagged ]
Secondary VLAN Tagging (with VLAN not equal to PVID):  [  Tagged  ]





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. VLAN Port Configuration Screen

Table 3-9 describes the VLAN Port Configuration screen fields.

Table 3-9. 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 on your keyboard to toggle the port numbers.
Filter Tagged Frames	Allows you to set this port to filter (discard) all received tagged packets. Default Value: No Range: No, Yes
Filter Untagged Frames	Allows you to set this port to filter (discard) all received untagged packets. Default Value: No Range: No, Yes
Filter Unregistered Frames	Allows you to set this port to filter (discard) all received unregistered packets. Default Value: No Range: No, Yes
Port Name	Allows you to assign a name to this port. Default Value: Port # (*port number*) Range: Any ASCII string of up to 16 printable characters
PVID	Port VLAN identifier field. Allows you to associate this port with a specific VLAN. For example, a port with a PVID of 3 assigns all untagged frames received on this port to VLAN 3. Default Value: 1 Range: 1 to 4094
Port Priority	Allows you to prioritize the order in which the switch forwards packets received on specified ports (see "IEEE 802.1p Prioritizing" on page 1-39). Default Value: 0 Range: 0 to 7

➡ **Note:** The following fields only appear when the port (selected in the Port field) is configured with an optional gigabit MDA.

(continued)

Table 3-9. VLAN Port Configuration Screen Fields (continued)

Field	Description
Primary VLAN Tagging	Allows a user to assign the associated gigabit MDA port as a tagged or untagged VLAN member for the VLAN corresponding to the port's PVID (see "Assigning Tagging to Gigabit MDA Ports" on page 3-26). Default Value: Untagged Range: Untagged, Tagged
Secondary VLAN Tagging	Allows a user to assign tagging parameter values (tagged or untagged) to all other VLANs (all VLANs with VIDs that are not equal to the PVID). See "Assigning Tagging to Gigabit MDA Ports" on page 3-26. Default Value: Tagged Range: Tagged, Untagged

Assigning Tagging to Gigabit MDA Ports

Note: The gigabit MDAs restrict the configuration of VLAN tagging. The gigabit MDA ports can be set up as tagged VLAN members or as untagged VLAN members for a VLAN that has a VID which is equal to the port's PVID. For all other VLANs configured on that port the VLAN port membership will be *all* tagged or *all* untagged.

This section shows how a user could assign the gigabit MDA port (port 25 shown in Figure 3-10) as a Tagged VLAN member. In this example, the MDA port in the example is configured with a PVID of 1. This means that the port-to-VLAN association for port 25 is VLAN 1 (see "IEEE 802.1Q Tagging" on page 1-19). If the PVID for port 25 is changed to another number (for example, PVID 7), port 25 becomes associated with VLAN 7. This is important to note because the rules applying to the gigabit MDA configuration only allow for one (primary) VLAN for the gigabit port. All other VLANs configured on that port are considered secondary VLANs, and the *secondary* VLAN memberships can only be *all* tagged or *all* untagged.

To assign the gigabit MDA port as a tagged VLAN member for the primary VLAN, complete the following steps:

1. **From the VLAN Port Configuration screen, change the (default) Primary VLAN Tagging field to Tagged, then Press [Return].**
2. **Press [Ctrl]-R to return to the previous menu.**

3. **Choose VLAN Configuration (or press v) from the VLAN Configuration Menu to open the VLAN Configuration screen.**
4. **In the VLAN Configuration screen, set the port membership field for port 25 to T (Tagged Port Member), then press [Return].**

   Be sure that VLAN displayed in the Create VLAN field is the same as the port's PVID (in this case, the PVID for port 25 is 1).

VLAN Display by Port

The VLAN Display by Port screen (Figure 3-9) allows you to view VLAN characteristics associated with a specified switch port.

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

```
                              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 3-11. VLAN Display by Port Screen

Table 3-10 describes the VLAN Display by Port screen fields.

Table 3-10. 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 3-12) 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 1-39 for more information about this screen.

Choose Traffic Class Configuration (or press t) from the VLAN Configuration Menu screen 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  ]








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 3-12. Traffic Class Configuration Screen

Table 3-11 describes the Traffic Class Configuration screen fields.

Table 3-11. Traffic Class Configuration Screen Fields

Field	Description
User Priority	Column header for the read-only fields that indicate the user-priority values from priority 0 to priority 7. These values are derived from the three-bit field in the header of 802.1Q tagged frames (see “IEEE 802.1Q Tagging” on page 1-19).
Traffic Class	Column header for the eight user-configurable fields that correspond to the adjacent user priority levels. Default Value: Low Range: Low, High

Port Configuration

The Port Configuration screen (Figure 3-13 and Figure 3-14) 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 fields, the Speed fields, and the 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 screen to open the Port Configuration screen.

```
                              Port Configuration

   Port    Trunk       Status      Link    Auto Negotiation      Speed  Duplex
   ----    -----    ------------   ----    ----------------    -----------------
     1              [ Enabled  ]   Up        [ Enabled  ]      [ 100Mbs / Half ]
     2              [ Enabled  ]   Up        [ Enabled  ]      [ 100Mbs / Half ]
     3              [ Enabled  ]   Up        [ Enabled  ]      [ 100Mbs / Full ]
     4              [ Enabled  ]   Down      [ Disabled ]      [ 100Mbs / Half ]
     5              [ Enabled  ]   Up        [ Enabled  ]      [  10Mbs / Full ]
     6       1      [ Enabled  ]   Up        [ Enabled  ]      [ 100Mbs / Full ]
     7       1      [ Enabled  ]   Up        [ Enabled  ]      [ 100Mbs / Full ]
     8              [ Enabled  ]   Up        [ Enabled  ]      [  10Mbs / Full ]
     9       1      [ Enabled  ]   Up        [ Disabled ]      [ 100Mbs / Full ]
    10              [ Enabled  ]   Down      [ Enabled  ]      [ 100Mbs / Full ]
    11              [ Enabled  ]   Down      [ Enabled  ]      [ 100Mbs / Full ]
    12              [ Enabled  ]   Down      [ Disabled ]      [ 100Mbs / Half ]
    13       2      [ Enabled  ]   Down      [ Disabled ]      [ 10Mbs  / Full ]
    14       2      [ Enabled  ]   Down      [ Disabled ]      [ 10Mbs  / 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 3-13. Port Configuration Screen (1 of 2)

```
                              Port Configuration

   Port    Trunk      Status       Link    Auto Negotiation     Speed  Duplex
   ----    -----   ------------    ----    ----------------   -----------------
    15             [ Enabled  ]    Up        [ Enabled  ]      [ 100Mbs / Full ]
    16             [ Enabled  ]    Down      [ Disabled ]      [ 100Mbs / Half ]
    17       1     [ Enabled  ]    Up        [ Disabled ]      [ 100Mbs / Half ]
    18             [ Enabled  ]    Down      [ Disabled ]      [ 100Mbs / Half ]
    19       3     [ Enabled  ]    Up        [ Disabled ]      [ 100Mbs / Half ]
    20       3     [ Enabled  ]    UP        [ Disabled ]      [ 100Mbs / Half ]
    21             [ Enabled  ]    Down      [ Disabled ]      [ 100Mbs / Half ]
    22       4     [ Enabled  ]    Up        [ Enabled  ]      [ 100Mbs / Full ]
    23       4     [ Enabled  ]    Up        [ Enabled  ]      [ 100Mbs / Full ]
    24             [ Enabled  ]    Down      [ Enabled  ]      [ 100Mbs / Full ]
    25       1     [ Enabled  ]    Up        [ Enabled  ]      [ 100Mbs / Full ]
    26       1     [ Enabled  ]    Up        [ Enabled  ]      [ 100Mbs / Full ]
    27             [ Enabled  ]    Down      [ Disabled ]      [ 10Mbs  / Full ]
    28             [ Enabled  ]    Down      [ Disabled ]      [ 10Mbs  / Full ]
    All            [ Enabled  ]              [ Disabled ]      [ 10Mbs  / Full ]


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 3-14. 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 3-32 to set the autonegotiation field for the gigabit MDA port. The gigabit MDA only supports 1000 Mb/s in full-duplex mode.

Table 3-12 describes the Port Configuration screen fields.

Table 3-12. 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 applied in the All row (bottom row) affect all switch ports (except the gigabit MDA port, when installed).

(continued)

Table 3-12. 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 3-35).
Status	Allows you to disable any of the switch ports. You can also use this field to control access to any switch port. Default Value: Enabled Range: Enabled, Disabled
Link	A read-only field that indicates the current link state of the corresponding port, as follows: • Up: The port is connected and operational. • Down: The port is not connected or is not operational.
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 Value: 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 Value: 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 3-15) allows you to set the port parameters for installed gigabit MDAs.

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

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

```
                    High Speed Flow Control Configuration




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


                   Active Phy                      None








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

Figure 3-15. High Speed Flow Control Configuration Screen

Table 3-13 describes the High Speed Flow Control Configuration screen fields.

Table 3-13. High Speed Flow Control Configuration Screen Fields

Field	Description
Autonegotiation	When enabled, the port advertises support for 1000 Mb/s operation, in full-duplex mode. Default Value: 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 3-34 for details about the two modes). Autonegotiation must be disabled for this port when using this feature. Default Value: Disabled Range: Disabled, Symmetric, Asymmetric

(continued)

Table 3-13. High Speed Flow Control Configuration Screen Fields (continued)

Field	Description
	Note: The following two fields only appear when a (single MAC) MDA with a separate redundant Phy port is installed.
Preferred Phy	Allows you to choose the preferred Phy port, the other Phy port reverts to backup. Default Value: Right Range: Right, Left
Active Phy	Indicates the operational Phy port.

Choosing a High Speed Flow Control Mode

The High Speed Flow Control feature allows you to control traffic and avoid congestion on the gigabit full-duplex link. If the receive port buffer becomes full, the BayStack 350 switch issues a flow-control signal to the device at the other end of the link to suspend transmission. When the receive buffer is no longer full, the switch issues a signal to resume the transmission. You can choose Symmetric or Asymmetric flow control mode:

Symmetric Mode

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

Asymmetric

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 screen (Figure 3-16) allows you to select the appropriate screen to configure up to six MultiLink trunks. You can group up to four switch ports together to form each trunk, 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.

For more information about configuring MultiLink Trunks, see "MultiLink Trunks" on page 1-43.

Note: When a trunk is not active (Trunk Status field set to Disabled), configuration changes do not take effect until the Trunk Status field is set to Enabled.

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

```
                        MultiLink Trunk Configuration Menu




                         MultiLink Trunk Configuration...
                         MultiLink Trunk Utilization...
                         Return to Switch Configuration Menu









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

Figure 3-16. MultiLink Trunk Configuration Menu Screen

Table 3-14 describes the MultiLink Trunk Configuration Menu screen options.

Table 3-14. MultiLink Trunk Configuration Menu Screen Options

Option	Description
MultiLink Trunk Configuration...	Displays the MultiLink Trunk Configuration screen (Figure 3-17). This screen allows you to configure up to six MultiLink trunks. You can group up to four switch ports together to form each trunk.
MultiLink Trunk Utilization...	Displays the MultiLink Trunk Utilization screen (Figure 3-18 and Figure 3-19). This screen allows you to monitor the bandwidth utilization of the configured trunks.
Return to Switch Configuration Menu	Exits the MultiLink Trunk Configuration Menu screen and displays the Switch Configuration Menu screen.

MultiLink Trunk Configuration Screen

The MultiLink Trunk Configuration screen 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. Figure 3-17 shows an example of the MultiLink Trunk Configuration screen. In this screen example (previously discussed on page 1-46), 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 1-46 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 screen 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 3-17. MultiLink Trunk Configuration Screen

Table 3-15 describes the MultiLink Trunk Configuration screen fields.

Table 3-15. 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	The Trunk Members column contains fields in each row that can be configured to create the corresponding trunk. Each switch port can only be a member of a single trunk. The appropriate trunk number for each trunk member configured within this field is shown adjacent to the corresponding switch port in the following screens: Port Configuration screen, and Spanning Tree Configuration screen. Gigabit ports cannot be configured as trunk members. Default Value: blank field Range: 1 to 28 (depending on model type)

(continued)

Table 3-15. MultiLink Trunk Configuration Screen Fields (continued)

Field	Description
STP Learning	The STP Learning column contains a single field for each row that, when enabled, allows the specified trunk to participate in the spanning tree. This setting overrides those of the individual trunk members. Fast is the same as Normal, except that the state transition timer is shortened to two seconds. Default Value: Normal Range: Normal, Fast, Disabled
Trunk Mode	The Trunk Mode column contains a single read-only field for each row that indicates the default operating mode for the switch. **Basic:** Basic mode is the default mode for the switch. When in this mode, source MAC addresses are dynamically assigned to specific trunk members for flooding and forwarding. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members. Default Value: Basic
Trunk Status	The Trunk Status column contains a single field for each row that allows users to enable or disable any of the trunks. Default Value: Enabled Range: Enabled, Disabled
Trunk Name	The Trunk Name column contains a single optional field in each row that can be used to assign names to the corresponding configured trunks. The names chosen for this example can provide meaningful information to the user (for example, S1:T1 to FS2 indicates trunk 1, in switch S1 connects to file server 2)

MultiLink Trunk Utilization Screen

The MultiLink Trunk Utilization screen (Figure 3-18 and Figure 3-19) allows you to monitor the percentage of bandwidth used by configured trunk members. You can choose the type of traffic to monitor.

Figure 3-18 shows an *example* of bandwidth utilization rates for the trunk member ports configured in Figure 3-17. 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 screen 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 3-18. 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 3-19. MultiLink Trunk Utilization Screen (2 of 2)

Table 3-16 describes the MultiLink Trunk Utilization screen fields.

Table 3-16. 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 Value: Rx and Tx Range: Rx and Tx, Rx, Tx
Port	This field lists the trunk member ports that correspond to the trunk specified in the Trunk column.

(continued)

Table 3-16. 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) utilized by the port in the last five minutes. This field provides a running average of network activity and is updated every 15 seconds.
Last 30 Minutes	This read-only field indicates the percentage of packets (of the type specified in the Traffic Type field) utilized by the port in the last 30 minutes. This field provides a running average of network activity and is updated every 15 seconds.
Last Hour	This read-only field indicates the percentage of packets (of the type specified in the Traffic Type field) utilized by the port in the last hour. 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. 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 1-61.

Figure 3-20 shows an example of a Port Mirroring Configuration screen where switch port 12 is designated as the monitoring port for ports 24 and 25.

Choose Port Mirroring Configuration (or press i) from the Switch Configuration Menu screen 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 3-20. Port Mirroring Configuration Screen

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

Table 3-17. Port Mirroring Configuration Screen Fields

Field	Description
Monitoring Mode	This field allows a user to select any one of six port-based monitoring modes or any one of five address-based monitoring modes (see Table 3-18): Selecting *any one* of the six *port-based modes* activates the port X and port Y screen fields, where a user can choose up to two ports to monitor. Selecting *any one* of the five *address-based modes* activates the Address A and Address B screen fields, where a user can specify MAC addresses to monitor. Default Value: Disabled Range: See Table 3-18

(continued)

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

Field	Description
Monitor Port	Indicates the switch port designated as the monitor port. Default Value: 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 X in the Monitoring Mode field (see Table 3-18). Default Value: 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 Y in the Monitoring Mode field (see Table 3-18). Default Value: 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 “Address A” in the selected Monitoring Mode field (see Table 3-18). 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 3-18). Default Value: 00-00-00-00-00-00 (no MAC address assigned) Range: 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF
Address B	Indicates the MAC addresses that will be monitored by the designated port monitor when one of the address-based monitoring modes is selected. This port will be monitored according to the value “Address B” in the selected Monitoring Mode field (see Table 3-18). 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 3-18). Default Value: 00-00-00-00-00-00 (no MAC address assigned) Range: 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF

Table 3-18 describes the various monitoring modes available from the Port Mirroring Configuration screen.

Table 3-18. Monitoring Modes

Fields	Description
Port-Based Fields:	
Disabled	Default Value: for this feature.
-> Port X	Monitor all traffic received by Port X.
Port X ->	Monitor all traffic transmitted by Port X.
<-> Port X	Monitor all traffic received and transmitted by Port X.
-> Port X or Port Y ->	Monitor all traffic received by Port X or transmitted by Port Y.
-> Port X and Port Y ->	Monitor all traffic received by Port X (destined to Port Y) and then transmitted by Port Y.
<-> Port X and Port Y <->	Monitor all traffic received/transmitted by Port X and received/ transmitted by Port Y.
Address-Based Fields:	
Disabled	Default Value: for this feature.
Address A -> any Address	Monitor all traffic transmitted from Address A to any address.
any Address -> Address A	Monitor all traffic received by Address A from any address.
<-> Address A	Monitor all traffic received by or transmitted by Address A.
Address A -> Address B	Monitor all traffic transmitted by Address A to Address B.
Address A <-> Address B	Monitor all traffic between Address A and Address B (conversation between the two stations).

Rate Limiting Configuration

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

Figure 3-21 and Figure 3-22 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 screen 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 3-21. 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 3-22. 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 3-19 describes the Rate Limiting Configuration screen fields.

Table 3-19. 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 settings 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 Value: Both Range: Both, Multicast, Broadcast
Limit	Sets the percentage of port bandwidth allowed for forwarding the packet types specified in the Packet Type field. When the threshold is exceeded, any additional packets (specified in the Packet Type field) are discarded*. Default Value: None Range: None, 10%, 9%, 8%, 7%, 6%, 5%, 4%, 3%, 2%, 1%
Last 5 Minutes	This read-only field indicates the percentage of packets (of the type specified in the Packet Type field) received by the port in the last five minutes. This field provides a running average of network activity and is updated every 15 seconds. Note that this field indicates the receiving port's view of network activity, regardless of the rate limiting setting.
Last Hour	This read-only field indicates the percentage of packets (of the type specified in the Packet Type field) received by the port in the last hour. This field provides a running average of network activity and is updated every five minutes. Note that this field indicates the receiving port's view of network activity, regardless of the rate limiting setting.
Last 24 Hours	This read-only field indicates the percentage of packets (of the type specified in the Packet Type field) received by the port in the last 24 hours. This field provides a running average of network activity and is updated every hour. Note that this field indicates the receiving port's view of network activity, regardless of the rate limiting setting.

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

IGMP Configuration

The IGMP Configuration screen allows you to set your switch ports to optimize IP multicast packets in a bridged Ethernet environment (see "IGMP Snooping" on page 1-34). Figure 3-23 shows an example of the IGMP Configuration screen with switch ports 8 and 14 set to receive/transmit multicast from the local multicast router. The configured ports are VLAN port members of VLAN 5.

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

```
                              IGMP Configuration

                    VLAN:                 [   5  ]
                    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
         ------    ------    ------    ------    ------
         ------    -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 3-23. IGMP Configuration Screen

Table 3-20 describes the IGMP Configuration screen fields.

Table 3-20. IGMP Configuration Screen Fields

Field	Description
VLAN	Allows you to set up or view IGMP VLAN configurations on specified VLANs. You can use the spacebar to toggle to any *existing* IGMP VLAN configurations (the maximum number of VLANs that can be displayed is 64). Default Value: 1 Range: 1 to 4094
Snooping	Allows you to enable or disable IGMP Snooping. This field affects all VLANs (for example, if you disable snooping on the VLAN specified in the screen's VLAN field, ALL VLANs are disabled for snooping). Default Value: Enabled Range: Enabled, Disabled
Proxy	Allows the switch to consolidate IGMP Host Membership Reports received on its downstream ports and to generate a consolidated proxy report for forwarding to its upstream neighbor. This field affects all VLANs (for example, if you disable proxy on the VLAN specified in the screen's VLAN field, ALL VLANs are disabled for proxy). The Proxy field cannot be disabled unless the Snooping field is Enabled. Default Value: Enabled Range: Enabled, Disabled
Robust Value	Allows a user to set the switch to offset expected packet losses on a subnet. If packet losses on a subnet are unacceptably high, the Robust Value field can be increased to a higher value. This field affects only the VLAN specified in the screen's VLAN field (for example, if you change the robust value on the VLAN specified in the screen's VLAN field, other VLANs are not affected). Default Value: 2 Range: 1 to 64

(continued)

Table 3-20. IGMP Configuration Screen Fields (continued)

Field	Description
Query Time	Allows a user to control the number of IGMP messages allowed on the subnet by varying the *Query Interval* (the Query Interval is the interval between general queries sent by the multicast router). This field affects only the VLAN specified in the screen's VLAN field (for example, if you change the Query Time value field on the VLAN specified in the screen's VLAN field, other VLANs are not affected). Default Value: 125 seconds Range: 1 to 512 seconds
Set Router Ports	Sets the IGMP Snooping feature to operate according to the IGMPv1 or IGMPv2 standard (see RFC 2236). This field affects all VLANs (for example, if you change the value of the Set Router Ports field on the VLAN specified in the screen's VLAN field, ALL VLANs are affected). Default Value: Version 1 Range: Version 1, Version 2
Static Router Ports	Allows a user to assign switch ports to any port that has a path to a multicast router. These configured ports do not filter any IP Multicast traffic. The Static Router Ports fields are displayed in six-port groups (for example, 1-6, 7-12, 13-18). The number of ports displayed depends on the switch model or type of optional MDA that is installed in the Uplink Module slot. This field affects all VLANs (for example, if you assign a port as a static router port in this screen, the port becomes a static router port for the VLAN specified in the screen's VLAN field, and also for any other VLAN where this port is a member). Default Value: - Range: -, X

Port Statistics

The Port Statistics screen (Figure 3-24) 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 3-16).

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

```
Port:  [ 1  ]                 Port Statistics
               Received                                Transmitted
------------------------------------    --------------------------------------
Packets:                            0    Packets:                          497
Multicasts:                         0    Multicasts:                       497
Broadcasts:                         0    Broadcasts:                         0
Total Octets:                       0    Total Octets:                   31808
Lost Packets:                       0    Lost Packets:                       0
FCS Errors:                         0    Collisions:                         0
Frame Errors:                       0    Single Collisions:                  0
Undersized Packets:                 0    Multiple Collisions:                0
Oversized Packets:                  0    Excessive Collisions:               0
Packets 64 bytes:                   0    Packets 64 bytes:                 497
        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
Filtered Packets:                   0    Deferred Packets:                   0
Flooded Packets:                    0    Late Collisions:                    0


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

Figure 3-24. Port Statistics Screen

Table 3-21 describes the Port Statistics screen fields.

Note: The Port Statistics screen appears in a slightly different format when the port selected in the Port fields is configured with a gigabit MDA.

Table 3-21. Port Statistics Screen Fields

Field	Description
Port	Allows you to select the number of the port you want to view or reset to zero. To view another port, type its port number and press Enter, or press the spacebar on your keyboard to toggle the port numbers.
Packets	*Received column:* Indicates the total number of packets received on this port, including bad packets, broadcast packets, and multicast packets. *Transmitted column:* Indicates the total number of packets transmitted successfully on this port, including broadcast packets and multicast packets.
Multicasts	*Received column:* Indicates the total number of good multicast packets received on this port, excluding broadcast packets. *Transmitted column:* Indicates the total number of multicast packets transmitted successfully on this port, excluding broadcast packets.
Broadcasts	*Received column:* Indicates the total number of good broadcast packets received on this port. *Transmitted column:* Indicates the total number of broadcast packets transmitted successfully on this port.
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.
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.
Frame Errors	Indicates the total number of valid-size packets that were received but discarded because of CRC errors and improper framing.

(continued)

Table 3-21. Port Statistics Screen Fields (continued)

Field	Description
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).
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.
Packets 64 bytes	*Received column:* Indicates the total number of 64-byte packets received on this port. *Transmitted column:* Indicates the total number of 64-byte packets transmitted successfully on this port.
65-127 bytes	*Received column:* Indicates the total number of 65-byte to 127-byte packets received on this port. *Transmitted column:* Indicates the total number of 65-byte to 127-byte packets transmitted successfully on this port.
128-255 bytes	*Received column:* Indicates the total number of 128-byte to 255-byte packets received on this port. *Transmitted column:* Indicates the total number of 128-byte to 255-byte packets transmitted successfully on this port.
256-511 bytes	*Received column:* Indicates the total number of 256-byte to 511-byte packets received on this port. *Transmitted column:* Indicates the total number of 256-byte to 511-byte packets transmitted successfully on this port.
512-1023 bytes	*Received column:* Indicates the total number of 512-byte to 1023-byte packets received on this port. *Transmitted column:* Indicates the total number of 512-byte to 1023-byte packets transmitted successfully on this port.
1024-1518 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.

(continued)

Table 3-21. Port Statistics Screen Fields (continued)

Field	Description
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.
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.

Console/Comm Port Configuration

The Console/Comm Port Configuration screen (Figure 3-25) allows you to configure and modify the console/comm port parameters.

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 Password:             [ Not Required         ]
          Console Read-Only Password:   [ user ]
          Console Read-Write Password:  [ secure ]






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 3-25. Console/Comm Port Configuration Screen

Table 3-22 describes the Console/Comm Port Configuration screen fields.

Table 3-22. Console/Comm Port Configuration Screen Fields

Field	Description
Comm Port Data Bits	A read-only field that indicates the current console/comm port data bit setting.
Comm Port Parity	A read-only field that indicates the current console/comm port parity setting.
Comm Port Stop Bits	A read-only field that indicates the current console/comm port stop bit setting.
Console Port Speed	Allows you to set the console/comm port baud rate to match the baud rate of the console terminal. Default Value: 9600 Baud Range: 2400 Baud, 4800 Baud, 9600 Baud, 19200 Baud, 38400 Baud

Caution: If you choose a baud rate that does not match your console terminal baud rate, you will lose communication with the configuration interface when you press [Enter]. If communication is lost, set your console terminal to match the new service port setting.

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.

(continued)

Table 3-22. Console/Comm Port Configuration Screen Fields (continued)

Field	Description
	Attenzione: Nel caso in cui si scelga una velocità di trasmissione non corrispondente a quella del terminale della console, la comunicazione con l'interfaccia della console cadrà premendo il tasto [Invio]. Se la comunicazione cade, impostare il terminale della console in modo tale che corrisponda alla nuova impostazione della porta di servizio. 注意: コンソール・ターミナルのボー･レートに合っていな 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 Password	Enables password protection for accessing the console interface (CI) through a TELNET session, a console terminal, or both. 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 Password and Console Read-Write Password for more information. Default Value: Not Required Range: Not Required, Required for TELNET, Required for Console, Required for Both
Console Read-Only Password	When the Console Password field is set to Required (for TELNET, for Console, or for Both), this field allows read-only password access to the CI. Users can access the CI using the correct password (see Default Value:), but cannot change any parameters or use the Reset option or Reset to Default option. Default Value: user Range: An ASCII string of up to 15 printable characters

(continued)

Table 3-22. Console/Comm Port Configuration Screen Fields (continued)

Field	Description
Console Read-Write Password	When the Console Password field is set to Required (for TELNET, for Console, or for Both), this field allows read-write password access to the CI. Users can log in to the CI using the correct password (see Default Value:), and can change any parameters. Note that you can change the default passwords for read-only access and read-write access to a private password. Default Value: secure Range: Any ASCII string of up to 15 printable characters

Caution: If you change the system-supplied default passwords, be sure to write the new passwords down and keep them in a safe place. If you forget the new passwords, you cannot access the console interface. In that case, contact Bay 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 Bay Networks, um Unterstützung zu erhalten.

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 Bay 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 Bay Networks.

(continued)

Table 3-22. 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 Bay 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 Bay 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。

Spanning Tree Configuration

The Spanning Tree Configuration Menu screen (Figure 3-26) 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 screen.

```
                         Spanning Tree Configuration Menu





                      Spanning Tree Port Configuration...
                      Display Spanning Tree Switch Settings
                      Return to Main Menu







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

Figure 3-26. Spanning Tree Configuration Menu Screen

Table 3-23 describes the Spanning Tree Configuration Menu screen options:

Table 3-23. Spanning Tree Configuration Menu Screen Options

Option	Description
Spanning Tree Port Configuration	Displays the Spanning Tree Port Configuration screen (see "Spanning Tree Port Configuration" on page 3-61).
Display Spanning Tree Switch Settings	Displays the Spanning Tree Switch Settings screen (see "Display Spanning Tree Switch Settings" on page 3-64).
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.

Figure 3-27 and Figure 3-28 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 3-27. 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 3-28. Spanning Tree Port Configuration Screen (2 of 2)

Table 3-24 describes the Spanning Tree Port Configuration screen fields.

Table 3-24. 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	The read-only data displayed in this column indicates the trunks that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen (see "MultiLink Trunk Configuration" on page 3-35).

(continued)

Table 3-24. 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 1-55). The Fast Learning parameter is the same as Normal Learning, except that the state transition timer is shortened to two seconds.	
	Default Value:	Normal Learning
	Range:	Normal Learning, Fast Learning, Disabled
Priority	This read-only field is a bridge spanning tree parameter that prioritizes the port’s lowest path cost to the root. When one or more ports have the same path cost, the STA selects the path with the highest priority (lowest numerical value). See also Path Cost.	
	Default Value:	128
	Range:	0 to 255
Path Cost	This read-only field is a bridge spanning tree parameter that determines the lowest path cost to the root.	
	Default Value:	10 or 100 (1 for gigabit port) Path Cost = 1000/LAN speed (in Mb/s) The higher the LAN speed, the lower the path cost. See also Priority.
	Range:	1 to 65535
State	This read-only field indicates the current port state within the spanning tree network. Each port can transition to various states, as determined by the Participation field setting. For example, when the Participation field is set to Disabled, the port does not participate in the STA and transitions to the Forwarding state (the default). When the Participation field is set to Enabled, the port transitions from the Disabled state through the Blocking, Listening, and Learning states before entering the Forwarding state.	
	Default Value:	Topology dependent
	Range:	Disabled, Blocking, Listening, Learning, Forwarding

Display Spanning Tree Switch Settings

The Spanning Tree Switch Settings screen (Figure 3-29) 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 screen to open the Spanning Tree Switch Settings screen.

```
                      Spanning Tree Switch Settings




              Bridge Priority:          8000
              Designated Root:          80000060FD000090
              Root Port:                0
              Root Path Cost:           0
              Hello Time:               2 seconds
              Maximum Age Time:         20 seconds
              Forward Delay:            15 seconds
              Bridge Hello Time:        2 seconds
              Bridge Maximum Age Time:  20 seconds
              Bridge Forward Delay:     15 seconds




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

Figure 3-29. Spanning Tree Switch Settings Screen

Table 3-25 describes the Spanning Tree Switch Settings parameters.

Table 3-25. Spanning Tree Switch Settings Parameters

Parameter	Description
Bridge Priority	Indicates the management-assigned priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. The STA uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values compared first, followed by the hardware addresses. Default Value: 8000 Range: 0 to 65535
Designated Root	Indicates the bridge ID of the root bridge, as determined by the STA. Default Value: 8000 (bridge_id) Range: 0 to 65535
Root Port	Indicates the switch port number that offers the lowest path cost to the root bridge. Default Value: 0 Range: 0 to 16
Root Path Cost	Indicates the path cost from this switch port to the root bridge. Default Value: 0 Range: Not applicable
Hello Time	Indicates the Actual Hello Interval, the amount of time between transmissions of configuration Bridge Protocol Data Units (BPDUs) that the root bridge is currently using. Note that all bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. *See also* Bridge Hello Time. Default Value: 2 seconds Range: 1 to 10 seconds
Maximum Age Time	Indicates the Maximum Age Time parameter value that the root bridge is currently using. This value specifies the maximum age that a Hello message can attain before it is discarded. Note that the root bridge's Maximum Age Time parameter value becomes the actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. *See also* Bridge Maximum Age Time. Default Value: 20 seconds Range: 6 to 40 seconds

(continued)

Table 3-25. Spanning Tree Switch Settings Parameters (continued)

Parameter	Description
Forward Delay	Indicates the Forward Delay parameter value that the root bridge is currently using. This value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. Note that the root bridge's Forward Delay parameter value becomes the actual Forward Delay parameter value for all bridges participating in the spanning tree network. *See also* Bridge Forward Delay. Default Value: 15 seconds Range: 4 to 30 seconds
Bridge Hello Time	Indicates the Hello Interval (the amount of time between transmissions of BPDUs) specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge. Note that, although you can set the Hello Interval for a bridge using bridge management software, once the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network. *See also* Hello Time. Default Value: 2 seconds Range: 1 to 10 seconds
Bridge Maximum Age Time	Specifies the maximum age (in seconds) that a Hello message can attain before it is discarded. This parameter, specified by management for this bridge, takes effect only when the bridge becomes the root bridge. Note that, if this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. *See also* Maximum Age Time. Default Value: 20 seconds Range: 6 to 40 seconds
Bridge Forward Delay	Indicates the Forward Delay parameter value specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge. The Forward Delay parameter value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. Note that all bridges participating in the spanning tree network use the root bridge's Forward Delay parameter value. *See also* Forward Delay. Default Value: 15 seconds Range: 4 to 30 seconds

TELNET Configuration

The TELNET Configuration screen (Figure 3-30) allows 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.

Choose TELNET Configuration (or press t) from the main menu to open the TELNET Configuration screen.

```
                        TELNET Configuration

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

      Allowed Source IP Address           Allowed Source Mask
      -------------------------           -------------------
         [ 0.0.0.0 ]                      [ 0.0.0.0 ]
         [ 255.255.255.255 ]              [ 255.255.255.255 ]
         [ 255.255.255.255 ]              [ 255.255.255.255 ]
         [ 255.255.255.255 ]              [ 255.255.255.255 ]
         [ 255.255.255.255 ]              [ 255.255.255.255 ]
         [ 255.255.255.255 ]              [ 255.255.255.255 ]
         [ 255.255.255.255 ]              [ 255.255.255.255 ]
         [ 255.255.255.255 ]              [ 255.255.255.255 ]
         [ 255.255.255.255 ]              [ 255.255.255.255 ]
         [ 255.255.255.255 ]              [ 255.255.255.255 ]


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

Figure 3-30. TELNET Configuration Screen

Table 3-26 describes the TELNET Configuration screen fields.

Table 3-26. TELNET Configuration Screen Fields

Field	Description	
TELNET Access	Allows a user remote access to the CI through a TELNET session.	
	Default Value:	Enabled
	Range:	Enabled, Disabled
Login Timeout	Specifies the amount of time a user has to enter the correct password at the console-terminal prompt.	
	Default Value:	1 minute
	Range:	0 to 10 minutes (0 indicates “no timeout”)
Login Retries	Specifies the number of times a user can enter an incorrect password at the console-terminal prompt before terminating the session.	
	Default Value:	3
	Range:	1 to 100
Inactivity Timeout	Specifies the amount of time the session can be inactive before it is terminated.	
	Default Value:	15 minutes
	Range:	0 to 60 minutes (0 indicates “no timeout”)
Event Logging	Specifies the types of events that will be displayed in the Event Log screen (see “Display Event Log” on page 3-74).	
	Default Value:	All
	Range:	All, None, Accesses, Failures
	Description:	*All:* Logs the following TELNET events to the Event Log screen: • TELNET connect: Indicates the IP address and access mode of a TELNET session. • TELNET disconnect: Indicates the IP address of the remote host and the access mode, due to either a logout or inactivity. • Failed TELNET connection attempts: Indicates the IP address of the remote host whose IP address is not on the list of allowed addresses, or indicates the IP address of the remote host that did not supply the correct password. *None:* Indicates that no TELNET events will be logged in the Event Log screen. *Accesses*: Logs only TELNET connect and disconnect events in the Event Log screen. *Failures:* Logs only failed TELNET connection attempts in the Event Log screen.

(continued)

Table 3-26. TELNET Configuration Screen Fields (continued)

Field	Description	
Allowed Source IP Address	Specifies up to 10 user-assigned host IP addresses that are allowed TELNET access to the CI.	
	Default Value:	0.0.0.0 (no IP address assigned)
	Range:	Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
Allowed Source Mask	Specifies up to 10 user-assigned allowed source address masks. The remote IP address is masked with the Allowed Source Mask and, if the resulting value equals the Allowed Source IP address, the connection is allowed. For example, a connection would be allowed with the following settings: remote IP address = 192.0.1.5 Allowed Source IP Address = 192.0.1.0 Allowed Source Mask = 255.255.255.0	
	Default Value:	0.0.0.0 (no IP mask assigned)
	Range:	Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point

Software Download

The Software Download screen (Figure 3-31) 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 3-7 to learn how to configure the switch’s IP address.)

Choose Software Download (or press f) from the main menu to open the Software Download screen.

You can monitor the software download process by observing the BayStack 350 switch LEDs (see “LED Indications During the Download Process” on page 3-72).

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。

```
                              Software Download



     Image Filename:                 [ b350_100.img ]
     TFTP Server IP Address:         [ 192.0.1.12 ]

     Start TFTP Load of New Image:   [ Yes ]

     The Software Download process has started.  Do NOT power down the
     switch before the process has completed (approximately 10 minutes).



Enter text, 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. Software Download Screen

Table 3-27 describes the Software Download screen fields.

Table 3-27. Software Download Screen Fields

Field	Description	
Image Filename	The software image load file name.	
	Default Value:	Zero-length string
	Range:	An ASCII string of up to 30 printable characters
TFTP Server IP Address	The IP address of your TFTP load host.	
	Default Value:	0.0.0.0 (no IP address assigned)
	Range:	Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
Start TFTP Load of New Image	Specifies whether to start the download of the switch software image (default is No). Use the spacebar to toggle the selection to Yes. Press Enter to initiate the software download process. **Note:** The software download process can take up to 60 seconds to complete (or more if the load host path is congested or there is a high volume of network traffic). To ensure that the download process is not interrupted, do not power down the switch for approximately 10 minutes.	
	Default Value:	No
	Range:	Yes, No

LED Indications During the Download Process

The software download process is automated so that it runs to completion without user intervention. The download process erases the contents of flash memory and replaces it with a new software image; therefore, it is important that the download process not be interrupted once initiated. When the download process is complete, the switch is reset automatically and the new software image initiates a self-test. The self-test results are displayed briefly in the BayStack 350 switch Self-Test screen, which is followed by the console interface screens.

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 3-28 describes the LED indications during the software download process.

Table 3-28. LED Indications During the Software Download Process

Phase	Description	LED indications
1	The new software image is being downloaded to the switch.	100 Mb/s port status LEDs (ports 7 to 12 only): The LEDs begin to turn on from right to left, beginning with port 12. The LED pattern indicates the progress of the download process. When LEDs 7 to 12 are all on, this indicates that the switch has received the new software image successfully.
2	The switch's flash memory is being erased.	10 Mb/s port status LEDs (ports 1 to 12 only): The LEDs begin to turn on from left to right, beginning with port 1. The LED pattern indicates that various sectors of the switch's flash memory are being erased. When LEDs 1 to 12 are all on, this indicates that the switch's flash memory has been erased.
3	The new software image is being programmed into the switch's flash memory.	100 Mb/s port status LEDs (ports 1 to 8 only): The LEDs begin to turn on from left to right, beginning with port 1. The LED pattern indicates that the new software image is being programmed into the switch's flash memory. When LEDs 1 to 8 are all on, this indicates that the new software image has been programmed successfully into the switch's flash memory.
4	The switch is reset automatically.	After the reset is complete, the new software image initiates the switch's 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, which is followed by the CI screens.

Display Event Log

This section describes the various functions of the Event Log screen (Figure 3-32).

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 3-32. 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 Configuration" on page 3-67.)
- **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 3-33 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 3-33. 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 3-34 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 3-34. 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 3-35 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 3-35. Sample Event Log Entry Showing Flash Update Status

Reset

The Reset option (accessed from the main menu) allows you to reset the BayStack 350 switch without erasing any configured switch parameters.

Resetting the switch 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 3-36), which is followed by the Bay Networks logo screen (Figure 3-37).

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
   Port internal loopback test      ... Pass

Self-test complete.
```

Figure 3-36. Self-Test Screen After Resetting the Switch

```
 ***********************************************
 * Bay Networks,Inc.                           *
 * Copyright (c) 1996,1998,1999                *
 * All Rights Reserved                         *
 * BayStack 350-XX T                           *
 * Versions: HW:Revx  FW:Vx.xx SW:Vx.x.x.x     *
 ***********************************************

Enter Ctrl-Y to begin.
```

Figure 3-37. Bay Networks Logo Screen

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

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 E, “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 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 3-38), which is followed by the Bay Networks logo screen (Figure 3-39).

.

```
BayStack 350-24T Self-Test

   CPU RAM test                     ... Pass
   ASIC addressing test             ... Pass
   ASIC buffer RAM test             ... Pass
   Port internal loopback test      ... Pass

Self-test complete.
```

Figure 3-38. Self-Test Screen After Resetting to Factory Default Settings

```
*************************************************
* Bay Networks,Inc.                             *
* Copyright (c) 1996,1998,1999                  *
* All Rights Reserved                           *
* BayStack 350-XX T                             *
* Versions: HW:Revx  FW:Vx.xx SW:Vx.x.x.x       *
*************************************************




Enter Ctrl-Y to begin.
```

Figure 3-39. Bay Networks Logo Screen After Resetting to Factory Default Settings

---

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

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 a user working at a password-protected console terminal or in an active TELNET session to terminate the session.

The Logout option works as follows:

- If the user is accessing the BayStack 350 switch through a TELNET session, the Logout option terminates the TELNET session.
- If the user is 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 3-40). The user must enter the correct password to access the CI screens.

```
BayStack Model 350-24T HW:Revx FW:Vx.xx SW:Vx.x.x.x




                  Password:  [ *************** ]

                  Enter Password:
```

Figure 3-40. 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 “Console/Comm Port Configuration” on page 3-54).

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 includes the following information:

- LED indications
- Diagnosing and correcting the problem
- Port connection problems

This chapter is organized to help lead you through a logical process for troubleshooting the BayStack 350 switch. For example, because the LEDs provide visual indications of problems, the section "LED Indications" on page 4-2 helps you to understand the various states that each LED can exhibit during 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 1-3).

If you need more help in determining the problem, the section "Diagnosing and Correcting the Problem" on page 4-4 provides a table that lists symptoms and corrective actions you can perform to resolve specific problems.

Subsequent sections provide step-by-step procedures for correcting the problems listed in the table.

LED Indications

Figure 4-1 shows the LED display panels used with the BayStack 350 switch.

Refer to Table 4-1 for a description of the LEDs.

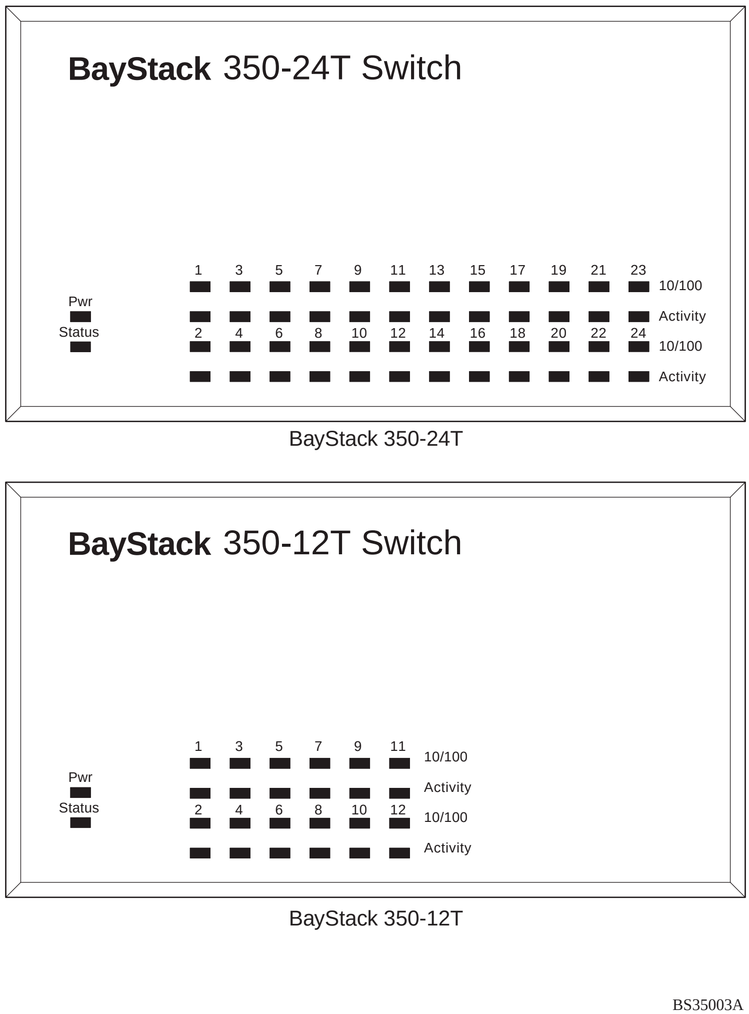


Figure 4-1. BayStack 350 Switch LED Locations

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.
		Amber	On	The corresponding port is set to operate at 10 Mb/s and the link is good.
		Amber	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 five 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.	See "Port Connection Problems" on page 4-6.
	The switch's link partner is not autonegotiating properly.	

(continued)

Table 4-2. Corrective Actions (continued)

Symptom	Probable cause	Corrective action
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 Bay 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 [Cntrl]-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 3-30).**
2. **Manually set the Speed/Duplex field to match the speed/duplex mode of the connected station (see Table 3-12 on page 3-31).**

   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:** Bay Networks recommends that you manually set the BayStack 350 switch port to the desired speed/duplex mode when connecting to any of the following Bay Networks products:

- Bay Networks 28000 product family
- Bay 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 D, “Connectors and Pin Assignments”).

Appendix A
Technical Specifications

This appendix lists the technical specifications for the BayStack 350 switch.

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	Model 350-24T	Model 350-12T
Height	7.03 cm (2.77 in)	7.03 cm (2.77 in)
Width	44.07 cm (17.55 in)	44.07 cm (17.55 in)
Depth	38.1 cm (15.0 in)	38.1 cm (15.0 in)
Weight	5.26 kg (11.60 lb)	5.26 kg (11.60 lb)

Performance 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
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 802.3 10BASE-T (ISO/IEC 8802-3, Clause 14)
- IEEE 802.3u 100BASE-TX (ISO/IEC 8802-3, Clause 25)
- IEEE 802.1p (Prioritizing)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1z (Gigabit)

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 Optic MDA --- 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
- 1000BASE-SX (Shortwave Gigabit Fiber) MDA --- SC connectors for shortwave 850 nm fiber optic connections over multimode (550 meter) fiber optic cable
- 1000BASE-LX MDA --- SC connectors for longwave 1300 nm fiber optic connections over single-mode (3 kilometer) or multimode (550 meter) 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 Bay 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
Media Dependent Adapters

This appendix describes the optional media dependent adapters (MDAs) that are available from Bay Networks. The MDAs can support high-speed connections to servers, shared Fast Ethernet hubs, or backbone devices.

Note: The MDA is *not* hot-swappable. Power down the switch before installing or removing an MDA.

The following MDA models are available:

Type	Model/Description	See Page:
10BASE-T/100BASE-TX	400-4TX MDA --- 4-port twisted pair RJ-45 connectors.	B-2
100BASE-FX (Fiber)	400-2FX MDA --- 2-port multimode fiber SC connectors. 400-4FX MDA --- 4-port multimode fiber MT-RJ connectors.	B-3
1000BASE-SX (Shortwave gigabit fiber)	450-1SR MDA --- Single MAC gigabit MDA with separate redundant PHY. 450-1SX MDA --- Single PHY gigabit MDA.	B-6
1000BASE-LX (Longwave gigabit fiber)	450-1LR MDA --- Single MAC gigabit MDA with separate redundant PHY. 450-1LX MDA --- Single PHY gigabit MDA.	B-8

Bay Networks is constantly adding new models and features to existing product lines; see your Bay Networks sales representative for a full range of available MDAs.

10BASE-T/100BASE-TX MDA

The 400-4TX MDA (see Figure B-1) uses four 10BASE-T/100BASE-TX RJ-45 (8-pin modular) port connectors to attach Ethernet devices.Table B-1 describes the 400-4TX MDA components and LEDs.

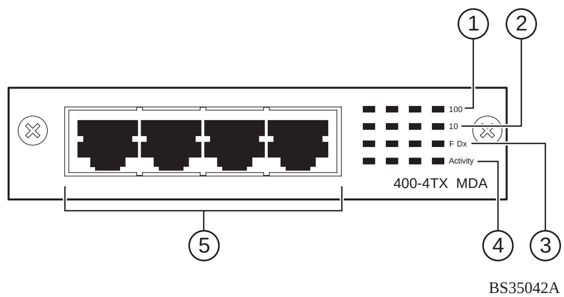


Figure B-1. 400-4TX MDA Front Panel

Table B-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 B-11.

100BASE-FX MDAs

There are two 100BASE-FX models:

- 400-2FX MDA

  The 400-2FX MDA uses two longwave 1300 nm SC connectors to attach devices over 62.5/125 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 micron multimode fiber optic cable.

Both models (see Figure B-2) can be used to attach fiber-based 100 Mb/s connections to other compatible Fast Ethernet devices.

Single-mode fiber cable is not supported.

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
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

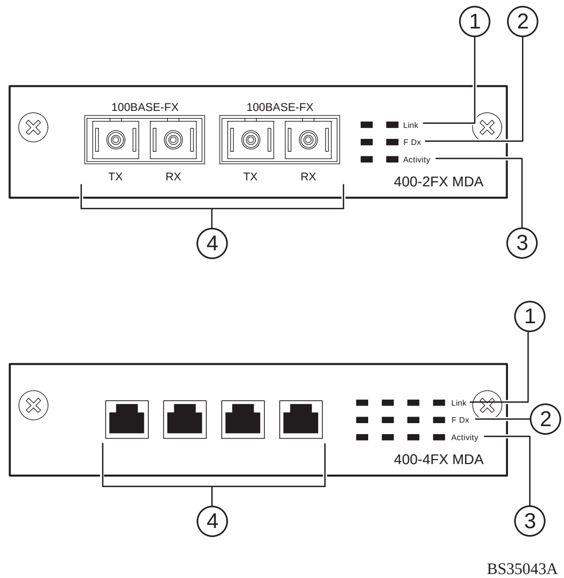


Figure B-2. 100BASE-FX MDA Front Panels

Table B-2 describes the 100BASE-FX components and LEDs.

For installation instructions, see "Installing an MDA" on page B-11.

Table B-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.

(continued)

Table B-2. 100BASE-FX MDA Components (continued)

Item	Label	Description
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.

There are two 1000BASE-SX (shortwave gigabit) MDA models:

- 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 (Figure B-3) use shortwave 850 nm fiber optic connectors to connect devices over multimode (550 meter) fiber optic cable.

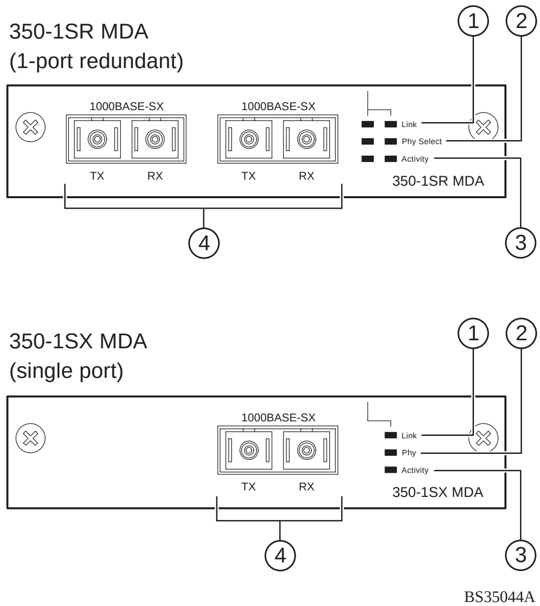


Figure B-3. 1000BASE-SX MDA Front Panels

Table 2 describes the 1000BASE-SX components and LEDs.

For installation instructions, see "Installing an MDA" on page B-11.

Table 2. 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.

(continued)

Table 2. 1000BASE-SX MDA Components

Item	Label	Description
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-FX 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.

There are two 1000BASE-LX (longwave gigabit) MDA models:

- 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 (Figure B-4) use longwave 1300 nm fiber optic connectors to connect devices over single mode (3 kilometer) or multimode (550 meters) 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 B-10)

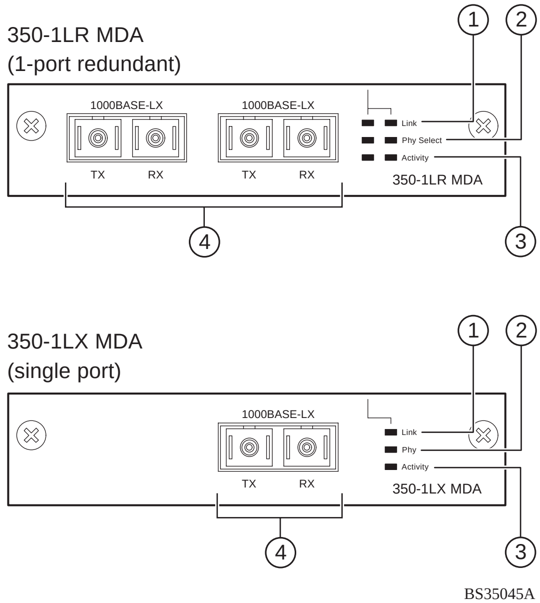


Figure B-4. 1000BASE-LX MDA Front Panels

Table B-3 describes the 1000BASE-LX MDA components and LEDs.

For installation instructions, see "Installing an MDA" on page B-11.

Table B-3. 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):

(continued)

Table B-3. 1000BASE-LX MDA Components

Item	Label	Description
		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-FX SC port connectors.

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 Bay 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 (Bay Networks part number 201540-B)

The publication is available on the World Wide Web at *support.baynetworks.com/library/tpubs/*

At the Web site, click on Accelar under the Routing Switches heading.

Installing an MDA

The Uplink Module slot on the BayStack 450 switches accommodates a single MDA. The connection can be either an RJ-45 10/100BASE-TX MDA or a fiber (100BASE-FX or 1000BASE-SX/LX) MDA with an SC or MT-RJ connector.

Note: The MDA is *not* hot-swappable. Power down the switch before installing or removing an MDA.

To install an MDA into the Uplink Module slot, follow these steps:

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.**

Note: If you are replacing an installed MDA with another type of MDA, see "Replacing an MDA with a Different Model" on B-12.

3. **Insert the MDA into the chassis slot (see Figure B-5) taking care to slide the MDA onto the guides provided on the chassis.**

Caution: Make sure the MDA slides in on the guides provided. Failure to align the guides could result in bent and broken pins.

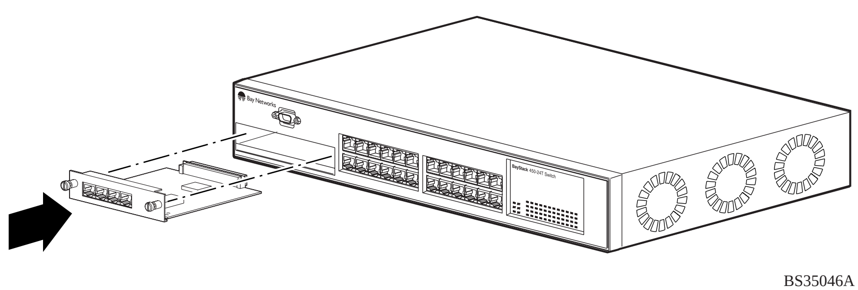


Figure B-5. Installing an MDA

4. **Press the MDA *firmly* into the chassis slot. Be sure that the MDA is fully seated into the mating connector.**
5. **Secure the MDA in the chassis by tightening the thumb screws on the MDA front panel.**
6. **Attach devices to the MDA ports.**

After connecting the port cables, continue to follow the instructions in that manual 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 with a Different Model

When replacing an installed MDA with another type of MDA, complete the following steps to clear the switch NVRAM:

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. **Cycle the switch power.**

   Power up the switch and wait for the Bay Networks logo screen to appear (approximately 10 seconds); then power down the switch.

4. **Install the replacement MDA.**

   Be sure to *firmly* tighten the two thumbscrews on the MDA front panel.

5. **Power up the switch.**

Appendix C
Quick Steps to Features

This appendix provides Quick Steps for using the BayStack 350 switch features. It is intended for system administrators who are familiar with the BayStack 350 switch features described in this manual.

If you have experience in configuring the BayStack 350 switch features (such as VLANs, MultiLink Trunking, Port Mirroring, IGMP Snooping, and more) you can use the configuration flowcharts provided in this appendix to guide you through the steps necessary to configure your switch. References to additional information about configuring the specific feature are provided within the steps of the flowcharts as required.

This appendix provides Quick Step flowcharts for the following features:

- 802.1Q VLANs
- MultiLink Trunks
- Port Mirroring
- IGMP Snooping

To learn more about:	Refer to this section:
802.1Q VLANs	"IEEE 802.1Q VLAN Workgroups" on page 1-18.
MultiLink Trunks	"MultiLink Trunks" on page 1-43.
Port Mirroring	"Port Mirroring (Conversation Steering)" on page 1-61.
IGMP Snooping	"IGMP Snooping" on page 1-34.

Configuring 802.1Q VLANs

This section shows how to create a new VLAN or to modify an existing VLAN (see Figure C-1 to Figure C-3).

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

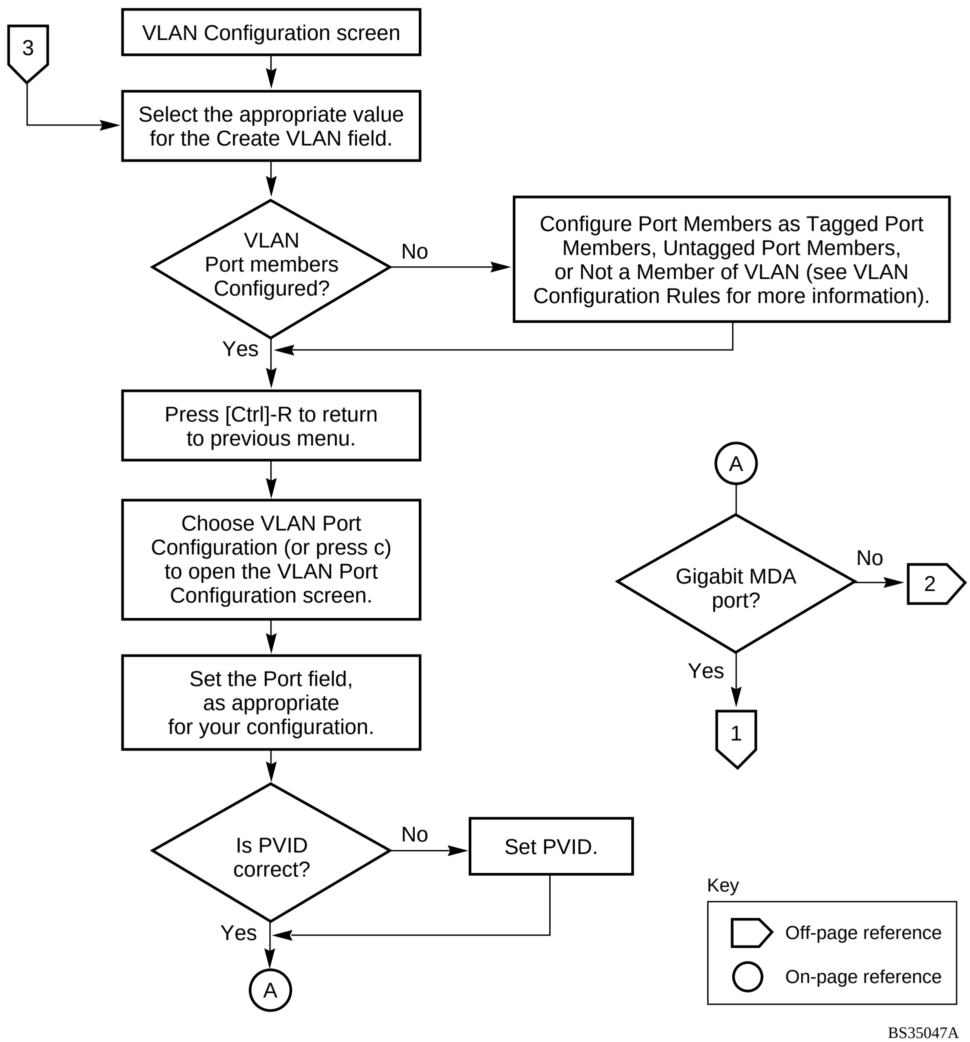


Figure C-1. Configuring 802.1Q VLANs (1 of 3)

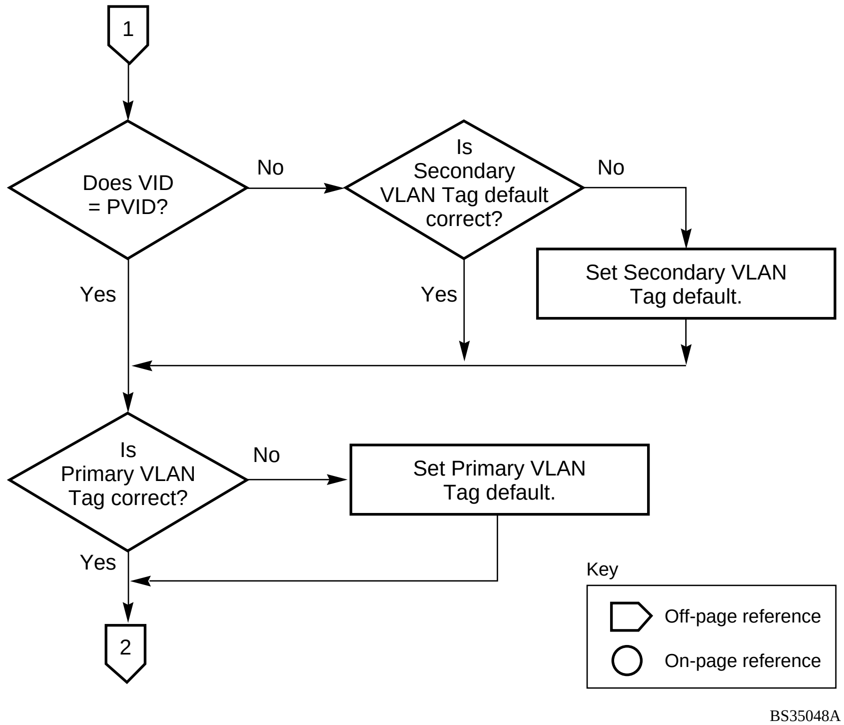


Figure C-2. Configuring 802.1Q VLANs (2 of 3)

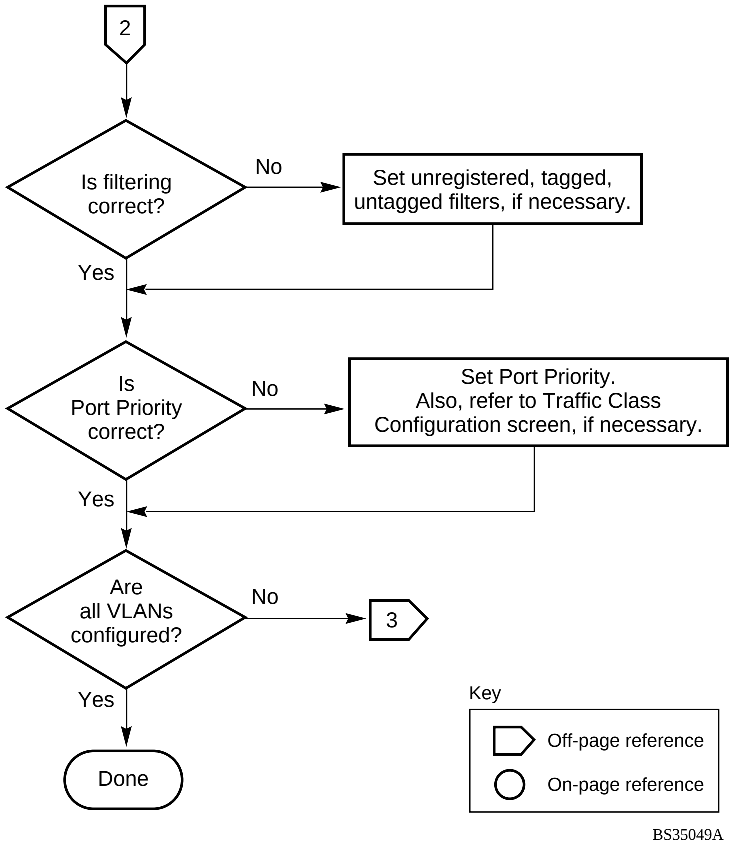


Figure C-3. Configuring 802.1Q VLANs (3 of 3)

Configuring MultiLink Trunks

This section shows how to create a new MultiLink trunk or to modify an existing MultiLink trunk (see Figure C-4).

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

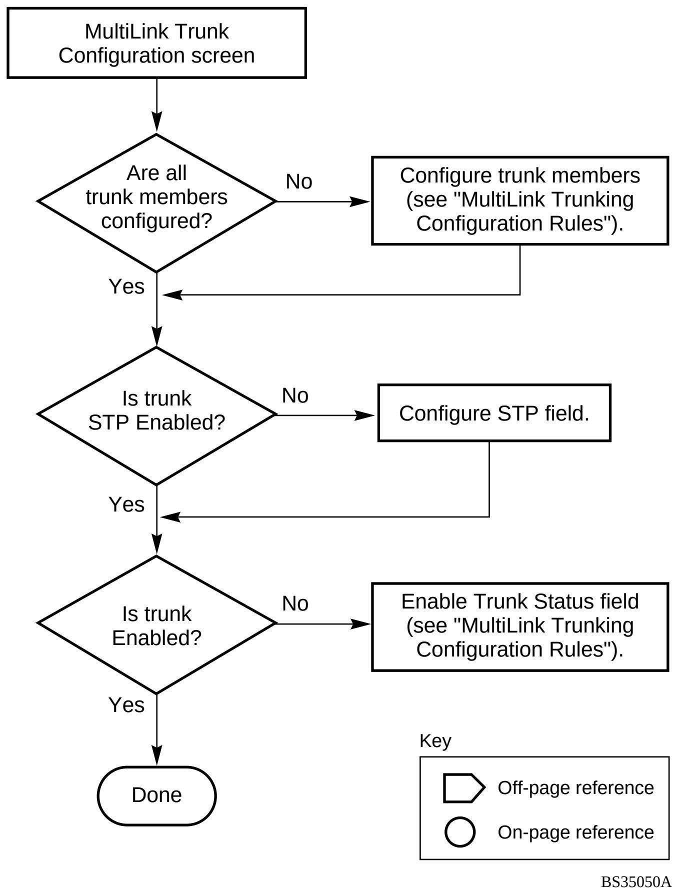


Figure C-4. Configuring MultiLink Trunks

Configuring Port Mirroring

This section shows how to configure switch ports for port mirroring or to modify existing port mirroring ports (see Figure C-5 and Figure C-6).

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

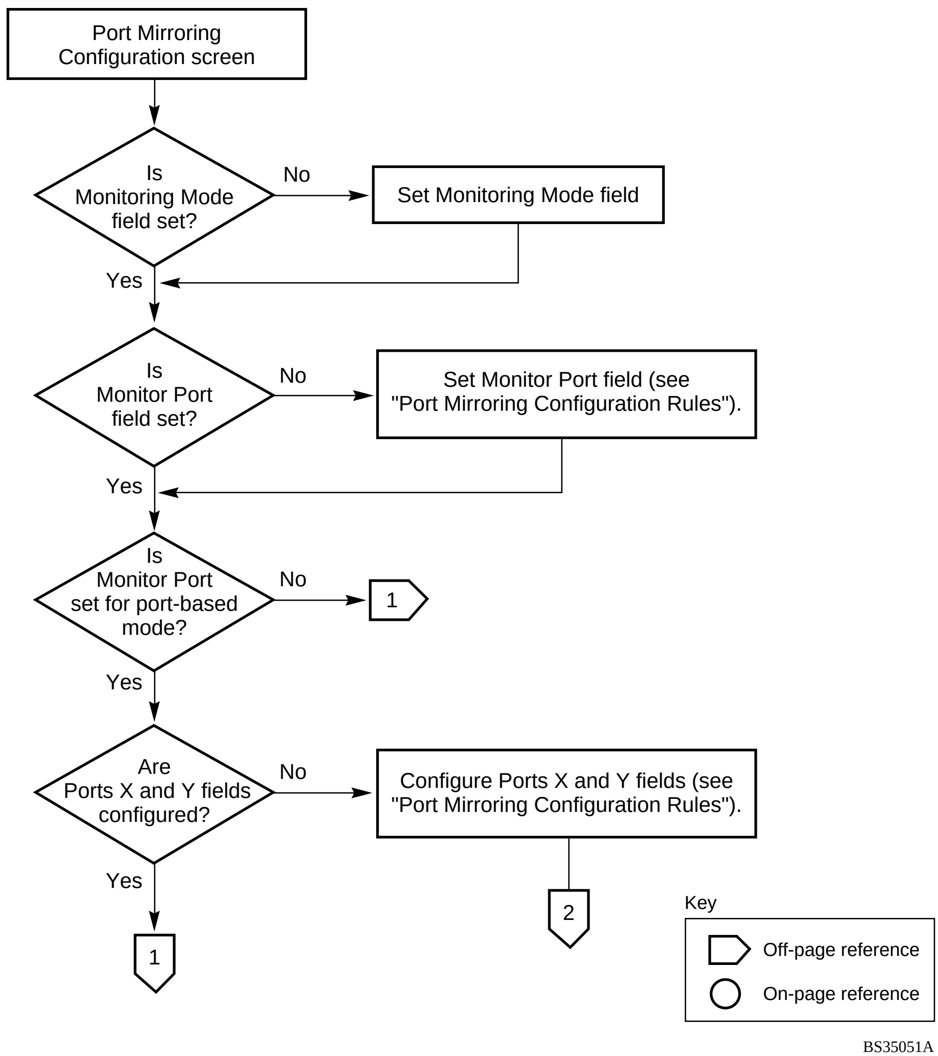


Figure C-5. Configuring Port Mirroring (1 of 2)

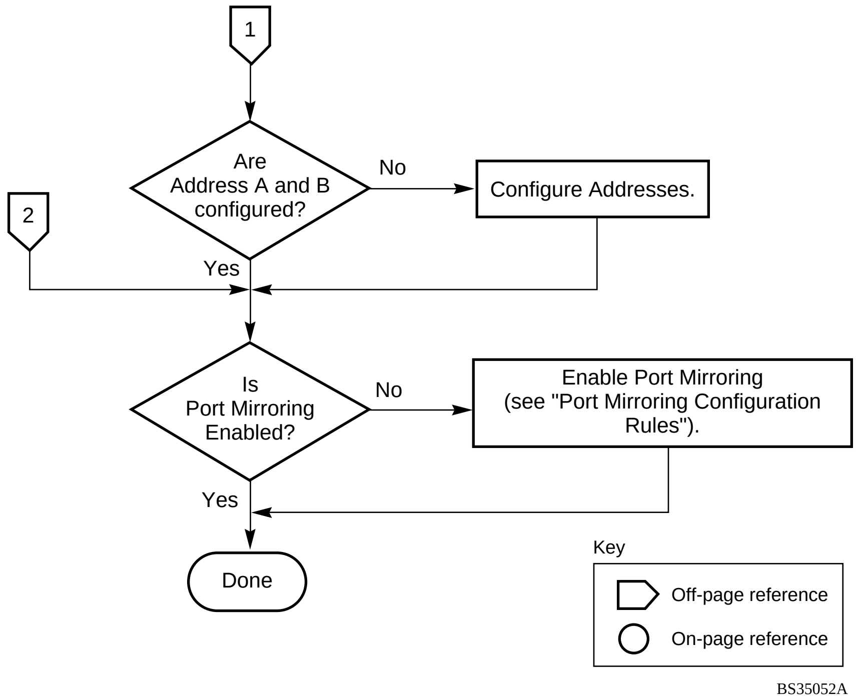


Figure C-6. Configuring Port Mirroring (2 of 2)

Configuring IGMP Snooping

This section shows how to configure switch ports for IGMP Snooping or to modify existing IGMP Snooping ports (see Figure C-7 to Figure C-9).

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

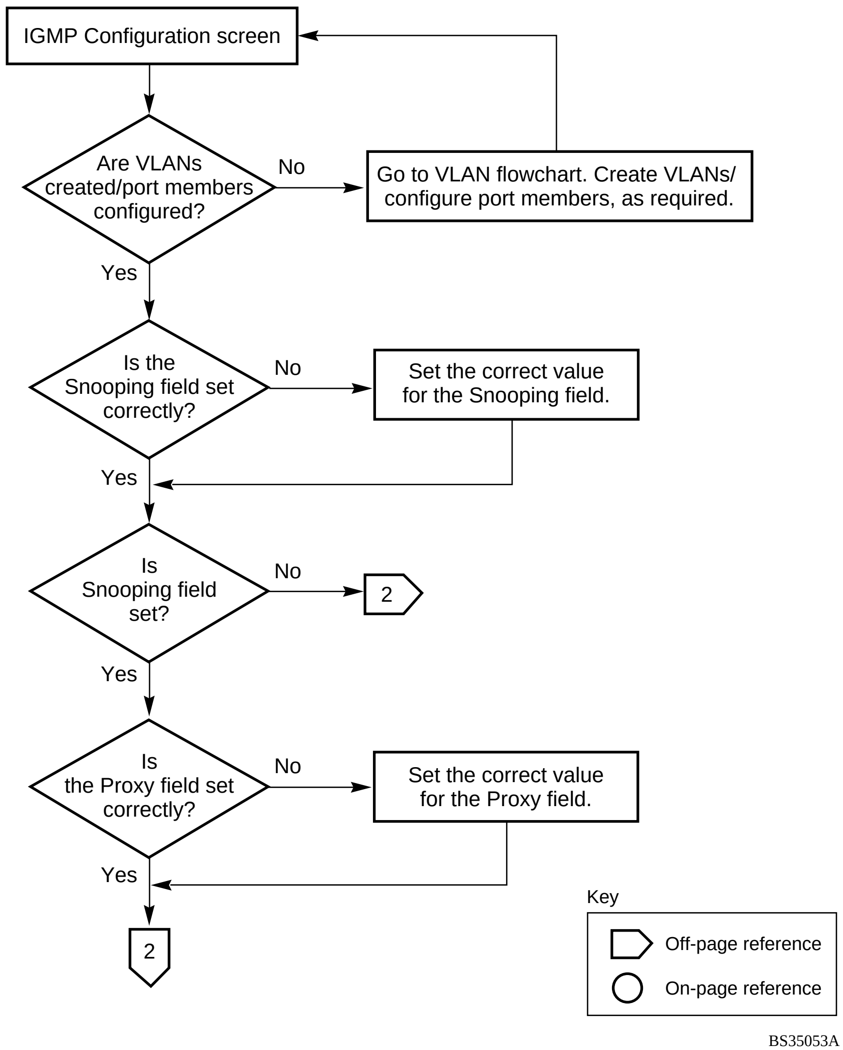


Figure C-7. Configuring IGMP Snooping (1 of 3)

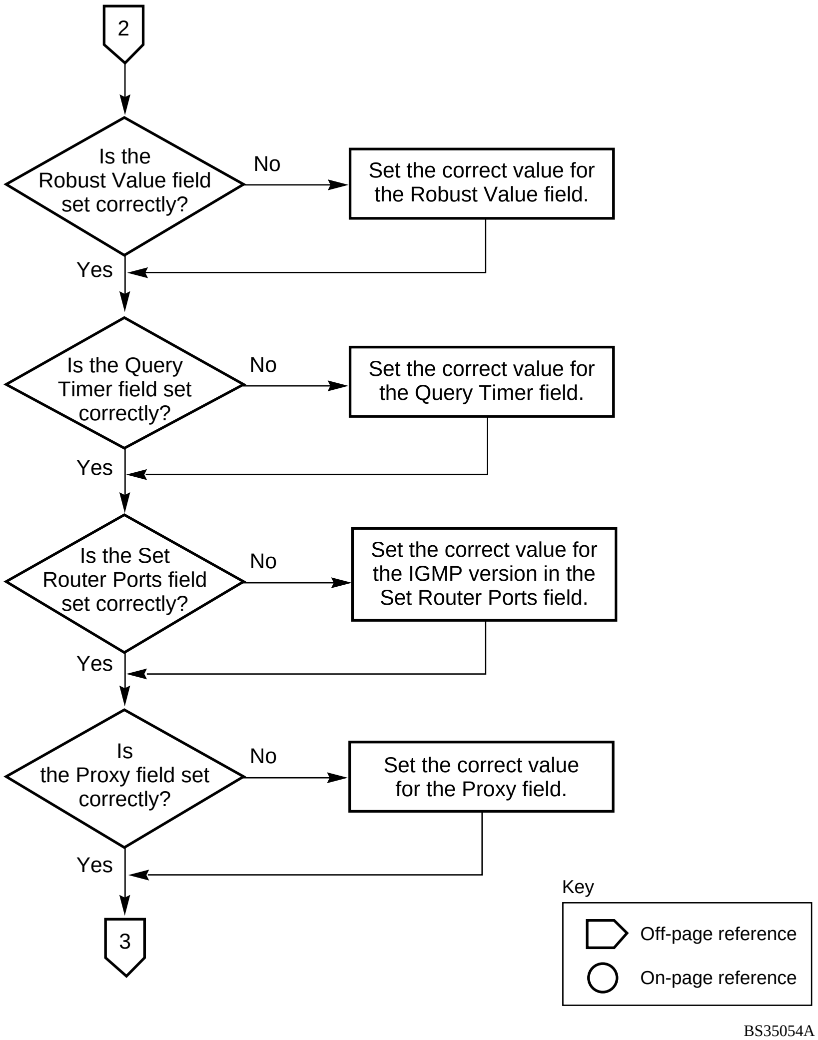


Figure C-8. Configuring IGMP Snooping (2 of 3)

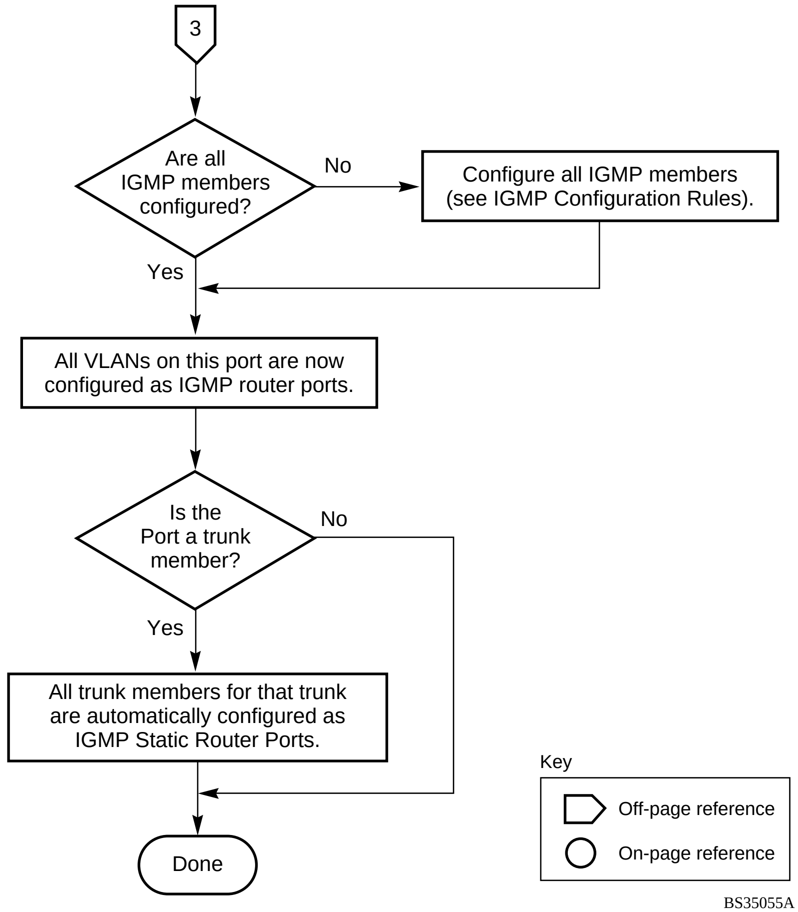


Figure C-9. Configuring IGMP Snooping (3 of 3)

Appendix D
Connectors and Pin Assignments

This appendix describes the BayStack 350 switch port connectors and pin assignments.

RJ-45 (10BASE-T/100BASE-TX) Port Connectors

The RJ-45 port connectors (Figure D-1) are wired as MDI-X ports to connect end stations without using crossover cables. (See "MDI and MDI-X Devices" on page D-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.

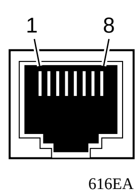


Figure D-1. RJ-45 (8-Pin Modular) Port Connector

Table D-1 lists the RJ-45 (8-pin modular) port connector pin assignments.

Table D-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 D-2).

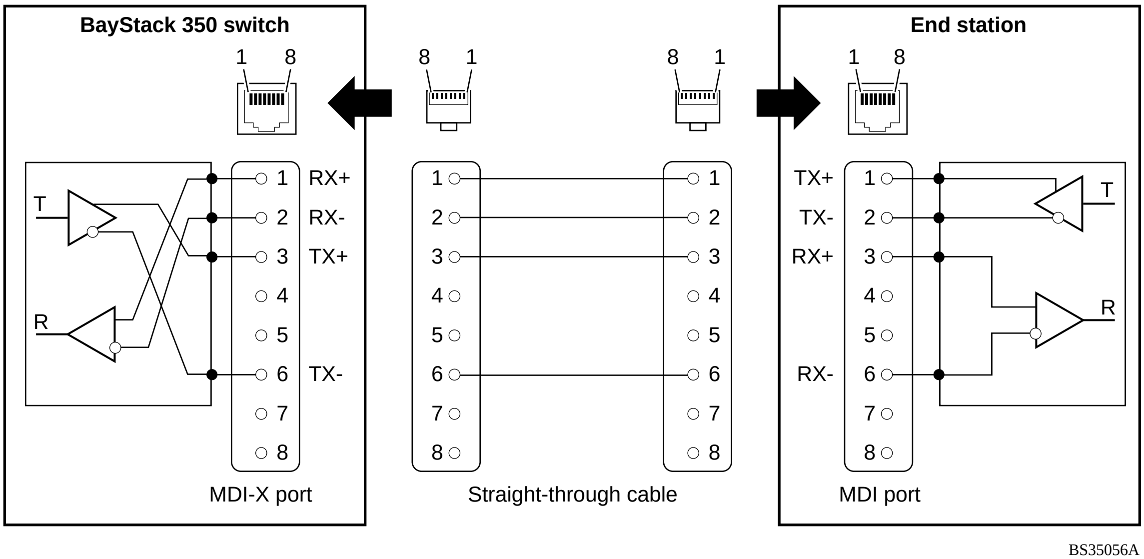


Figure D-2. MDI-X to MDI Cable Connections

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 D-3).

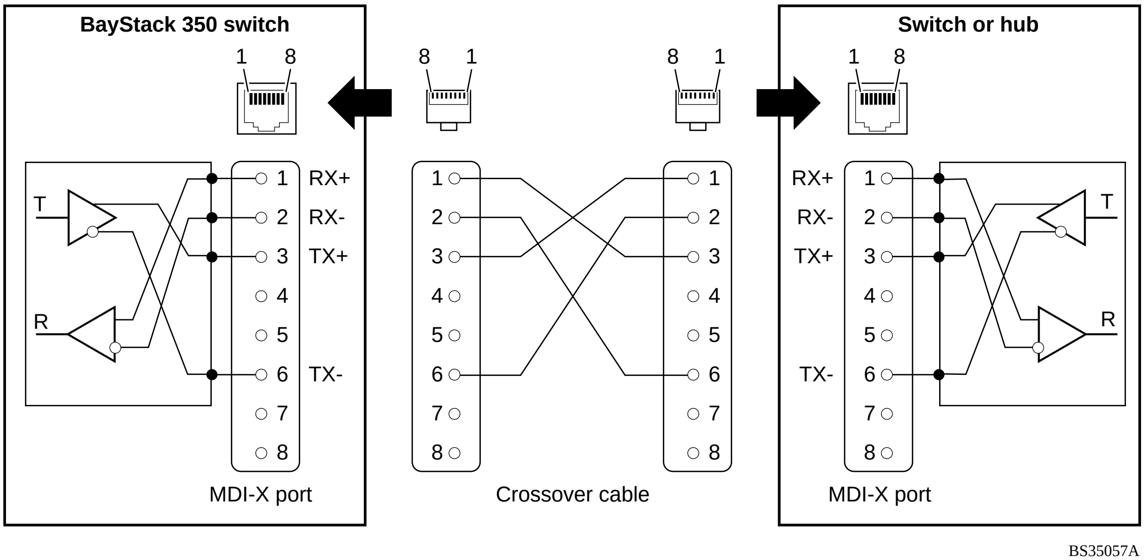


Figure D-3. MDI-X to MDI-X Cable Connections

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

The DB-9 Console/Comm Port connector (Figure D-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.

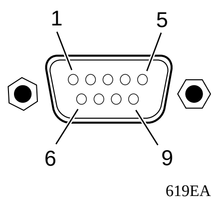


Figure D-4. DB-9 Console/Comm Port Connector

Table D-2 lists the DB-9 Console/Comm Port connector pin assignments.

Table D-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 E
Default Settings

Table E-1 lists the factory default settings for the BayStack 350 switch.

Table E-1. Factory Default Settings for the BayStack 350 Switch

Field	Default setting	Appears in this CI screen
BootP Request Mode	BootP Disabled	IP Configuration/Setup (page 3-7)
In-Band IP Address	0.0.0.0 (no IP address assigned)	
In-Band Subnet Mask	0.0.0.0 (no subnet mask assigned)	
Default Gateway	0.0.0.0 (no IP address assigned)	
Read-Only Community String	public	SNMP Configuration (page 3-12)
Read-Write Community String	private	
Trap IP Address	0.0.0.0 (no IP address assigned)	
Community String	Zero-length string	
Authentication Trap	Enabled	
Reset Count	1	System Characteristics (page 3-14)
Last Reset Type	Power Cycle	
Power Status	Primary Power	
sysContact	Zero-length string	
sysName	Zero-length string	
sysLocation	Zero-length string	

(continued)

Table E-1. Factory Default Settings for the BayStack 350 Switch (continued)

Field	Default setting	Appears in this CI screen
Aging Time	300 seconds	MAC Address Table (page 3-18)
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)	
Create VLAN	1	VLAN Configuration (page 3-22)
Delete VLAN	blank field	
VLAN Name	VLAN # (*VLAN number*)	
Port Membership	U (all ports assigned as untagged members of VLAN 1)	
Port	1	VLAN Port Configuration (page 3-24)
Filter Tagged Frames	No	
Filter Untagged Frames	No	
Filter Unregistered Frames	No	
Port Name	Port # (*port number*)	
PVID	1	
Port Priority	0	
Note: The following two fields only appear when the port selected in the Port field is configured with an optional gigabit MDA.		
Primary VLAN Tagging	Untagged	
Secondary VLAN Tagging	Tagged	
Port	1	VLAN Display by Port (page 3-27)
PVID	1 (read only)	
Port Name	Port # 1 (read only)	
Traffic Class	Low	Traffic Class Configuration (page 3-28)
Status	Enabled (for all ports)	Port Configuration (page 3-30)
Autonegotiation	Enabled (for all ports)	
Speed/Duplex	100Mbs/Half (when Autonegotiation is Disabled)	

(continued)

Table E-1. Factory Default Settings for the BayStack 350 Switch (continued)

Field	Default setting	Appears in this CI screen
Autonegotiation	Enabled	High Speed Flow Control Configuration (page 3-32)
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)	
Trunk Members	blank field	MultiLink Trunk Configuration (page 3-36)
STP	Normal	
Trunk Mode	Basic	
Trunk Status	Enabled	
Trunk Name	Trunk #1 to Trunk #6	
Traffic Type	Rx and Tx	MultiLink Trunk Utilization (page 3-39)
Monitoring Mode	Disabled	Port Mirroring Configuration (page 3-41)
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)	
Packet Type	Both	Rate Limiting Configuration (page 3-45)
Limit	None	
VLAN	1	IGMP Configuration (page 3-48)
Snooping	Enabled	
Proxy	Enabled	
Robust Value	2	

(continued)

Table E-1. Factory Default Settings for the BayStack 350 Switch (continued)

Field	Default setting	Appears in this CI screen
Query Time	125 seconds	
Set Router Ports	Version 1	
Static Router Ports	- (for all ports)	
Port	1	Port Statistics (page 3-51)
Console Port Speed	9600 Baud	Console/Comm Port Configuration (page 3-54)
Console Password	Not Required	
Console Read-Only Password	user	
Console Read-Write Password	secure	
Participation	Normal Learning	Spanning Tree Port Configuration (page 3-61)
Priority	128	
Path Cost	10 or 100	
Bridge Priority	8000 (read only)	Spanning Tree Switch Settings (page 3-64)
Designated Root	8000 (bridge_id) (read only)	
Root Port	0 (read only)	
Root Path Cost	0 (read only)	
Hello Time	2 seconds (read only)	
Maximum Age Time	20 seconds (read only)	
Forward Delay	15 seconds (read only)	
Bridge Hello Time	2 seconds (read only)	
Bridge Maximum Age Time	20 seconds (read only)	
Bridge Forward Delay	15 seconds (read only)	
TELNET Access	Enabled	TELNET Configuration (page 3-67)
Login Timeout	1 minute	
Login Retries	3	
Inactivity Timeout	15 minutes	

(continued)

Table E-1. Factory Default Settings for the BayStack 350 Switch (continued)

Field	Default setting	Appears in this CI screen
Event Logging	All	
Allowed Source IP Address (10 user-configurable fields)	First field: 0.0.0.0 (no IP address assigned)	
	Remaining nine fields: 255.255.255.255 (any address is allowed)	
Allowed Source Mask (10 user-configurable fields)	First field: 0.0.0.0 (no IP address assigned)	
For details about this field, see Table 3-26 on page 3-68.	Remaining nine fields: 255.255.255.255 (any address is allowed)	
Image Filename	Zero-length string	Software Download (page 3-70)
TFTP Server IP Address	0.0.0.0 (no IP address assigned)	
Start TFTP Load of New Image	No	

Appendix F
Sample BootP Configuration File

This appendix provides a sample BootP configuration file. The BootP server searches for this file, called bootptab (or BOOTPTAB.TXT, depending on your operating system), which contains the site-specific information (including IP addresses) needed to perform the software download and configuration. You can modify this sample BootP configuration file or create one of your own.

A sample BootP configuration file follows:

```
# The following is a sample of a BootP configuration file that was extracted
# from a 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

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V