Using the BayStack 310-24T Ethernet Switch

Part No. 201875-A
February 1999

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95052

8 Federal Street
Billerica, MA 01821

Trademarks

Bay Networks and Optivity are registered trademarks of Bay Networks, Inc. BayStack, Autotopology, Expanded View, OmniView, and the Bay Networks logo are trademarks of Bay Networks, Inc.

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

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

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 310-24T Ethernet 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

This digital apparatus (BayStack 310-24T Ethernet 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 310-24T Ethernet 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

Appendix D
BayStack 310-24T Switch Console Interface

Appendix E
Web Management Interface

Figures

Tables

Preface

The BayStack 310-24T Ethernet Switch is part of the Bay Networks® BayStack™ line of communication products. The BayStack 310-24T Ethernet Switch is intended for small segment workgroups and power-user desktops and provides both 10BASE-T ports and 100BASE-T ports.

Before You Begin

This guide presents information about using the features and capabilities of the BayStack 310-24T Ethernet Switch, installing a switch, and configuring the switch through the console or Web-based user interface.

This guide is intended for Ethernet administrators with the following background:

- Working knowledge of basic Ethernet and network management concepts and terminology
- Familiarity with 10BASE-T and 100BASE-T specifications
- Familiarity with the use of a World Wide Web browser
- Working knowledge of tools and procedures for installing and operating sensitive electronic equipment

Text Conventions

This guide uses the following text conventions:

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`

Related Publications

For more information about the BayStack 310-24T switch, refer to the following publications:

- *BayStack 310-24T Ethernet Switch Installation Instructions*
  (Bay Networks part number 201876-A)

  A quick installation guide for the BayStack 310-24T switch, including translations into French, German, Spanish, Italian, Japanese, and Chinese.

- *Installing the BayStack 30x and 310 Ethernet Switch Media Adapters*
  (Bay Networks part number 893-01023-B)

  Installation instructions and LED explanations for the optional 10100BASE-TX and 100BASE-FX media dependent adapters (MDAs) for the BayStack 310-24T Ethernet Switch.

You can now print Bay Networks technical manuals and release notes free, directly from the Internet. Using a Web browser, 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, or information about educational services, go to the following URL:

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

Or telephone the Bay Networks Technical Solutions Center at:

800-2LANWAN

Chapter 1
Introduction to the BayStack 310-24T Ethernet Switch

This chapter introduces the BayStack 310-24T Ethernet Switch and covers the following topics:

About the BayStack 310-24T Ethernet Switch

The BayStack 310-24T Ethernet Switch belongs to the Bay Networks BayStack family of high-performance Ethernet solutions. These switches are designed to begin Ethernet frame switching functions immediately after setup with no configuration required. Minimal configuration is required for network management. These BayStack switches provide switch connectivity between 802.3 Ethernet devices running any network protocols.

The BayStack 310-24T Ethernet Switch provides 24 10 Mb/s ports, one autonegotiating 10/100 Mb/s port, and two media adapter (MDA) slots for either 10/100BASE-TX or 100BASE-FX fiber port connections. The 100 Mb/s ports provide a high-throughput connection to a backbone or server and can be configured to operate in either half- or full-duplex data transfer mode. The 100 Mb/s ports can also be used to provide a link between traditional 10BASE-T networks and the faster 100 Mb/s networks.

Multiple switches can be connected to one another to form a switched/segmented Ethernet network. The IEEE 802.1d Spanning Tree Protocol provides automatic network configuration of a loop-free topology and redundant inter-switch links. You can selectively disable Spanning Tree Protocol on individual ports when the switch is set up with Spanning Tree Protocol enabled.

The BayStack 310-24T switch provides access control for management functions based on the IP addresses of stations authorized to access these functions. In addition, the switch provides MAC address-based network security that allows network access only to those stations with authorized MAC addresses.

A MultiLink Trunking feature allows a user to group multiple high-speed ports (up to three) together when forming a link to another switch or server, thus increasing aggregate throughput.

The BayStack 310-24T switch supports up to 31 port-based VLANs with IEEE 802.1Q tagging available per port. VLANs allow network flexibility because you can reassign VLANs to accommodate network moves, additions, and changes, eliminating the need to change physical cabling.

Features

The BayStack 310-24T Ethernet Switch has the following hardware features:

- 10 Mb/s and 100 Mb/s switched ports in the following configurations:
  - 24 10BASE-T full- or half-duplex ports with standard RJ-45 connections
  - One 10/100BASE-TX full/half-duplex port
  - Addition of two optional full/half-duplex ports:
    - 10/100BASE-TX unshielded twisted pair (UTP) port
    - 100BASE-FX fiber port
- Front panel indicators for power, system, and port link status for the 10 Mb/s ports; indicators for full- or half-duplex mode and speed for the 100 Mb/s ports.

The BayStack 310-24T switch has the following operational features:

- Store-and-forward switching
- Support for the IEEE 802.3u autonegotiation standard on all the 10/100BASE-TX ports and the 10/100BASE-TX MDA

- Up to 2048 media access control (MAC) addresses per switch on all ports not configured as uplinks and an unlimited number of MAC addresses on the uplink ports
- Full-duplex line rate aggregate throughput of 651 kp/s for 64-byte packets
- Two user-selectable address-learning modes on high-speed ports:
  - — Normal mode—address learning takes place on the port.
  - — Uplink mode—address learning does not occur on the port; connecting uplink ports to a network center limits addresses learned by the switch to those learned on normal ports.
- MAC table lookup for learned addresses
- Limited MAC address filtering to prevent communication to specific stations (up to eight)
- Conversation steering capability from any switch port to facilitate network troubleshooting and traffic monitoring
- TFTP remote software image download via the console, Telnet, SNMP, or the Web with a delayed reset/upgrade option for scheduling the upgrade several hours in the future, when network traffic is light
- Switch configuration using the Bootstrap Protocol (BootP) to download network parameters and software image
- Support for Spanning Tree Protocol in two modes:
  - — IEEE 802.1d compliant
  - — Fast Start mode, which allows the port to reach forwarding state faster
- Support for up to 31 port-based virtual LANs (VLANs) compliant with IEEE 802.1q frame tagging
- Network access control based on MAC addresses of authorized network station (Responses to unauthorized access include sending a trap, disabling the port, and enabling destination address filtering.)
- Link aggregation support on multiple high-speed (100 Mb/s) ports
- Duplicate MAC address support (use of one MAC address in different VLANs)

For management of the switch, the BayStack 310-24T switch provides the following features:

- Three methods of switch setup and management:
  - — A character-based, menu-driven user interface accessible by way of local serial port or Telnet connection (Two Telnet sessions are supported simultaneously with the local console.)
  - — A Web-based management graphical user interface (GUI) accessible from any network node through a World Wide Web browser with Java capability (Recommended browsers include Netscape 4.0 or Microsoft Explorer 4.0 or later. The management interface uses an embedded http server for in-band management and allows you to configure, monitor, and maintain your network.)
  - — Simple Network Management Protocol (SNMP) manageability
- A character-based, menu-driven user interface
- Management access control based on IP addresses of authorized network stations
- In-band Telnet connections through any port
- Password protection for console, Telnet, and Web-based interfaces with a single, changeable password
- Support for features of Bay Networks Optivity® NMS 9.0 network management software:
  - — Expanded View™ (configuration and monitoring tool that graphically displays all components of the switch chassis)
  - — OmniView™ (monitoring tool that displays statistics, status, and profiles using EtherLike and RMON MIBs)
  - — Multisegment Autotopology™ (topology MIBs and port-to-MAC association/Bridge MIBs)
- SNMP MIB II EtherLike and Bridge MIB support
- Support for four RMON MIB groups: Statistics, History, Alarm, and Events
- Configuration file support
- Device Manager support

Half-Duplex and Full-Duplex Mode

By definition, the Ethernet carrier sense multiple access/collision detection (CSMA/CD) protocol operates in half-duplex mode, allowing either data transmission or reception, but never both at the same time. Point-to-point network connections, such as DTE-to-switch ports, do not need CSMA/CD to resolve media access contention from multiple devices; therefore, point-to-point network connections allow a file server to transmit frames to a switch while simultaneously receiving frames from the same switch. This two-way, non-CSMA/CD full-duplex communication provides an effective bandwidth of 200 Mb/s between two 100 Mb/s devices.

The indicator for the built-in 10/100BASE-TX port is located on the LED panel on the right of the front panel. The indicator for the MDA port is located on the MDA. When the full-duplex indicator is lit, the port is operating in full-duplex mode and the effective available bandwidth is 20 Mb/s (10 Mb/s transmitting and 10 Mb/s receiving) or 200 Mb/s (100 Mb/s transmitting and 100 Mb/s receiving). When the indicator is not lit, the port is operating in half-duplex mode, which is 10 Mb/s or 100 Mb/s.

Note: The 100BASE-FX MDA port has an effective bandwidth of 100 Mb/s (half-duplex mode) or 200 Mb/s (full-duplex mode).

The 10BASE-T ports can operate in half- and full-duplex mode. You can verify the duplex mode for the ports using the console management interface or Web management interface.

Autonegotiation

Autonegotiation is the IEEE 802.3u standard allowing two devices with autonegotiation active sharing a common link to advertise their speed capabilities, acknowledge understanding of shared modes of operation, and reject modes of operation that are not shared. All ports on the BayStack 310-24T switch support the IEEE 802.3u autonegotiation standard. When autonegotiation is enabled on a high-speed port of the BayStack 310-24T switch and the port is connected to a device that also supports the standard, the two devices negotiate the best speed (10 or 100 Mb/s) and duplex mode (half or full) of operation. If the BayStack 310-24T switch port is connected to a device that does not autonegotiate, the port

automatically operates in half-duplex mode. The 10 Mb/s ports autonegotiate only for half/full duplex operation. All the ports on the BayStack 310-24T switch support full-duplex operation. Refer to "Autonegotiation" on page 7-2 for information about troubleshooting autonegotiation problems.

When the link is first brought up, the BayStack 310-24T switch senses the speed of the connecting device. If the connecting device changes speed without performing a link down, the BayStack 310-24T switch can correctly sense a change. If the device connected to the switch does not support autonegotiation, you should configure the switch with autonegotiation disabled.

MultiLink Trunking

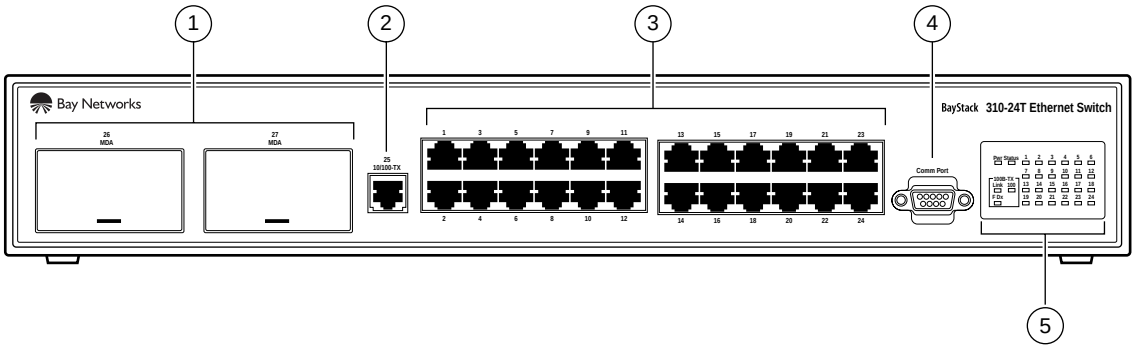
The MultiLink Trunking (MLT) feature allows you to group multiple high-speed ports (up to three) together when forming a link to another switch or server, thus increasing aggregate throughput of the interconnection between two devices, up to 600 Mb/s in full-duplex mode. BayStack 310-24T switches can be configured with a single multilink trunk.

The trunk members form a physical collection of ports that are treated as a single logical link of higher bandwidth by the Spanning Tree Protocol and the learning, forwarding, and filtering functions. The MultiLink Trunking software can detect broken trunk links and redirect all traffic from the broken trunk member to other member ports within the trunk.

For more information about the MultiLink Trunking feature, see "MultiLink Trunking Rules" on page 2-15.

Physical Description

The front panel of the BayStack 310-24T switch (Figure 1-1) provides RJ-45 10BASE-T ports, an RJ-45 10/100BASE-TX port, two expansion slots for the addition of 10/100BASE-TX or 100BASE-FX ports, a DB-9 connector for a console, and status LEDs.



1 = Expansion slots for 10/100BASE-TX or 100BASE-FX MDAs
2 = 10/100BASE-TX port
3 = 10BASE-T ports
4 = Console port connection
5 = Status indicators

Figure 1-1. BayStack 310-24T Switch Front Panel

10BASE-T Ports

The 10BASE-T port connections allow you to attach 10 Mb/s Ethernet segments or nodes to the BayStack 310-24T switch. Each port has an associated LED that indicates link status of the line. The RJ-45 jacks accept standard Category 3, 4, or 5 unshielded twisted pair (UTP) cable connections. For pin assignments for the standard RJ-45 connectors, refer to Appendix A, "Technical Specifications."

The BayStack 310-24T switch is shipped with the 10BASE-T connectors configured as MDI-X (medium-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 attaching device (see "MDI and MDI-X Connections" on page A-6 for a description of the crossover cable).

The 10 Mb/s ports can operate in full- or half-duplex mode.

10/100BASE-TX Port

The BayStack 310-24T switch has one built-in and two optional 10/100BASE-TX ports designed to operate either at 10 Mb/s or at 100 Mb/s depending on the connecting device. The 10/100BASE-TX port supports half- and full-duplex mode operation. This port supports the IEEE 802.3u autonegotiation standard, so that when it is connected to another device that also supports the IEEE 802.3u autonegotiation standard, the two devices negotiate the best speed and duplex mode of operation. For more information about autonegotiation, see "Connecting the 10/100BASE-TX Port" on page 3-7.

The 10/100 Mb/s port consists of a standard 8-pin modular RJ-45 connector used to connect hubs, switches, and end stations using only 2-pair Category 5 UTP cabling. 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 attaching device (see "MDI and MDI-X Connections" on page A-6 for a description of the crossover cable).

Like the 10BASE-T ports, all 10/100BASE-T ports are also configured as MDI-X. For pin assignments for the RJ-45 connector, refer to Appendix A, "Technical Specifications."

MDA Slots

The BayStack 310-24T switch has two expansion slots for optional plug-in media-dependent adapters (MDAs) to support high-speed connections to servers, shared Fast Ethernet hubs, or backbone devices. The following two types of media adapters are available:

- Model MTX-1, 10/100BASE-TX UTP connection
- Model MFX-1, 100BASE-FX fiber connection

Both media types support half- and full-duplex operation and have an LED to indicate when the port is operating in full-duplex mode. See Appendix C, "Media Dependent Adapters (MDAs)," for a full description of the MDAs.

Warning: Power to the switch must be turned off before you install the MDA.

Console Port Connector

The console port has a DB-9 male connector used to connect a management terminal to the BayStack 310-24T switch. The console interface operates as a data communication equipment (DCE) interface; that is, you connect a terminal using a straight-through cable. Using a terminal, you can monitor the results of startup self-diagnostics, perform manual boot configuration and SNMP agent configuration, and customize your network using the supplied menus and screens.

The console port runs at 9600 baud and uses 8 data bits, 1 stop bit, and no parity as the communications format, with flow control disabled.

For pin assignments for the console port, refer to "Pin Assignments" on page A-5.

In less complex applications with no network management, where no configuration changes are required, you do not need to use the console port on the BayStack 310-24T switch except for the initial switch setup described on page 3-13. You can also perform the same monitoring and management functions using the Web-based management interface.

For information about connecting a terminal to the console port, refer to "Connecting to the Console Port" on page 3-9.

LEDs

The LEDs (Figure 1-2) on the front panel of the BayStack 310-24T switch help you to identify the unit port status and MDA operational mode. LEDs associated with the RJ-45 port connectors identify the link status and link activity of each port.

The AC power supply status LED and the system status LED work together to provide status information.

The link status indicator for the 100BASE-TX port is on the LED panel on the front of the switch. This area also contains a full-duplex (F Dx) status indicator that lights when the port is operating in full-duplex mode. When the port is operating in half-duplex mode, the indicator is off. See "Half-Duplex and Full-Duplex Mode" on page 1-5 for more information on duplex mode.

A speed LED (100) indicates when the port is operating as a 100 Mb/s port. The LED is off when the port is operating as a 10 Mb/s port.
See "Autonegotiation" on page 1-5 for more information about autonegotiation of wire speed.

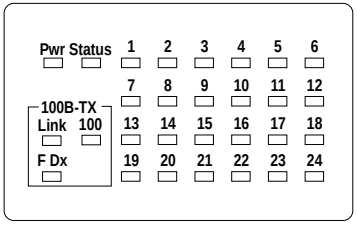


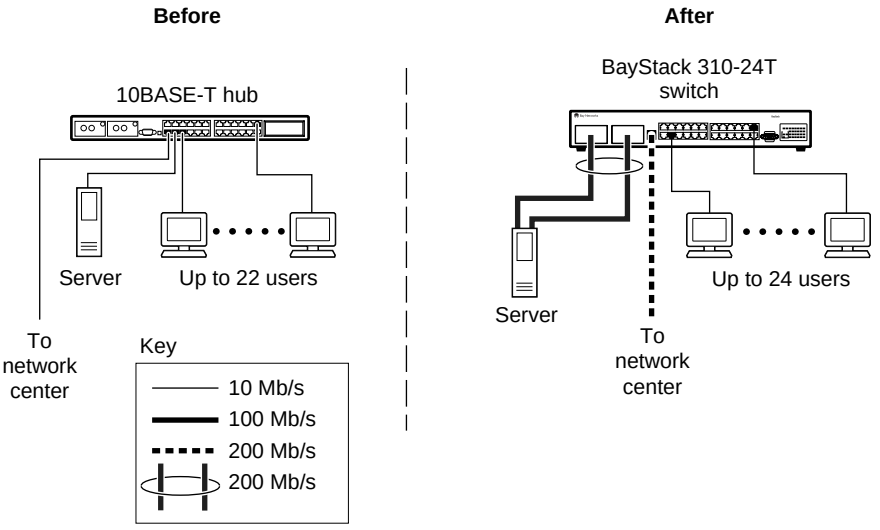
Figure 1-2. LEDs on the BayStack 310-24T Ethernet Switch

Configuration Examples

The BayStack 310-24T switch is well suited for the initial migration from shared 10BASE-T segments to dedicated bandwidth for switch connections between segments, end stations, 100BASE-T Fast Ethernet servers, and Fast Ethernet backbone connections.

Desktop Switch Application

Figure 1-3 shows the BayStack 310-24T switch used as a desktop switch, where desktop workstations are connected directly to switch ports. This configuration provides a 100 Mb/s connection to the network center, a dedicated 200 Mb/s connection to the server, and dedicated 10 Mb/s connections instead of shared 10 Mb/s connections to up to 24 users. The connection to the server can be implemented as a multilink trunk.



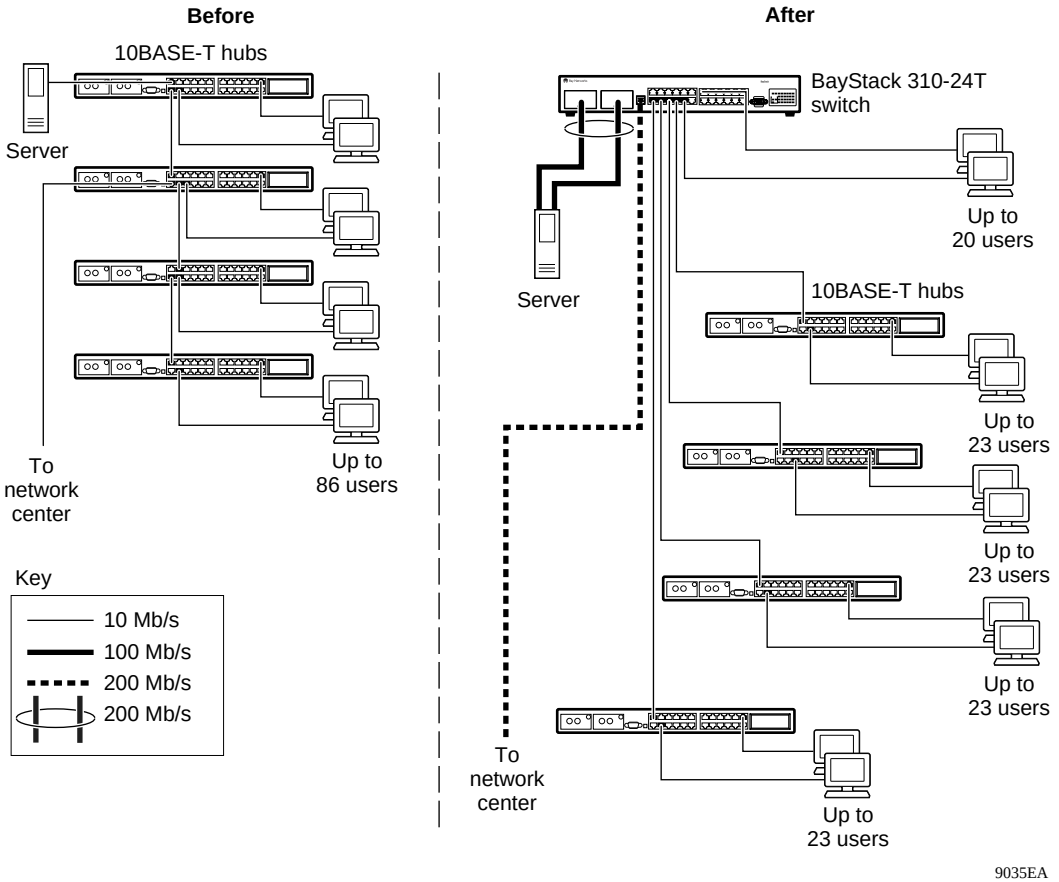
- 22 users sharing 10 Mb/s (10/22 Mb/s per user)
- Server bottleneck (10 Mb/s connection)
- Network center bottleneck (10 Mb/s connection)

- 24 users each with a dedicated half- or full-duplex 10 Mb/s connection
- Server with dedicated 200 Mb/s connection using MultiLink Trunking
- Network center with dedicated 100 Mb/s full-duplex connection (200 Mb/s bidirectional)

Figure 1-3. BayStack 310-24T Switch Used as a Desktop Switch

Segment Switch Application

Figure 1-4 illustrates adding a BayStack 310-24T switch as a segment switch to alleviate user contention for bandwidth and eliminate server and network center bottlenecks.



- 86 users share 10 Mb/s (10/86 Mb/s per user)
- Server bottleneck (10 Mb/s pipe)
- Network center bottleneck (10 Mb/s pipe)
- Total of 86 users

- Four sets of 23 users; each set shares 10 Mb/s (10/23 Mb/s per user)
- Addition of 20 users each with half- or full-duplex 10 Mb/s dedicated connection
- Server with dedicated 200 Mb/s connection using MultiLink Trunking
- Network center with dedicated 100 Mb/s full-duplex pipe (200 Mb/s bidirectional)
- Total of 112 users

Figure 1-4. BayStack 310-24T Switch Used as a Segment Switch

Before segmentation, 86 users had only a total bandwidth of 10 Mb/s available. After segmentation, 92 users effectively have 40 Mb/s, four times the previous bandwidth, while adding 20 dedicated 10 Mb/s connections. This configuration can be extended to add more segments without degrading performance.

High-Density Switched Workgroup Application

Figure 1-5 shows an example of using BayStack 310-24T switches with a BayStack 350-24T switch in a high-density switched workgroup. (See the Bay Networks library Web page—*support.baynetworks.com/library/*—for online documentation about the BayStack 350-24T switch.) The BayStack 310-24T switches have 100 Mb/s connections to the BayStack 350-24T switch, a 100BASE-TX hub, and a 100 Mb/s server. They have 10 Mb/s connections to DTE (data terminal equipment). The BayStack 310-24T switches act as desktop switches, while the BayStack 350-24T switch serves as the backbone switch.

The 200 Mb/s connections are set up as multilink trunks between high-speed ports on the BayStack 310-24T switches. The BayStack 310-24T switch supports one multilink trunk with either two or three high-speed ports. The member ports must all have the same port VLAN identifier (PVID). They must also have the same settings for the following parameters:

- VLAN port type (access or interswitch)
- Switch port type (uplink or normal)

See "Virtual LANs" on page 2-4 for more information about port types.

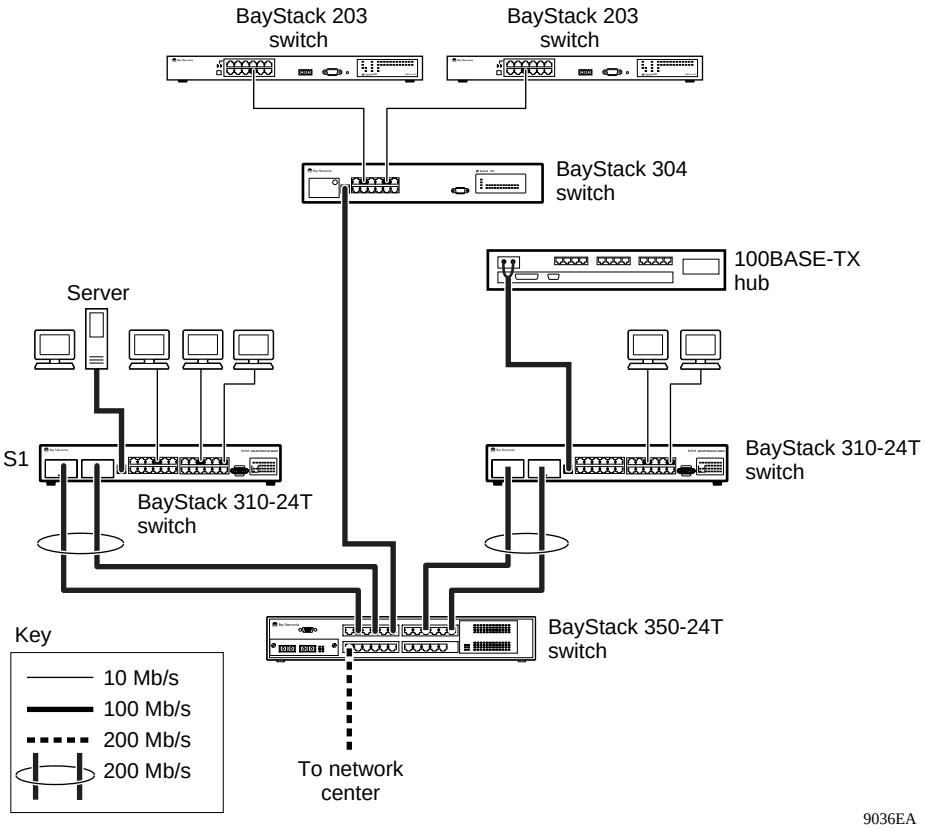


Figure 1-5. BayStack 310-24T Switches in a High-Density Switched Workgroup

Chapter 2
Setting Up a Network Using the BayStack 310-24T Switch

This chapter discusses factors to consider when setting up a network with the BayStack 310-24T switch, including when to enable optional switch features and ways to manage and upgrade the switch. For information about using the console or Telnet interface, refer to Chapter 5, "Managing the BayStack 310-24T Switch Using the Console Interface." For information about using the Web interface, refer to Chapter 6, "Managing the BayStack 310-24T Switch Using a Web Browser."

This chapter includes the following information:

- Feature setup options (this page)
- Managing the BayStack 310-24T switch (page 2-20)
- Upgrading switch software through a TFTP connection (page 2-23)

Refer to Chapter 3, "Installing the BayStack 310-24T Switch," for installation, connection, and quick configuration procedures.

Feature Setup Options

This section describes some of the advanced features of the BayStack 310-24T switch to help you decide whether or not to enable them on switch setup. The following features are described:

- Spanning Tree Protocol (page 2-2)
- Virtual LANs and 802.1Q tagging (page 2-4)
- MultiLink trunking (page 2-15)
- Address learning (page 2-16)

- MAC-based address filtering (page 2-17)
- Security (page 2-18)

Spanning Tree Protocol

The Spanning Tree Protocol is compliant with the IEEE 802.1d standard that detects and eliminates physical loops in a bridged or switched network. When multiple paths exist, the spanning tree algorithm puts some links in a standby state so that there is only one active path between any two nodes. If any of the active network links fail, standby links are brought online to maintain network connectivity. To avoid interoperability problems, use the same spanning tree algorithm throughout a network.

The Spanning Tree Protocol becomes necessary as networks grow, interconnect with other networks, and generally become more complex. In complex networks, it is possible to route a message from any given source to any given destination by more than one path. Routing a message over multiple paths can cause several bridges to claim priority in sending the same message. In addition to needless duplication, this situation can result in a loop where messages travel endlessly as each bridge learns the wrong information about where individual nodes are located.

The Spanning Tree Protocol resolves the problem of loops in the network by establishing only one “primary” path between any two switches in a complex network. Any duplicate paths are barred from use and become standby or blocked paths until the primary path fails, at which point the standby path can be brought into service. Every switch periodically broadcasts a Bridge Protocol Data Unit (BPDU) to all other switches in the network with topology information. The Spanning Tree Protocol determines the root bridge and the loop-free path configuration. It does not take into account the VLAN configuration of the port; it looks only at physical links to determine the forwarding link.

To be able to connect multiple VLANs across switches with redundant links, you must disable Spanning Tree Protocol on all participating switches that do not support 802.1Q tagging (see page 2-7). Figure 2-1 shows possible consequences of enabling the Spanning Tree Protocol when VLANs are set up with a switch that does not support tagging.

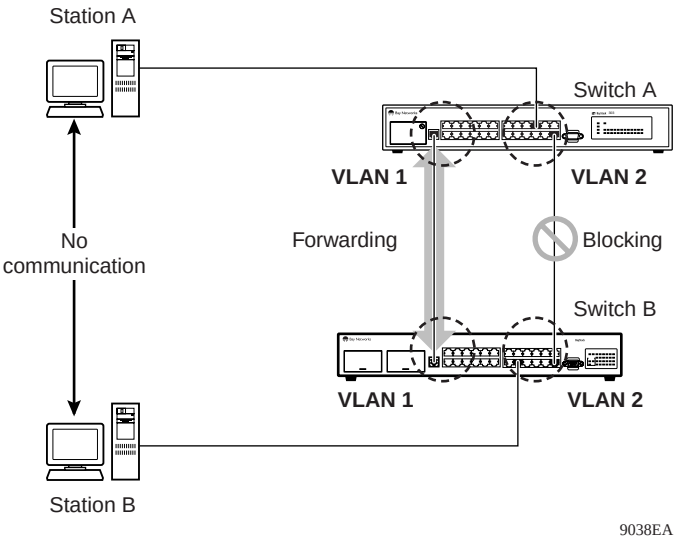


Figure 2-1. Possible Problems with VLAN and Spanning Tree Protocol

Spanning Tree Protocol is enabled for all ports by default; you can change this setting as follows:

- From the console interface, select the Switch Network Configuration option from the System Configuration menu (see "Enabling Spanning Tree Protocol" on page 5-21).
- From the Web interface, use the Configuration: Spanning Tree page (see "Customizing Spanning Tree Protocol Operation" on page 6-21).

When Spanning Tree Protocol is enabled for the switch, you can selectively disable it on individual ports or set the mode of operation. When Spanning Tree Protocol is enabled, you can set ports to operate in one of three modes:

- IEEE 802.1d Spanning Tree Protocol enabled (default setting)

  In IEEE 802.1d mode, the port operation is compliant with the IEEE standard. Transition to the Forwarding state typically takes 30 seconds.

- Spanning Tree Protocol enabled with Fast Start operation

  Fast Start operation for Spanning Tree Protocol allows the port to transition to the Forwarding state faster than it does in the 802.1d mode. This rapid transition provides connectivity to stations within 4 seconds of the time the link is established, if you use the recommended default timer values for Spanning Tree Protocol operation. (Using 802.1d mode, a port typically takes 30 seconds to reach the Forwarding state.) Fast Start operation imposes shorter convergence times on the operation of the Spanning Tree Protocol. As a result, although the protocol still tries to detect and eliminate network loops, the probability that a loop may occur is greater with Fast Start operation than with IEEE 802.1d operation.

- Spanning Tree Protocol disabled

  When the Spanning Tree Protocol is disabled, the switches cannot detect network loops connected to these ports.

Note: Spanning Tree Protocol resolves duplicate paths in networks and is not necessary for ports that have workstations directly attached to the switch. When Spanning Tree Protocol is enabled on these ports (the default), workstations are unable to attach to servers until Spanning Tree Protocol stabilizes.

Virtual LANs

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

Two kinds of ports can be assigned to VLANs:

- An access port belongs to a single VLAN domain. This port is an untagged port (see “IEEE 802.1Q Tagging” on page 2-7).
- An interswitch port belongs to all VLAN domains in the switch. This port is a tagged port and is used for VLAN trunking between switches.

BayStack 310-24T switches provide several benefits when they are connected to other devices that support 802.1Q tagging, such as the BayStack 450 switch or other BayStack 310-24T switches. An interswitch (tagged) port is a member of all VLANs and can therefore transmit data from all VLANs to another device. At the destination device, the tag is read and the frame is distributed only to the same VLAN number as the VLAN where it originated. This feature allows you to extend all VLANs across two or more devices through a single link, while you maintain the security of keeping the data within the same VLAN numbers.

The BayStack 310-24T switch supports up to 31 port-based VLANs with 802.1Q tagging available per access port. Each access port is assigned to a single VLAN. Ports are grouped into broadcast domains by assigning them to the same VLAN. Frames received in one VLAN can be forwarded only within that VLAN, and unknown unicasts are flooded only to ports in the same VLAN.

In the BayStack 310-24T switch, ports can be assigned to VLANs using the console, Telnet, or Web interfaces. You can assign different ports (and therefore the devices attached to these ports) to different broadcast domains. This feature provides network flexibility because you can reassign VLANs to accommodate network moves, additions, and changes, eliminating the need to change physical cabling.

Figure 2-2 illustrates how you can use virtual LANs with access or interswitch ports in a BayStack 310-24T switch to segment a network.

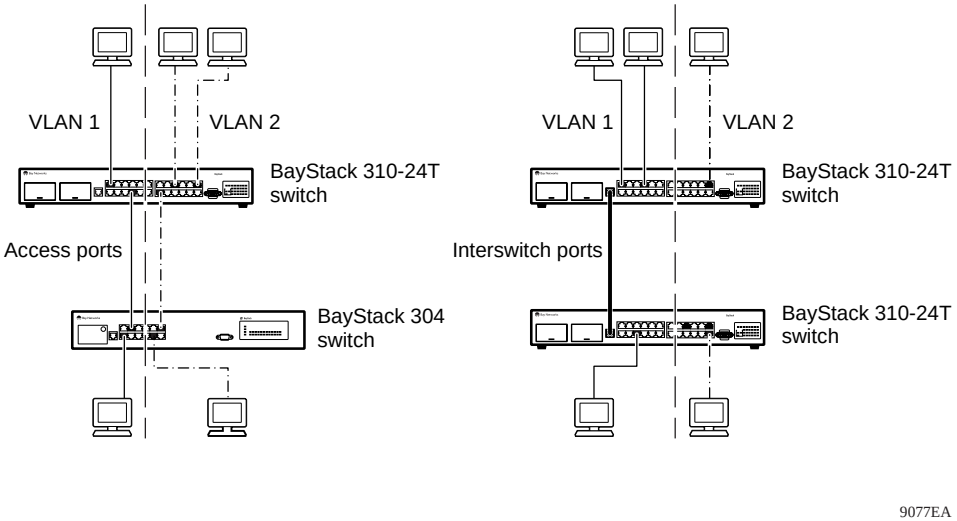


Figure 2-2. Access Ports and Interswitch Ports in the BayStack 310-24T Switch

A BayStack 304 switch does not support 802.1Q tagging, Therefore, in the left part of Figure 2-2, access ports are used to connect the VLANs, and each VLAN has a separate connection. Spanning Tree Protocol is disabled in this configuration. In the right part of the figure, two BayStack 310-24T switches are connected using a single interswitch port. The interswitch port allows VLAN 1 and VLAN 2 to use the same link between the switches.

You assign ports to VLANs in one of the following ways:

- From the console interface, use the System Configuration screen to assign ports to VLANs (see "Assigning Ports to VLANs" on page 5-28).
- From the Web interface, use the Configuration: VLAN page to assign ports to VLANs (see "Assigning Ports to VLANs" on page 6-25).

IEEE 802.1Q Tagging

BayStack 310-24T switches operate in accordance with the IEEE 802.1Q tagging rules, which define a classification system that identifies the VLAN where a frame originated. In the specification, an additional 4-octet (“tag”) header is inserted in a frame after the source address and before the frame type. The tag contains the VLAN ID with which the frame is associated. By coordinating VLAN IDs across multiple switches, VLANs can be extended to multiple switches.

If your network includes devices that use 802.1Q tagging, you can extend multiple VLANs across multiple switches using only a single cable between switches.

The following terms are used in describing 802.1Q tagging:

- 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 VLAN ID remains).

The default configuration settings for BayStack 310-24T 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 2-3, all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID =1). Untagged packets enter and leave the switch unchanged.

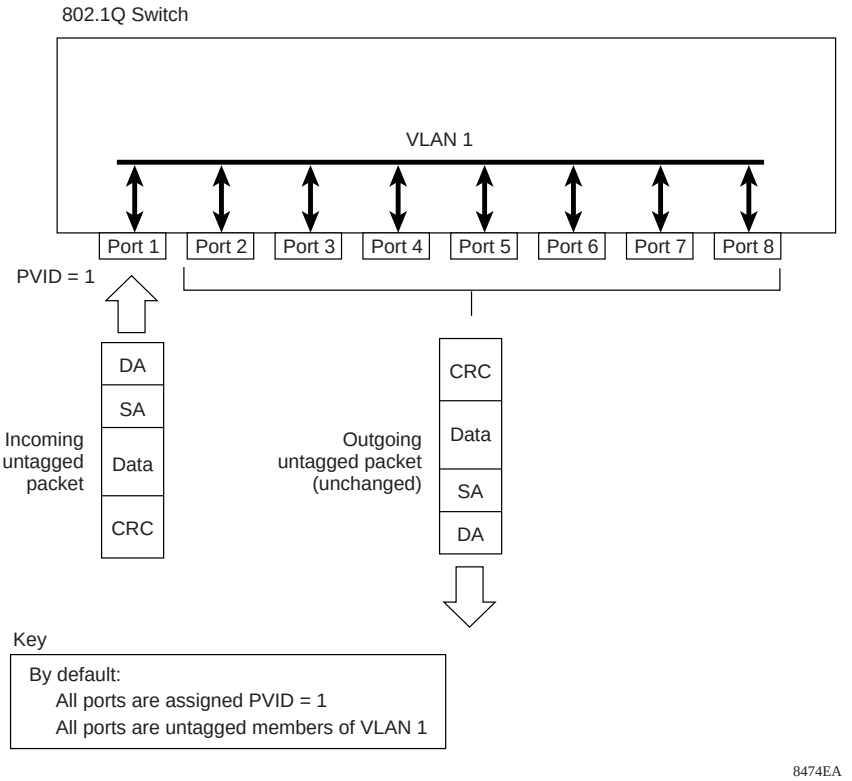
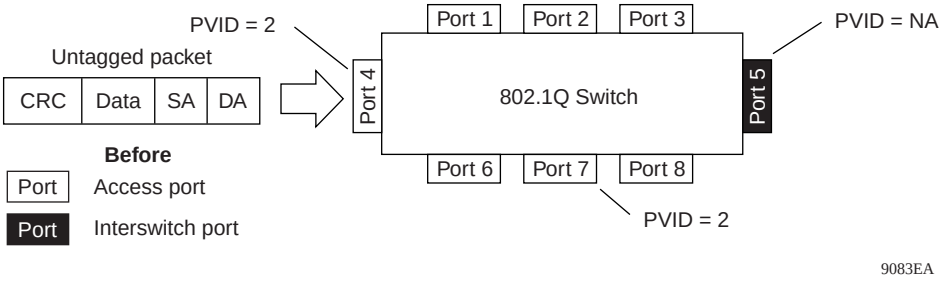


Figure 2-3. Default VLAN Settings

To configure VLANs, you can set the switch ports as *tagged* or *untagged* members of specific VLANs. Figure 2-4 through Figure 2-7 show how packets are handled by tagged and untagged ports.

In Figure 2-4, untagged incoming packets on port 4 are assigned directly to VLAN 2 (PVID = 2). Ports 4 and 7 are configured as *untagged* members of VLAN 2 and are assigned a PVID value of 2. Port 5 is configured as a tagged (interswitch) port and is assigned to all VLANs in the switch.



- Ports 4 and 7 belong to VLAN 2 (PVID = 2)
- Port 5 (interswitch port belongs to all VLANs configured in the switch)

Figure 2-4. 802.1Q Tagging: Untagged Packet Entering an Access Port

As shown in Figure 2-5, the untagged packet that entered through port 4 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.

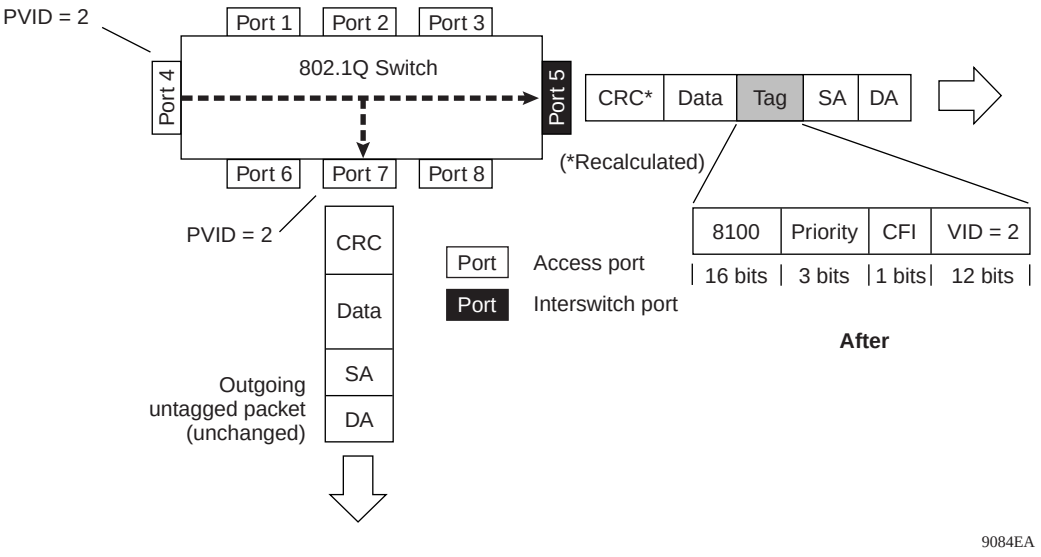


Figure 2-5. 802.1Q Tagging: Untagged Packet Leaving the Switch

In Figure 2-6, tagged incoming packets on port 4 are assigned directly to VLAN 2 because of the tag assignment in the packet. Port 5 is configured as a *tagged* (interswitch) port, and port 7 is configured as an *untagged* member of VLAN 2.

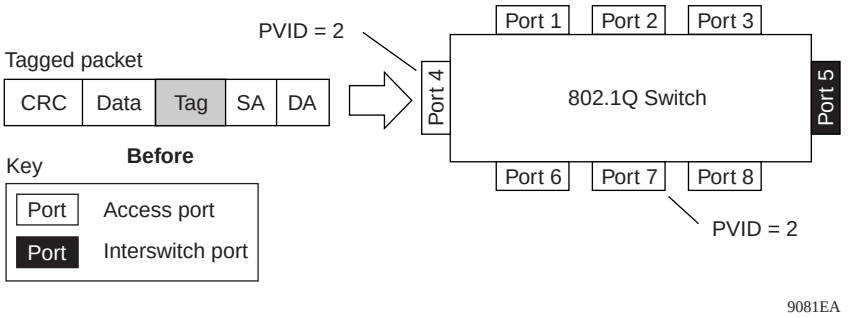


Figure 2-6. 802.1Q Tagging: Tagged Packet Entering an Access Port

As shown in Figure 2-7, 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.

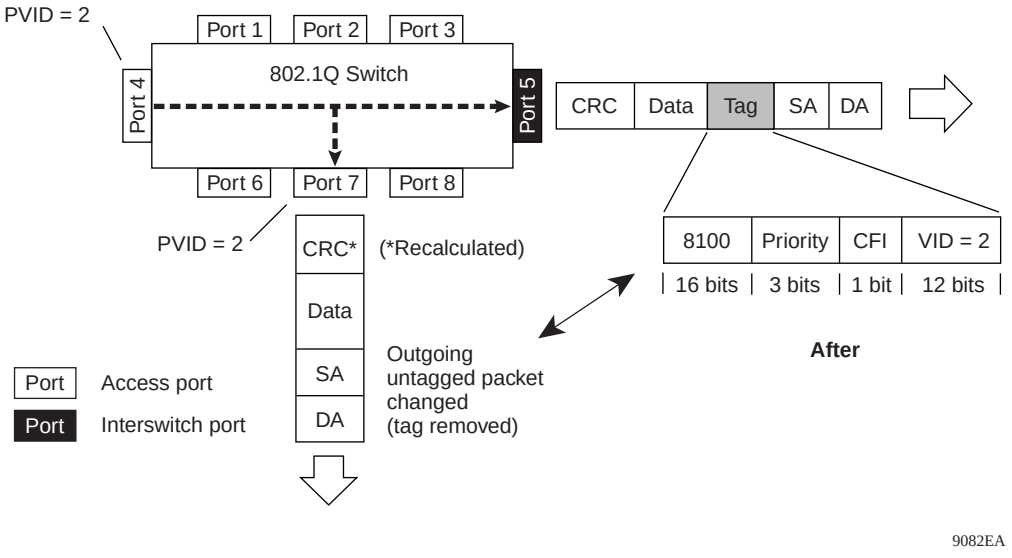


Figure 2-7. 802.1Q Tagging: Tagged Packet Leaving the Switch

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.

In the BayStack 310-24T switch, whether or not tagged frames are sent or received is configured at the port level. Ports in a VLAN are designated as either interswitch ports (tagging enabled) or access ports (tagging not enabled). With tagging enabled on a port for a VLAN, all frames leaving the port for that VLAN are marked as belonging to that specific VLAN.

A BayStack 310-24T switch interswitch port is a port from which all frames sent are tagged. Because all frames are explicitly tagged with a VLAN ID, interswitch ports are typically used to multiplex traffic belonging to multiple VLANs to other IEEE-802.1Q-compliant devices.

A port that does not send tagged frames (designated as an access port or untagged port) is used to connect BayStack 310-24T switches to devices that do not support IEEE 802.1Q tagging. If a tagged frame is forwarded through an untagged port, the switch removes the tag from the frame before sending it out the port.

VLANS Spanning Multiple 802.1Q Tagged Switches

Figure 2-8 shows VLANs spanning two BayStack 310-24T switches, that is, two devices that support 802.1Q tagging. 802.1Q tagging is enabled on S1, port 2 and on S2, port 1.

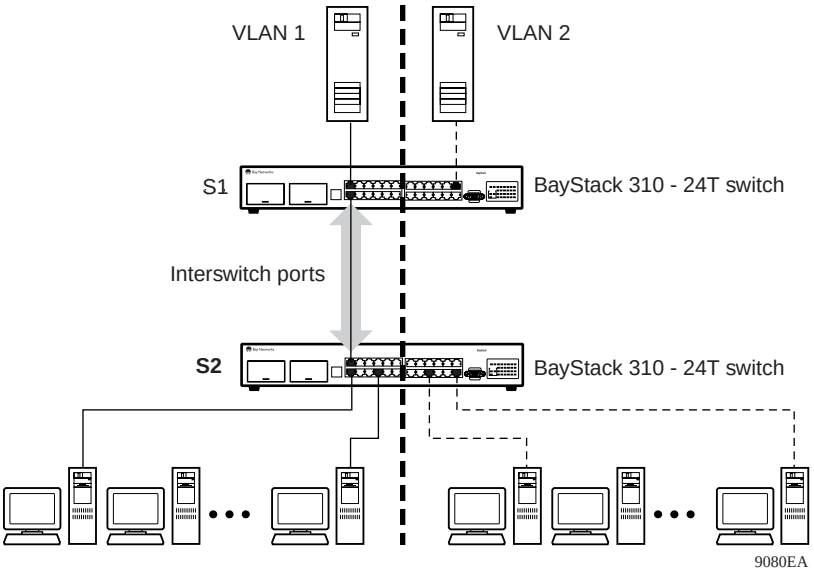


Figure 2-8. VLANs Spanning Multiple 802.1Q Tagged Switches

Because there is only one link between the two switches, the Spanning Tree Protocol treats this configuration like 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 2-9 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 Spanning Tree Protocol is not supported across multiple LANs.

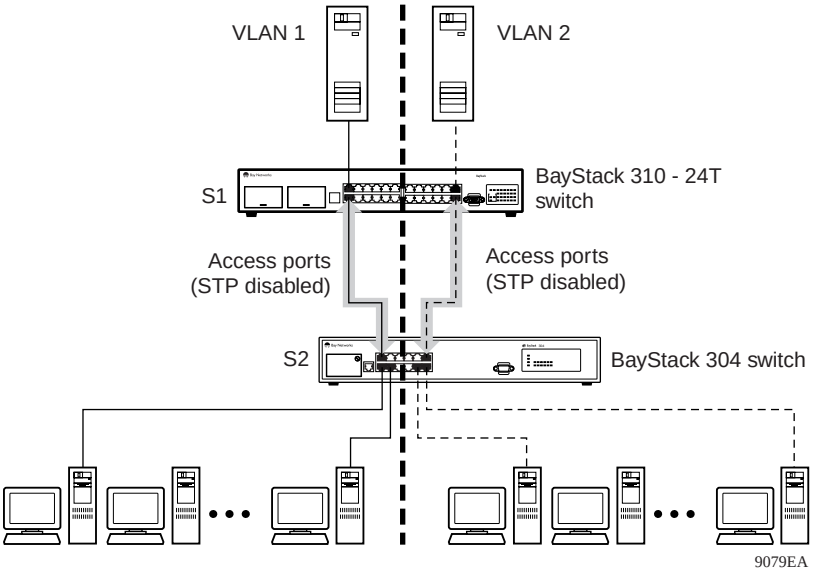


Figure 2-9. VLANs Spanning Multiple Untagged Switches

When the Spanning Tree Protocol 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. When you configure the switches, you must make sure the VLAN configuration does not conflict with spanning tree configuration.

VLANs Spanning Both Tagged and Untagged Switches

Figure 2-10 shows VLANs spanning a combination of tagged and untagged switches. Because the BayStack 303 switch does not support 802.1Q tagging, a single access port on each switch must be used for each VLAN. The connection between the two BayStack 310-24T switches requires only one link through an interswitch port.

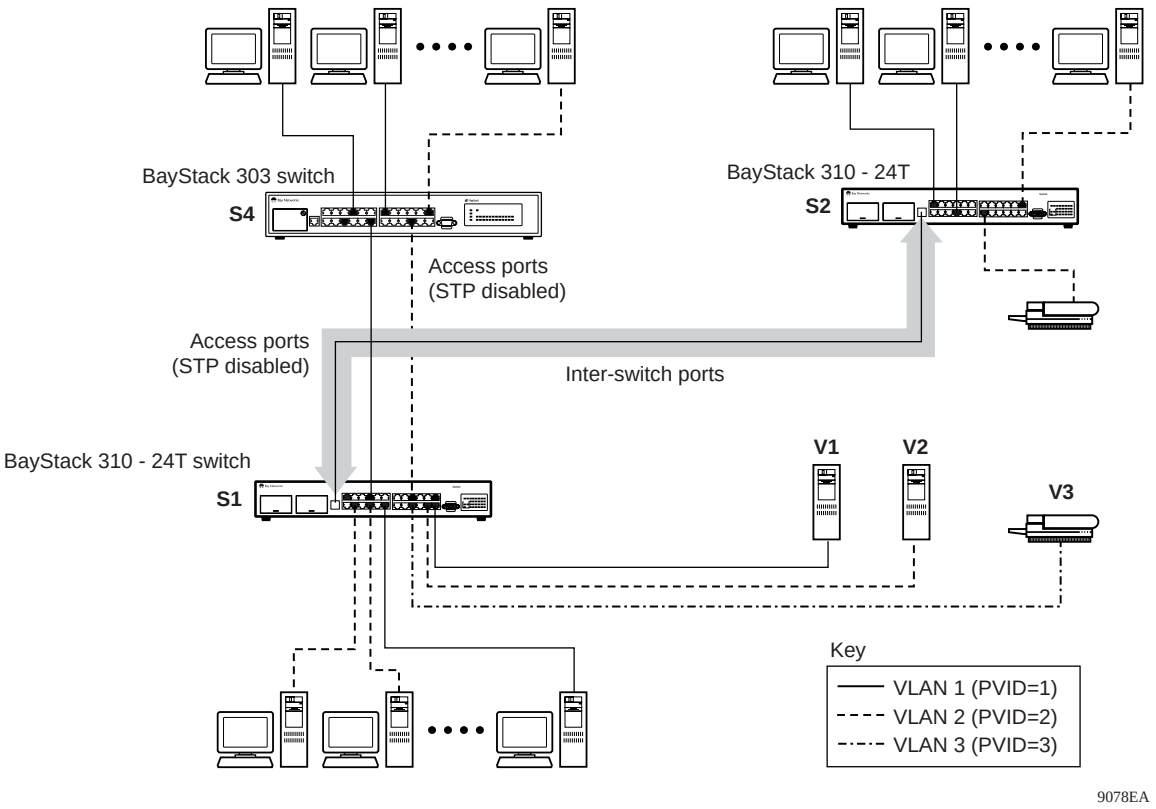


Figure 2-10. VLANS Spanning Tagged and Untagged Switches

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:

- VLANs are not dependent on the Spanning Tree Protocol setting.
- An access port is assigned to only one VLAN.
- An interswitch port is assigned to all VLANs in the switch.

MultiLink Trunking Rules

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

- The BayStack 310-24T switch supports one multilink trunk per switch.
- Only high-speed ports (25, 26, and 27) can be part of the multilink trunk.
- All multilink trunk members must be assigned to the same VLAN (see "Virtual LANs" on page 2-4).
- All ports in the multilink trunk must be set with the same speed, duplex mode, and port type (normal or uplink) settings (see "Assigning Ports to VLANs" on page 5-28 or "Assigning Ports to VLANs" on page 6-25).
- All multilink trunk ports behave as a single spanning tree.
- If the switch is transferring tagged frames, you must set multilink trunk ports as inter-switch ports. (For more information about tagged frames, refer to "IEEE 802.1Q Tagging" on page 2-7.)
- Multilink trunk members cannot be set up as monitoring ports; however, multilink trunk members can be monitored (see "Setting Up Conversation Steering" on page 5-31 or "Setting Up Conversation Steering" on page 6-27).

Address Learning

By default, the frame-forwarding behavior is the same for all BayStack 310-24T switch ports. Asymmetric MAC address learning can be used on the high-speed ports to prevent excessive flooding of switch traffic when the number of addresses in the forwarding table (MAC table) exceeds its capacity (2048 entries). Asymmetric address learning groups switch ports into normal or uplink ports, which operate as follows:

- On normal ports, new source addresses are learned when frames are received. Frames with unknown destination addresses are forwarded only to uplink ports in the same VLAN if any uplink ports are configured.
- Uplink ports do not learn unknown source addresses, so that only addresses from local stations consume space in the filtering database. These ports are suitable for backbone connections.

Table 2-1 defines the forwarding behavior of these ports.

Table 2-1. Frame-Forwarding Behavior

Receive Frame	On Normal Port	On Uplink Port (High-Speed Port Option)
Known destination address	Forward	Forward
Unknown unicast destination address	Flood to uplink ports	Drop
Unknown multicast destination address	Flood to all ports	Flood to all ports
Known source address	Reset aging time	Age out address
Unknown source address	Learn source address	Do not learn source address
Known unicast destination address	Forward to known destination	Forward to known destination
Broadcasts	Flood to all ports	Flood to all ports

Note: The default setting for all ports, including high-speed ports, is Normal.

The frame-forwarding behavior of the normal ports is determined by the existence of uplink ports in the same VLAN. Therefore, configuring high-speed ports as uplink ports can affect the entire switch.

Caution: Configuring a high-speed port as an uplink port can, in some cases, result in loss of connectivity in a switch. Note the following example:
On uplink ports, all unicast frames (for example, some ping requests) with aged out destination addresses are dropped. In a VLAN with a high-speed port configured as uplink, if the MAC address of a server connected to a normal port is aged out, the only way a client can find the server is by broadcasting for it since only broadcasts are flooded to all ports. The client will not be able to reach the server using unicast frames because the asymmetric operation will cause them to be forwarded only to the uplink ports.

Connecting other switches to uplink ports and end stations to normal ports allows the forwarding database to be used for only those addresses in the local network. When a port is configured as an uplink port, all addresses previously learned on that port are deleted from the MAC table.

To enable asymmetric MAC address learning on the BayStack 310-24T switch, configure the high-speed ports as uplink ports in one of two ways:

- Using the console interface, from the System Configuration menu, go to the High-Speed Port Configuration menu and select Uplink mode (see "Setting Up High-Speed Ports and Multilink Trunking" on page 5-27).
- Using the Web interface, on the High Speed MLT Port page, select Uplink from the Normal/Uplink Mode field (see "Setting Up High-Speed Ports and MultiLink Trunking" on page 6-24).

MAC Address-Based Filtering

The MAC address filtering feature of the BayStack 310-24T switch allows you to enter up to eight MAC addresses into the filtering database to prevent communication from specific end stations. A database entry for filtering is a combination of the MAC address and the VLAN ID. Frames with the MAC address and VLAN ID that match a filtering entry are discarded by the switch, regardless of whether the MAC address is a source address or destination address.

You can also enter the MAC address of the switch itself, which cuts off connection with the switch. When you do this, all frames with the switch MAC address are dropped, limiting switch management access to only the local console.
To reestablish communication with a MAC address, you must remove the address from the filtering database.

Caution: Be careful when entering addresses into the filtering database. Entering the address of the switch itself causes the switch to lose connection with management stations.

You can set or remove filters in one of two ways:

- From the console interface, select option 6 from the System Configuration menu (see "Setting Up Address Filtering" on page 5-26).
- From the Web interface, use the Configuration: Filtering page (see "Setting Up Address Filtering" on page 6-23).

Security Options

BayStack 310-24T switches provide two types of access control:

- Management access control based on IP addresses of the authorized management stations
- Network access control based on MAC addresses of authorized stations

You can set these features using the console menus or the Web management interface. In addition, you can set up MAC address-based security using SNMP.

Management Access Control

Access to management functions for the switch is either unrestricted or restricted. In unrestricted mode (the default setting), the switch is accessible to all users. In restricted mode, access is restricted to up to eight stations whose IP addresses have been authorized for management access. For each authorized station you can individually enable or disable Telnet, SNMP, and Web access to the switch management functions. If a violation occurs, the system generates a trap with the unauthorized IP address and the type of access that was attempted.

This feature operates independently of and in addition to the password protection or SNMP community string protection for access to the switch. For example, if a password is set for Telnet or Web access to the switch, users at authorized IP addresses must still enter the password to access the switch.

Note: If you are going through a proxy to manage the switch, you must include the IP address of the proxy device in the list of authorized addresses.

For instructions to set up management access control through the console interface, see "Setting Up Management Access Control" on page 5-12.

For instructions to set up management access control through the Web management interface, see "Setting Up Management Access Control" on page 6-11.

MAC Address-Based Security

Network access control is based on source MAC addresses of the authorized stations. You can specify a range of system responses to unauthorized access, ranging from sending a trap to disabling the port. MAC address-based security operates in one of the following three modes:

- Single MAC per port—Only one MAC address is allowed to use each switch port. Any other address learned on that port causes the specified security action to be taken. One MAC address cannot be assigned to multiple ports.When the switch software detects a violation of the security, the response can be to send a trap, turn on destination address filtering, disable the port, or combine sending a trap with one of the other two actions. The default response is to send a trap.
- MAC list—You can specify a list of up to 64 MAC addresses authorized or not authorized to connect to the switch. For each address, you can select the ports the address is allowed to be on. Choices for allowed ports include none, all, and ports specified in a list.

Note: Be sure to include the MAC address of any router that is connected to the switch.

- Autolearn—The switch learns the first MAC address that accesses the port and afterward allows only this station to access the switch.

Note: If you power cycle the switch, it goes through a reset and loses learned MAC addresses. Ports set for autolearn will then learn the first address that passes through after the power cycle.

When the switch software detects a violation of the security, the response can be to send a trap, turn on destination address filtering, disable the port, or combine sending a trap with one of the other two actions.

For instructions to set up network access control through the console port interface, see "Setting Up Management Access Control" on page 5-12.

For instructions to set up network access control through the Web management interface, see "Setting Up Management Access Control" on page 6-11.

Managing the BayStack Switches

You can manage your BayStack 310-24T switch in any of the following four ways:

- In-band connection using SNMP (see "Network Management with SNMP" on this page)
- Out-of-band connection using the RS-232 console port interface (see "Network Management Through a Serial I/O Connection" on page 2-22)
- In-band connection using Telnet (see "Network Management Using the Telnet Interface" on page 2-22)
- In-band connection using a Web browser interface (see "Network Management Using the Web Interface" on page 2-22)

Network Management with SNMP

The BayStack 310-24T switch uses the Simple Network Management Protocol (SNMP), a communications protocol that simplifies the management of network devices. SNMP agents respond to queries sent by network management software. Responses to these queries are presented on a network management station. These agents collect the performance and activity information and forward the

data to a network management station, where network managers perform diagnostic and advanced planning operations. The use of SNMP, a common and well-defined protocol, allows the network manager to manage any SNMP-compliant device in a multivendor environment.

The Management Information Base (MIB) is a database that stores all of the collected statistics and holds them in specific structures. MIB data includes configuration and control parameters and statistical data such as the number of errors sent and received on a port.

Additional information is collected in the following MIBs:

- MIB II
- Bridge MIB
- EtherLike MIB
- RMON Groups 1, 2, 3, and 9
  - — Group 1: Stats (EtherStats table)
  - — Group 2: History (history control table, Ether history control table)

    Only EtherStats is supported by history, and the number of buckets is limited to 150.
  - — Group 3: Alarm (alarm table)
  - — Group 9: Events (event table, log table)

Note: EtherStats Alarms and Events entries are saved through a power cycle of the switch. History entries are not saved through a power cycle. Alarms, events, and logs are limited to 20 entries each.

  - — Bay Networks private MIBs: Chassis, Agent, Autotopology, VLAN, MultiLink Trunking

The BayStack 310-24T switch has a management core that gathers statistics from each of the network ports; maintains the MIB; and, when a message for the SNMP manager arrives, retrieves the information, puts it into the right form, and sends it out the appropriate port.

Access to the switch through SNMP is controlled by community names. The community names set for the switch must match those used by the SNMP management station for successful communication to occur. The switch uses two community names. The read community name allows read-only access to the device through SNMP; its default setting is “public.” The read-write community name allows read-write access; its default setting is “private.”

You can set up the community names in one of the following ways:

- Using the console interface, set SNMP parameters from the SNMP Configuration menu from the System Configuration menu (see page 5-7).
- Using the Web interface, set SNMP parameters from the SNMP Configuration page (see page 6-22).

Network Management Through a Serial I/O Connection

You can manage the BayStack 310-24T switch using a PC or terminal connected to the switch through the RS-232 console port located on the front of the switch. The serial connection allows you to view statistics and change parameter settings using the built-in console menus.

See “Connecting to the Console Port” on page 3-9 for instructions. Refer to Appendix D, “BayStack 310-24T Switch Console Interface,” for descriptions of the menus and screens you can use to manage the switch.

Network Management Using the Telnet Interface

If Telnet access to the switch is enabled, you can establish a Telnet connection to the switch using a workstation on the network. When the connection is established, you use the console menus and commands in the same way you would if using a terminal connected directly to the console port.

Network Management Using the Web Interface

The BayStack 310-24T switch supports a Web-based user interface with functionality comparable to that provided by the console interface serial I/O connection. The interface also allows you to access Help and user documentation.

For information about the Web page layout and how to use the Web interface to manage the switch, refer to Chapter 6, "Managing the BayStack 310-24T Switch Using a Web Browser." For details about all the Web pages, parameter fields, and information displays, refer to Appendix E, "Web Management Interface."

Upgrading Switch Software Through a TFTP Connection

Software upgrades are provided by Bay Networks in the form of image files that you can download into the flash memory of your BayStack 310-24T switch. Upgrades can be incorporated into your BayStack 310-24T switch by using Trivial File Transfer Protocol (TFTP) through a network connection from a networked PC or UNIX workstation acting as a TFTP file server.

Operating as a TFTP client, the BayStack 310-24T switch can open a TFTP session with a TFTP server to download the new software. You can initiate the TFTP session and download the necessary software images through the System Reset/Upgrade menu from the console/Telnet interface, from the Boot Options menu, or from the Web interface. Using the System Reset/Upgrade menu allows you to schedule the upgrade for several hours in the future, when network traffic is lighter.

For more information about downloading a software upgrade, refer to Chapter 4, "Loading Switch Software and Configuration Files."

Chapter 3
Installing the BayStack 310-24T Switch

This chapter provides the following information about installing the BayStack 310-24T switch:

- Installation requirements (this page)
- Installation procedure (page 3-2)
- Instructions for attaching devices (page 3-6)
- Instructions for the initial switch setup (page 3-15)

To further configure your BayStack 310-24T switch, refer to Chapter 4, "Loading Switch Software and Configuration Files," Chapter 5, "Managing the BayStack 310-24T Switch Using the Console Interface," and Chapter 6, "Managing the BayStack 310-24T Switch Using a Web Browser."

Installation Requirements

Before installing a BayStack 310-24T switch, verify that the package contains the following items in addition to this guide:

- A BayStack 310-24T switch
- Power cable (See "Power Cord Specifications" on page A-3.)
- Rack-mounting kit
- Warranty card

You need a Phillips screwdriver for the installation.

Install the BayStack 310-24T 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, review the environmental guidelines listed in Appendix A, "Technical Specifications."

Installation Procedure

This section provides the requirements and instructions for installing the BayStack 310-24T switch on a flat surface or in a standard 19-inch equipment 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.

Installing the BayStack 310-24T Switch on a Flat Surface

The BayStack 310-24T switch can be installed on any appropriate level surface that can safely support the weight of a switch and its attached cables. Make sure there is adequate space around the unit for ventilation and access to cable connectors.

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

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

   Feet are optional but recommended to keep the unit from slipping.

2. **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.

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

   See "Attaching Devices to the BayStack Switch" starting on page 3-6.

Installing the BayStack 310-24T Switch in a Rack

Each BayStack 310-24T switch occupies 1.75 U (single-unit) rack spaces 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.

The brackets can be installed at different locations on the side of the switch to position it in the rack. Decide how far you want the switch to extend from the rack (Figure 3-1).

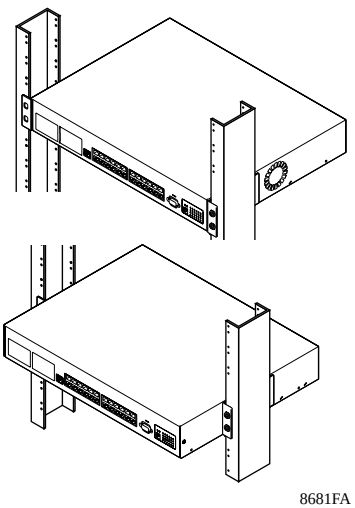


Figure 3-1. Possible Switch Positions in the Rack

The rack mounting brackets use slots in the sides of the chassis. Select the appropriate slots based on the position you want for the switch in the rack (Figure 3-1).

To install the switch in a rack:

1. **Locate the appropriate mounting slots for the rack-mounting brackets.**

   There are three slots on each side of the switch. To install the switch flush with the rack, use the front and middle slots. To install the switch so it extends in front of the rack, use the middle and back slots.

2. **Slide the brackets into the slots on the switch and insert the bracket screws through the bottom of the chassis to secure the brackets (Figure 3-2).**

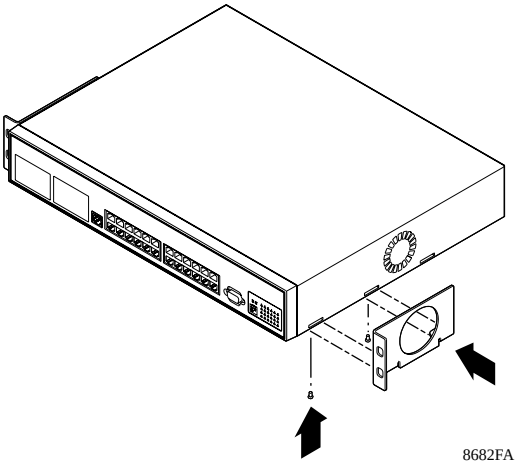
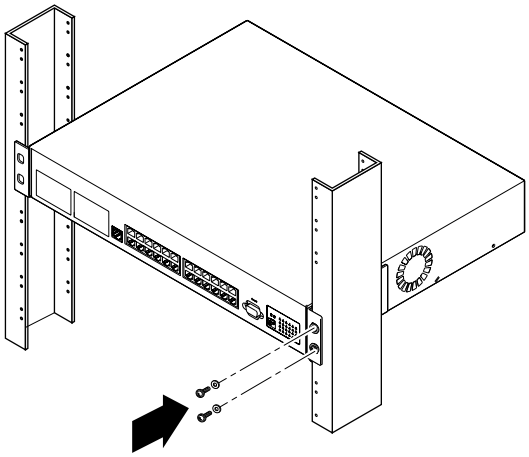


Figure 3-2. Attaching the Rack-Mounting Brackets

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



8683FA

Figure 3-3. Installing the Switch in the Rack

4. **Insert two screws, appropriate for your 19-inch rack, into each of the mounting brackets and tighten with a suitable screwdriver (Figure 3-3).**
5. **To continue installation, go to the next section, "Attaching Devices to the BayStack Switch."**

Attaching Devices to the BayStack Switch

After you have installed the BayStack 310-24T switch, you can connect it to any equipment that conforms to the IEEE 802.3 standard, such as the following devices:

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

Connecting 10BASE-T Ports

You can connect network devices to the switch using the following types of cables:

- Category 3 or 5 unshielded twisted pair (UTP) for connecting ports 1 through 24
- Category 5 UTP for connecting the 100BASE-T port on the switch or the 100BASE-T MDA
- 62.5/125 µm multimode fiber cable for connecting the 100BASE-FX port on the 100BASE-FX MDA

The 10BASE-T jacks on the BayStack 310-24T switch accept standard unshielded twisted pair (UTP) cable connections. The BayStack 310-24T switch is shipped with the 10BASE-T connectors configured as MDI-X.

To connect network devices to the 10BASE-T ports on the BayStack 310-24T switch, follow these guidelines:

- Use Category 3 or 5 UTP cable with RJ-45 connectors for the ports on the BayStack 310-24T switch.
- Use straight-through cables to connect the network interface card (NIC) in a node or server. These devices typically have MDI connectors.
- Use a crossover cable to connect to ports configured as MDI-X (such as other switches or Ethernet hubs).

The 10BASE-T ports on the BayStack 310-24T switch connect to Ethernet hubs, network devices, individual workstations, or servers through an MDI-X configured connection. Media Dependent Interface (MDI) is the IEEE standard for the interface to unshielded twisted pair (UTP) cable.

For more information about using crossover cables, see "MDI and MDI-X Connections" on page A-6.

Connecting the 10/100BASE-TX Port

The BayStack 310-24T switch contains an onboard 10/100 Mb/s port that uses autonegotiation with the connecting device to determine the wire speed. One or two additional 10/100 Mb/s ports can be added by installing 10/100BASE-TX MDAs in the MDA slots. The 10/100 Mb/s ports must use Category 5 UTP cable to accommodate the 100BASE-TX functionality. A standard RJ-45 connection (Figure 3-4) is provided to connect devices to the switch through the high-speed port. Like the 10BASE-T ports, the 10/100BASE-TX ports are configured as MDI-X.

Both the onboard port and the optional MDA ports have dedicated LEDs that indicate wire speed (10 Mb/s or 100 Mb/s) and duplex mode (half or full). See "10BASE-T Ports" on page 1-7 and "LEDs" on page 1-9 for more information.

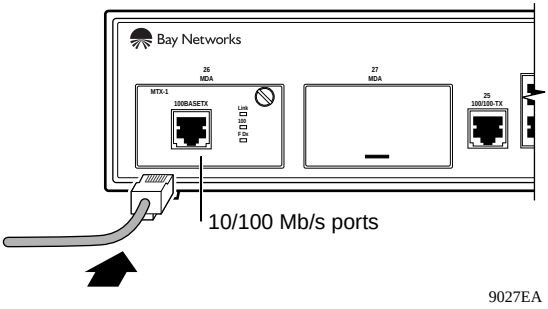


Figure 3-4. 10/100 Mb/s Port Connections

Connecting the 100BASE-FX Port

The 100BASE-FX fiber media adapter uses a multimode fiber connector to provide direct connection to other compatible Fast Ethernet devices over 62.5/125 µm multimode fiber optic cable. Connection to the 100BASE-FX port is through a standard SC connector (Figure 3-5). The 100BASE-FX media adapter can be used as a direct attachment to end stations, servers, switches, or repeaters where multimode fiber optic cabling is already installed.

Warning: The 100BASE-FX media adapter uses a Class 1 laser as a data transfer element. Be careful to avoid exposing your eyes to laser beams.

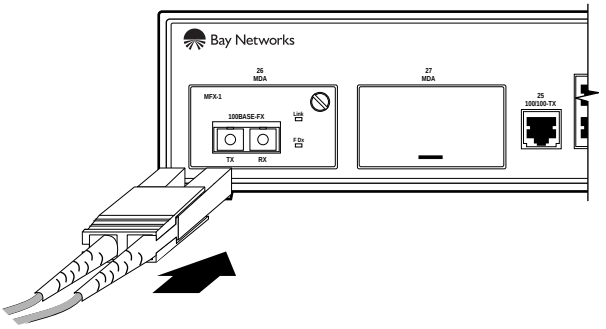


Figure 3-5. SC Connection for the 100BASE-FX MDA Port

When the BayStack 310-24T switch has valid link status, it automatically learns the MAC level station address of each attached device. If you monitor the traffic, you may initially see some extra transmissions as the switch learns the network connectivity; after that, however, the network is fully switched.

The green link LED of each port lights if you correctly cable and connect each attached device to the switch port. If the attached device is off, is disabled from sending link-status pulses, or is wired incorrectly, the link status LED of the associated switch port does not light. If this is the case, you need to determine the cause of the problem and take the appropriate corrective action.

Connecting to the Console 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 implemented as a data communication equipment (DCE) connection, using a male DB-9 connector.

See "Pin Assignments" on page A-5 for a description of the pin assignments for this connector.

To use the console 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

- 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.

To connect a terminal to the console port:

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.**
   a. **Connect the female connector of the RS-232 cable directly to the console port on the switch, and tighten the captive retaining screws (Figure 3-6).**

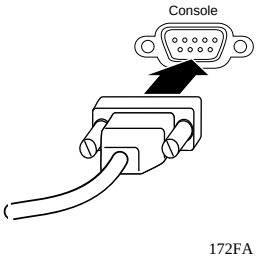


Figure 3-6. Connecting to the Console Port

   b. **Connect the other end of the cable to a terminal or the serial connector of a personal computer running communications software.**
3. **Turn on the terminal.**
4. **If the switch power is already turned on, press [Esc] to display the Main Menu.**

You can now access the configuration menus to observe self-tests and to modify operating parameters for the switch.

For instructions on using the console interface to manage the switch, see Chapter 5, "Managing the BayStack 310-24T Switch Using the Console Interface."

For descriptions of all the console menus, commands, and information fields, see Appendix D, "BayStack 310-24T Switch Console Interface."

Connecting Power

The BayStack 310-24T switch does not have a power on/off switch. When you connect the AC power cord to a suitable AC outlet, the switch powers up immediately.

To connect power to the switch:

1. **Attach the power cord to the back of the switch.**

Warning: Removing 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.

2. **Attach the other end of the power cord to a grounded AC power outlet.**

   As soon as the cord is plugged into the AC outlet, power is applied to all components in the switch.

With power applied to the switch, power-up diagnostics are performed and the switch goes into normal switch mode. To set the basic switch configuration, see "Initial Setup of a BayStack 310-24T Switch" on page 3-13. To understand the complete software interface, see Chapter 5, "Managing the BayStack 310-24T Switch Using the Console Interface" and Chapter 6, "Managing the BayStack 310-24T Switch Using a Web Browser."

When power is applied to the switch, the switch performs a series of power-on self tests. If a monitor is connected to the switch, you can observe the Power On Self Test screen display (Figure 3-7). (See "Connecting to the Console Port" on page 3-9 for instructions to connect to the console port.)

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

********************************************************************************
                              Power On Self Test

UART Local Loopback Test… PASSED
CPU Test… PASSED
Stack DRAM Test… PASSED
DRAM Test… PASSED
Watchdog Timer Test… PASSED
Timer Module Test… PASSED
FLASH Image Checksum Test… PASSED
Software Version (1.0)


Enter ".<RETURN>" to go to Boot Options Menu
Booting Switch software
Decompressing......
```

Figure 3-7. Power-On Self-Test Screen

The Boot Options Menu, accessed by pressing [.]+[Return] during the power-up sequence, provides the ability to upgrade switch software by establishing a trivial file transfer protocol (TFTP) link (see "Using the Boot Options Menu to Upgrade Switch Software" on page 4-5). The more usual methods for upgrading software are to use the System Reset/Upgrade console menu or the Reset/Upgrade page on the Web interface, or to use SNMP network management such as Optivity NMS 9.0. For instructions on upgrading switch software, refer to Chapter 4, "Loading Switch Software and Configuration Files."

Upon successful completion of the power-on self-tests, the switch is ready for normal operation. If you have a terminal or console connected to the switch, the Main Menu is displayed.

Initial Setup of a BayStack 310-24T Switch

In most cases, after installing the BayStack 310-24T switch, you can immediately begin operation using the system default settings. Minimal configuration is required when you plan to use 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. For information about managing and monitoring the switches, refer to Chapter 5, "Managing the BayStack 310-24T Switch Using the Console Interface" or Chapter 6, "Managing the BayStack 310-24T Switch Using a Web Browser."

Using Factory Default Settings

When you first turn on power to the switch, it begins operation using the factory default settings for configuration parameters. Table 3-1 lists the default values.

Table 3-1. Factory Default Settings

Type	Parameter	Default Value
Miscellaneous	High Speed Ports (Speed and Duplex)	Autonegotiation Enabled
	Ports (Enabled/Disabled)	Enabled
	Address Filtering	No Entries
	Port-Based VLANs	All ports in VLAN 1
	Uplink Ports	None
	Forwarding during broadcast storms	Enabled
Conversation Steering	Conversation steering	Disabled
	Monitored Port	None
	Monitoring Port	None
IP	IP Address	127.0.0.2
	IP Subnet Mask	0.0.0.0
	Default Gateway Address	0.0.0.0
TFTP	TFTP Server Address	0.0.0.0
	TFTP Default Gateway Address	0.0.0.0
	Download File Name	None
Reset	Reset Action	None
	Reset counter	0 (delay not in effect)

Table 3-1. Factory Default Settings (continued)

Type	Parameter	Default Value
Access	Telnet Access	Enabled
	Web Access	Enabled
	Telnet/Web/Console Password	None Assigned
	Console/Telnet Timeout	15 minutes (fixed)
SNMP	Read Community String	Public
	Read/Write Community String	Private
	Trap Receiver Server IP (1 through 4)	0.0.0.0
	Trap Receiver Community String (1 through 4)	Public
	Trap Receiver Status (1 through 4)	Unknown
	Authentication Trap Generation	Disabled
	Link Up/Down Trap Generation	Enabled
	Autotopology	Enabled
Spanning Tree Protocol	Spanning Tree Protocol	Enabled on all ports
	Aging Time (4-1000000)	300 seconds
	Bridge Priority (0-65535)	32768
	Hello Time (1 through 10)*	2 seconds
	Bridge Max Age Time (6 through 40)*	20 seconds
	Bridge Forward Delay (4 through 30)*	15 seconds
	Port Priority (0 through 255)	128
	Port Path Cost (1-65535)† • Note: 10 Mb/s ports are half duplex only	10 Mb/s Half duplex: 100 10 Mb/s Full duplex: 50 100 Mb/s Half duplex: 10 100 Mb/s Full duplex: 5
RMON	Alarm Entries	None (maximum: 20)
	Event Entries	None (maximum: 20)
	Log Entries	None (maximum: 20)
	History (history buckets)	None (maximum: 150)

* Maximum ranges are limited by the following interrelationship of these parameters:
2x (Bridge Forward Delay - 1) ≥ Bridge Maximum Age Time ≥ 2x (Bridge Hello Time +1)

† Port path cost manually set by the user will remain unchanged regardless of duplex mode.

Initial Switch Setup

The BayStack 310-24T switch is designed for plug-and-play operation. The switch can be inserted into an existing network as a hub replacement using the factory default settings, with no further configuration required. However, certain parameters must be set before the switch can be managed through the network. The default setting for the switch is to use BootP to request these parameters from a server when it is powered on for the first time. If you have set up a BootP server with the necessary files, the switch automatically retrieves its network configuration and some parameters from the server. This process updates the following parameters:

- IP address of the switch
- IP subnet mask
- Default gateway IP address
- TFTP server IP address
- Software image file name

While the switch starts the BootP download, a console message also asks you if you want to manually configure the switch. If you answer no, the system proceeds with the automatic configuration process. If you answer yes, the system prompts you to enter the following parameters:

- IP address of the switch
- IP subnet mask
- Default gateway IP address

If a BootP server is set up, the switch may be able to retrieve these parameters while you are entering the information at the console terminal.

Note: If you want the switch to obtain its configuration parameters using BootP, you must set up a BootP server before you install the switch.

If the switch cannot find a BootP server, it tries five more times to find one and then defaults to the factory settings.

When the switch finishes booting, the Main Menu is displayed (Figure 3-8). The console menu hierarchy is described in Appendix D, "BayStack 310-24T Switch Console Interface."

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                               [134.177.221.67]
MAC Address:                              [00:00:81:0a:0b:13]
Software Version:                         [1.0]
System Up Time:                           [0d:00h:53m:07s]
Switch Status:                            [Switching]
********************************************************************************

                        Main Menu

1 ---System Information
2 ---System Configuration
3 ---Troubleshooting
4 ---Management Access
5 ---System Reset/Upgrade
6 ---Exit




Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen):
```

Figure 3-8. Main Menu

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

1. **Type 2 to select System Configuration from the Main Menu.**

   The System Configuration menu is displayed (Figure 3-9).

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:01h:00m:38s]
Switch Status:                           [Switching]
********************************************************************************

                        System Configuration

1 ---Switch Network Configuration
2 ---Port/MLT Configuration
3 ---Spanning Tree Configuration
4 ---SNMP Configuration
5 ---System Characteristics
6 ---MAC-Based Address Filtering Configuration
7 ---MAC Address-Based Security
8 ---Conversation Steering
9 ---Port VLAN Configuration
0 ---Reset to Defaults

Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen):
```

Figure 3-9. System Configuration Menu

2. **Type 1 to select Switch Network Configuration from the System Configuration menu.**

   The Switch Network Configuration menu is displayed (Figure 3-10).

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:01h:00m:57s]
Switch Status:                           [Switching]
********************************************************************************

                        Switch Network Configuration

1 ---IP Address
2 ---IP Subnet Mask Address
3 ---Default Gateway Address
4 ---Spanning Tree Protocol (Enable/Disable)
5 ---BootP Request Mode
6 ---Execute BootP Now
7 ---Execute Configuration File Host Update Now




Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure 3-10. Switch Network Configuration Menu

3. **Type 1 in the command line.**

   This action refreshes the screen and displays the current IP address value.

4. **Enter the IP address of the switch in the command line and press any key to continue.**

   The new IP address value is displayed in the IP Address area of the menu.

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.

5. **Type 2 in the command line.**

   This action refreshes the screen and displays the current IP subnet mask address value.

6. **Enter the IP subnet mask address and press any key.**

   This action refreshes the screen, but the new IP subnet mask address value is not displayed in the field.

7. **Type 3 in the command line.**

   This action refreshes the screen and displays the current default gateway address value.

8. **Enter the default gateway address and press any key.**

   This action refreshes the screen, but the new value is not displayed in the field.

   This step completes the required minimum switch setup to allow management of the switch using SNMP.

When you change any of these parameters, you must reset the switch for the new values to take effect. To reset the switch, you may power cycle the switch or reset using the console interface. To use the console interface, press [Esc] twice to return to the Main Menu. Then type 5 to see the System Reset/Upgrade menu. This menu allows you to perform a software-controlled reset.

Note: Before you reset the switch, it may be useful to configure certain other parameters, such as BootP Request Mode on the Switch Network Configuration menu or Telnet and Web access and passwords in the Access Control menu (selection 4 from the Main Menu). For more information about setting these parameters, see Chapter 5, "Managing the BayStack 310-24T Switch Using the Console Interface."

Loading Switch Configuration Files and Switch Software

When you finish setting up your BayStack 310-24T switch, you can save the configuration settings as a file on a server, and later use this file to configure other BayStack 310-24T switches in your network. Also, before you fully integrate the BayStack 310-24T switches into the rest of your network, you may want to upgrade the switching software to the latest image. For instructions to use a configuration file and to upgrade switching software, refer to Chapter 4, "Loading Switch Software and Configuration Files."

Chapter 4
Loading Switch Software and Configuration Files

Software upgrades are provided by Bay Networks in the form of image files that you can download into the flash memory of your BayStack 310-24T switch. Upgrades can be incorporated into your switch by using Trivial File Transfer Protocol (TFTP) through a network connection from a networked PC or UNIX workstation acting as a TFTP file server.

In addition, when you set up switch configuration using the console menus or the Web management interface, you can save the settings as a configuration file stored on a TFTP server. Then you can configure the remaining BayStack 310-24T switches in your network by downloading the configuration file to each switch rather than setting parameters individually.

Operating as a TFTP client, the BayStack 310-24T switch can open a TFTP session with a TFTP server to download the new software or configuration file. You can initiate the TFTP session and download the necessary files through the System Reset/Upgrade menu from the console/Telnet interface, from the Boot Options menu, or from the Web interface. Using the System Reset/Upgrade menu allows you to schedule the upgrade for several hours in the future, such as at night when network traffic is lighter.

Configuring Switches Using a Configuration File

The BayStack 310-24T switch provides binary configuration file support. You cannot manually edit the file itself once it has been created. First you must set up a BayStack 310-24T switch with the parameters you want to save to a file. Then use the console interface or Web interface to upload the file to a TFTP server. Finally, download the file to other switches in the network.

Using the Console Menus

This section provides instructions for four procedures:

- Uploading a configuration file to a TFTP server
- Downloading a configuration file to a switch
- Downloading new switch software
- Downloading a configuration file and switch software at the same time

Uploading a File to a Server

To upload a file using the System Reset/Upgrade menu:

1. **From the Main Menu, type 5 to select System Reset/Upgrade (Figure 4-1).**

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                               [134.177.160.117]
MAC Address:                              [00:00:80:bb:20:44]
Software Version:                         [1.0]
System Up Time:                           [1d:02h:33m:58s]
Switch Status:                            [Switching]
********************************************************************************

                        System Reset/Upgrade

1 ---TFTP Server IP Address [134.177.160.93]
2 ---Default Gateway IP Address [134.177.160.1]
3 ---Software Image File Source [Remote / reload.wire]
4 ---Configuration File Source [Local /]
5 ---Specify Reset Action [Reset]
6 ---Set/Clear Reset Action Timer [0 min.]

0 ---Immediate Reset Action


Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure 4-1. System Reset/Upgrade Menu

2. **Type 3 to specify the software image file source, including the full path. At the prompt, select Local.**
3. **Type 4 to specify the configuration file source. At the prompt, select Remote and type the file name (such as *bs310.cfg*).**
4. **Press [Esc] to return to the Main Menu.**
5. **Type 2 to display the System Configuration menu.**
6. **Type 1 to display the Switch Network Configuration menu.**
7. **Type 7 to execute an immediate configuration file host update.**

Downloading a Configuration File to a Switch

To download a configuration file:

1. **From the Main Menu, type 5 to select System Reset/Upgrade.**
2. **Type 3 to specify the software image file source. At the prompt, select Local.**
3. **Type 4 to specify the configuration file source. At the prompt, select Remote and type the file name.**
4. **Type 5 to select a Reset Action. At the prompt, select Download.**
5. **Type 0 to execute an immediate reset action. At the prompt, answer yes.**

Downloading Switch Software

To download a switch software upgrade:

1. **From the Main Menu, type 5 to select System Reset/Upgrade.**
2. **Type 3 to specify the software image file source. At the prompt, select Remote and enter the file name (include the full path).**
3. **Enter the values for the following parameters:**
   - TFTP server IP address
   - Default gateway IP address
4. **Type 5 to select a Reset Action. At the prompt, select Download.**
5. **Type 6 to set the reset action timer and schedule the upgrade for a later time, or type 0 to execute an immediate reset action.**

Downloading Switch Software and a Configuration File

You can download a configuration file and switch software in the same operation.

To download a configuration file and switch software at the same time:

1. **From the Main Menu, type 5 to select System Reset/Upgrade.**
2. **Type 3 to specify the software image file source. At the prompt, select Remote and enter the file name (include the full path).**
3. **Type 4 to specify the configuration file source. At the prompt, select Remote and type the file name (such as *bs310.cfg*).**
4. **Type 5 to select a Reset Action. At the prompt, select Download.**
5. **Type 6 to set the reset action timer and schedule the upgrade for a later time, or type 0 to execute an immediate reset action.**

Using the Boot Options Menu to Upgrade Switch Software

You can also access the System Reset/Upgrade menu from the Boot Options Menu following a system reset. After a reset, the Power On Self Test screen is displayed (Figure 4-2).

```
**************************************************************************
Bay Networks BayStack 310-24T Ethernet Switch

**************************************************************************
Power On Self Test

UART Local Loopback Test… PASSED
CPU Test… PASSED
Stack DRAM Test… PASSED
DRAM Test… PASSED
Watchdog Timer Test… PASSED
Timer Module Test… PASSED
FLASH Image Checksum Test… PASSED
Software Version (1.0)


Enter ".<RETURN>" to go to Boot Options Menu
Booting Switch software
```

Figure 4-2. Power On Self Test Screen

To access the System Reset/Upgrade menu:

1. **Press [.]+[Return] when the Power On Self Test screen is displayed.**

   Pressing [.]+[Return] interrupts the power-up self-tests and displays the Boot Options Menu (Figure 4-3).

```
********************************************************************************
Bay Networks BayStack 310-24T Ethernet Switch
MAC Address: 00.00.00.00.00.00
********************************************************************************
Boot Options Menu

1---Upgrade Switch Software
2---Boot Switch Software
3---Clear switch configuration


Enter Command: [2]
```

Figure 4-3. Boot Options Menu

2. **Type 1 to select Upgrade Switch Software.**

   The System Reset/Upgrade menu is displayed (Figure 4-1 on page 4-2).

3. **Continue with steps 2 through 5 under "Downloading Switch Software" on page 4-3.**

Using the Web Interface

You can also perform or schedule software upgrades or configuration file downloads through the Web interface. You start from the Reset/Upgrade page (Figure 4-4).

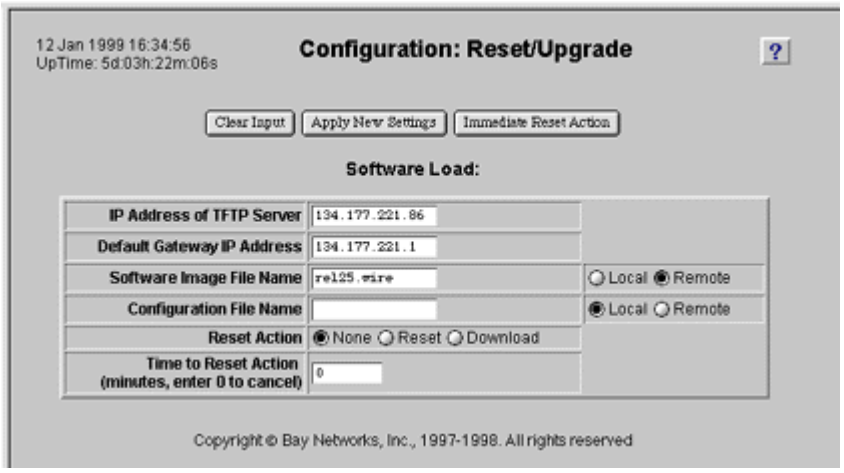


Figure 4-4. Reset/Upgrade Web Page

To upload a configuration file to a server:

1. **On the Reset/Upgrade page, enter the IP address of the TFTP server and the default gateway IP address.**
2. **Enter the Configuration File name and click on Remote.**
3. **Click on Apply New Settings.**
4. **Click on Configuration: System in the Navigation Bar.**
5. **On the System page, click on Execute Configuration File Host Update Now.**

To download a configuration file to a switch:

1. **On the Reset/Upgrade page, enter the IP address of the TFTP server and the default gateway IP address.**
2. **Enter the Configuration File name and click on the Remote radio button.**
3. **Click on Apply New Settings.**
4. **To specify the Reset Action, click on the Download radio button.**
5. **Click on the Immediate Reset Action task button.**

To upgrade software:

1. **On the Reset/Upgrade page, enter the IP address of the TFTP server and the default gateway IP address.**
2. **Enter the Software Image File name and click on Remote.**
3. **Click on Apply New Settings.**
4. **To specify the Reset Action, click on the Download radio button.**
5. **To schedule a delayed software download, enter a value in the Time to Reset Action field (up to 65535 minutes), and click on Apply New Settings to set.**
6. **To download immediately, click on Immediate Reset. This action overrides any previous settings.**

Note: The switch will reset twice during the upgrade process. Do not power down the switch before the process is completed (approximately 10 minutes).

Chapter 5
Managing the BayStack 310-24T Switch Using the Console Interface

This chapter describes using the console or Telnet interface to access the agent software that provides management and configuration control of the BayStack 310-24T switch. For information about using the Web interface, refer to Chapter 6, "Managing the BayStack 310-24T Switch Using a Web Browser." For descriptions of all the console menus and options, refer to Appendix D, "BayStack 310-24T Switch Console Interface." Refer to Chapter 3, "Installing the BayStack 310-24T Switch," for installation, connection, and initial configuration procedures.

This chapter includes the following information:

- Requirements for using the console or Telnet interface (this page)
- A description of how the menus and screens are set up (page 5-2)
- Instructions for performing management tasks (starting on page 5-12)
- Instructions for accessing the console interface using a Telnet connection (page 5-35)

Accessing the Console Interface

To access the console interface, you must connect a terminal or a computer with terminal-emulation software to the console port on the switch.

To connect the terminal or computer to the switch:

1. **Set the terminal protocol.**
2. **Connect the terminal (or a computer in terminal-emulation mode) to the console port using the RS-232 cable.**
3. **Turn on the terminal.**
4. **If the switch power is already turned on, press [Esc] to display the Main Menu.**

For more details about the terminal and cable requirements, refer to "Connecting to the Console Port" on page 3-9.

For instructions to set up and use a Telnet connection, refer to "Network Management Using a Telnet Connection" on page 5-35.

Menus and Screens

The agent software on the BayStack 310-24T switch provides menus and screens that allow you to configure and manage your network environment. A menu provides the ability to set and change parameters, and a screen presents current status and parameter settings. The menus and screens can be accessed from the console or through a Telnet connection.

The menus and screens of the console and Telnet interface include the following three distinct areas (Figure 5-1):

- Switch status area
- Central screen area—menu commands and status
- Navigation commands and command line area

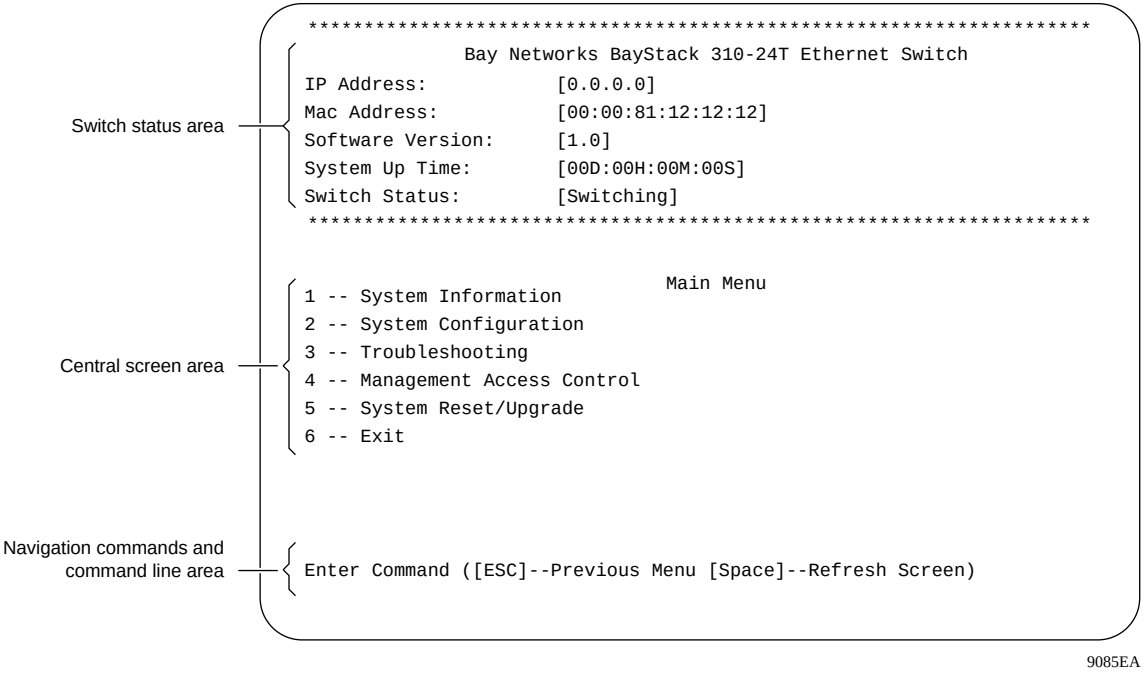


Figure 5-1. Menu and Screen Areas

Switch Status Area

The switch status area appears in the top portion of each menu and screen. This area contains the information necessary to identify the BayStack switch and see its current status. The switch status area provides the following information:

- IP address
- MAC address
- Software version
- System uptime
- Switch status

Central Screen Area

The central screen area is used to present lists of system menus, status information, and switch parameters. In this area, information displayed in square brackets ([ ]) indicates current settings.

When you select a parameter to enter new data, the screen refreshes and the command line displays the current parameter setting followed by space for you to enter the new parameters.

Navigation Commands and Command Line Area

The navigation commands display the control key commands that are used to move through the menu hierarchy. Some commands are displayed on all menus and screens while others are displayed only on particular menus and screens. The control key is displayed as [ctrl-] on the screen. The following navigational commands are used in the menus and screens:

- [Esc]—Escape

  Pressing Escape returns you to the previous menu within the menu structure. To view the Language selection menu, press [Esc] from the Main Menu.

- [ctrl-n]—Next Page

  When the displayed information requires additional pages, press [Control]+[n] to scroll through all the information.

- [ctrl-p]—Previous Page

  Press [Control]+[p] to return to the previously displayed page when displayed information requires more than one page.

You use the command line and response area to enter menu selections and to change parameter data.When changing parameter data, the command line displays the current parameter and waits for you to enter the new data, as shown below:

```
Enter Default Gateway Address: [0.0.0.0]
```

Values enclosed in square brackets indicate the current settings.

The cursor ( ) prompts you to enter a new default gateway address. Enter the new data in the command line.

Typing [Control]+[u] in a Configuration screen clears the information strings you have entered, except for Access Control screen password information.

Typing [Control]+[d] at any time terminates a console or Telnet session.

If you enter parameter values that are out of the acceptable range, an “Out of Range” message is displayed, and the values are not accepted.

The Telnet and console interface inactivity timeout is 15 minutes. Inactive sessions are automatically terminated after that time has elapsed.

Initial Switch Setup

When you install a new BayStack 310-24T switch, the switch needs certain parameters set before it can be managed through the network. The default setting for the switch is to retrieve its configuration settings using BootP. The switch immediately tries to find a BootP server. At the same time, a console menu asks you if you want to manually configure the switch. If you answer no, the system proceeds with the automatic configuration process. If you answer yes, the system prompts you to enter the following parameters:

- IP address of the switch
- IP subnet mask
- Default gateway IP address

If a BootP server is set up, the switch may be able to retrieve these parameters while you are entering the information at the console terminal.

Note: If you want the switch to obtain its configuration parameters using BootP, you must set up a BootP server before you install the switch.

Using BootP for Switch Configuration

The BayStack 310-24T switches are set for configuration using BootP as the default. When you power on the switch for the first time, it tries to find a BootP server from which it can download its network parameters. If the switch cannot find a BootP server, it tries five more times to find one and then defaults to the factory settings. If the server is set up with the correct information, the switch downloads the following network parameters:

- IP address of the switch
- IP subnet mask
- Default gateway IP address
- TFTP server IP address
- Software image file name

You can customize the conditions for BootP configuration using the Switch Network Configuration Menu.

To set up the conditions for BootP configuration:

1. **From the System Configuration menu, type 1 to display the Switch Network Configuration Menu.**
2. **Type 5 to set the BootP Request Mode parameter.**
3. **At the prompt, select one of the following settings:**
    - 1: When Needed (default setting)—If the IP address stored in the nonvolatile memory is the factory default value (127.0.0.2), the switch uses BootP to request configuration settings. If the stored IP address is different from the factory default value, the switch uses the stored network parameters.
    - 2: Always—The switch boots, ignoring any stored network parameters, and uses BootP to request network configuration parameters. If the BootP request fails, the switch continues to send BootP requests at one-minute intervals. This setting disables remote management if no BootP server is set up for the switch, but it allows the switch to operate normally.
    - 3: Disabled—The switch boots using the IP configuration parameters stored in nonvolatile memory. If a BootP configuration is in progress when you issue this command, the BootP configuration stops.

- 4: Last Address—At startup, the switch tries to obtain its IP configuration using BootP. If the BootP request fails, the switch uses the network parameters stored in its nonvolatile memory.

Note: When the switch uses BootP to obtain network parameters, it updates the existing parameters only if the new ones are valid values for the parameters. Valid parameters obtained using BootP always replace current information stored in the nonvolatile memory.

4. **If you want to execute a BootP request, type 6.**

   The switch immediately sends a BootP request.

Configuring the Switch Manually

If a BootP server is not set up, you must perform the initial switch configuration using the Switch Network Configuration Menu.

To set the switch parameters:

1. **From the Main Menu, type 2 to display the System Configuration Menu.**
2. **From the System Configuration Menu, type 4 to display the SNMP Configuration Menu.**
3. **For each parameter, type the command number.**

   If a value exists for the parameter, that value is displayed on the screen.
4. **Type the new value and press [Enter].**

Loading Switch Software and Configuration Files

You can download the latest switch software to the switch or you can create a configuration file to be used for configuring other switches in the network. This section includes the following four procedures:

- Uploading a configuration file to a TFTP server
- Downloading a configuration file to a switch
- Downloading new switch software
- Downloading a configuration file and switch software at the same time

Uploading a File to a Server

To upload configuration files:

1. **From the Main Menu, type 5 to select System Reset/Upgrade (Figure 5-2).**

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                               [134.177.160.117]
MAC Address:                              [00:00:80:bb:20:44]
Software Version:                         [1.0]
System Up Time:                           [1d:02h:33m:58s]
Switch Status:                            [Switching]
********************************************************************************

                        System Reset/Upgrade

1 ---TFTP Server IP Address [134.177.160.93]
2 ---Default Gateway IP Address [134.177.160.1]
3 ---Software Image File Source [Local / reload.wire]
4 ---Configuration File Source [Local /]
5 ---Specify Reset Action [Reset]
6 ---Set/Clear Reset Action Timer [0 min.]

0 ---Immediate Reset Action


Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure 5-2. System Reset/Upgrade menu

2. **Type 3 to specify the software image file source, and at the prompt, select Local.**
3. **Type 4 to specify the configuration file source. At the prompt, select Remote and type the file name (such as *bs310.cfg*).**
4. **Press [Esc] to return to the Main Menu.**
5. **Type 2 to display the System Configuration menu.**
6. **Type 1 to display the Switch Network Configuration menu.**
7. **Type 7 to execute an immediate configuration file host update.**

Downloading a Configuration File to a Switch

To download a configuration file:

1. **From the Main Menu, type 5 to select System Reset/Upgrade.**
2. **Type 3 to specify the software image file source. At the prompt, select Local.**
3. **Type 4 to specify the configuration file source. At the prompt, select Remote and type the file name.**
4. **Type 5 to select a Reset Action. At the prompt, select Download.**
5. **Type 0 to execute an immediate reset action. At the prompt, answer yes.**

Downloading Switch Software

Software upgrades are provided by Bay Networks in the form of image files that you can download into the flash memory of your BayStack 310-24T switch. You can incorporate upgrades into your BayStack 310-24T switch using TFTP through a network connection from a networked PC or UNIX workstation acting as a TFTP file server. Operating as a TFTP client, the BayStack 310-24T switch can open a TFTP session with a TFTP server to download the new software. You can schedule the upgrade for several hours in the future, when network traffic is lighter.

To download a switch software upgrade:

1. **From the Main Menu, type 5 to select System Reset/Upgrade.**
2. **Type 3 to specify the software image file source. At the prompt, select Remote and enter the file name.**
3. **Type 5 to select a Reset Action. At the prompt, select Download.**
4. **Type 6 to set the reset action timer and schedule the upgrade for a later time, or type 0 to execute an immediate reset action.**

You can also access the System Reset/Upgrade menu from the Boot Options menu following a system reset. After a reset, the Power On Self Test screen is displayed. If you press [.]+[Return] while the Power On Self Test screen is displayed, the power-up self-tests are interrupted and the Boot Options menu is displayed (Figure 5-3).

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch
MAC Address: 00.00.00.00.00.00
********************************************************************************
                                Boot Options Menu


1---Upgrade Switch Software
2---Boot Switch Software
3---Clear Switch Configuration


Enter Command: [2]
```

Figure 5-3. Boot Options Menu

Type 1 to display the System Reset/Upgrade menu. The follow steps 2 through 4 under "Downloading Switch Software" on page 5-9.

Downloading Switch Software and a Configuration File

You can download a configuration file and switch software in the same operation.

To download a configuration file and switch software at the same time:

1. **From the Main Menu, type 5 to select System Reset/Upgrade.**
2. **Type 3 to specify the software image file source. At the prompt, select Remote and enter the file name (include the full path).**
3. **Type 4 to specify the configuration file source. At the prompt, select Remote and type the file name (such as *bs310.cfg*).**
4. **Type 5 to select a Reset Action. At the prompt, select Download.**
5. **Type 6 to set the reset action timer and schedule the upgrade for a later time, or type 0 to execute an immediate reset action.**

Setting the Management Access Password

To set the management access password:

1. **From the Main Menu, type 4 to display the Management Access menu (Figure 5-4).**

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                               [134.177.155.153]
MAC Address:                              [00:00:81:0b:82:f4]
Software Version:                         [2.1]
System Up Time:                           [1d:20h:07m:15s]
Switch Status:                            [Switching]
********************************************************************************

                        Management Access

1 ---Telnet Access (enable/disable)
2 ---Web Access (enable/disable)
3 ---Change Password
4 ---Management Access Control




Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure 5-4. Management Access Menu

2. **Type 3 to change the password (or set one initially).**
3. **At the prompts, enter the old password, if one exists, followed by the new password, then the new password again for verification.**

Setting Up Management Access Control

Management access control limits access to the switch configuration functions. It is set up through the Management Access menu. (You cannot set up management access control using SNMP.) Management access control is based on IP addresses allowed to access management functions. You can specify a list of up to eight IP addresses, each of which can access the switch through the Web, Telnet, or SNMP. These settings are independent of the password protection available for access to the console port interface. If you set a password, it is still required for access from the authorized IP addresses.

To set up management access control:

1. **From the Main Menu, type 4 to display the Management Access menu.**
2. **Use commands 1 and 2 to enable or disable Telnet and Web access to the switch management functions.**
3. **Type 4 to display the Management Access Control Menu.**
4. **If you selected Restricted, type 2 to modify the list of IP addresses allowed to access the switch management functions.**
5. **On the Modify IP Address List Menu, enter up to eight IP addresses; for each address, enable or disable Telnet, Web, and SNMP access.**

Caution: Make sure you include the IP address of your own management station if you set up management access control remotely. Otherwise, you may be locked out accidentally.

6. **Type 1 to set the management access control mode, and select 1 (Restricted) or 2 (Unrestricted).**

   In unrestricted mode (the default setting), the switch is accessible to all users. In restricted mode, access is restricted to up to eight stations whose IP addresses have been authorized for management access.

To delete an IP address from the switch, type the number of the IP address in the list. When the screen prompt asks if you want to remove the address, type y for yes.

To delete all IP addresses, use the 0 (zero) command.

Note: Make sure you specify at least one IP address for restricted access. If you select restricted management access but do not specify IP addresses, access to the switch is still unrestricted. If you have specified a trap receiver, traps will be sent for each violation.

Setting Up MAC Address-Based Network Security

MAC address-based security allows you to monitor and minimize unauthorized network access by restricting access to unauthorized stations based on their MAC addresses. You can establish two types of security: single MAC address per port or MAC address list. You can also specify the action to be taken if a violation occurs.

Note: Ports configured in uplink mode do not perform MAC address learning and are not subject to security enforcement.

This section describes the basic tasks required for the initial setup of MAC address-based security. Perform the setup tasks in the following order:

1. Specify the stations that can use the ports. Select either single MAC per port or MAC list as the security mode, and enter MAC addresses as needed (see "Specifying Stations that Can Access the Switch Ports" next).
2. Select the action to be taken if a violation occurs (page 5-16).
3. Specify whether or not to allow SNMP write access to the security functions (page 5-16).
4. After all the other security parameters are set, enable MAC address-based security (page 5-17).

Specifying Stations that Can Access the Switch Ports

To specify the stations that can access switch ports:

1. **From the Main Menu, type 2 to display the System Configuration menu.**
2. **From the System Configuration menu, type 7 to display the MAC Address-based Security menu (Figure 5-5).**

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.155.79]
MAC Address:                             [00:00:81:3a:02:36]
Software Version:                        [2.1]
System Up Time:                          [0d:17h:37m:24s]
Switch Status:                           [Switching]
********************************************************************************

                        MAC Address-based Security

1 ---Security Status: [Disabled]
2 ---SNMP Security Configuration: [Locked]
3 ---Security Mode: [Single-MAC-per-port]
4 ---Security Action: [noAction]
5 ---Add/Modify Allowed MAC Address
6 ---Add/Modify Not-Allowed MAC Address
7 ---Delete DA Filter MAC Address
8 ---Allowed MAC Address Lookup




Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure 5-5. MAC Address-based Security Menu

3. **Type 3 to set the security mode.**

   The following prompt is displayed:

   ```
   Select Security Mode (1:Single-MAC-per-port 2:MAC-list):
   ```

Select one of the following modes:

- 1: Single-MAC-per-port (default)—Only one MAC address is allowed per port (and only one port can be specified for each allowed MAC address). Any other address learned on that port triggers the specified security action.
- 2: MAC-list—You can apecify a list of MAC addresses that are allowed to connect to the switch; for each address, you can specify the individual ports it can connect to. You can choose no ports, all ports, or a list of ports.
- 3: Autolearn—Tthe switch learns the first MAC address that access a port and afterward allows only that MAC address to access the port.

Note: When you change the security mode, all the entries are deleted from the lists of allowed and not-allowed MAC addresses. You must reenter MAC addresses in the lists.

4. **Use the following commands to specify the allowed MAC addresses:**

   - 5—Add/Modify Allowed MAC Address

     The following prompt is displayed:

     ```
     Enter Allowed MAC Address: (xx:xx:xx:xx:xx:xx):
     ```

     MAC addresses are case sensitive.

     When you enter a MAC address, you are prompted to enter one or more port numbers (only one for Single-MAC-Per-Port mode).

Note: Make sure the MAC address of the management station is on the list of allowed addresses before you turn on the security feature. If a router is connected to the switch, make sure the MAC address of the router is in the list of allowed addresses.

   - 6—Add/Modify Not-Allowed MAC Address

     At the prompts, enter a MAC address and port numbers.

Note: The Single-MAC-per-port setting does not support a not-allowed MAC list. If you try to enter a not-allowed MAC address when this mode is selected, an error message is displayed.

Specifying the Security Action

When you have specified the stations that can or cannot access switch ports, you must specify the action to be taken if a security violation occurs. To specify the security action:

1. **From the MAC Address-based Security menu, type 4.**
2. **Select one of the following actions:**
   - 1—No action
   - 2—Send a trap to the network management software (default)
   - 3—Enable destination address filtering on that address
   - 4—Enable destination address filtering on that address and send a trap
   - 5—Partition the port
   - 6—Partition the port and send a trap

Note: If you change the action from destination address filtering to some other action, you must manually remove the destination address filters that have been set up by the security feature.

Setting SNMP Access

You can enable or disable SNMP access to security settings for the switch. If you enable SNMP access, the security settings can be changed from a management station using SNMP-based network management software such as Bay Networks Optivity software.

To set SNMP access to switch security settings:

1. **From the System Configuration menu, type 7 to display the MAC Address-based Security menu.**
2. **Type 2 to set the SNMP security configuration.**

   The following prompt is displayed:

   ```
   Select SNMP Security Configuration (1:locked 2:unlocked):
   ```

3. **Select either Locked or Unlocked.**

   If you select Locked, the security settings cannot be changed from Optivity or other SNMP-based network management software. You can change the settings only from the console port interface.

Enabling MAC Address-Based Security

After you have set up the operating parameters, you can enable MAC address-based security. Check the following items before you enable security:

- Make sure the MAC address of the management station is on the list of allowed MAC addresses.
- If a router is attached to the switch, make sure the MAC address of the router is on the list of allowed addresses.

To enable MAC address-based security:

1. **From the MAC Address-based Security menu, type 1.**

   The following prompt is displayed:

   ```
   Select Security Status (1:Enable 2:Disable):
   ```

2. **Type 1 to select Enable.**

   MAC address-based security is enabled. The switch monitors port usage and takes the security actions you have specified.

Modifying MAC Address-Based Network Security

This section describes other management tasks for MAC address-based security in the switch. This section includes the following tasks:

- Changing the allowed MAC address list and not-allowed MAC address lists (this page)
- Verifying MAC addresses (page 5-19)
- Disabling MAC address-based security (page 5-19)

Changing the MAC Address Lists

You can change the MAC address lists from the MAC Address-based Security menu in several ways.

To delete a single allowed MAC address:

1. **Type 5 to add or modify the allowed MAC address list.**

   At the prompt, enter the MAC address you want to delete.

2. **A screen prompt asks for a port number. Instead of entering a port number, press [Ctrl] + u.**

   The address is deleted.

To delete all MAC addresses, change the security mode and then change it back.

One of the possible security actions is to set up destination address (DA) filtering on a port. You can delete single MAC addresses for filtering, or you can clear all filters that have been created by the security feature.

To delete a single destination address filter MAC address:

1. **Type 7 to delete a destination filter MAC address.**
2. **At the prompt, enter the MAC address.**

Note: This command applies only to destination addresses that are part of the security feature and does not affect user-specified filters set from the System Configuration Menu.

To delete all destination address filters that have been created by the security feature:

1. **Use command 1 to disable security.**

   This action clears all the security-based destination filters.

2. **Use command 1 to reenable security.**

   Security is reenabled with no destination address filters set as part of the MAC address-based security.

Verifying MAC Addresses

To verify a single MAC address:

1. **From the MAC Address-based Security menu, type 8.**
2. **At the prompt, enter the MAC address you are checking.**

   A message is displayed showing the port number that MAC address is allowed to access or the port that address is not allowed to access.

Note: To display a list of all allowed MAC addresses for the switch, use the Security: Network Access page in the Web management interface.

Disabling MAC Address-Based Security

To disable MAC address-based security:

1. **From the MAC Address-based Security menu, type 1.**
2. **Select option 2 (Disabled).**

Disabling MAC address-based security removes all destination address filters created during operation of the security feature.

If ports have been partitioned by the MAC address-based security, they are not automatically unpartitioned when you disable the security feature. You must manually enable the ports from the Port Configuration menu.

Setting Up Spanning Tree Protocol Operation

The BayStack 310-24T switches can have different settings on different ports for Spanning Tree Protocol operation. The factory default setting for a switch is to boot with spanning tree enabled on all ports. You can disable spanning tree on all ports or selectively disable it on individual ports. In addition, you can set all the spanning tree ports or individual ports for Fast Start connection.

Note: Spanning Tree Protocol resolves duplicate paths in networks and is not necessary for ports that have workstations directly attached to the switch. When Spanning Tree Protocol is enabled on these ports (the default), workstations are unable to attach to servers for a few seconds until Spanning Tree Protocol stabilizes.

Setting up spanning tree operation consists of the following general tasks:

1. Check the current state of Spanning Tree Protocol in the switch (see page 5-21). Because the default setting is Spanning Tree Protocol enabled for the entire switch, you may not need to do any further configuration of spanning tree operation for your switch. If you want to customize the spanning tree operation, you can proceed with the remaining tasks.
2. If you want to customize spanning tree operation for the switch or for selected ports, make sure Spanning Tree Protocol is enabled for all ports (page 5-21). If necessary, set the Spanning Tree Protocol parameters using the Spanning Tree General Configuration Menu (step 3 on page 5-22). Then use the Port Configuration Menu to disable Spanning Tree Protocol on ports where you do not want it to operate (step 6 on page 5-23).
3. If you want the switch or selected ports to use Fast Start spanning tree instead of IEEE 802.1d spanning tree, see the procedures starting on page 5-24.

Checking the Current Spanning Tree Protocol State

To check the current spanning tree state from the console port interface:

1. **From the Main Menu, type 1 to display the System Information Menu.**
2. **Type 1 to display the Switch Information Menu.**

   The Switch Information display includes the current mode selected for spanning tree operation (either Enabled or Disabled).

If Spanning Tree Protocol is enabled (the default), you may not need to set any other switching parameters. The switch is ready to operate in most network environments. If you want to customize the port settings, continue to the next section.

Enabling Spanning Tree Protocol

If Spanning Tree Protocol is disabled for the switch, you must enable it on all ports before you can customize operation for selected ports.

To enable Spanning Tree Protocol:

1. **From the Main Menu, type 2 to display the System Configuration Menu.**
2. **Type 1 to display the Switch Network Configuration Menu.**
3. **Type 4 to set Spanning Tree Protocol operation for the entire switch.**

   The screen displays the following prompt:

   `Enter selection of STP (1:Enable 2:Disable) [`*current mode*`]:`
4. **Type 1 to enable Spanning Tree Protocol.**

Customizing Spanning Tree Protocol Operation

You can set overall Spanning Tree Protocol parameters for the switch, or you can disable Spanning Tree Protocol on some (or all) ports. You can also set individual ports for Fast Start Spanning Tree Protocol operation, which allows ports to reach a Forwarding state faster than IEEE 802.1D operation does.

To customize the Spanning Tree Protocol operation:

1. **From the Main Menu, type 2 to display the System Configuration Menu.**
2. **Type 3 to display the Spanning Tree Configuration Menu (Figure 5-6).**

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.155.79]
MAC Address:                             [00:00:81:3a:02:36]
Software Version:                        [2.1]
System Up Time:                          [0d:17h:28m:49s]
Switch Status:                           [Switching]
********************************************************************************

                        Spanning Tree Configuration

1 ---General Configuration
2 ---Port Configuration
3 ---STP Mode for ALL Spanning Tree Ports









Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure 5-6. Spanning Tree Configuration Menu

3. **To set overall spanning tree operation, type 1 to display the Spanning Tree General Configuration Menu. (If you are not modifying these parameters, go directly to step 6.)**

   The Spanning Tree General Configuration Menu is displayed. This menu allows you to set the following Spanning Tree Protocol parameters for the entire switch:

   - 1—Aging time
   - 2—Bridge priority
   - 3—Bridge hello time
   - 4—Bridge maximum age time
   - 5—Bridge forward delay

4. **For each parameter you set, type the option number and respond to the prompt by entering the parameter value.**

   For descriptions of the parameter meanings, refer to "Spanning Tree General Information" on page D-14.

5. **From the Spanning Tree General Configuration menu, press [Esc] to return to the Spanning Tree Configuration menu.**

6. **To enable or disable spanning tree for individual ports, type 2 to display the Port Configuration Menu.**

The Spanning Tree Port Configuration Menu is displayed. This menu allows you to select a port and enable or disable spanning tree for that port.

Note: When you connect a BayStack 310-24T switch to another switch or bridge, Spanning Tree Protocol must be enabled on all the interconnecting ports for reliable loop detection. Disabling Spanning Tree Protocol on individual ports connecting switches or bridges may cause loops to go undetected when redundant links are used between devices.

7. **Type the number of each port you want to configure.**

   The following prompt is displayed:

   `Connectivity on Port` *n*`: (1:Enable 2:Disable) [`*current mode*`]:`

Note: In this prompt, Enable and Disable refer to the ability of the port to carry traffic and not to the state of Spanning Tree Protocol.

8. **Type 1 or 2 to select Enable or Disable for each port you are configuring, or press [Return] to maintain the current value.**

9. **If you select Enable, respond to the following prompts to select operating parameters for Spanning Tree Protocol on this port:**

   `STP Mode (1:802.1D, 2:FastStartSTP, 3:NoSTP)for Port` *n* [*current mode*]:

   Type 1, 2, or 3 to select a mode for Spanning Tree Protocol operation, or press [Return] to leave the current setting active.

   `Enter Port Priority for Port` *n*:

   Enter a value or press [Return] to leave the current value active.

   `Enter Port Path Cost for Port` *n*:

   Enter a value or press [Return] to leave the current value active.

Setting or Disabling Fast Start Operation for the Switch

The Spanning Tree Configuration Menu provides a convenient way to set the spanning tree mode for the entire switch with a single command. (This command affects only ports with Spanning Tree Protocol enabled.) The default setting for Spanning Tree Protocol is IEEE 802.1d operation. Fast Start mode allows ports to reach the Forwarding state faster than they do in IEEE 802.1d operation.

To set all the spanning tree ports on the switch for Fast Start operation:

1. **From the Main Menu, type 2 to display the System Configuration Menu.**
2. **Type 3 to display the Spanning Tree Configuration Menu.**
3. **Type 3 to set the spanning tree mode for the ports with Spanning Tree Protocol enabled.**
4. **At the prompt, select one of the following modes:**
   - 802.1d—follows the IEEE 802.1d standard for reaching the Forwarding state. This process typically takes approximately 30 seconds.
   - Fast Start STP—allows ports to transition to the Forwarding state faster than it does in the 802.1d mode. With a standard Bridge Hello time of 2 seconds, this faster transition provides connection to stations within 4 seconds of the time the link is established.

Note: Enabling or disabling Fast Start operation does not affect any ports that have spanning tree operation disabled.

Verifying System Information

Before you change parameters for the BayStack 310-24T switch, it may be useful to verify the current settings. To verify these settings from the console interface, you use the System Information screens. All the screens associated with system information are read only. To change any parameter or setting, you must go through the System Configuration menu, except for the Forwarding During Broadcast Storm option, which is enabled or disabled from the Troubleshooting menu.

To verify switch parameter settings:

1. **From the Main Menu, type 1 to display the System Information menu.**

   The System Information menu is displayed. This menu includes four options for displaying specific categories of information. The following options are available from this menu:

   1—Switch Information

   2—SNMP Information

   3—Spanning Tree Information

   4—Port Statistics and Status Information

2. **Type the number that corresponds to the screen you want to look at.**

For definitions of the system parameters and default values, see Appendix D, "BayStack 310-24T Switch Console Interface."

Setting SNMP Parameters

The SNMP Configuration menu allows you to specify parameters and addresses for the SNMP management of the switch. You can specify the following parameters:

- SNMP Read Community string
- SNMP Read/Write Community string
- Up to four trap receivers with community strings
- Generation of authentication traps
- Generation of link up/link down traps

To set the SNMP parameters:

1. **From the Main Menu, type 2 to display the System Configuration menu.**
2. **Type 4 to display the SNMP Configuration menu.**
3. **Type the number of each parameter you are setting.**
4. **At each screen prompt, enter the requested information.**

Setting the System Characteristics

System characteristics provide general identifying information about the switch, such as a name for the switch, its location, and the name of a contact person.

To set the system characteristics for the switch:

1. **From the Main Menu, type 2 to display the System Configuration menu.**
2. **Type 5 to display the System Characteristics menu.**
3. **Type the option number for each characteristic you are setting, and enter the requested information.**

Note: To operate correctly with the Web interface, the System Contact parameter should be in the form of an Internet e-mail address.

Setting Up Address Filtering

You can enter up to eight MAC addresses for destination address filtering. The switch will drop all incoming packets destined to any of these addresses.

To set up destination address filtering:

1. **From the Main Menu, type 2 to display the System Configuration menu.**
2. **Type 6 to display the MAC-Based Address Filtering Configuration menu.**
3. **Enter the command number for each successive filter and then the MAC address to be excluded.**

   An additional option (0) allows you to remove all existing filters.

For a more detailed explanation of this feature, refer to "MAC Address-Based Filtering" on page 2-17.

Setting Up High-Speed Ports and Multilink Trunking

The high-speed ports on the BayStack 310-24T switch are port 25 (the fixed port) and optional ports on installed MDAs (ports 26 and 27). For these ports, you can specify the operating speed, duplex mode, and address learning mode. You can also designate these ports as members of a multilink trunk. For more information about address learning, refer to "Address Learning" on page 2-16. For information about interswitch ports, refer to "Virtual LANs" on page 2-4.

To set up one or more high-speed ports:

1. **From the Main Menu, type 2 to display the System Configuration menu.**
2. **From the System Configuration menu, type 2 to display the Port/MLT Configuration menu.**

   If necessary, press [Ctrl]+[p] or [Ctrl]+[n] until the configuration parameters for ports 25 through 27 are displayed (Figure 5-7).

```
********************************************************************************
               Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:01h:03m:54s]
Switch Status:                           [Switching]
********************************************************************************

                        Port/MLT Configuration

Command             Autonegotiation              Duplex
1 ---Port 25        Enabled                      Half Duplex
              Normal/100 Mbps/MLT
2 ---Port 26        Disabled                     Full Duplex
              Normal/100 Mbps/Fiber/MLT
3 ---Port 27        Enabled                      Full Duplex
              Normal/100 Mbps/Copper/No MLT
4 ---MLT Selection
5 ---Port 1-24 Configuration

[ctrl-n]---Next Page    [ctrl-p]---Previous Page
Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen):
```

Figure 5-7. Port/MLT Configuration Menu

3. **Select a port.**

   The following prompts are displayed, one at a time:

   ```
   Enter Port Autonegotiation Mode (1:enable 2:disable): [Disabled]
   Enter Address Learning Mode (1:Uplink 2:Normal): [Normal]
   Enter Port Speed (1:100 2:10): [100]
   Enter Port Duplex Mode (1:half 2:full): [Half Duplex]
   ```

   The Enter Port Speed and Enter Port Duplex Mode lines appear only if autonegotiation is not enabled.

   For each prompt, select the appropriate value. If you plan to set up a multilink trunk and you want it to operate in uplink mode, set the ports to uplink mode at this time. This setting disables address learning on the trunk ports.

4. **To set up or modify a multilink trunk, type 4.**

5. **Select an option to group any two or all three high-speed ports as a multilink trunk, or select zero (0) for no trunking group.**

Assigning Ports to VLANs

You can create as many as 31 virtual networks (VLANs) and assign each switch port to any one of the VLANs.

To assign ports to VLANs:

1. **From the Main Menu, type 2 to display the System Configuration menu.**

2. **Type 9 to display the Port VLAN Configuration menu (Figure 5-8).**

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                               [134.177.221.67]
MAC Address:                              [00:00:81:0a:0b:13]
Software Version:                         [1.0]
System Up Time:                           [0d:01h:18m:40s]
Switch Status:                            [Switching]
********************************************************************************

                        Port VLAN Configuration

1 ---Create/Modify VLAN
2 ---Delete VLAN
3 ---Display VLAN
4 ---Add InterSwitch Port
5 ---Delete InterSwitch Port
6 ---Display InterSwitch Port
7 ---Configure CPU VLAN [1]


0 ---Reset All Ports to default VLAN 1


Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure 5-8. Port VLAN Configuration Menu

3. **Type 1 to create a new VLAN or to modify an existing one.**
4. **At the prompt, enter a VLAN number.**
5. **At the prompt, enter port numbers separated by commas.**

Caution: Make sure the management station is on the same VLAN as the CPU. Otherwise, you will lose management connection to the switch.

An additional option (0) allows you to reset all ports to VLAN 1.

For a more detailed explanation of the principles used in setting up VLANs, see “Virtual LANs” on page 2-4.

Setting Up Interswitch Ports

Interswitch ports allow you to set up an interconnection between two devices that allows VLAN IDs to be common between those two devices.

To set up interswitch ports:

1. **From the Main Menu, type 2 to display the System Configuration menu.**
2. **Type 9 to display the Port VLAN Configuration menu (Figure 5-9).**

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:01h:18m:40s]
Switch Status:                           [Switching]
********************************************************************************

                       Port VLAN Configuration

1 ---Create/Modify VLAN
2 ---Delete VLAN
3 ---Display VLAN
4 ---Add InterSwitch Port
5 ---Delete InterSwitch Port
6 ---Display InterSwitch Port
7 ---CPU VLAN Assignment [1]




0 ---Reset All Ports to default VLAN 1


Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure 5-9. Port VLAN Configuration Menu

3. **Type 4 to add one or more interswitch ports, and at the prompt enter one or more port numbers separated by commas.**

4. **To find out which ports have been set as interswitch ports, type 6.**

   The screen shows which ports are interswitch ports.

5. **To delete interswitch ports that have been set up previously, type 5. At the prompt, enter the port numbers.**

Setting Up Conversation Steering

Conversation steering is a troubleshooting aid that allows one port to monitor traffic on another port (port-based conversation steering). All incoming and outgoing traffic on the monitored port is copied to the monitoring port. The BayStack 310-24T switch also allows MAC address-based conversation steering. This method allows you to monitor packets sent to one or more specific MAC addresses. You can monitor a port and MAC addresses at the same time.

To set up conversation steering:

1. **From the Main Menu, type 2 to display the System Configuration menu.**
2. **Type 8 to display the Conversation Steering menu (Figure 5-10).**

```
********************************************************************************
Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:01h:15m:46s]
Switch Status:                           [Switching]
********************************************************************************

                        Conversation Steering

1 --- Monitoring Mode (Dedicated to a probe, UnTagged)
2 --- Port # to be Monitored (None)
3 --- View/Select Destination MAC Addresses to monitor
4 --- Monitoring/mirroring Port (None)
5 --- Conversation Steering Mode (Disabled)



Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure 5-10. Conversation Steering Menu

3. **Type 1 to select the monitoring mode for the port.**

   At the prompt, select one of the following modes:

   - Dedicated—The port is dedicated to the use of a network probe and does not pass any other traffic. At the prompt, select either tagged or untagged, based on whether you plan to use a tag-aware or non-tag aware probe.
   - Non-dedicated—The port can share traffic with the monitored traffic and another network device.

4. **To set port-based conversation steering, type 2 to specify the port to be monitored. At the prompt, enter a port number.**

5. **To set MAC address-based monitoring, type 3 to specify one or more MAC addresses.**

   The Destination MAC Conversation Steering menu is displayed (Figure 5-11).

```
********************************************************************************
               Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:01h:17m:07s]
Switch Status:                           [Switching]
********************************************************************************

               Destination MAC Conversation Steering

1 -- Frames to MAC [00:00:00:00:00:00] in VLAN [0001]     [Disabled]
2 -- Frames to MAC [00:00:00:00:00:00] in VLAN [0001]     [Disabled]
3 -- Frames to MAC [00:00:00:00:00:00] in VLAN [0001]     [Disabled]
4 -- Frames to MAC [00:00:00:00:00:00] in VLAN [0001]     [Disabled]
5 -- Frames to MAC [00:00:00:00:00:00] in VLAN [0001]     [Disabled]
6 -- Frames to MAC [00:00:00:00:00:00] in VLAN [0001]     [Disabled]
7 -- Frames to MAC [00:00:00:00:00:00] in VLAN [0001]     [Disabled]
8 -- Frames to MAC [00:00:00:00:00:00] in VLAN [0001]     [Disabled]

0 - Enable/Disable All MAC Entries

Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure 5-11. Destination MAC Conversation Steering Menu

a. **Select entry numbers and enter MAC addresses (up to eight) to be monitored. To delete a MAC address that has already been entered, type 0.**

b. **At the prompts, enter the VLAN ID for each MAC address and enter Enable or Disable.**

   The MAC address entry now shows in the displayed table.

c. **Press [Esc] to return to the Conversation Steering Menu.**

6. **Type 4 to specify the port to do the monitoring, and at the prompt enter a port number.**

7. **Type 5 to enable conversation steering. At the prompt, select Enabled.**

Resetting the Switch to Default Values

The Reset to Defaults option (0 from the System Configuration menu) allows you to reset the switch to all the factory default settings.

Caution: If you choose the Reset to Defaults option, all of your configuration settings are replaced with factory default settings when you press [Enter] after confirmation. If you reset the switch without reentering the IP address, the default [0.0.0.0] takes effect and you will have to reenter the IP address, IP subnet address, and default gateway address from the console and reset the switch before you can open another Telnet session.

Resetting the Switch

The System Reset/Upgrade menu allows you to perform a software-controlled reset of your BayStack switch.

To reset the switch:

1. **From the Main Menu, type 5 to display the System Reset/Upgrade Menu.**
2. **Type 5 to select a system reset or software download.**
3. **Select option 1 (System Reset).**
4. **To delay the system reset until a later time, type 6. Then enter a period of up to 65,535 minutes.**

   If you type 5 when no reset action has been specified in option 4, an error message is displayed.
5. **To start the reset immediately, type 0. Typing 0 overrides any previous setting.**

When Reset is selected, the switch restarts as if power had been cycled and displays the Main Menu. This reset differs from the Reset to Defaults option because it does not reset any parameter settings. Selecting Reset from a Telnet connection terminates the connection.

Note: When you download software, the switch resets twice. Do not power down the switch before the process is completed (approximately 10 minutes).

Network Management Using a Telnet Connection

Telnet is a common terminal-emulation application used in TCP/IP networks for remote terminal access to computer devices. You can use the Telnet application over an Ethernet network to remotely configure and monitor the BayStack 310-24T switch. After you have configured an IP address for the switch, access to its management system is available from any networked resource using a standard Telnet application.

To open a Telnet session:

1. **Check to make sure that Telnet Access is enabled.**
   a. **From the Main Menu, type 4 to display the Access Control menu.**
   b. **From the Access Control menu, type 1 to view the Telnet Access selection.**
   c. **Verify that Telnet Access is enabled or type 1 to enable it (the default setting for this parameter is enabled). If this parameter is disabled, then no Telnet access is allowed from any device.**

Note: You can also enable Telnet access or change the access password from the System Configuration Web page.

2. **With Telnet Access enabled, invoke the Telnet application with the IP address of the switch from any TCP/IP-based workstation.**

   This action displays the Password Verification screen.

3. **Enter the password to enable the Telnet session.**

With Telnet enabled, the switch can support up to two simultaneous Telnet connections. The Telnet inactivity timeout is 15 minutes. Inactive Telnet sessions are automatically terminated after that time has elapsed.

Some Telnet implementations do not work reliably when you use multiple Telnet hops. Whenever possible, connect directly to the switch using Telnet and avoid going through intermediate stations.

When you use a Telnet (or console) connection, typing [Control]+[d] at any time terminates (closes) the session.

Chapter 6
Managing the BayStack 310-24T Switch Using a Web Browser

The agent software on the BayStack 310-24T switch uses an embedded HTTP server that allows device-level management through a World Wide Web browser from anywhere on your network. Management functionality is comparable to that provided through the console or Telnet interface.

This chapter describes using the Web interface to manage the BayStack switches and includes information about the following topics:

- Requirements for using the Web-based interface (next)
- How to log on and access the Web-based interface (page 6-2)
- The layout of the Web pages (page 6-3)
- Instructions for performing management (beginning on page 6-10)

For information about using the console or a Telnet connection to manage the switch, refer to Chapter 5, “Managing the BayStack 310-24T Switch Using the Console Interface.” For descriptions of all the Web pages and options, refer to Appendix E, “Web Management Interface.” Refer to Chapter 3, “Installing the BayStack 310-24T Switch,” for installation, connection, and initial configuration procedures.

Requirements

To use the Web-based management interface you need:

- Netscape Navigator, version 4.0 or later, or Microsoft Internet Explorer Web browser, version 4.0 or later, installed on your computer
- The IP address of the BayStack 310-24T switch

Note: If the IP address of the switch does not respond when you try to access the Web management interface, the switch CPU may be connected to a different VLAN from the one your computer is connected to. Use the console interface to verify the VLAN port assignments and to make sure your computer and the CPU are connected to the same VLAN.

Accessing the Web Management Interface

Before you can use the Web-based management interface for the BayStack 310-24T switch, make sure Web access is enabled for the switch. To do so:

1. **From the console or Telnet user interface, type 4 from the Main Menu to display the Access Control menu.**
2. **From the Access Control menu, type 2 to view the Web Access selection.**
3. **Verify that Web Access is enabled or type 1 to enable it (default setting for this parameter is enabled). If this parameter is disabled, then Web access to switch configuration information is not allowed.**

To log on to the Web-based management interface for the BayStack 310-24T switch:

1. **Start your Web browser on a computer connected to any of the network ports.**
2. **Enter the IP address for the switch in the URL field of your Web browser, and open the connection.**

   The Login link is displayed.

3. **Click the Login button.**

   The user name is fixed as “Manager.” The password is the same as the Telnet and console password (set from the Access Control menu), with a default of no password.

4. **Enter the word *manager* as the user ID or user name. (The user ID for login is not case sensitive.) If a password has been set, enter the password in the appropriate field and click OK or press [Enter].**

Caution: The HTTP server in the BayStack 310-24T switches is version 1. If your browser is Internet Explorer 4.0, the default is HTTP 1.1. To properly view the Web management pages, you must disable versions 1.1 and later. In Internet Explorer 4.0, you do this from the View: Internet Options: Advanced menu. Scroll down to the bottom of the options list and deselect HTTP 1.1.

With Web access enabled, the switch can support up to four concurrent Web page users.

When you have logged in to the Web-based management interface, you can use the Web pages to view or change switch parameters.

Web Page Layout

With the exception of the login page, all Web pages for managing the switch are partitioned into the same three areas (Figure 6-1):

- Title bar
- Navigation bar
- Content area

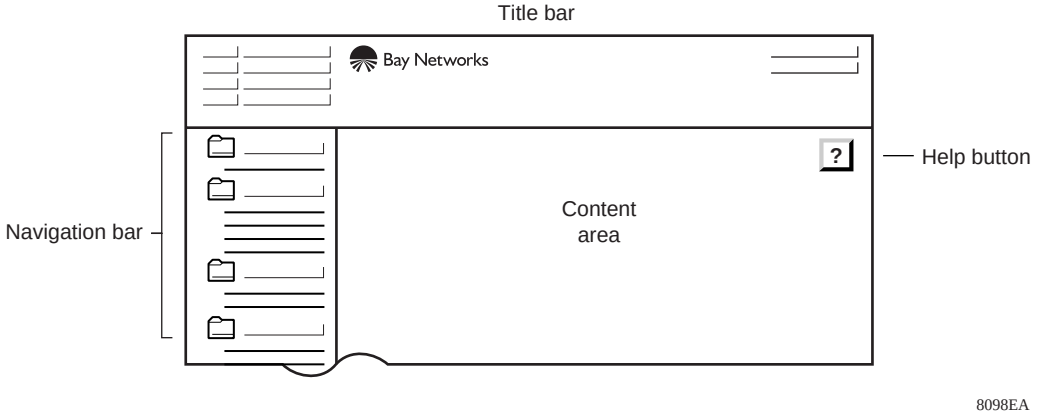


Figure 6-1. Web Page Components

Title Bar

The title bar includes a contact area, the Bay Networks logo, and the product name.

- The contact area includes the system name and location, the IP address, and the system contact. Clicking on the IP address links you to your browser's Telnet application. Clicking on the Contact links you to your browser's e-mail application. Telnet and mail must be properly configured in the browser to activate these links.
- Clicking on the Bay Networks logo links you to the Bay Networks home page.
- The product name is not an active link.

The title bar is constant for all pages and does not scroll.

Navigation Bar

The navigation bar is the same for all pages and includes an indented tree of folders providing direct links to all pages. In the navigation bar, the pages are grouped in the following folders:

- Summary
- Configuration
- Security
- Fault Management
- Statistics
- Support

The indented items in each folder, indicated by underlined text, are linked to the pages. The first four folders contain the pages for viewing and changing switch parameters. The Support folder includes the following selections:

- Click Help to link to a Help page that provides explanations for the information fields of the screens and menus. A Help button (?) on each page also links you to the appropriate paragraph of the Help page.
- Click Release Notes or Manuals to link to the appropriate documentation page on the Bay Networks Web site.

- Click Feedback to link to an e-mail screen that allows you to send comments, questions, or other feedback information to Bay Networks about the BayStack 310-24T switch.

Note: To ensure prompt response, do *not* use this e-mail link to request technical support.

From these links, use the browser Back button to return to the Web management screen.

For more information about the Web page hierarchy, see Appendix E, "Web Management Interface."

Content Area

The content area contains the actual pages that correspond to the menus and screens used in the console interface. There are 19 first-level pages as indicated by the navigation bar. The content area includes the following information:

- Date and time (from the Web browser)
- System uptime (from the switch)
- Tables and input forms.

  Gray cells are displayed values, which cannot be changed; white cells are input fields. The inverted triangle at the right of an input box indicates a pull-down selection menu.

- Check boxes

  Many parameters are enabled or disabled by clicking a check box. When a check mark shows in the box, that parameter is enabled.

- Task buttons

  The task buttons perform an action concerning the displayed page or the switch. Some pages include a task button that opens another page or updates the values shown on the current page. Other pages include buttons that initiate an action, such as setting parameter values to defaults or setting a parameter for the entire switch.

The following three task buttons appear on each page:

— Apply New Settings: Click this button after you have entered values or selected new menu items to make the new settings take effect. (Note that some parameter settings take effect at the next reset only.)

— Clear Input: Click this button if you have made a mistake and want to start again on a page. This button erases all the new information in the fields on the page.

— **?**: Click this button to access Help information about the fields on this page. From the Help page, click the Back button in the browser to return to the page.

- Radio buttons

  The radio buttons represent available options for the indicated parameter. The selected button in a category shows the current setting. To change a selection, click the appropriate radio button. A new setting does not take effect until you click the Apply New Settings task button.

Using BootP for Switch Configuration

The BayStack 310-24T switches are set for configuration using BootP as the default. When you power on the switch for the first time, it tries to find a BootP server from which it can download its network parameters. If the switch cannot find a BootP server, it tries five more times to find one and then defaults to the factory settings.

If the server is set up with the correct information, the switch downloads the following network parameters:

- IP address of the switch
- IP subnet mask
- Default gateway IP address
- TFTP server IP address
- Software image file name

You can customize the conditions for BootP configuration or request a BootP configuration at any time while the switch is running.

To set up the conditions for BootP configuration from the Web management interface:

1. **Click Configuration: System in the navigation bar.**

   The System Configuration page opens.

2. **Select one of the following settings for Bootp Current Setting:**

   - When Needed (default setting)—If the IP address stored in the nonvolatile memory is the factory default value (127.0.0.2), the switch uses BootP to request configuration settings. If the stored IP address is different from the factory default value, the switch uses the stored network parameters.
   - Always—The switch boots, ignoring any stored network parameters, and uses BootP to request network configuration parameters. If the BootP request fails, the switch boots with the factory default IP configuration. This setting disables remote management if no BootP server is set up for the switch, but it allows the switch to boot normally.
   - Disabled—The switch boots using the IP configuration parameters stored in nonvolatile memory. If a BootP configuration is in progress when you issue this command, the BootP configuration stops.
   - Last Address—At startup, the switch tries to obtain its IP configuration using BootP. If the BootP request fails, the switch uses the network parameters stored in its nonvolatile memory.

Note: When the switch uses BootP to obtain network parameters, it updates the existing parameters only if the new ones are valid values for the parameters. Valid parameters obtained using BootP always replace current information stored in the nonvolatile memory.

3. **To start a BootP configuration, click Execute BootP Now.**

   The switch immediately sends a BootP request and downloads configuration parameters if it finds a BootP server.

Loading Switch Software and Configuration Files

You can set up one switch and upload its configuration file to a TFTP server on the network. Then you can use the stored file to configure other switches in the network. You can also upgrade switch software from a TFTP server.

To upload a configuration file to a server:

1. **Click Configuration: Reset/Upgrade to open the Reset/Upgrade page (Figure 6-2).**

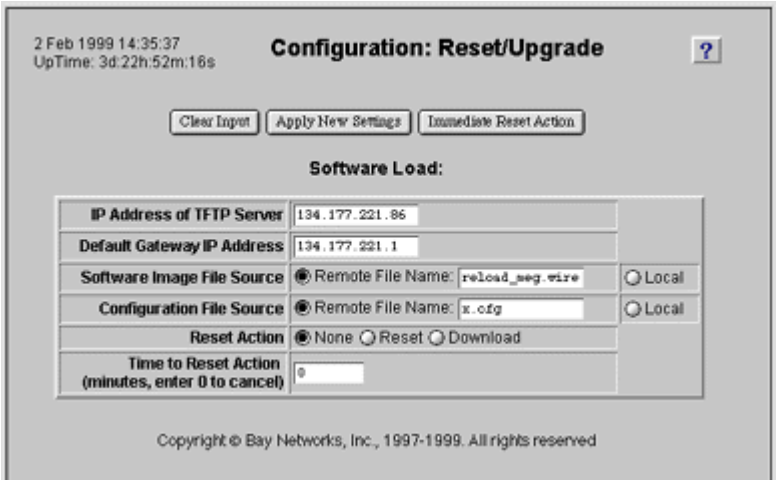


Figure 6-2. Reset/Upgrade Page

2. **On the Reset/Upgrade page, enter the IP address of the TFTP server and the default gateway IP address.**
3. **Enter the Configuration File Name and click the Remote radio button.**
4. **Click Apply New Settings.**
5. **Click Configuration: System in the Navigation Bar.**
6. **On the System page, click Execute Configuration File Host Update Now.**

To download a configuration file to a switch:

1. **On the Reset/Upgrade page, enter the IP address of the TFTP server and the default gateway IP address.**
2. **Enter the Configuration File name and click the Remote radio button.**
3. **Click Apply New Settings.**
4. **To specify the Reset Action, click the Download radio button.**
5. **Click the Immediate Reset Action task button.**

To upgrade software:

1. **On the Reset/Upgrade page, enter the IP address of the TFTP server and the default gateway IP address.**
2. **Enter the Software Image File name and click Remote.**
3. **Click Apply New Settings.**
4. **To specify the Reset Action, click the Download radio button.**
5. **To schedule a delayed software download, enter a value in the Time to Reset Action field (up to 65535 minutes), and click Apply New Settings to set.**
6. **To download immediately, click Immediate Reset. This action overrides any previous settings.**

Note: The switch resets twice during the upgrade process. Do not power down the switch before the process is completed (approximately 10 minutes).

To download a software upgrade and configuration file at the same time:

1. **On the Reset/Upgrade page, enter the IP address of the TFTP server and the default gateway IP address.**
2. **Enter the Configuration File name and click the Remote radio button.**
3. **Enter the Software Image File name and click Remote.**
4. **Click Apply New Settings.**
5. **To specify the Reset Action, click the Download radio button.**
6. **Click the Immediate Reset Action task button.**

Setting the Management Access Password

Password protection for access to the console port interface and the Web management interface is set using the Password page in the Security folder (Figure 6-3).

Figure 6-3. Password Page

The switch is shipped with no password set up. To set a password the first time, type the text for the password in both “new password” fields and click Apply New Settings.

To change an existing password:

1. **Type the old password in the “old password” field.**
2. **Type the new password twice.**
3. **Click Apply New Settings.**

Setting Up Management Access Control

Management access control limits access to the switch configuration functions. This control is based on IP addresses that are allowed to access the management functions. You set up management access control from the Management Access page.You can specify a list of up to eight IP addresses, each of which can access the switch through the Web, Telnet, or SNMP. These settings work in conjunction with the password protection that is available for access to the management functions. If you set a password, it is still required for access from the authorized IP addresses. To set the management access password, see "Setting the Management Access Password" on page 6-10.

Caution: Make sure you include the IP address of your own management station. Otherwise, you may be locked out accidentally.

To set up management access control:

1. **Click Security: Management Access in the navigation bar.**

   The Management Access page opens (Figure 6-4).

Figure 6-4. Management Access Page

2. **To allow Telnet access, make sure the Telnet Access Enabled check box is checked.**

   Deselecting this check box blocks all Telnet access. Selecting it allows access that can be further restricted in the next three steps.

3. **Check the Management Access Control Restricted check box to restrict access.**

   Checking this box causes the switch to process management packets only according to the information in the management access control table on this Web page. Deselecting this check box removes any restrictions on how the switch processes management packets, and any information in this table is not used.

4. **If you intend to restrict management access, enter the IP addresses that are allowed to access management functions.**

Caution: Do not forget to include the IP address of the station you are currently using, or you will lose access as you apply the settings.

5. **For each IP address, click the check box to enable or disable Telnet, Web, and SNMP access.**
6. **Click Apply New Settings to make the changes take effect.**

Note: Make sure you specify at least one IP address for restricted access. If you select restricted management access but do not specify IP addresses (or if the IP address is set to 0.0.0.0), access to the switch is still unrestricted.

To delete an IP address, click in the address field and backspace over the address. Then click Apply New Settings.

Setting Up MAC Address-Based Security

MAC address-based security allows you to monitor and minimize unauthorized network access by restricting access to unauthorized stations based on their MAC addresses. You can establish two types of security: single MAC address per port or MAC address list. You can also specify the action to be taken if a violation occurs. You set up MAC address-based security from the Security: Network Access page.

This section describes the basic tasks required for the initial setup of MAC address-based security. Perform the setup tasks in the following order:

1. Select either Single-MAC-per-port, MAC-list, or Auto-Learn as the security mode and specify the action to be taken if a violation occurs (page 6-14).
2. Specify the MAC addresses that are allowed to access ports or (for MAC-list only) not allowed to access ports (page 6-15).
3. Specify whether or not to allow SNMP write access to the security functions (page 6-16).
4. After all the other security parameters are set, enable MAC address-based security (page 6-16).

Setting the Security Mode and Action

To set the security mode and action:

1. **Click Security: Network Access in the navigation bar.**

   The Network Access page opens (Figure 6-5).

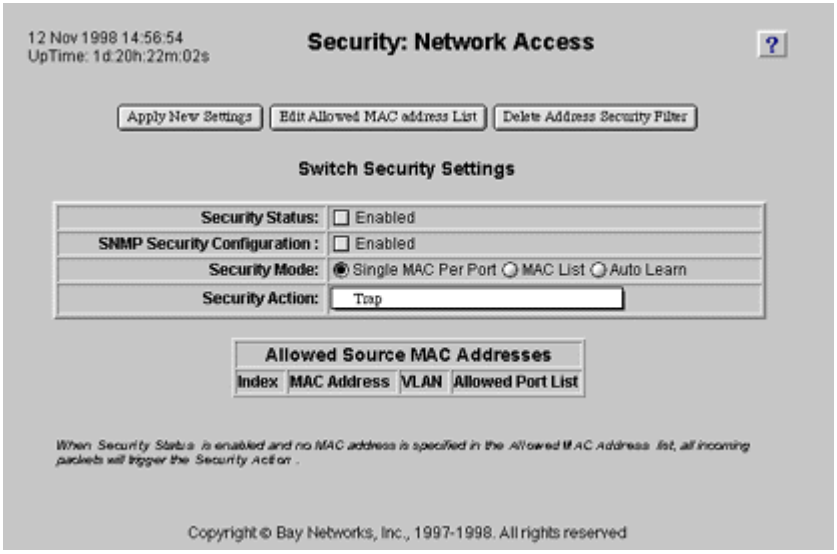


Figure 6-5. Network Access Page

2. **Select one of the following security modes:**

   - Single MAC Per Port—In this mode, only one MAC address is allowed to use the specified port. Any other address learned on that port causes the specified security action.

Note: The Single MAC Per Port setting does not support a not-allowed MAC list. If you try to enter a not-allowed MAC address when this mode is selected, an error message is displayed.

   - MAC List—In this mode, you can specify a list of MAC addresses that are allowed to connect to the switch, and for each address you can specify the individual ports it can connect to. You can choose no ports, all ports, or a list of ports.

- Auto-Learn—In this mode, the switch learns the first MAC address that passes through a port. Thereafter, any other MAC addresses are prohibited from access the port.

3. **Select one of the following actions to be taken if a violation occurs:**
   - No Action
   - Trap—Send a trap to the network management software (default)
   - Partition Port
   - Partition Port and Send Trap
   - MAC DA Filtering
   - MAC Filtering and Send Trap
4. **Click Apply New Settings.**

When you have set the security mode and action, go to the next section to set up the allowed and not-allowed MAC address lists.

Setting Up MAC Address Lists

To set up MAC address lists:

1. **From the Network Access page, click Edit Allowed MAC Address List.**

   A page opens with fields for entering MAC addresses and port numbers.
2. **Enter a MAC address and click port members to specify the ports this address is allowed to access.**
3. **Click All Ports to allow this MAC address on all ports.**
4. **Click Apply New Settings.**
5. **Enter more MAC addresses as needed, up to a total of 64.**

Note: Make sure the MAC address of the management station is on the list of allowed addresses before you turn on the security feature. If a router is connected to the switch, make sure the MAC address of the router is in the list of allowed addresses.

6. **When you finish entering MAC addresses, click Back to Network Access.**

Setting Up SNMP Access to Security Settings

You can enable or disable SNMP access to security settings for the switch. If you enable SNMP access, the security settings can be changed from a management station using SNMP-based network management software such as Bay Networks Optivity software.

From the Network Access page, select one of the following settings for SNMP Security Configuration:

- Disabled (check box not selected)—Prevents security configuration settings from being modified using SNMP.
- Enabled (check box selected)—Allows access to security configuration settings using SNMP.

Click Apply New Settings to make the change take effect.

Enabling MAC Address-Based Network Access Security

After you have set up the operating parameters, you can enable MAC address-based security. The Allowed Source MAC Address table on the Network Access page (see page 6-14) summarizes security settings for the specified MAC addresses. Verify your settings and check the following items before you enable security:

- Make sure the MAC address of the management station is on the list of allowed MAC addresses.
- If a router is attached to the switch, make sure the MAC address of the router is on the list of allowed addresses.

To enable MAC address-based security:

1. **Click the Enabled check box for Security Status.**
2. **Click Apply New Settings.**

Modifying MAC Address-Based Security

This section describes other management tasks for MAC address-based security in the switch. This section includes the following tasks:

- Changing the allowed MAC address list and not-allowed MAC address lists (this page)
- Verifying MAC addresses (page 6-18)
- Disabling MAC address-based security (page 6-18)

Changing the MAC Address Lists

You can change the MAC address lists in several ways.

To delete a single allowed MAC address:

1. **Click Security: Network Access in the navigation bar.**
2. **On the Network Access page, click Edit Allowed MAC Address List.**
3. **Enter the MAC address in the Security Configuration for Source MAC Address field.**
4. **Click Delete Address.**
5. **Click Back to Network Access (optional).**

To delete all MAC addresses, change the Security Mode setting on the Network Access page, and then change it back.

One of the possible security actions is to set up destination address (DA) filtering on an address. You can delete a single MAC address filter or you can clear all filters that have been created by the security feature.

To delete a single destination MAC address filter:

1. **Click Security: Network Access in the navigation bar.**
2. **On the Network Access page, click Delete Destination Address Filter.**
3. **Enter the destination MAC address and click Delete Destination Address Filter.**
4. **Click Back to Network Access (optional).**

To delete all destination filter MAC addresses:

1. **Click Security: Network Access in the navigation bar.**
2. **Select Disable for Security Status and click Apply New Settings.**
3. **Select Enable for Security Status and click Apply New Settings.**

Verifying MAC Addresses

To verify MAC addresses:

- Click Fault Management: MAC Address Table in the **navigation bar**.

  The MAC Address Table page opens showing a complete list of all MAC addresses that have been learned by the switch, the ports they have been learned on, which addresses are permanent (static) and which are subject to aging (dynamic), and which addresses are subject to filtering.

Disabling MAC Address-Based Security

To disable MAC address-based security:

1. **Click Security: Network Access in the navigation bar.**
2. **For Security Status, click the Enabled check box to deselect it.**
3. **Click Apply New Settings.**

Setting Up Spanning Tree Protocol Operation

The BayStack 310-24T switch allows you to disable Spanning Tree Protocol operation on selected ports. The factory default setting for a switch is spanning tree enabled on all ports. You can disable spanning tree on all ports or selectively disable it on individual ports. In addition, you can set all the spanning tree ports or individual ports for Fast Start connection.

Note: Spanning Tree Protocol resolves duplicate paths in networks and is not necessary for ports that have workstations directly attached to the switch. When Spanning Tree Protocol is enabled on these ports (the default), workstations are unable to attach to servers for a few seconds until Spanning Tree Protocol stabilizes.

Setting up spanning tree operation from the Web management interface consists of the following general tasks:

1. Check the current state of Spanning Tree Protocol in the switch (see the next section). Because the default setting is Spanning Tree Protocol enabled for all ports, you may not need to do any further configuration of spanning tree operation for your switch. If you want to customize the spanning tree operation, you can proceed with the remaining tasks.
2. If you want to customize spanning tree operation for the switch or for selected ports, make sure Spanning Tree Protocol is enabled for all ports (step 2 on page 6-20). If necessary, set general Spanning Tree Protocol parameters using the Configuration: Spanning Tree page. Then use the Configuration for Port page to disable Spanning Tree Protocol on selected ports or to set selected ports for Fast Start spanning tree operation.

Checking the Current Spanning Tree Protocol State

To check the current Spanning Tree Protocol state:

1. **Click Configuration: Spanning Tree in the navigation bar.**

   The Spanning Tree page opens (Figure 6-6).

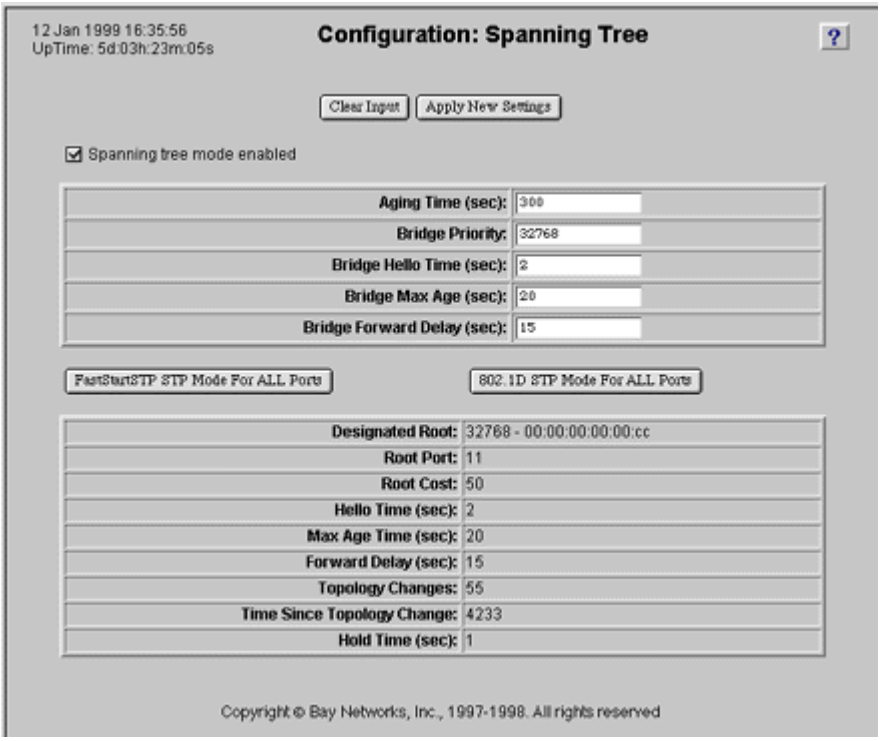


Figure 6-6. Spanning Tree Page

2. **Verify whether or not the check box for Spanning tree mode enabled is checked at the top of the page.**

   This setting enables or disables Spanning Tree Protocol for the entire switch.

If Spanning Tree Protocol is enabled (the default), you may not need to set any other switching parameters. The switch is ready to operate in most network environments. If you want to disable spanning tree operation only on selected ports, make sure Spanning Tree Protocol is set to Enabled on this page.
Then continue to the next section.

Customizing Spanning Tree Protocol Operation

To customize spanning tree operation:

1. **Click Configuration: Port in the navigation bar.**

   The Port Configuration page opens showing a table of the ports and their current configuration settings.

2. **Click the number of the port you want to set up.**

   A configuration page opens for the selected port.

3. **Select one of the following settings for Port STP mode:**

   - 802.1D—Sets the port for IEEE 802.1d spanning tree operation.
   - NoSTP—Disables Spanning Tree Protocol on that port only.
   - FastStartSTP—Sets the port for Fast Start spanning tree operation, which allows the port to transition to the Forwarding state faster than the time specified in the IEEE standard.

Note: When you connect a BayStack 310-24T switch to another switch or bridge, Spanning Tree Protocol must be enabled on all the interconnecting ports for reliable loop detection. Disabling spanning tree on individual ports connecting switches or bridges may cause loops to go undetected when redundant links are used between devices.

4. **You can specify a port priority and port path cost or use the current settings.**
5. **Click Apply New Settings to make the changes take effect.**
6. **To verify the changes, click Refresh.**

   The display refreshes and shows current settings.

7. **Return to the Port Configuration page to select other ports, and repeat steps 2 through 6.**

Setting SNMP Parameters

To set SNMP parameters for the switch:

1. **Click Configuration: System in the navigation bar.**
2. **Enter IP addresses in the fields for IP address, IP Subnet Mask, and Default Gateway Address.**
3. **Enter information in the fields to set up trap receivers.**
4. **Click Apply New Settings.**

Setting the System Characteristics

To set system characteristics:

1. **Click Configuration: System in the navigation bar.**
2. **Under System Identification, type character strings for System Name, System Location, and System Contact.**
3. **Click Apply New Settings.**

Setting Up Address Filtering

To set up address filtering:

1. **Click Configuration: Filtering in the navigation bar.**

   The Filtering configuration page opens (Figure 6-7).

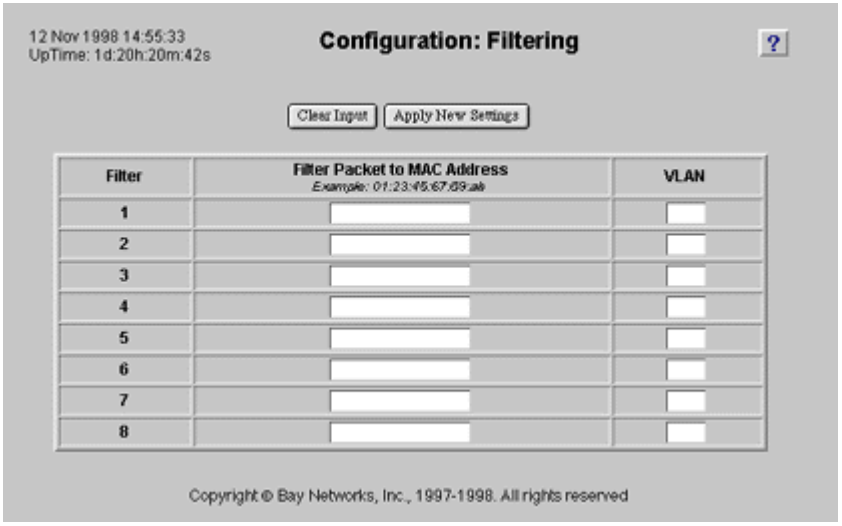


Figure 6-7. Filtering Configuration Page

2. **Enter up to eight MAC addresses and VLAN numbers in the fields.**
3. **Click Apply New Settings.**

Setting Up High-Speed Ports and MultiLink Trunking

The high-speed ports on the BayStack 310-24T switch are port 25 (the fixed port on the front panel) and optional ports on installed MDAs (ports 26 and 27). For these ports, you can specify the operating speed, duplex mode, and address learning mode. You can also set these ports as members of a multilink trunk.

To set up a high-speed port:

1. **Click Configuration: MultiLink Trunking in the navigation bar.**

   The High Speed MLT Port page opens (Figure 6-8).

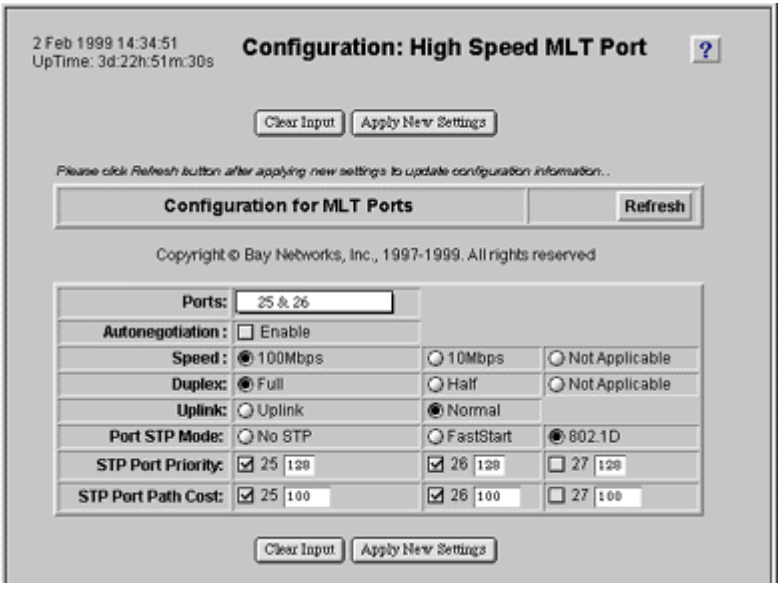


Figure 6-8. High Speed MLT Port Page

2. **Click the Ports parameter field and select the ports to be grouped into a multilink trunk.**

   You can choose any two ports, all three, or none.

3. **Click the Autonegotiation Enabled check box to enable or disable autonegotiation on these ports.**

4. **Click the radio buttons to select speed, duplex mode, and uplink mode.**

   If autonegotiation is enabled, the speed and duplex mode selections are disabled.

   Uplink mode for the ports disables address learning for the ports.

5. **Click the appropriate Port STP Mode radio button to select the mode for Spanning Tree Protocol operation.**

   Fast Start mode allows the port to transition to the Forwarding state faster than it does in the 802.1d mode. The probability that a loop may occur is greater with Fast Start operation than with IEEE 802.1d operation.

6. **Click Apply New Settings.**

Assigning Ports to VLANs

To assign ports to VLANS:

1. **Click Configuration: VLAN in the navigation bar.**

   The VLAN-ID configuration page opens (Figure 6-9).

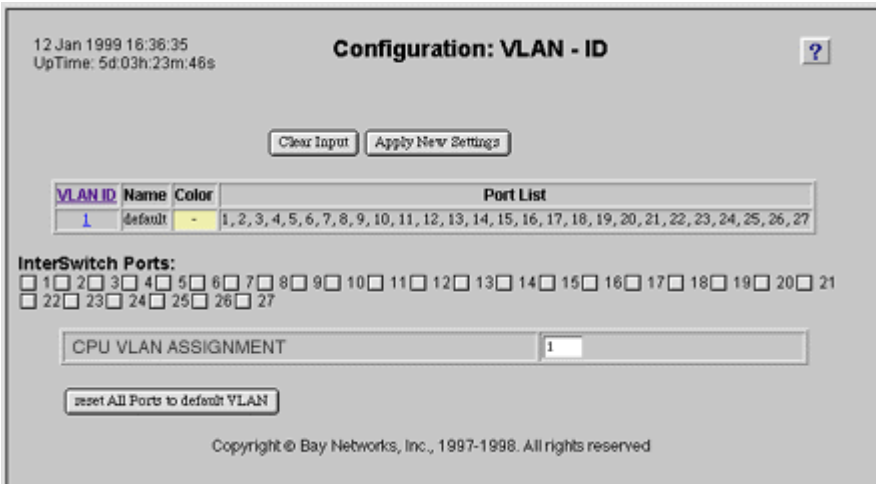


Figure 6-9. VLAN-ID Page

2. **To set ports as interswitch ports (members of all VLANs), click the check boxes to the left of the port numbers.**

   For more information about interswitch ports, refer to "Virtual LANs" on page 2-4

3. **To create a new VLAN, click on VLAN ID.**

   A configuration page opens for setting up a new VLAN (Figure 6-10). The system assigns the next available VLAN ID.

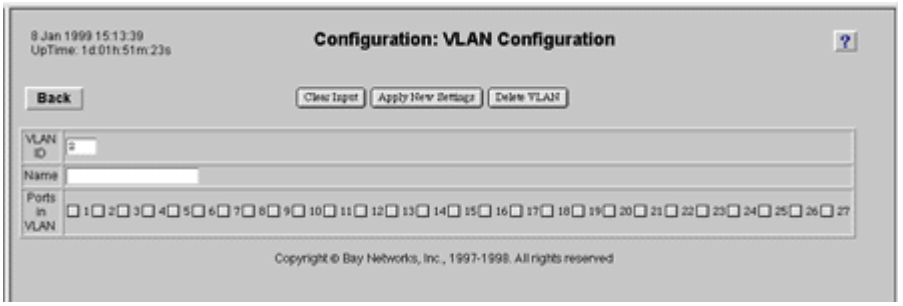


Figure 6-10. VLAN Configuration Page

4. **Type a new VLAN ID, or leave the default value in the field.**
5. **You can type a VLAN name or leave this field blank.**
6. **Click the check boxes to assign ports to this VLAN.**
7. **Click Apply New Settings.**
8. **To modify an existing VLAN, click the VLAN ID number.**
9. **Click the check boxes to add or delete ports.**

   To assign all ports on the switch to VLAN 1 (the default VLAN), click the Reset All Ports to Default VLAN task button.

10. **Click Apply New Settings.**

Note: The CPU VLAN Assignment parameter field shows the VLAN that the CPU (management interface) is assigned to. The network management station must also be a member of this VLAN to manage the switch through a Telnet connection, Web connection, or SNMP management. The CPU can be a member of only one VLAN. The default assignment is VLAN 1.

Setting Up Conversation Steering

Conversation steering is a troubleshooting aid that allows you to use one port to monitor other traffic in the switch. With port-based conversation steering, all incoming and outgoing traffic on the monitored port is copied to the monitoring port. The BayStack 310-24T switch also allows MAC address-based conversation steering. This method allows you to monitor packets sent to one or more specific MAC addresses. You can monitor a port and MAC addresses at the same time.

To set up conversation steering:

1. **Click Configuration: Conversation Steering in the navigation bar.**

   The Conversation Steering page opens (Figure 6-11).

2. **Click the Conversation Steering Mode Enabled check box to enable conversation steering.**

3. **Type a port number in the Monitoring Port parameter field.**

4. **Click the appropriate radio button to select a dedicating mode for the port. Choices are:**

   - Dedicated Mode, tagged—An 802.1Q tag is inserted into the frame to identify the VLAN the frame is associated with. This setting allows you to use a dedicated monitoring port and a tag-aware probe.
   - Dedicated Mode, untagged—No frames are tagged. This setting allows you to use a dedicated monitoring port and a probe that is not tag-aware.
   - Nondedicated Mode—The monitoring port doubles as an active port. This setting allows you to another network device to share the port connection with a probe.

5. **To set up port-based conversation steering, enter a port number in the Monitored Port parameter field.**

6. **To set up MAC address-based conversation steering, enter one or more MAC addresses and VLAN IDs in the MAC Address Table, and click the Enabled check box for each entry.**

7. **Click Apply New Settings.**

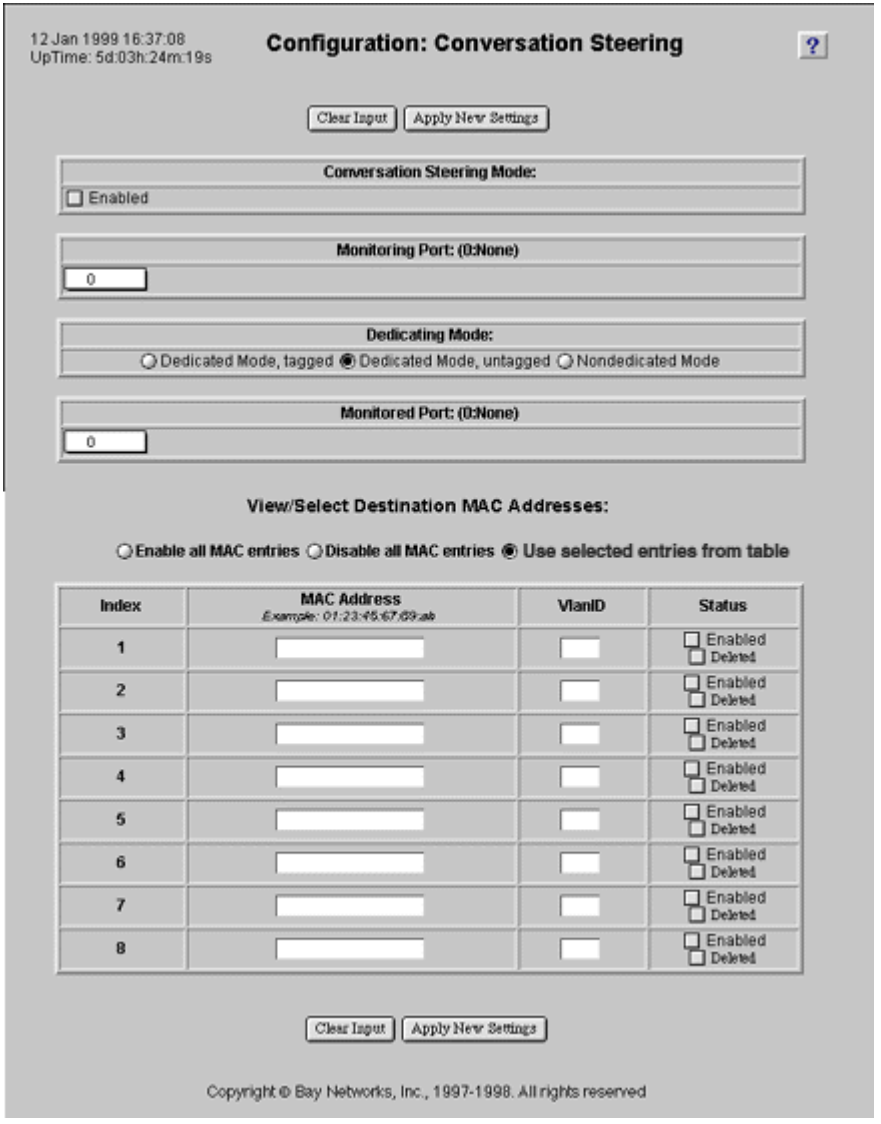


Figure 6-11. Conversation Steering Page

Checking Network Topology

You can display information about devices connected to the network. For those devices that support Web-based management, you can also connect to them from the BayStack 310-24T switch Web management interface. For devices that support Telnet access, you can initiate a Telnet session from the Web management interface.

To check the network topology:

1. **Click Fault Management: Topology in the navigation bar.**

   The Topology page opens (Figure 6-12).

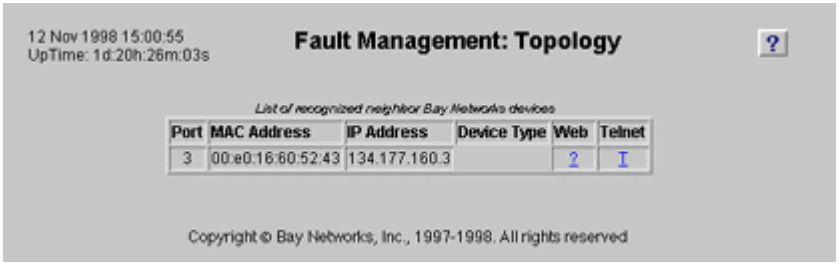


Figure 6-12. Topology Page

   The Topology page shows a table of switch port numbers with the MAC addresses, IP addresses, and device types that are connected to each port. In addition, links allow you to connect to the connected devices using the Telnet Protocol or the Web.

2. **To connect to a device using the Telnet Protocol, click T in the row for that device.**

   A window opens as a Telnet session is initiated. With proper authorization, you can access the console port interface and perform any of the switch configuration and management functions. (A password may be required.)

Note: This operation assumes that your browser can initiate a Telnet session on your system. If you see an error message when you try to initiate a Telnet session, you may need to modify your browser's preferences menu to select the supporting application.

3. **To connect to a device using the Web, click W in the row for that device.**

   If the device supports Web access, a browser window opens showing the Web management interface for that device. With proper authorization, you can perform management and configuration functions. (A password may be required.)

Note: Not all Bay Networks devices can support a Web connection. In addition, security and management settings on the remote device may limit your ability to establish a Telnet or Web connection.

Resetting the Switch to Factory Defaults

To reset the switch to factory defaults:

1. **Click Configuration: System in the navigation bar.**
2. **Click Reset to Defaults.**
3. **A warning message asks if you really want to reset the switch. Click OK to proceed.**

Caution: When the switch is reset to its factory default values, all IP addresses are erased and you lose connectivity to the switch through the Web interface. For a list of factory default settings, refer to Appendix A, "Technical Specifications."

Resetting the Switch

To reset the switch:

1. **Click Configuration: Reset/Upgrade in the navigation bar.**
2. **Click Reset for Reset Action.**
3. **Enter a time interval to wait before the reset takes place, or click Immediate Reset Action.**

Chapter 7
Troubleshooting and Diagnostics

The BayStack 310-24T switch is designed to be as simple and reliable as possible. Occasionally, problems may arise that are largely associated with two areas: problems related to the BayStack 310-24T switch and problems related to the installation.

Warning: To avoid bodily injury from hazardous electrical current, never remove the top cover of the device. There are no user-serviceable components inside.

Switch-Related Issues

The BayStack 310-24T switches have a powerful set of system diagnostics that check all internal resources of a switch whenever it is turned on. After the master core processor (management processor) has tested itself, each port is tested in sequence. The switch attempts to transfer Ethernet packets only if all diagnostic tests complete without errors.

This section includes information about the following common switch-related issues:

- Password Recovery
- Autonegotiation
- MDI and MDI-X connections

Password Recovery

If you set a password, it applies to console, Telnet, and Web access. If you forget your password, call the Bay Networks Technical Solutions Center for assistance.

Autonegotiation

Port connection problems can occur when a port is connected to a station that is not operating in a compatible mode (for example, connecting a full-duplex port to a half-duplex port). When autonegotiation is enabled on a high-speed port, problems and mismatches can occur when that port is connected to a port that:

- Does not support autonegotiation.
- Supports a form of autonegotiation that is not compatible with the IEEE 802.3u autonegotiation standard.
- Supports autonegotiation but has the feature disabled.

In the situations described here, the BayStack 310-24T switch senses the speed of the connected port and, by default, reverts to half-duplex mode. If the connected station is operating in full-duplex mode, the stations cannot communicate properly and a mismatch occurs. To resolve this mismatch, disable autonegotiation and manually set the speed and duplex mode (see "Setting Up High-Speed Ports and Multilink Trunking" on page 5-27 to manually set speed and duplex mode from the console interface).

When the link is first brought up, the BayStack 310-24T switch senses the speed of the connecting device. If the connecting device changes speed without performing a link down, the BayStack 310-24T switch can correctly sense a change from 100 Mb/s to 10 Mb/s. If the device connected to the switch does not support autonegotiation, you should configure the switch with autonegotiation disabled.

MDI and MDI-X Connections

The BayStack 310-24T switch uses MDI-X ports that allow you to connect directly to end stations without using crossover cables (Figure 7-1). Ports that implement the crossover function internally are known as MDI-X ports (where "X" refers to the crossover function).

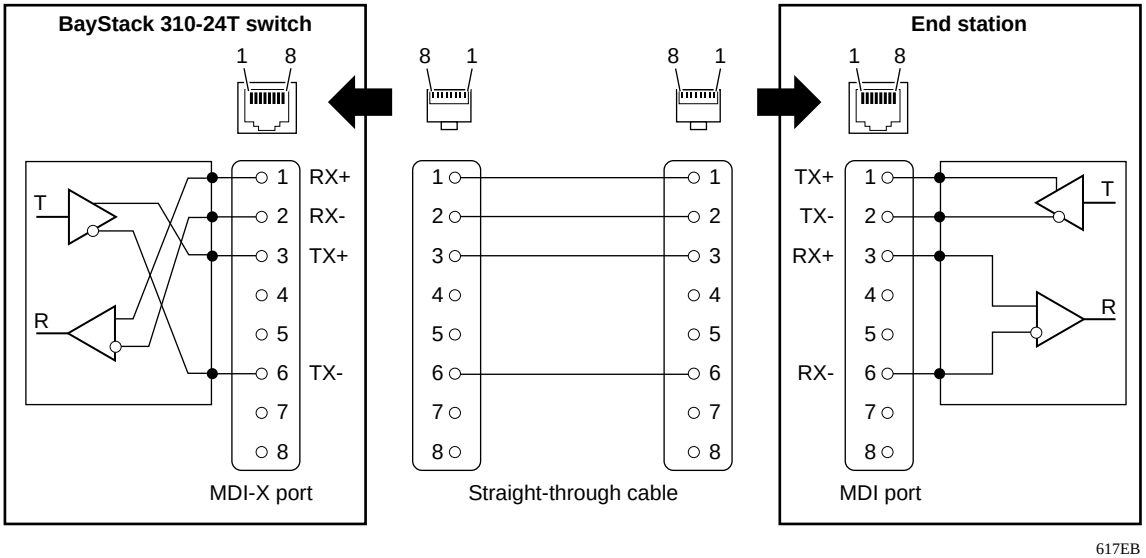


Figure 7-1. MDI-X to MDI Cable Connections

If you are connecting a device to the BayStack 310-24T switch that also implements MDI-X ports (Figure 7-2), use a crossover cable.

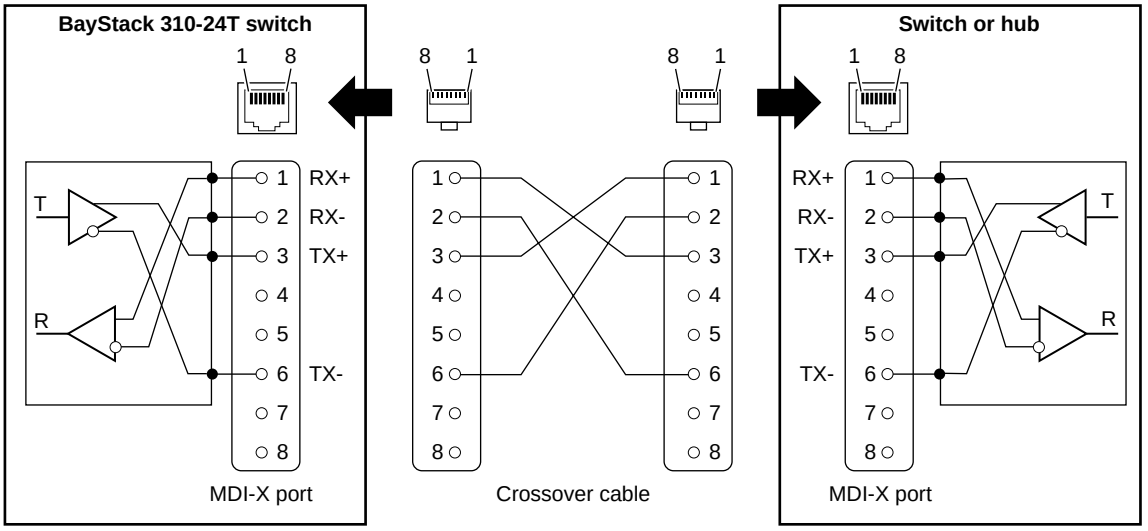


Figure 7-2. MDI-X to MDI-X Cable Connections

Installation-Related Issues

Ethernet 10BASE-T networks tend to be fairly simple, but they can still have problems that take time to resolve. The most common problems are associated with the actual network wiring.

If you have problems with a newly established network (initial setup), the trouble is most likely related to cabling or addressing. If the network has been operational for an extended period and is now beginning to have problems, the trouble is probably related to recent additions or changes.

Addresses

Remember that each BayStack 310-24T switch has a MAC station address and an IP address. The MAC station addresses are unique because each address contains the Bay Networks manufacturer ID and node ID codes. The switch is shipped with a default IP address of 127.000.000.002.

A valid IP address is not required for normal switching operation or if you are managing the switch from a console. However, for management over the network (Web, SNMP, or Telnet session), a valid IP address is required.

You can change the IP address of the unit to match your own network addressing structures. Ensure that the IP address of the BayStack 310-24T switch is unique in your network. You can change the IP address using the Switch Network Configuration menu from the console interface or the System page from the Configuration folder in the Web-based management interface. You will need to set a valid IP address if you intend to use network management with SNMP, Telnet, or the Web interface.

Cabling

Cabling for 10BASE-T networks can consist of 2-pair Category 3, 4, or 5 unshielded twisted pair (UTP) wiring. However, to cover future upgrades to Fast Ethernet, Bay Networks strongly recommends that you use all Category 5 cable in your network.

Ethernet 10BASE-T network installations use cables consisting of two pairs of twisted pair wires—one pair to send data and one to receive data. These wires must connect to another 10BASE-T station that has the sending pair attached to its receiving pair and vice versa. In this way, the two nodes can exchange data. If the two nodes are wired alike, they both attempt to send data out on the same RJ-45 pins. In such a case, a straight-through cable would not work (Figure 7-2 on page 7-4). However, a crossover cable (Figure 7-1 on page 7-3) would operate normally.

The BayStack 310-24T switch is designed to have Ethernet NICs connect directly to its RJ-45 ports using straight-through cables. However, if the BayStack 310-24T switch must connect to a hub and that hub follows usual conventions, a crossover cable is required.

The 100 Mb/s ports are designed to operate using Category 5 UTP cabling only. Category 5 UTP cable is a 2-pair cable certified to handle up to 100 MHz bandwidth. To minimize crosstalk noise, maintain the twist ratio of the cable up to the point of termination; untwist at any termination should not exceed 0.5 inch (1.27 cm).

For best performance with respect to noise immunity and emissions, the unused pairs in the 2-pair cable should be terminated at their characteristic impedance (that is, 100 ohms) in the equipment at each end of the cable. All Bay Networks 100BASE-TX equipment includes such a Common Mode Termination (CMT).

The fiber media adapter for the 100BASE-FX port uses only multimode 62.5/125 μm fiber cable. The Bay Networks 100BASE-FX media adapter is not supported on single-mode fiber. SC connectors are used on all fiber port connections.

Link Status

The 10BASE-T ports use link test pulses to provide a mechanism to ensure that the link between the connected devices is valid. When the link is inactive, link test pulses are transmitted approximately every 16 microseconds (ms). The 100 Mb/s port also ensures valid links between connected devices.

When link status is shown in an LED, you can immediately see if the cables are connected correctly, assuming that the other equipment also sends link status pulses. Link status should be used whenever possible to check for potential wiring issues.

Type 1 Connectors

When spanning tree is enabled, a blocked port might be caused by an open Type 1 connector. High speed ports operating in full duplex mode can detect an open Type 1 connector and block the port until a device is connected to that connector. Type 1 connectors are intended primarily for token ring networks and use an internal shorting mechanism to create a loopback condition when no device is connected to them.

Using Troubleshooting Features in the Console Interface

The console interface provides the following commands and menu to help troubleshoot the switch:

- Conversation Steering option on the System Configuration Menu
- Troubleshooting Menu with the following options:
  - Ping Remote Station
  - MAC Table Lookup
  - Forwarding During Broadcast Storms
  - Topology Table

Conversation Steering

Conversation steering is a troubleshooting aid that allows you to use one port to monitor other traffic in the switch. With port-based conversation steering, all incoming and outgoing traffic on the monitored port is copied to the monitoring port. When a port is operating as a dedicated monitoring port, forwarding is disabled and only the mirrored traffic is transmitted from that port.

The BayStack 310-24T switch also allows MAC address-based conversation steering. This method allows you to monitor packets sent to one or more specific MAC addresses. You can monitor a port and MAC addresses at the same time.

The default for conversation steering is disabled; you can enable conversation steering through the console or Web interface. You must select the port (or MAC addresses) to be monitored and the port doing the monitoring. Only one monitored/monitoring port pair can be active on the switch at one time. Any port (10 Mb/s or 100 Mb/s) can be the monitored or monitoring port.

Caution: If the monitored port is a high-speed port or a high-speed full-duplex port and the monitoring port is not, data may be lost.

For instructions to set up conversation steering from the console interface, refer to "Setting Up Conversation Steering" on page 5-31.

For instructions to set up conversation steering from the Web management interface, refer to "Setting Up Conversation Steering" on page 6-27.

Using the Ping Feature

The BayStack 310-24T switch lets you easily determine if an IP station is on the network and active by allowing you to send a ping request to its IP address. You can send a ping request from the console interface or from the Web interface.

To send a ping request from the console interface:

1. **From the Main Menu, type 3 to display the Troubleshooting Menu.**
2. **Type 1 to select Ping Remote Station, and enter the IP Address of the remote station.**

   The switch pings this station and then informs you if the station is “alive” or if there is no answer.

From the Web interface, select the Ping/Telnet page from the Fault Management folder and enter the IP address.

MAC Table Lookup

The Troubleshooting Menu in the console or Telnet interface (accessed by typing 3 from the Main Menu) also has a MAC Table Lookup option (2).

The MAC Table Lookup allows you to look up specific entries in the switch forwarding table using a specific MAC address as the access key. After typing 2 from the Troubleshooting menu, you are asked to enter the MAC address. If the address is a learned address, information about the port on which it was learned and the type of address (static, dynamic, or filtered) is displayed. If the address is not a learned address, a Not Found message is displayed.

Broadcast Storm Protection

To protect the CPU from being overloaded by processing excessive packets during broadcast storms, the BayStack 310-24T switch automatically disables broadcast traffic to the CPU when broadcast and multicast traffic exceeds 500 packets per second. Traffic to the CPU is restored when the number of packets drops below 200 packets per second. During this time, unicast traffic to the CPU is not affected and traffic through the switch continues to be forwarded normally.

In addition, when Spanning Tree Protocol is enabled, if broadcast and multicast traffic exceeds 3,000 packets per second, the ports are momentarily put into a listening state and then into the forwarding state. If the switch is the source of the broadcast storm due to unresolved loops, this momentary transition alleviates the problem.

The BayStack 310-24T switch provides an additional option for broadcast protection by allowing you to disable packet forwarding to ports when a high threshold is reached and maintain this state until a low threshold is reached. Forwarding During Broadcast Storms is enabled as a default. When Spanning Tree Protocol is enabled, you can disable forwarding, putting forwarding ports in the listening state when the broadcast storm reaches the high threshold. During the broadcast storm, the port states appear to the console/Telnet interface, the Web interface, or SNMP as they were before the high threshold was reached. Spanning Tree Protocol packets continue to be received by the CPU. After the broadcast storm drops below the low threshold, the original states of the ports are restored.

The high threshold is reached when more than 10,000 broadcast or multicast packets per second are received for five seconds. The low threshold is reached when the number of broadcast or multicast packets per second drops below 3,000 for three seconds. Changing the devices attached to the switch or loss of BPDUs due to the broadcast storm may cause the Spanning Tree Protocol to reconfigure and put some ports into forwarding mode again even if the broadcast storm condition still exists. Note that this option is valid only when Spanning Tree Protocol is enabled.

Caution: Disabling forwarding during broadcast storms can cause loss of connectivity through the switch during broadcast storms.

You enable or disable this feature from the Troubleshooting menu in the console or Telnet interface (accessed by typing 3 from the Main Menu).

Using the Boot Options Menu to Upgrade Switch Software

You can access the System Reset/Upgrade menu from the Boot Options Menu following a system reset. After a reset, the Power On Self Test screen is displayed (Figure 7-3).

```
************************************************************************
Bay Networks BayStack 310-24T Ethernet Switch

************************************************************************
Power On Self Test

UART Local Loopback Test… PASSED
CPU Test… PASSED
Stack DRAM Test… PASSED
DRAM Test… PASSED
Watchdog Timer Test… PASSED
Timer Module Test… PASSED
FLASH Image Checksum Test… PASSED
Software Version (1.0)


Enter ".<RETURN>" to go to Boot Options Menu
Booting Switch software
```

Figure 7-3. Power On Self Test Screen

1. **Press [.]+[Return] when the Power On Self Test screen is displayed.**

   Pressing [.]+[Return] interrupts the power-up self-tests and displays the Boot Options Menu (Figure 7-4).

```
************************************************************************
Bay Networks BayStack 310-24T Ethernet Switch
MAC Address: 00.00.00.00.00.00
************************************************************************
Boot Options Menu

1---Upgrade Switch Software
2---Boot Switch Software
3---Clear switch configuration


Enter Command: [1]
```

Figure 7-4. Boot Options Menu

2. Type 1 to select Upgrade Switch Software.

The System Reset/Upgrade menu is displayed (Figure 7-5).

```
************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                             [134.177.160.117]
MAC Address:                            [00:00:80:bb:20:44]
Software Version:                       [1.0]
System Up Time:                         [1d:02h:33m:58s]
Switch Status:                          [Switching]
************************************************************************

                       System Reset/Upgrade

1 ---TFTP Server IP Address [134.177.160.93]
2 ---Default Gateway IP Address [134.177.160.1]
3 ---Software Image File Source [Remote / reload.wire]
4 ---Configuration File Source [Local /]
5 ---Specify Reset Action [Reset]
6 ---Set/Clear Reset Action Timer [0 min.]

0 ---Immediate Reset Action


Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure 7-5. System Reset/Upgrade Menu

3. **Type 3 to specify the software image file source. At the prompt, select Remote and enter the file name.**
4. **Type 5 to select a Reset Action. At the prompt, select Download.**
5. **Type 6 to set the reset action timer and schedule the upgrade for a later time, or type 0 to execute an immediate reset action.**

Appendix A
Technical Specifications

This appendix provides the following technical specifications for the BayStack 310-24T switch:

- General specifications (starting on this page)
- Power cord specifications (page A-3)
- Connector pin assignments (page A-5)
- Factory default settings (page A-8)

General Specifications

Network Protocols	Ethernet Fast Ethernet
Standards Supported	802.1d 802.1q 802.3i, 10BASE-T 802.3u, 100BASE-T 802.3x
Data Rate	
Ports 1 through 24	10 Mb/s
Port 25	10/100 Mb/s
Ports 26 and 27 (Optional)	10/100 Mb/s (10/100BASE-TX MDA) or 100 Mb/s (100BASE-FX MDA)

Electrical Specifications	
Input current:	1.5 to 0.6 Amps
Input voltage (rms):	90 to 250 VAC @ 47 to 63 Hz
Power consumption:	60 W maximum
Environmental Specifications	
Operating temperature:	0° to 40° C (32° to 104° F)
Storage temperature:	–25° to 70° C (–13° to 158° F)
Operating humidity:	85% maximum relative humidity, noncondensing
Storage humidity:	95% maximum relative humidity, noncondensing
Operating altitude:	3024 m (10,000 ft)
Physical Specifications	
Height: Depth: Width: Weight:	2.77 in. (7 cm) 13.55 in. (34.4 cm) 17.25 in. (43.8 cm) 7 lb 5 oz (3.28 kg)
Performance Specifications	
Maximum Frame Forward Rate (64-byte packets, full duplex unicast traffic):	Line rate: 651 kp/s
Port forwarding Performance (64-byte packet) RX:	For 10 Mb/s: 14,880 packets per second max For 100 Mb/s: 148,810 packets per second
Address database size:	2048 entries
Address:	48-bit MAC address
Frame length:	64 to 1535 bytes
MTBF (estimated):	**420,000** hours
Hardware Architecture	
Processor:	68340 16 MHz
EEPROM:	4 KB (nonvolatile)
Processor DRAM:	4 MB
Buffer pool:	4 MB SDRAM
Flash memory:	1 MB

Electromagnetic Immunity	
RF Susceptibility:	IEC801-3, Level 2
Electrostatic discharge (ESO):	IEC801-2, Level 2/3
Electrical Fast Transitions (EFT/B):	IEC801-4, Level 1/2
Electromagnetic Emissions	FCC Class A digital devices En 55 022 (CISPR 22), Class A VCCI Class 1 ITE
Safety Agency Approvals	UL Listed CUL CB report and certificate ANSI/NFPA 70 National electrical code; article 110-16, 110-17, 110-18

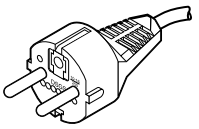
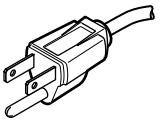
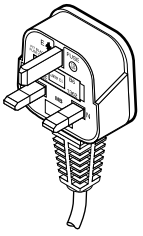
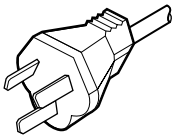
Power Cord Specifications

For installation outside North America, make sure 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.

Caution: Use only power cords with a grounding path. Without a proper ground, a person touching the unit is in danger of receiving an electrical shock. Lack of a grounding path to the unit may result in excessive conducted or radiated emissions.

Table A-1 lists specifications for international power cords.

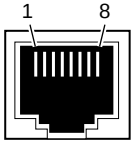
Table A-1. International Power Cord Specifications

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

Pin Assignments

Table A-2 shows the pin assignments for the 10BASE-T ports on the BayStack 310-24T switch.

Table A-2. RJ-45 Connector Pin Assignments

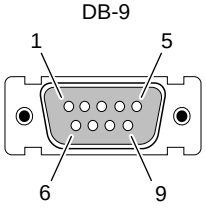


3165.1

Pin	MDI-X Signal
1	Receive data + (RD+)
2	Receive data – (RD–)
3	Transmit data + (TR+)
4	Not used
5	Not used
6	Transmit data – (TD–)
7	Not used
8	Not used

Table A-3 shows pin assignments for the console port.

Table A-3. DB-9 Connector Pin Assignments



3166.3

Pins	Signal Name	Direction
1	Not used	
2	Transmit data, TD	To terminal
3	Receive data, RD	From terminal
4	Not used	
5	Common signal ground	
6	Not used	
7	Not used	
8	Not used	
9	Not used	

MDI and MDI-X Connections

For communication to take place between two devices, the transmitter of one device must connect to the receiver of the other device. The connection must be achieved through a crossover function, which could be a crossover cable or a port that implements the crossover function internally.

The BayStack 310-24T switch uses MDI-X ports that allow you to connect directly to end stations without using crossover cables (Figure A-1). Ports that implement the crossover function internally are known as MDI-X ports (where "X" refers to the crossover function).

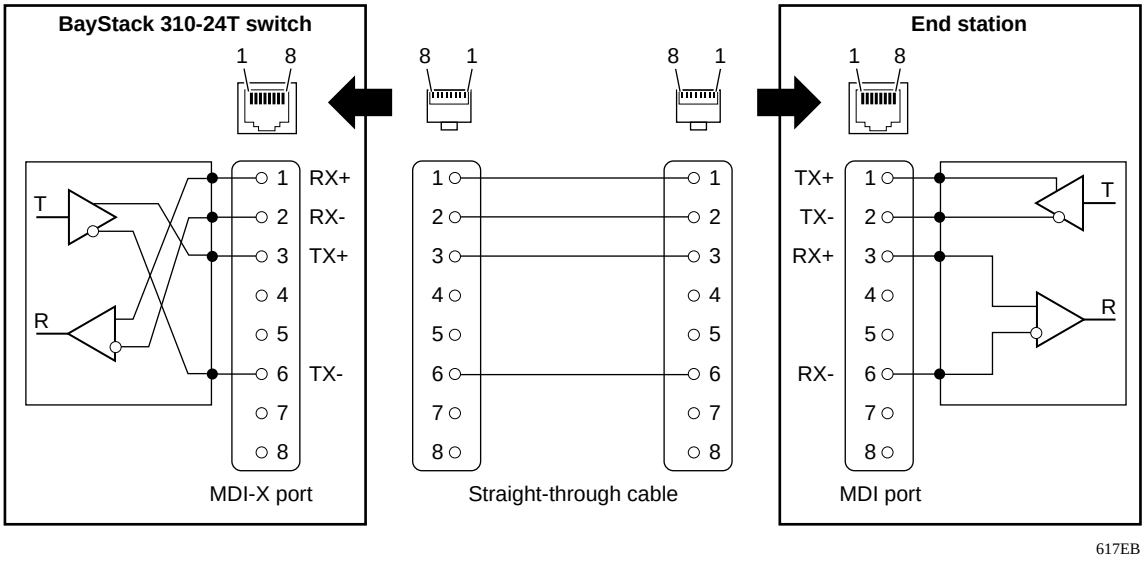


Figure A-1. MDI-X to MDI Cable Connections

If you are connecting a device to the BayStack 310-24T switch that also implements MDI-X ports (Figure A-2), use a crossover cable.

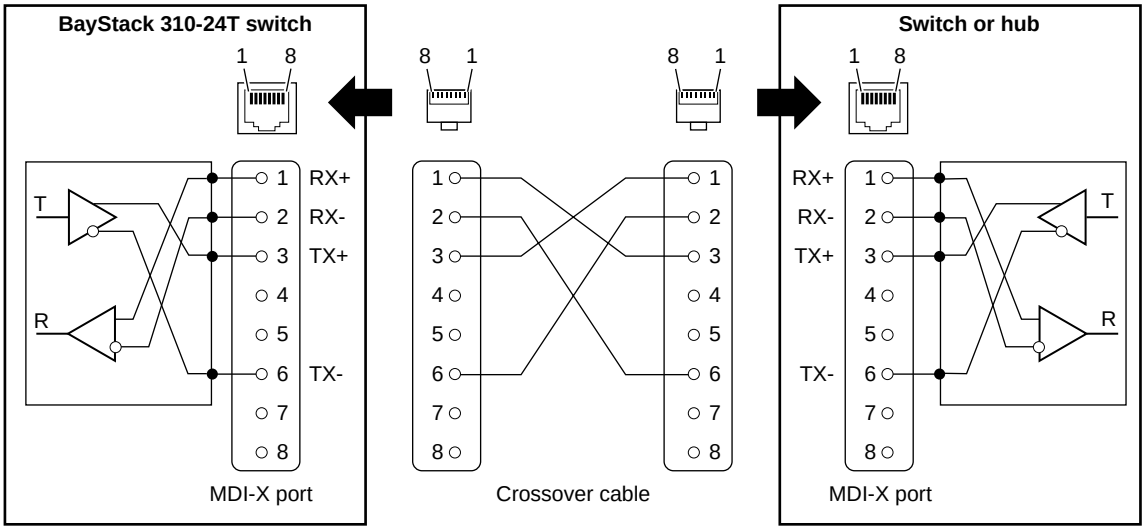


Figure A-2. MDI-X to MDI-X Cable Connections

Factory Default Settings

When you first turn on power to the switch, it begins operation using the factory default settings for configuration parameters. Table A-4 lists the default values.

Table A-4. Factory Default Settings

Type	Parameter	Default Value
Miscellaneous	High Speed Ports (Speed and Duplex)	Autonegotiation Enabled
	Ports (Enabled/Disabled)	Enabled
	Address Filtering	No Entries
	Port-Based VLANs	All ports in VLAN 1
	Uplink Ports	None
	Forwarding during broadcast storms	Enabled
Conversation Steering	Conversation steering	Disabled
	Monitored Port	None
	Monitoring Port	None
IP	IP Address	127.0.0.2
	IP Subnet Mask	0.0.0.0
	Default Gateway Address	0.0.0.0
TFTP	TFTP Server Address	0.0.0.0
	TFTP Default Gateway Address	0.0.0.0
	Download File Name	None
Reset	Reset Action	None
	Reset counter	0 (delay not in effect)
Access	Telnet Access	Enabled
	Web Access	Enabled
	Telnet/Web/Console Password	None Assigned
	Console/Telnet Timeout	15 minutes (fixed)

Table A-4. Factory Default Settings (continued)

Type	Parameter	Default Value
SNMP	Read Community String	Public
	Read/Write Community String	Private
	Trap Receiver Server IP (1–4)	0.0.0.0
	Trap Receiver Community String (1–4)	Public
	Trap Receiver Status (1–4)	Unknown
	Authentication Trap Generation	Disabled
	Link Up/Down Trap Generation	Enabled
	Autotopology	Enabled
Spanning Tree Protocol	Spanning Tree Protocol	Enabled on all ports
	Aging Time (4–1000000)	300 seconds
	Bridge Priority (0–65535)	32768
	Hello Time (1–10)*	2 seconds
	Bridge Max Age Time (6–40)*	20 seconds
	Bridge Forward Delay (4–30)*	15 seconds
	Port Priority (0–255)	128
	Port Path Cost (1–65535)† • Note: 10 Mb/s ports are half duplex only	10 Mb/s Half duplex: 100 10 Mb/s Full duplex: 50 100 Mb/s Half duplex: 10 100 Mb/s Full duplex: 5
RMON	Alarm Entries	None (maximum: 20)
	Event Entries	None (maximum: 20)
	Log Entries	None (maximum: 20)
	History (history buckets)	None (maximum: 150)

* Maximum ranges are limited by the following interrelationship of these parameters:
2x (Bridge Forward Delay - 1) ≥ Bridge Maximum Age Time ≥ 2x (Bridge Hello Time +1)

† Port path cost manually set by the user will remain unchanged regardless of duplex mode.

Appendix B
LEDs

Table B-1 provides details of the operation of the LEDs on the BayStack 310-24T Ethernet Switch.

Table B-1. Front-Panel LEDs

Type	Label	Color	State	Meaning
Port link status	Link	Green	On	The connection to a device is active.
			Blinking	Data is being transmitted over the link.
			Off	The link is inoperative or improperly connected.
AC power supply status	Power	Green	On	The switch is receiving valid AC power.
			Off	The switch is not receiving valid AC power, or the internal power supply has failed.
System status	Status	Green	On	The unit is operating properly.
			Blinking	The unit is performing self-tests or network configuration.
			Off	A system fault has occurred.
100 Mb/s speed indicator*	100	Green	On	The port is operating at 100 Mb/s.
			Off	The port is operating at 10 Mb/s.
Full-duplex indicator*	F Dx	Green	On	The 10/100 Mb/s port is operating in full-duplex mode (simultaneous transmit and receive).
			Off	The 10/100 Mb/s port is operating in half-duplex mode (transmit or receive).

* Indicator applies to 10/100BASE-TX port only.

The AC power supply status LED and the system status LED work together to provide status information. Table B-2 defines the meanings of these two LEDs.

Table B-2. Power and Status LEDs

Power	Status	Meaning
Off	Off	System off.
On	Off	System fault detected by power-up diagnostics.
On	Blinking	System is powered on and performing self-tests or network configuration.
On	On	Normal operation.

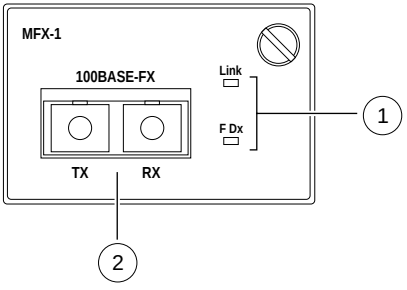
Appendix C
Media Dependent Adapters (MDAs)

The BayStack 310-24T switch has two slots for media adapters to provide additional 100 Mb/s ports. The media adapter slots accept either a 10/100BASE-TX (UTP) or 100BASE-FX (fiber) media adapter to provide a switched Fast Ethernet link to high-speed servers, switches, hubs, or routers.

This appendix describes the MDA types available and provides instructions for installing them in the switch.

100BASE-FX MDA

The 100BASE-FX MDA is used to attach a fiber-based 100 Mb/s connection to the switch. The 100BASE-FX media adapter (Figure C-1) can be used to provide a direct attachment to end stations, switches, or servers where multimode fiber is installed. This adapter accepts standard SC connections using 62.5/125-µm fiber optic cable. The 100BASE-FX MDA is not supported on single-mode fiber cable.



1 = LEDs
2= 100BASE-FX SC port connector

Figure C-1. 100BASE-FX MDA

A link LED indicates when there is a valid link connection, and a mode LED indicates when the port is operating in full- or half-duplex mode (effectively 200 Mb/s or 100 Mb/s).

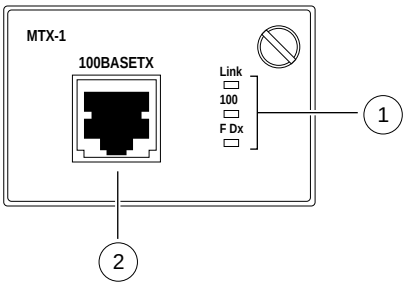
The 100BASE-FX MDA has the LEDs listed in Table C-1.

Table C-1. 100BASE-FX MDA LEDs

Label	Color	State	Meaning
Link	Green	On	Link is active and connected correctly.
		Off	Link is inoperative or improperly connected.
F Dx	Green	On	Port is set to operate in full-duplex mode (200 Mb/s).
		Off	Port is set to operate in half-duplex mode (100 Mb/s).

10/100BASE-TX MDA

The 10/100BASE-TX MDA (Figure C-2) supports autonegotiation for either 10 Mb/s or 100 Mb/s operation, depending on the connecting device.



1 = LEDs
2 = 10/100BASE-TX RJ-45 connector

Figure C-2. 10/100BASE-TX MDA

Because this port is capable of operating at 100 Mb/s, Bay Networks recommends that only Category 5 UTP cabling be used for connections to the RJ-45 port connector (see Table A-2 on page A-5 for RJ-45 pin assignments). For operation at 10 Mb/s, Category 3 or 4 cable is adequate.

The 10/100BASE-TX port also supports operation in full- and half-duplex mode. In full-duplex mode, the aggregate transfer can be either 20 Mb/s or 200 Mb/s (for simultaneous transmit and receive at 100 Mb/s each), depending on the speed of the connecting device. In half-duplex mode, the transfer speed is either 10 Mb/s or 100 Mb/s (transmit or receive).

Table C-2 lists the LEDs on the 10/100BASE-TX MDA.

Table C-2. 10/100BASE-TX MDA LEDs

Label	Color	State	Meaning
Link	Green	On	Link is active and connected correctly.
		Off	Link is inoperative or improperly connected.
100	Green	On	Port is set to operate at 100 Mb/s.
		Off	Port is set to operate at 10 Mb/s.
F Dx	Green	On	Port is set to operate in full-duplex mode (200 Mb/s).
		Off	Port is set to operate in half-duplex mode (100 Mb/s).

Installing an MDA

Before you install an MDA, disconnect the switch from all power.

Warning: The switch must be taken offline and have all power removed prior to installing the MDA. Failure to remove power can result in damage to sensitive components and void all equipment warranties.

To install an MDA:

1. **Unplug the AC power cord from the power outlet.**
2. **Remove the filler panel over an expansion slot.**

3. **Insert the MDA into the slot, taking care to slide the MDA onto the guides (see Figure C-3).**

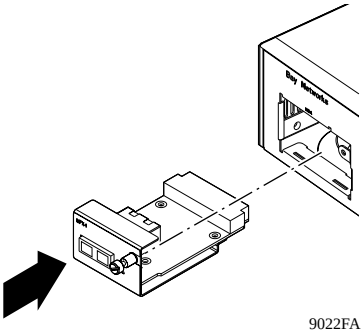


Figure C-3. Installing an MDA

The guides ensure that the MDA connector plugs correctly into the switch motherboard.

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

4. **Tighten the thumb screw to secure the MDA in the switch.**
5. **Attach the high-speed device to the port.**
6. **Plug the AC power cord into the power outlet.**

Appendix D
BayStack 310-24T Switch Console Interface

This appendix describes the menus and screens that make up the console or Telnet interface for the BayStack 310-24T switch. This interface allows you to access the agent software that provides management and configuration control of the switch. For information about using the Web interface, refer to Chapter 6, "Managing the BayStack 310-24T Switch Using a Web Browser." Refer to Chapter 3, "Installing the BayStack 310-24T Switch" for installation, connection, and quick configuration procedures.

This appendix includes the following information:

- A map of the Main Menu hierarchy (page D-2)
- Descriptions of the information found on the interface menus and screens (beginning on page D-5)

Menu and Screen Navigation

The agent software on the BayStack 310-24T switch provides menus and screens that allow you to configure and manage your network environment. A menu provides the ability to set and change parameters, and a screen presents current status and parameter settings. The menus and screens can be accessed from the console or through a Telnet connection.

Figures D-1 through D-4 show the menu and command hierarchy. The following sections describe each menu and screen and the associated submenu and screen displays.

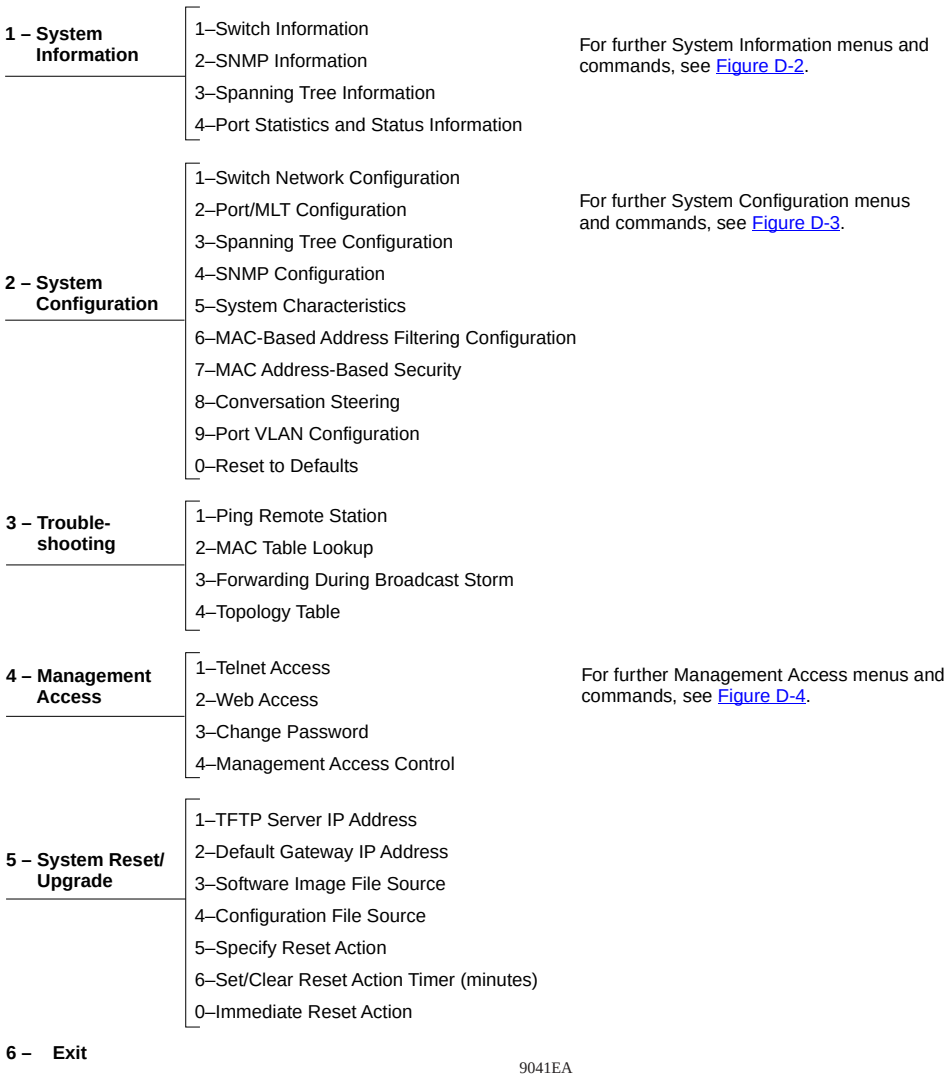


Figure D-1. Main Menu and Command Hierarchy

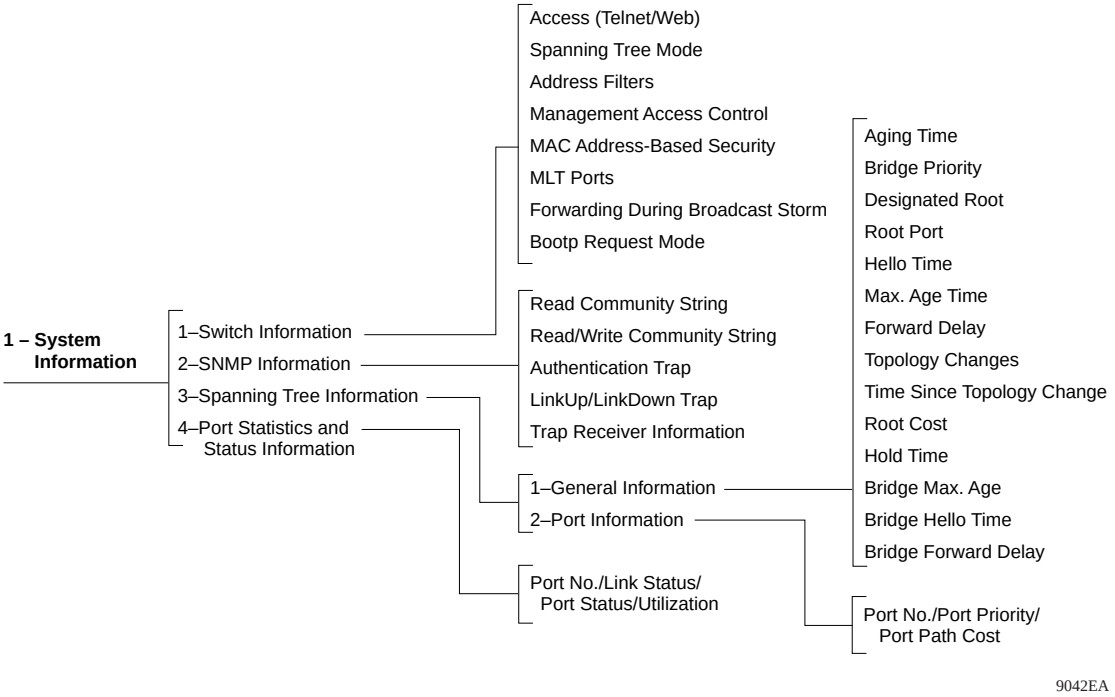


Figure D-2. System Information Menus and Commands

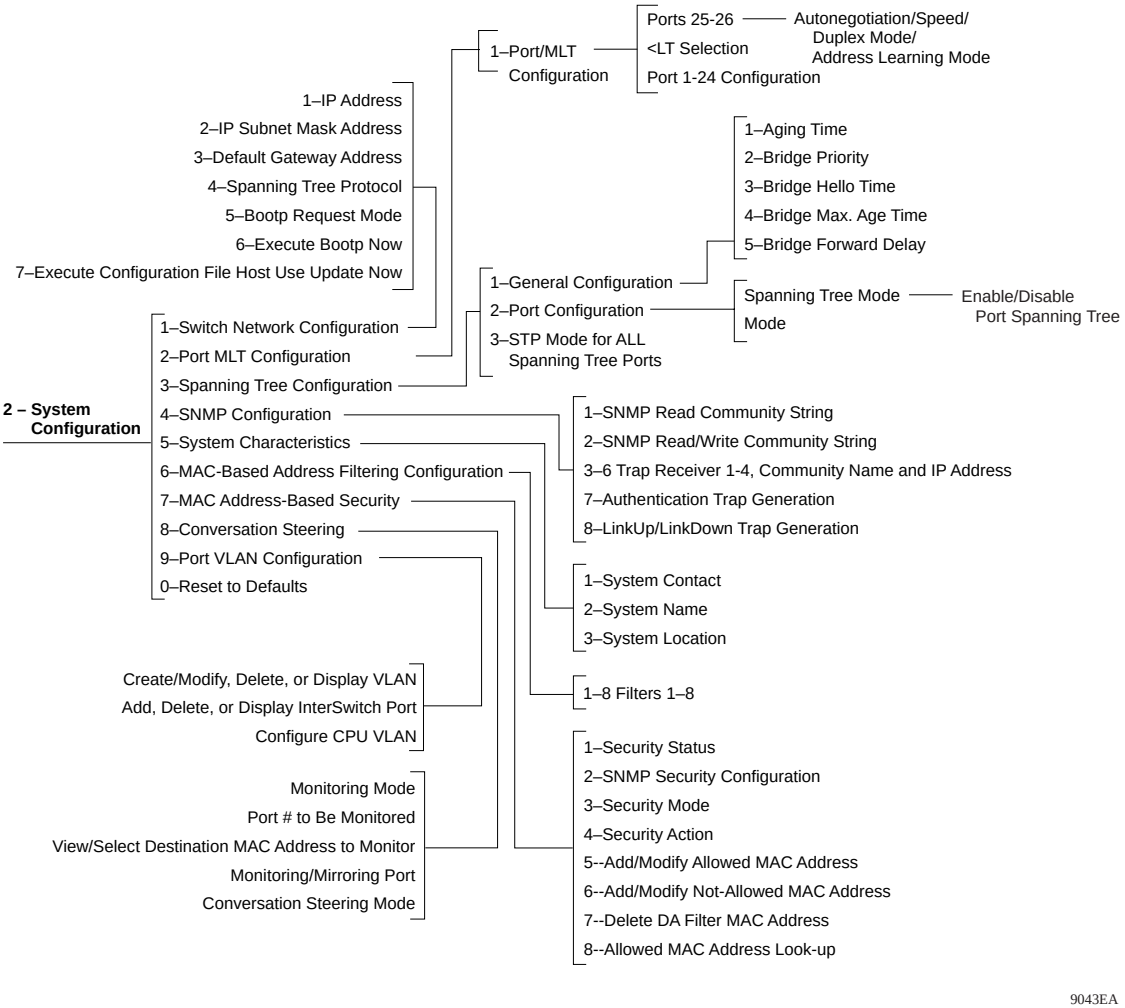


Figure D-3. System Configuration Menus and Commands

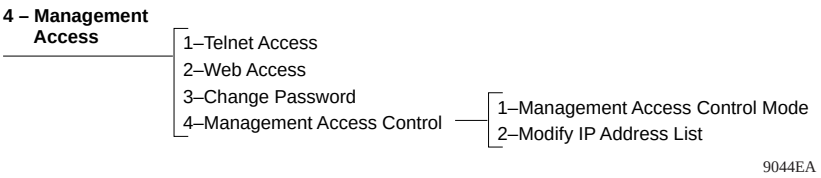


Figure D-4. Access Control Menus and Commands

Main Menu

The Main Menu (Figure D-5) is displayed when the switch boots.

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:00h:53m:07s]
Switch Status:                           [Switching]
********************************************************************************

                        Main Menu

1 ---System Information
2 ---System Configuration
3 ---Troubleshooting
4 ---Management Access
5 ---System Reset/Upgrade
6 ---Exit




Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen):
```

Figure D-5. Main Menu

Table D-1 shows the options available from the Main Menu.

Table D-1. Main Menu Commands

Command	Meaning
1—System Information	Displays the System Information Menu, which allows you to view current parameter settings for the switch, SNMP configuration, spanning tree configuration, and port statistics.
2—System Configuration	Displays the System Configuration Menu, which allows you to set or change switch parameters.
3—Troubleshooting	Displays the Troubleshooting Menu, which allows you to perform some basic troubleshooting steps.
4—Management Access	Displays the Access Control Menu, which allows you to set or change the system password and to set up management access and network access controls.
5—System Reset/Upgrade	Displays the System Reset/Upgrade Menu, which allows you to reset the switch or upgrade software.
6—Exit	Terminates the current session.

System Information

When you type 1 from the Main Menu, the System Information Menu is displayed (Figure D-6). This menu includes commands that display screens showing the current parameter settings for the switch. All of the screens associated with system information are read only. To change any parameter or setting, you must go through the System Configuration Menu, except for the Forwarding During Broadcast Storm option, which is enabled or disabled from the Troubleshooting screen.

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:00h:56m:04s]
Switch Status:                           [Switching]
********************************************************************************

                        System Information

1 ---Switch Information
2 ---SNMP Information
3 ---Spanning Tree Information
4 ---Port Statistics and Status Information









Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen):
```

Figure D-6. System Information Menu

The System Information menu provides four paths to switch statistics and status information. Table D-2 shows the commands available from this menu.

Table D-2. Commands on the System Information Menu

Command	Meaning
1—Switch Information	Displays the Switch Information screen.
2—SNMP Information	Displays the SNMP Information screen.
3—Spanning Tree Information	Displays the Spanning Tree Information screen.
4—Port Statistics and Status Information	Displays the Port Statistics and Status Information screen.

Switch Information

When you type 1 from the System Information menu, the Switch Information screen is displayed (Figure D-7).

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:00h:56m:44s]
Switch Status:                           [Switching]
********************************************************************************

                        Switch Information

Access (Telnet/Web): [Enabled/Enabled]
Spanning Tree Mode: [Enabled]
Address Filters: [0]
Management Access Control: [Unrestricted]  Specified Addresses: [0]
MAC-Address-Based Security: [Disabled/Single-MAC-per-port]
MLT Ports: [25, 26]
Forwarding During Broadcast Storm: [Enabled]
BootP Request Mode: [When Needed]




Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen):
```

Figure D-7. Switch Information Screen

The Switch Information screen lists the switch parameters described in Table D-3.

Table D-3. Switch Information Screen Parameters

Parameter	Meaning
Access (Telnet/Web)	Indicates whether Telnet access to the console interface and network access to the Web management interface are enabled or disabled. The default is Enabled.
Spanning Tree Mode	Indicates whether the Spanning Tree Protocol is enabled or disabled on all ports. The default is Enabled.
Address Filters	Indicates the number of address filters (0 to 8) that have been set for the switch.
Management Access Control	Indicates whether management access is restricted or unrestricted. Restricted access means only a maximum of eight specified IP addresses can access the management functions of the switch. Unrestricted means all users can access the switch management functions. **Note:** This setting operates independently of the password function.
MAC Address-Based Security	Indicates whether MAC address based security is enabled for network access. Choices are: • Disabled • Single-MAC-per-port, which allows only a single specified MAC address to access a specified port • MAC List, which specifies a list of MAC addresses that can access the switch. For each address you can specify the ports it is allowed to connect to.
MLT Ports	Shows which high-speed ports are assigned to a multilink trunk.

Table D-3. Switch Information Screen Parameters (continued)

Parameter	Meaning
Forwarding During Broadcast Storm	Indicates whether broadcast storm blocking is selected (forwarding disabled) for all ports. This option is valid only if Spanning Tree mode is enabled. The default is Enabled.
BootP Request Mode	Indicates the BootP request mode for the switch. Choices are: • When Needed (default setting)—If the IP address stored in the nonvolatile memory is the factory default value (127.0.0.2), the switch uses BootP to request configuration settings. If the stored IP address is different from the factory default value, the switch uses the stored network parameters. • Always—The switch boots, ignoring any stored network parameters, and uses BootP to request network configuration parameters. If the BootP request fails, the switch continues to send BootP requests at one-minute intervals. This setting disables remote management if no BootP server is set up for the switch, but it allows the switch to operate normally. • Disabled—The switch boots using the IP configuration parameters stored in nonvolatile memory. If a BootP configuration is in progress when you issue this command, the BootP configuration stops. • Last Address—At startup, the switch tries to obtain its IP configuration using BootP. If the BootP request fails, the switch uses the network parameters stored in its nonvolatile memory.

SNMP Information

When you type 2 from the System Information menu, the SNMP Information Screen is displayed (Figure D-8).

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                               [134.177.221.67]
MAC Address:                              [00:00:81:0a:0b:13]
Software Version:                         [1.0]
System Up Time:                           [0d:00h:57m:10s]
Switch Status:                            [Switching]
********************************************************************************
                        SNMP Information

SNMP Read Community String: [public]
SNMP Read/Write Community String: [private]
Authentication Trap: [Disabled]
LinkUp/LinkDown Trap: [Enabled]

Trap Receiver Information:
No.      Status        IP Address        Community String
1        None          0.0.0.0           public
2        None          0.0.0.0           public
3        None          0.0.0.0           public
4        None          0.0.0.0           public

Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen):
```

Figure D-8. SNMP Information Screen

The SNMP Information screen includes the switch parameters described in Table D-4.

Table D-4. Information on the SNMP Information Screen

Parameter	Meaning
SNMP Read Community String	Displays the community string used for in-band read-only SNMP operations. The default is public.
SNMP Read/Write Community String	Displays the community string used for in-band read-only SNMP operations. The default is private.
Authentication Trap	Indicates if authentication trap generation is enabled or disabled. The default is disabled.
LinkUp/LinkDown Trap	Indicates if link up/down trap authentication is enabled or disabled. The default is enabled.
Trap Receiver Information	Indicates if Trap Receivers 1 through 4 are enabled, disabled, or none. If traps are set, this parameter also displays the associated IP address and community string.

Spanning Tree Information

When you type 3 from the System Information menu, the Spanning Tree Information menu is displayed (Figure D-9).

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:00h:57m:33s]
Switch Status:                           [Switching]
********************************************************************************

                        Spanning Tree Information

1 ---Spanning Tree General Information
2 ---Spanning Tree Port Information









Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen):
```

Figure D-9. Spanning Tree Information Menu

The Spanning Tree statistics and information are divided into two areas:

- 1—Spanning Tree General Information
- 2—Spanning Tree Port Information

Spanning Tree General Information

A series of Spanning Tree General Information screens (Figure D-10) display information about how Spanning Tree Protocol is set up for the entire switch.

```
********************************************************************************
Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:00h:57m:53s]
Switch Status:                           [Switching]
********************************************************************************

                        Spanning Tree General Information

Aging Time (sec): [300]
Bridge Priority: [32768]
Designated Root: [32768 - 00:00:81:0a:0b:13]
Root Port: [0]
Hello Time (sec): [2]
Max Age Time (sec): [20]
Forward Delay (sec): [15]



[ctrl-n]---Next Page    [ctrl-p]---Previous Page
Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen):
```

Figure D-10. Spanning Tree General Information Screen

General Spanning Tree information requires several screens to display all the listed parameters. Pressing [Ctrl +n] or [Ctrl+p] scrolls the display from screen to screen of the parameters.

Table D-5 lists the parameters included in the General Spanning Tree Information screens.

Table D-5. Information on the Spanning Tree General Information Screens

Parameter	Meaning
Aging Time	The number of seconds a learned MAC address can be inactive before it is “aged” or unlearned. This field is configurable in the range of 4 to 1,000,000 seconds with a default of 300 seconds.
Bridge Priority	Which bridge within the network is designated as the root bridge (bridge with the highest priority). This field is configurable in the range of 0 to 65535 (where low number = high priority) with a default of 32768. **Note:** When Spanning Tree Protocol is disabled, the spanning tree default parameters are reset to “0.” Values you set manually are not changed.
Designated Root	The identifier for the root bridge.
Root Port	The port that offers the lowest cost path from this bridge to the root bridge.
Hello Time	The number of seconds that elapse between hello time messages that are sent from the root switch to all other switches; this value is determined by the Spanning Tree Protocol root switch.
Max Age Time	The maximum age (in seconds) of information before it is discarded. This value is learned from the network and determined by the Spanning Tree Protocol root switch.
Forward Delay	How many seconds the switch delays forwarding frames after a network topology change. This value is also determined by the Spanning Tree Protocol root switch.
Topology Changes	The total number of topology changes detected by this bridge since the management entity was last reset or initialized.
Time Since Topology Change	The time since the last topology change was detected by the bridge entity.
Root Cost	The path cost from the switch to the designated root bridge.
Hold Time	The time interval (1-10 seconds) during which no more than two configuration bridge PDUs will be transmitted by this node.

Table D-5. Information on the Spanning Tree General Information Screens (continued)

Parameter	Meaning
Bridge Max Age	The maximum age (in seconds) that a hello message can attain before it is discarded. The parameter set for this bridge through the interface takes effect only if this bridge becomes the root bridge. The root bridge maximum age time parameter value becomes the (actual) Maximum Age Time parameter value for all bridges in the spanning tree network (see also Maximum Age Time parameter). This field is configurable in the range of 6 to 40 seconds with a default of 20 seconds
Bridge Hello Time	The Hello interval (the amount of time between transmissions of Configuration Bridge PDUs) that is specified through the management interface for this bridge. This parameter takes effect only when this bridge becomes the root bridge. The range is 1 to 10 seconds with a default of 2 seconds. **Note:** Although you can set the hello time for a bridge with bridge management software, once the spanning tree computation process is complete, all bridges participating in spanning tree 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 in the spanning tree network (see also Hello Time parameter).
Bridge Forward Delay	The Forward Delay parameter value that is specified for this bridge. All bridges participating in the spanning tree network use the root bridge's Forward Delay parameter value (see also the Forward Delay parameter definition on page D-15). The range is 4 to 30 seconds with a default of 15 seconds.

Spanning Tree Port Information

The Spanning Tree Port Information screen (Figure D-11) shows port-specific information about the Spanning Tree Protocol.

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:00h:58m:41s]
Switch Status:                           [Switching]
********************************************************************************

                        Spanning Tree Port Information

Port #              Port Priority            Port Path Cost
1                   [128       ]             [100       ]
2                   [128       ]             [100       ]
3                   [128       ]             [100       ]
4                   [128       ]             [100       ]
5                   [128       ]             [50        ]
6                   [128       ]             [50        ]
7                   [128       ]             [50        ]
8                   [128       ]             [50        ]

[ctrl-n]---Next Page    [ctrl-p]---Previous Page
Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen):
```

Figure D-11. Spanning Tree Port Information Screen

Table D-6 shows the information included in the Spanning Tree Port Information screen.

Table D-6. Information on the Spanning Tree Port Information Screen

Parameter	Meaning
Port #	The number of each port on the switch.
Port Priority	The priority of each port, which is used in conjunction with the port number to create a unique port identifier. The valid range for this value is from 0 to 255. The default value is 128.
Port Path Cost	The path cost to the designated root bridge. The valid range for this value is from 1 to 65,535. Entering a value of 0 (from the Port Configuration menu) resets to the factory default setting so the switch software can automatically compute the path cost proportional to speed and duplex mode.

Port Statistics and Status Information

The Port Status Information screens (Figure D-12) list all port numbers with information about each port. The screens also allow you to view statistics for individual ports. Each screen lists eight port numbers. Press [ctrl-n] to see the next set of port numbers or [ctrl-p] to see the previous set of port numbers.

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:00h:59m:56s]
Switch Status:                           [Switching]
********************************************************************************

                        Port Status Information

Command            Link Status/Duplex   Port Status         Utilization
1 ---Port 1        Down/Half            Disabled            0%
2 ---Port 2        Up/Half              Forwarding          0%
3 ---Port 3        Down/Half            Disabled            0%
4 ---Port 4        Down/Half            Disabled            0%
5 ---Port 5        Down/Half            Disabled            0%
6 ---Port 6        Down/Half            Disabled            0%
7 ---Port 7        Down/Half            Disabled            0%
8 ---Port 8        Down/Half            Disabled            0%

[ctrl-n]---Next Page    [ctrl-p]---Previous Page
Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen):
```

Figure D-12. Port Status Information Screen

Table D-7 lists the information on the Port Status Information Screen.

Table D-7. Information on the Port Status Information Screen

Parameter	Meaning
Link Status/Duplex	Whether or not a device link is active, and what duplex mode is set for the port.
Port Status	Whether a port is enabled or disabled. If the port is enabled, the spanning tree status (forwarding or blocking) is also indicated.
Utilization	The percentage of the available bandwidth on the port being used by traffic. Port utilization is computed for the previous five seconds.

To view statistics for a single port, type the command number corresponding to the desired port in the command line. The Port Statistics screen (Figure D-13) displays statistical information about the port using two sets of counters:

- Cumulative:
  These counters provide statistics of data traffic on the port since the switch was powered on or since the last reset. Because all counters contain 32-bit unsigned numbers, counter values on switches that have been powered on for a long time may “roll over” and reset the count to zero.
- Incremental:
  These counters set to zero each time you enter the screen for that port. When you press the SPACE bar to refresh the screen, the displayed values represent the increments to the counters since entering the screen.

```
********************************************************************************
               Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.160.117]
MAC Address:                             [00:00:80:bb:20:44]
Software Version:                        [1.0]
System Up Time:                          [0d:05h:03m:12s]
Switch Status:                           [Switching]
********************************************************************************

                              Port 1 Statistics
                                                 Cumulative    Incremental
Rx Good Frames                                   [7          ] [0          ]
Rx Align Error Frames                            [0          ] [0          ]
Rx CRC Error Frames                              [0          ] [0          ]
Rx Frames Too Long                               [0          ] [0          ]
Tx Good Frames                                   [31         ] [0          ]
Tx Single Collisions                             [0          ] [0          ]
Tx Multiple Collisions                           [2          ] [0          ]
Deferred Transmissions                           [0          ] [0          ]
Tx Late Collisions                               [0          ] [0          ]
Tx Excessive Collisions                          [0          ] [0          ]
Tx Carrier Sense Errors                          [0          ] [0          ]
Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen):
```

Figure D-13. Port Statistics Screen

Table D-8 lists the information on the Port Statistics screen.

Table D-8. Information on the Port Statistics Screen

Parameter	Meaning
Rx Good Frames	The counter increments whenever a frame is received successfully on the port.
Rx Align Error Frames	The counter records frame alignment errors for the 10 Mb/s ports. Misaligned frames are those that do not start or end on a byte boundary.
Rx CRC Error Frames	The cyclic redundancy check (CRC) error counter increments whenever a corrupt frame is received and integrity of the data is lost.

Table D-8. Information on the Port Statistics Screen (continued)

Parameter	Meaning
Rx Frames Too Long	The counter increments whenever a frame is received on this port that is greater than 1,518 octets in length.
Tx Good Frames	The counter increments whenever a frame is transmitted successfully from the port.
Tx Single Collisions	The number of frames transmitted on the port that had a single collision and were transmitted successfully on the second try.
Tx Multiple Collisions	The number of frames transmitted on the port that had more than one collision and were then transmitted successfully within 16 attempts. If a frame transmits successfully after only one collision, it increments the single collision counter. If there are anywhere from two to 16 retries for a successful transmission, then the multiple counter increments. If, after 16 tries, a collision is still detected, the excessive transmission counter increments and no more retries are attempted.
Deferred Transmissions	The number of frames transmitted on the port that were delayed because the wire was busy.
Tx Late Collisions	The number of times a collision on the port has been detected later than 512 bit times into the frame duration.
Tx Excessive Collisions	The number of frames on the port that, due to excessive (16 consecutive) collisions, were not successfully transmitted.
Tx Carrier Sense Errors	The number of times on the port that carrier sense was not seen or was lost during the transmission of a frame without a collision.

System Configuration

When you type 2 on the Main Menu, the System Configuration menu is displayed (Figure D-14). This menu provides the means to change parameter settings within specific areas of the switch network.

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:01h:00m:38s]
Switch Status:                           [Switching]
********************************************************************************

                        System Configuration

1 ---Switch Network Configuration
2 ---Port/MLT Configuration
3 ---Spanning Tree Configuration
4 ---SNMP Configuration
5 ---System Characteristics
6 ---MAC-Based Address Filtering Configuration
7 ---MAC Address-Based Security
8 ---Conversation Steering
9 ---Port VLAN Configuration
0 ---Reset to Defaults

Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen):
```

Figure D-14. System Configuration Menu

This menu contains the following selections, each corresponding to a configuration menu:

- 1—Switch Network Configuration
- 2—Port/MLT Configuration
- 3—Spanning Tree Configuration
- 4—SNMP Configuration
- 5—System Characteristics
- 6—MAC-Based Address Filtering Configuration

- 7—MAC Address-Based Security Configuration
- 8—Conversation Steering
- 9—Port VLAN Configuration
- 0—Reset to Defaults

When you type the appropriate number at the command line, the corresponding menu is displayed.

Switch Network Configuration

When you type 1 from the System Configuration menu, the Switch Network Configuration menu is displayed (Figure D-15).

```
********************************************************************************
               Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:01h:00m:57s]
Switch Status:                           [Switching]
********************************************************************************

                        Switch Network Configuration

1 ---IP Address
2 ---IP Subnet Mask Address
3 ---Default Gateway Address
4 ---Spanning Tree Protocol (Enable/Disable)
5 ---BootP Request Mode
6 ---Execute BootP Now
7 ---Execute Configuration File Host Update Now




Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure D-15. Switch Network Configuration Menu

Table D-9 lists the options on the Switch Network Configuration Menu.

Table D-9. Options on the Switch Network Configuration Menu

Command	Meaning
1—IP Address	Allows you to sets the Internet Protocol (IP) address of the unit. The IP address must be a unique address for initiating a Telnet session or managing a BayStack 310-24T switch using SNMP. The factory default setting of the IP address for the BayStack 310-24T switch switch is 127.0.0.2.
2—IP Subnet Mask Address	Allows you to set the subnet mask that indicates which bits are used for network/subnet identification and which are used for end nodes or stations. The subnet mask is written in the form of an IP address, with all network/subnet bits set to one. The default subnet mask is 0.0.0.0.
3—Default Gateway Address	Allows you to set the address of the IP gateway during normal switch operation. The default gateway address is 0.0.0.0. This address is set separately from the TFTP gateway address used for downloading upgrades from the System Reset/Upgrade screen as described on page D-51.
Note: The switch must be reset for parameters 1–3 to take effect.	
4—Spanning Tree Protocol [Enable/Disable]	Allows you to enable or disable the Spanning Tree Protocol. The default for this field is Enabled **Caution:** The Spanning Tree Protocol protects your network from infinite packet circulation caused by inadvertently creating a configuration containing a loop in the topology. Before you disable Spanning Tree Protocol, be certain that your network is loop-free, or it will instantly become saturated and lock up from the infinite loop traffic.

Table D-9. Options on the Switch Network Configuration Menu (continued)

Command	Meaning
5—BootP request mode	Specifies the conditions under which the switch uses BootP configuration. Choices are: • When Needed (default setting) The switch sends a BootP request when the switch IP address stored in nonvolatile memory is the factory default value. If the stored IP address is different from the factory default value, the switch uses the stored network parameters. If the switch cannot find a BootP server, it tries five more times to find one and then defaults to the factory settings. • Always Each time the switch boots, it ignores any stored network parameters and sends a BootP request. If the BootP request fails, the switch boots with the factory default IP configuration. This setting disables remote management if no BootP server is set up for the switch, but it allows the switch to boot normally. • Disable The switch boots using the IP configuration parameters stored in nonvolatile memory. If a BootP configuration is in progress when you issue this command, the BootP configuration stops • Last Address At startup, the switch tries to obtain its IP configuration using BootP. If the BootP request fails, the switch uses the network parameters stored in its nonvolatile memory. **Note:** Valid parameters obtained using BootP always replace current information stored in the nonvolatile memory
6—Execute BootP now	Initiates an immediate BootP download.
7—Execute Configuration File Host Update Now	Updates a configuration file with the current settings for switch parameters.

Port/MLT Configuration

When you type 2 from the System Configuration menu, the Port/MLT Configuration menu is displayed (Figure D-16). This menu allows you to configure ports 25, 26, and 27. Port 25 is the fixed high-speed port on the BayStack 310-24T switch. Ports 26 and 27 are installed MDAs.

The Port/MLT Configuration menu also provides access to configuration menus for the other ports. When you press [Ctrl-n], a Port Configuration Menu for ports 1 through 24 is displayed.

```
********************************************************************************
               Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:01h:03m:54s]
Switch Status:                           [Switching]
********************************************************************************

                        Port/MLT Configuration

Command             Autonegotiation              Duplex
1 ---Port 25        Enabled                      Half Duplex
              Normal/100 Mbps/MLT
2 ---Port 26        Disabled                     Full Duplex
              Normal/100 Mbps/Fiber/MLT
3 ---Port 27        Enabled                      Full Duplex
              Normal/100 Mbps/Copper/No MLT
4 ---MLT Selection
5 ---Port 1-24 Configuration

[ctrl-n]---Next Page    [ctrl-p]---Previous Page
Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen):
```

Figure D-16. Port/MLT Configuration Menu

Table D-10 describes the commands on the Port/MLT Configuration menu.

Table D-10. Commands on the Port/MLT Configuration Menu

Command	Meaning
1—Port 25, 2—Port 26, and 3—Port 27	Allows you to set to set autonegotiation mode, port speed, duplex mode, and address learning mode (Normal or Uplink). Selecting Uplink for a port disables address learning on the port. Using uplink ports reduces flooding on the local ports. **Note:** If autonegotiation is enabled, you cannot set port speed or duplex mode. Also, you cannot set port speed for an installed 100BASE-FX MDA. These ports operate only at 100 Mb/s.
4—MLT Selection	Allows you to display the Multi-Link Trunking Configuration menu (see the next section, "Multi-Link Trunking Configuration").
5—Port 1–24 Configuration	Displays a port configuration menu for low-speed ports.

Multi-Link Trunking Configuration

When you type 4 from the Port/MLT Configuration menu, the Multi-Link Trunking Configuration menu is displayed (Figure D-17).

This menu allows you to set combinations of the high-speed ports as MultiLink Trunking groups. An information line shows which ports are in the group.

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:02h:51m:25s]
Switch Status:                           [Switching]
********************************************************************************

                        Multi-Link Trunking Configuration

1 ---Port 25 & 26 as a trunking group
2 ---Port 25 & 27 as a trunking group
3 ---Port 26 & 27 as a trunking group
4 ---All port (25, 26 & 27) as a trunking group

0 ---No trunking group

MLT Ports: [25, 26]



Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure D-17. Multi-Link Trunking Configuration Menu

Table D-11 shows the commands on the Multi-Link Trunking Configuration menu.

Table D-11. Commands on the Multi-Link Trunking Configuration Menu

Command	Meaning
1—Port 25 & 26 as a trunking group	Sets these ports as members of a multilink trunk.
2—Port 25 & 27 as a trunking group	Sets these ports as members of a multilink trunk.
3—Port 26 & 27 as a trunking group	Sets these ports as members of a multilink trunk.
4—All ports (25, 26, & 27) as a trunking group	Sets all three high-speed ports as members of a multilink trunk.
0—No trunking group	Specifies that there is no multilink trunking group in this switch.

Spanning Tree Configuration

When you type 3 from the System Configuration menu, the Spanning Tree Configuration menu is displayed (Figure D-18).

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                               [134.177.221.67]
MAC Address:                              [00:00:81:0a:0b:13]
Software Version:                         [1.0]
System Up Time:                           [0d:01h:07m:04s]
Switch Status:                            [Switching]
********************************************************************************

                        Spanning Tree Configuration

1 ---General Configuration
2 ---Port Configuration
3 ---STP Mode For ALL Spanning Tree Ports









Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure D-18. Spanning Tree Configuration Menu

The Spanning Tree Configuration menu provides the commands listed in Table D-12.

Table D-12. Commands on the Spanning Tree Configuration Menu

Command	Meaning
1—General Configuration	Displays the Spanning Tree General Configuration menu.
2—Port Configuration	Displays the Spanning Tree Port Configuration menu.
3—STP Mode For ALL Spanning Tree Ports	Sets Spanning Tree Protocol operating mode for all ports on the switch.

General Configuration

The Spanning Tree General Configuration menu (Figure D-19) provides the ability to change the parameters for spanning tree operation for the entire switch.

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                               [134.177.221.67]
MAC Address:                              [00:00:81:0a:0b:13]
Software Version:                         [1.0]
System Up Time:                           [0d:01h:07m:22s]
Switch Status:                            [Switching]
********************************************************************************

                       Spanning Tree General Configuration

1 ---Aging Time
2 ---Bridge Priority
3 ---Bridge Hello Time
4 ---Bridge Max Age Time
5 ---Bridge Forward Delay









Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure D-19. Spanning Tree General Configuration Menu

Table D-13 lists the commands on the Spanning Tree General Configuration menu and the parameters these commands allow you to set.

Table D-13. Commands on the Spanning Tree General Configuration Menu

Command	Meaning
1—Aging Time	The number of seconds a learned MAC address can be inactive before it is “aged” or unlearned. This field is configurable in the range of 4 to 1,000,000 seconds with a default of 300 seconds.
2—Bridge Priority	Which bridge within the network is designated as the root bridge (bridge with the highest priority). This field is configurable in the range of 0 to 65535 (where low number = high priority) with a default of 32768.
3—Bridge Hello Time	How many seconds elapse between hello time messages that are sent from this switch to all other switches, if the Spanning Tree Protocol has defined this switch as the root switch. This field is configurable in the range of 1 to 10 seconds with a default of 2 seconds.
4—Bridge Max Age Time	How many seconds the network waits to discard a hello time frame if a response is not received. This field is configurable from 6 to 40 seconds with a default of 20 seconds.
5—Bridge Forward Delay	How many seconds the switch or port delays forwarding frames after a network topology change. The field value is configurable in the range of 4 to 30 seconds with a default of 15 seconds. **Note:** The maximum ranges for Bridge Hello Time, Max Age Time, and Forward Delay are limited by the following interrelationship formula: 2 x (Bridge Forward Delay - 1) Bridge Maximum Age Time $\geq$ 2 x (Bridge Hello Time + 1). If you try to enter values that deviate from this formula, you receive an error message that the values are out of range.

Port Configuration

The Spanning Tree Port Configuration menu (Figure D-20) lists the port numbers with the port priority and the port path cost. Press [ctrl-n] to see the next set of port numbers or [ctrl-p] to see the previous set of port numbers.

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:01h:07m:51s]
Switch Status:                           [Switching]
********************************************************************************

                       Spanning Tree Port Configuration

Command            Mode                 Priority            Path Cost
1 ---Port 1        802.1D               128                 100
2 ---Port 2        802.1D               128                 100
3 ---Port 3        802.1D               128                 100
4 ---Port 4        802.1D               128                 100
5 ---Port 5        802.1D               128                 100
6 ---Port 6        802.1D               128                 100
7 ---Port 7        802.1D               128                 100
8 ---Port 8        802.1D               128                 100
9 ---Port 9        802.1D               128                 100
[ctrl-n]---Next Page    [ctrl-p]---Previous Page
Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure D-20. Spanning Tree Port Configuration Menu

This menu allows you to change the parameters listed in Table D-14.

Table D-14. Parameters on the Spanning Tree Port Configuration Menu

Parameter	Meaning
Mode	Setting for Spanning Tree Protocol operation at this port. Choices are: • FastStart—Specifies Fast Start operation for Spanning Tree Protocol. This setting allows the port to transition to the Forwarding state faster than it does in the 802.1d mode. The probability that a loop may occur is greater with Fast Start operation than with IEEE 802.1d operation. • 802.1D—Specifies IEEE 802.1D Spanning Tree Protocol operation. In this mode, the port operation is compliant with the IEEE standard.
Priority	Value used in conjunction with the port number to create a unique port identifier. The valid range is from 0 to 255 and the default is 128.
Path cost	The path cost to the designated root bridge. The valid range for this value is from 1 to 65,535. Entering a value of 0 resets to the factory default setting so the switch software can automatically compute the path cost proportional to speed and duplex mode. See Table 3-1 on page 3-13 for default values for each speed and duplex mode.

SNMP Configuration

The SNMP Configuration menu (Figure D-21) displays a list of the parameters that allow you to set and change values, parameters, and addresses within an SNMP management environment.

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:01h:09m:54s]
Switch Status:                           [Switching]
********************************************************************************

                        SNMP Configuration

1 ---SNMP Read Community String
2 ---SNMP Read/Write Community String
3 ---Trap Receiver 1 Community Name and IP Address
4 ---Trap Receiver 2 Community Name and IP Address
5 ---Trap Receiver 3 Community Name and IP Address
6 ---Trap Receiver 4 Community Name and IP Address
7 ---Authentication Trap Generation
8 ---LinkUp/LinkDown Trap Generation



Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure D-21. SNMP Configuration Menu

Table D-15 lists the parameters in the SNMP Configuration menu.

Table D-15. Parameters on the SNMP Configuration Menu

Parameter	Meaning
1—SNMP Read Community String	Set the community string used for in-band read-only SNMP operations by entering an alphanumeric character string of up to 20 characters. The default is “public.”
2—SNMP Read/Write Community String	Set the community string used for in-band read/only SNMP operations by entering an alphanumeric character string of up to 20 characters. The default setting is private.
3—Trap Receiver 1 Community Name and IP Address (Also commands 4, 5, and 6 for three more trap receivers)	Set up to four allowed Trap IP Addresses. Successive Trap Address fields are numbered #2, #3, and #4. Each of the trap addresses has an associated community string, an alphanumeric character string of up to 20 characters. and an IP address for a trap receiver. Default values are 0.0.0.0. (no IP address assigned) and “public.”
7—Authentication Trap Generation	Enables or disables sending a trap on an SNMP authentication failure. Default setting is Disabled.
8—LinkUp/LinkDown Trap Generation	Enables or disables trap LinkUp/LinkDown. Default setting is Enabled.

System Characteristics

The System Characteristics menu (Figure D-22) shows system characteristics and allows you to specify a new string for the parameters.

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                               [134.177.221.67]
MAC Address:                              [00:00:81:0a:0b:13]
Software Version:                         [1.0]
System Up Time:                           [0d:01h:09m:54s]
Switch Status:                            [Switching]
********************************************************************************

                        System Characteristics

System Description: [Bay Networks, Inc. BayStack 310-24T Ethernet Switch
Rev: 0-1.0.2.13]
Manufacturing Date Code: []
System Object ID: [1.3.6.1.4.1.45.3.32.2]
System Services: [datalink]

1 ---System Contact: []
2 ---System Name: []
3 ---System Location: []


Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure D-22. System Characteristics Menu

Table D-16 shows the parameters on the System Characteristics menu.

Table D-16. Parameters on the System Characteristics Menu

Parameter	Meaning
1—System Contact: [ ]	A string that identifies the person to be contacted concerning switch operation. To operate correctly with the Web interface, this string should be in the format of an Internet e-mail address.
2—System Name: [ ]	A string of characters that identify the switch, for example Finance Group
3—System Location: [ ]	A string of characters that identifies the switch location, for example 1st floor.

MAC-Based Address Filtering Configuration

When you type 6 from the System Configuration menu, the MAC-Based Address Filtering Configuration menu is displayed (Figure D-23).

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:01h:12m:02s]
Switch Status:                           [Switching]
********************************************************************************

                MAC-Based Address Filtering Configuration

Command        Filtering MAC Address  Vlan Number
1 ---Filter 1:
2 ---Filter 2:
3 ---Filter 3:
4 ---Filter 4:
5 ---Filter 5:
6 ---Filter 6:
7 ---Filter 7:
8 ---Filter 8:

0 ---Remove All Filters
Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure D-23. MAC-Based Address Filtering Configuration Menu

This option allows you to enter up to eight MAC addresses. The switch drops all incoming packets destined to any of these addresses. Enter the command number for each successive filter and then the MAC address to be excluded. An additional option (0) allows you to remove all existing filters.

For a more detailed explanation of this feature, refer to "MAC Address-Based Filtering" on page 2-17.

MAC Address-Based Security

When you type 7 from the System Configuration menu, the MAC Address-Based Security menu is displayed (Figure D-24).

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:01h:12m:29s]
Switch Status:                           [Switching]
********************************************************************************

                        MAC Address-Based Security

1 ---Security Status: [Disabled]
2 ---Security Configuration Changes Via SNMP: [Locked]
3 ---Security Mode: [Single-MAC-per-port]
4 ---Security Action: [Trap Only]
5 ---Add/Modify Allowed MAC Address
6 ---Add/Modify Not-Allowed MAC Address
7 ---Delete DA Filter MAC Address
8 ---Allowed MAC Address Look-up



Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure D-24. MAC Address-Based Security Menu

Table D-17 shows the options available on the MAC-Address-Based Security menu.

Table D-17. Commands on the MAC Address-Based Security Menu

Option	Meaning
1—Security Status	Enables or disables MAC address-based security.
2—Security Configuration Changes Via SNMP	Allows or prevents access to this feature from SNMP management system.
3—Security Mode	Specifies the security mode for the switch. Possible choices are: • Single-MAC-per-port—Only one MAC address is allowed to access each port. • MAC-list—You can specify a list of up to eight MAC addresses that are allowed to access each port. • Auto-Learn—The switch learns the first two MAC addresses that access each port and prevents access from all subsequent MAC addresses.
4—Security Action	Specifies the action to be taken if a security violation occurs. Possible choices are: • No action • Send trap to network management software • Partition the port • Partition the port and send a trap • Enable destination address filtering on the violating address • Enable destination address filtering and send a trap
5—Add/Modify Allowed MAC Address	Allows you to add a new MAC address or change a MAC address that is already in the list of MAC addresses allowed to access the switch ports.
6—Add/Modify Not-Allowed MAC Address	Allows you to add a new MAC address or change a MAC address that is already in the list of MAC addresses that are prohibited from accessing the switch ports.
7—Delete DA Filter MAC Address	Allows you to delete an address from the list of destination MAC addresses that are used as the basis for destination address filtering.
8—Allowed MAC Address Look-up	Allows you to verify whether or not a particular address is in the list of MAC addresses that are allowed to access the switch ports.

Conversation Steering

When you type 8 from the System Configuration menu, the Conversation Steering menu is displayed (Figure D-25).

```
********************************************************************************
Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:01h:15m:46s]
Switch Status:                           [Switching]
********************************************************************************

                        Conversation Steering

1 --- Monitoring Mode (Dedicated to a probe, UnTagged)
2 --- Port # to be Monitored (None)
3 --- View/Select Destination MAC Addresses to monitor
4 --- Monitoring/mirroring Port (None)
5 --- Conversation Steering Mode (Disabled)









Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure D-25. Conversation Steering Menu

Two kinds of conversation steering are available. Port-based conversation steering specifies a single port to be monitored by another port. MAC address-based conversation steering specifies up to eight MAC addresses whose traffic is monitored by a monitoring port. You can monitor a port and MAC addresses at the same time.

When you enable port-based conversation steering, you are asked to enter numbers for both ports.

Table D-18 shows the options that are available on the Conversation Steering menu.

Table D-18. Options on the Conversation Steering Menu

Option	Meaning and Choices
1—Monitoring Mode	Choices are: • Dedicated to a probe (tagged or untagged)—The port is dedicated to the use of a network probe and does not pass any other traffic through. Set the port tagging parameter based on whether you plan to use a tag-aware or non-tag aware probe. • Undedicated—The port can share traffic with the monitored traffic and another network device.
2—Port # to be Monitored	Enter either a port number or 0 (zero) to specify no port.
3—View/Select Destination MAC Addresses to monitor	Displays the Destination MAC Conversation Steering Menu, which shows the destination MAC addresses whose traffic is being monitored.
4—Monitoring/mirroring Port	Enter either a port number or 0 (zero) to specify no port.
5—Conversation Steering Mode	Enables or disables conversation steering. The default is disabled.

Destination MAC Conversation Steering Menu

When you type 3 from the Conversation Steering Menu, the Destination MAC Conversation Steering Menu is displayed (Figure D-26).

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:01h:17m:07s]
Switch Status:                           [Switching]
********************************************************************************

                Destination MAC Conversation Steering

1 -- Frames to MAC [00:00:00:00:00:00] in VLAN [0001]     [Disabled]
2 -- Frames to MAC [00:00:00:00:00:00] in VLAN [0001]     [Disabled]
3 -- Frames to MAC [00:00:00:00:00:00] in VLAN [0001]     [Disabled]
4 -- Frames to MAC [00:00:00:00:00:00] in VLAN [0001]     [Disabled]
5 -- Frames to MAC [00:00:00:00:00:00] in VLAN [0001]     [Disabled]
6 -- Frames to MAC [00:00:00:00:00:00] in VLAN [0001]     [Disabled]
7 -- Frames to MAC [00:00:00:00:00:00] in VLAN [0001]     [Disabled]
8 -- Frames to MAC [00:00:00:00:00:00] in VLAN [0001]     [Disabled]

0 - Enable/Disable All MAC Entries

Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure D-26. Destination MAC Conversation Steering Menu

This menu allows you to enable or disable monitoring of traffic to the specified MAC addresses, either individually or for the entire group.

Port VLAN Configuration

When you type 9 from the System Configuration menu, the Port VLAN Configuration menu is displayed (Figure D-27). This menu allows you to assign switch ports to one of up to 31 virtual networks (VLANs) that you may set up.

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.221.67]
MAC Address:                             [00:00:81:0a:0b:13]
Software Version:                        [1.0]
System Up Time:                          [0d:01h:18m:40s]
Switch Status:                           [Switching]
********************************************************************************

                        Port VLAN Configuration

1 ---Create/Modify VLAN
2 ---Delete VLAN
3 ---Display VLAN
4 ---Add InterSwitch Port
5 ---Delete InterSwitch Port
6 ---Display InterSwitch Port
7 ---CPU VLAN Assignment [1]



0 ---Reset All Ports to default VLAN 1


Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure D-27. Port VLAN Configuration Menu

Table D-19 lists the commands on the Port VLAN Configuration menu.

Table D-19. Commands on the Port VLAN Configuration Menu

Command	Meaning
1—Create/Modify VLAN	Allows you to set up a new VLAN or modify an existing one.
2—Delete VLAN	Allows you to delete a VLAN; this action reassigns the ports from that VLAN to VLAN 1 (the default).
3—Display VLAN	Prompts you to enter a VLAN number and then displays a screen that lists the ports assigned to that VLAN.
4—Add InterSwitch Port	Allows you to designate a port as an interswitch port.
5—Delete InterSwitch Port	Allows you to change a port from an interswitch port to a normal port.
6—Display InterSwitch Port	Shows which ports have been set up as interswitch ports.
7—CPU VLAN Assignment	Allows the system administrator to specify the VLAN that the CPU (management interface) will be a member of. The network management station must also be a member of this VLAN to manage the switch through a Telnet or Web connection or using SNMP network management. The CPU can be a member of only one VLAN. The default for this setting is VLAN 1.
0—Reset All Ports to default VLAN 1	Assigns all ports on the switch to VLAN 1 (the default). This action removes all VLANS you may have set up.

Reset to Defaults

This option (0 from the System Configuration screen) allows you to reset the switch to all the factory default settings.

Caution: If you choose the Reset to Defaults option, all of your configuration settings are replaced with factory default settings when you press [Enter] after confirmation. If you are accessing the switch through a Telnet connection, the connection to the switch will end, and you will have to reenter the IP address, IP subnet address, and default gateway address from the console and reset the switch before you can open another Telnet session.

Troubleshooting

When you type 3 from the Main Menu, the Troubleshooting menu is displayed (Figure D-28).

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                               [134.177.160.117]
MAC Address:                              [00:00:80:bb:20:44]
Software Version:                         [1.0]
System Up Time:                           [1d:02h:24m:23s]
Switch Status:                            [Switching]
********************************************************************************

                        Troubleshooting

1 ---Ping Remote Station []
2 ---MAC Table Lookup []
3 ---Forwarding During Broadcast Storm [Enabled]
4 ---Topology Table









Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure D-28. Troubleshooting Menu

Table D-20 lists the commands on the Troubleshooting menu.

Table D-20. Commands on the Troubleshooting Menu

Command	Meaning
1—Ping Remote Station [ ]	By sending a Ping signal to a remote station, you can determine if a station is connected to the network. Enter 1 to access a command line that allows you to enter the IP address of the remote station. The switch pings this station and then informs you if the station is “alive” or if there is no answer.
2—MAC Table Lookup [ ]	Allows you to look up specific entries in the switch forwarding table using a specific MAC address as the access key. If the address is a learned address, the switch displays the type of address (static, dynamic, or filtered). If it is not a learned address, it shows a “not found” status.
3—Forwarding During Broadcast Storm [Enabled/Disabled]	Enables or disables packet forwarding during broadcast storms. For more information about this feature, refer to “Broadcast Storm Protection” on page 7-9.
4—Topology Table	Shows the MAC address and IP address of stations connected to the switch ports.

Management Access Control

When you type 4 from the Main Menu, the Management Access menu is displayed (Figure D-29).

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                              [134.177.160.117]
MAC Address:                             [00:00:80:bb:20:44]
Software Version:                        [1.0]
System Up Time:                          [1d:02h:28m:07s]
Switch Status:                           [Switching]
********************************************************************************

                        Management Access

1 ---Telnet Access (Enable/Disable)
2 ---Web Access (Enable/Disable)
3 ---Change Password
4 ---Management Access Control









Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure D-29. Management Access Menu

Table D-21 lists the commands on the Management Access menu.

Table D-21. Commands on the Management Access Menu

Command	Meaning
1—Telnet Access (Enable/Disable)	Enables or disables Telnet access to the switch.
2—Web Access (Enable/Disable)	Enables or disables Web management access to the switch.
3—Change Password	Allows you to change the password for management access. You are prompted to enter the current password, the new password, and then verification of the new password. The same password is used for console, Telnet, or Web login.
4—Management Access Control	Allows you to restrict access to the management functions or to specify IP addresses of stations that can access the management functions.

System Reset/Upgrade

When you type 5 from the Main Menu, the System Reset/Upgrade menu is displayed (Figure D-30).

```
********************************************************************************
                Bay Networks BayStack 310-24T Ethernet Switch

IP Address:                               [134.177.160.117]
MAC Address:                              [00:00:80:bb:20:44]
Software Version:                         [1.0]
System Up Time:                           [1d:02h:33m:58s]
Switch Status:                            [Switching]
********************************************************************************

                        System Reset/Upgrade

1 ---TFTP Server IP Address [134.177.160.93]
2 ---Default Gateway IP Address [134.177.160.1]
3 ---Software Image File Source [Local / reload.wire]
4 ---Configuration File Source [Local / ]
5 ---Specify Reset Action [Reset]
6 ---Set/Clear Reset Action Timer [0 min.]

0 ---Immediate Reset Action


Enter Command ([ESC]-Previous Menu   [Space]-Refresh Screen)
```

Figure D-30. System Reset/Upgrade Menu

The System Reset/Upgrade selection (5 from the Main Menu) allows you to perform a software-controlled reset of your BayStack switch or to upgrade system software.

Table D-22 shows the commands on the System Reset/Upgrade menu.

Table D-22. Commands on the System Reset/Upgrade Menu

Command	Meaning
1—TFTP Server IP Address	The server location where the software upgrade can be found.
2—Default Gateway IP Address	The IP address of the gateway used for downloading upgrades
3—Software Image File Source	The source (local or remote), path name, and file name of the software upgrade file.
4—Configuration File Source	The source (local or remote), path name, and file name of the configuration file.
5—Specify Reset Action: [none]	Type of reset action. Choices are: • None (no reset action) • 1—System reset performs a switch reset. • 2—Software download upgrades the software from the selected server with the selected file name. **Note:** When you download software, the switch resets twice. Do not power down the switch before the process is completed (approximately 5 minutes).
6—Set/Clear Reset Action Timer: [0 min.]	Number of minutes before the specified reset action will happen, up to a maximum of 65,535 minutes. Enter 0 to cancel the previously specified timer value.
0—Immediate Reset Action	Initiates an immediate switch reset or software download. This command overrides any value set for the reset action timer.

Note: A switch reset executed from the System Reset/Upgrade menu differs from the Reset to Defaults option because it does not reset any parameter settings. Selecting Reset from a Telnet connection terminates the connection.

Appendix E
Web Management Interface

This appendix describes the page hierarchy, links, data fields, and commands in the Web management interface.

Refer to Chapter 3, “Installing the BayStack 310-24T Switch,” for switch installation procedures. Refer to Appendix D, “BayStack 310-24T Switch Console Interface,” for descriptions of the console management interface.

Figure E-1 through Figure E-6 illustrate the Web page hierarchy, indicating the navigation bar page links in each of the first four folders and the parameters that can be viewed or changed from each page.

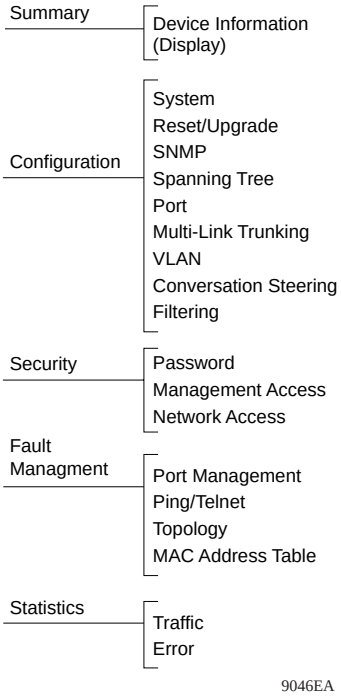


Figure E-1. Folders and First-Level Web Pages

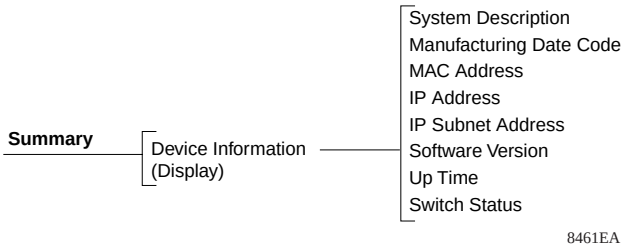


Figure E-2. Information on the Device Information Page

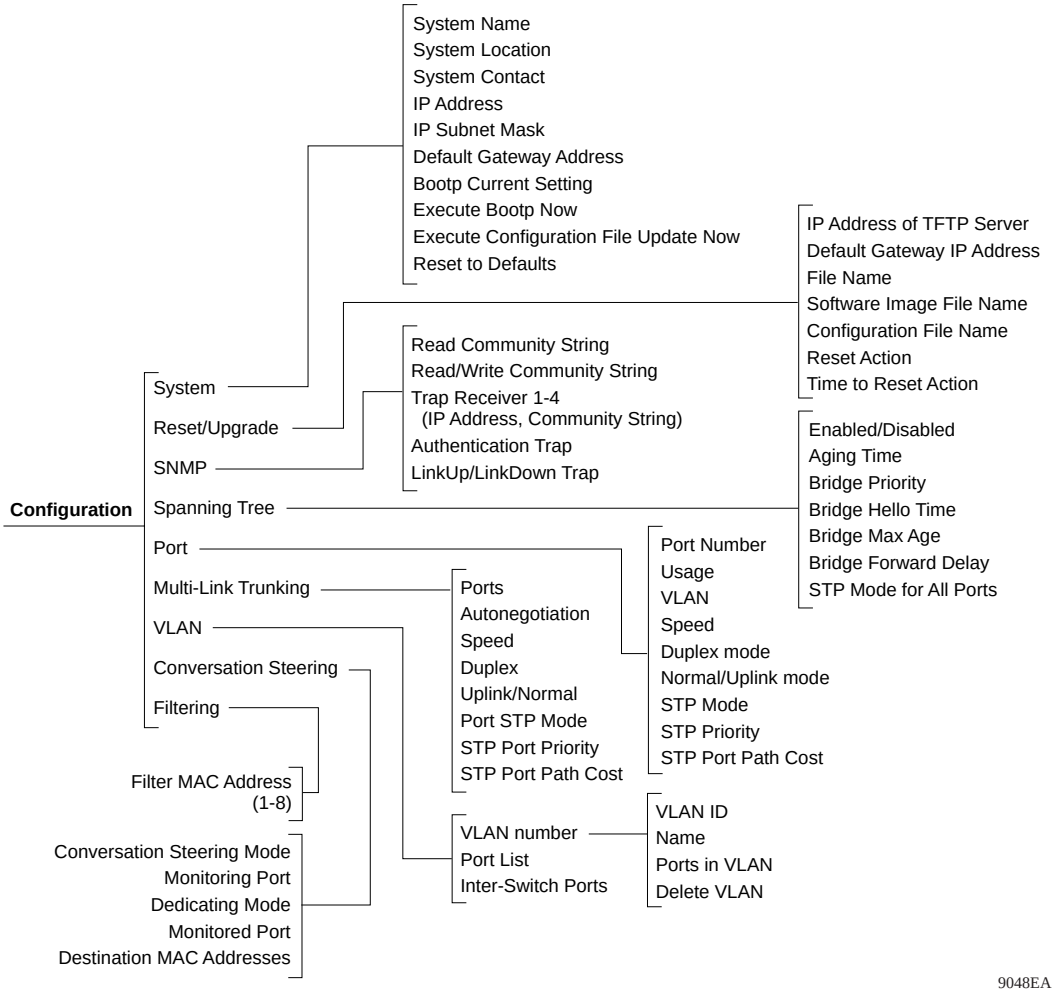


Figure E-3. Configuration Web Pages

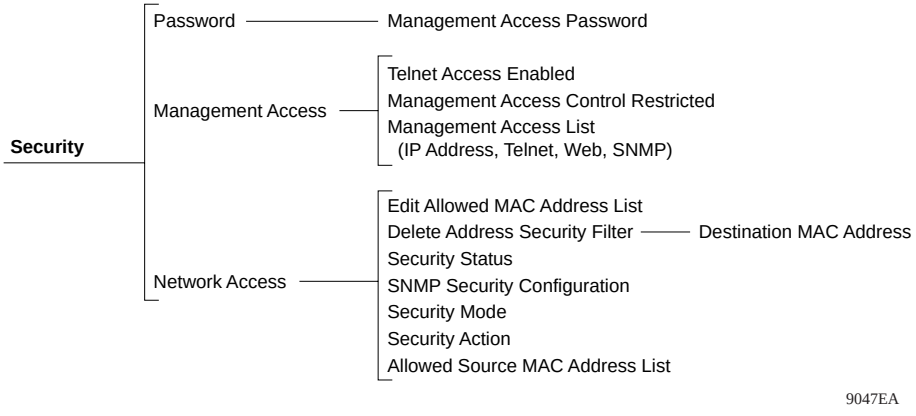


Figure E-4. Security Web Pages

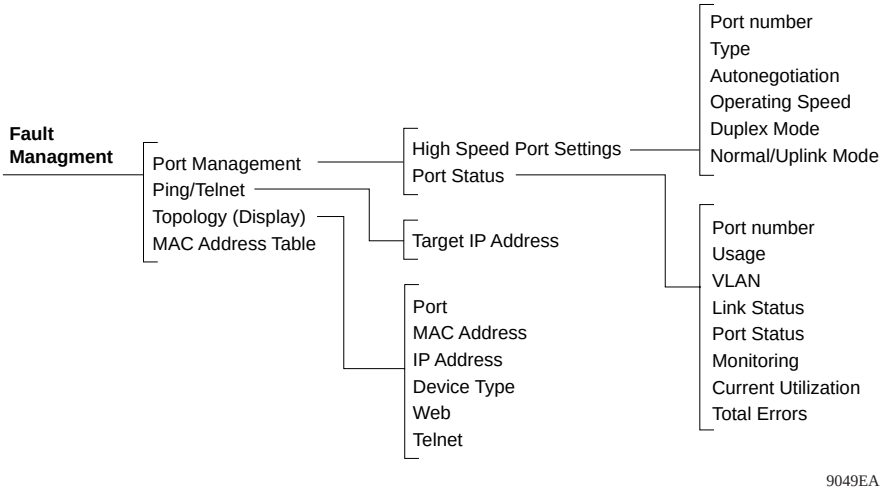


Figure E-5. Fault Management Web Pages

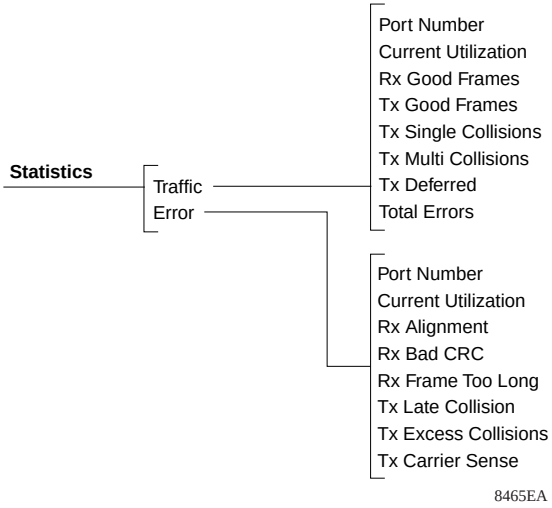


Figure E-6. Statistics Web Pages

Device Information Page

The Summary folder contains one link, Device Information, that opens the Device Information page (Figure E-7).

This display-only page includes an illustration of your switch along with the following information:

- System Description: switch model and version
- Manufacturing Date Code
- MAC Address
- IP Address (Current)
- IP Subnet Mask (Current)
- Software Version
- Up Time
- Switch Status

  A switch status of Ready indicates that none of the switch ports are currently forwarding traffic, most likely because nothing is connected to the switch. A switch status of Switching indicates that one or more ports are forwarding traffic.

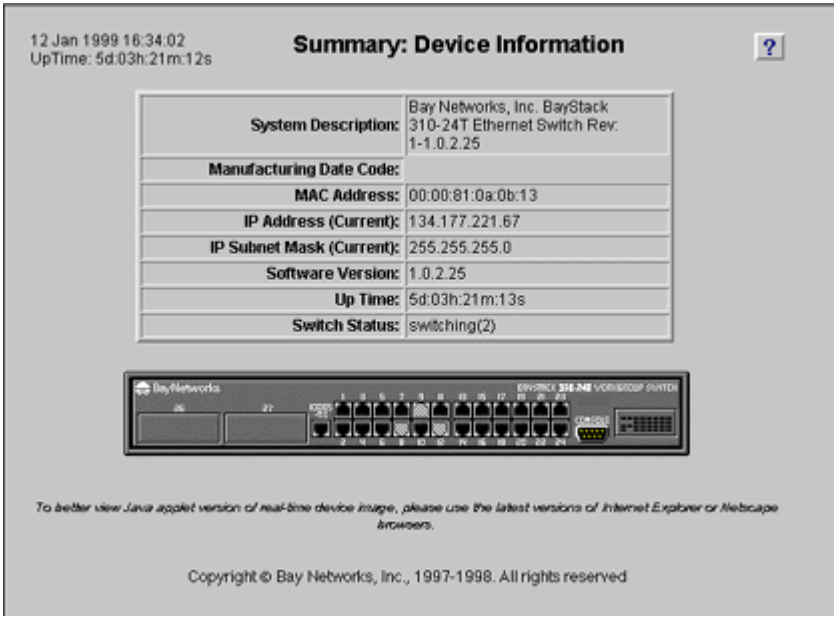


Figure E-7. Device Information Page

The Device Information page is for information only and does not link to any other page. However, if you click on a port shown on the switch picture, a window opens showing current statistics for that port (Figure E-8).

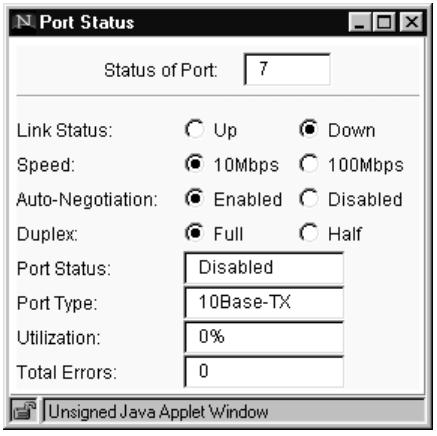


Figure E-8. Port Status Window

You can change the IP address and IP subnet mask parameters from the Configuration pages. You cannot change any other of the parameters on the Device Information page.

Configuration Pages

The following pages are listed under the Configuration folder:

- System (page E-8)
- Reset/Upgrade (page E-11)
- SNMP (page E-13)
- Spanning Tree (page E-15)
- Port (page E-18)
- Multi-Link Trunking (page E-22)
- VLAN (page E-24)
- Conversation Steering (page E-27)
- Filtering (page E-29)

System

The System page (Figure E-9) allows you to set or change basic system identifying information and to execute a BootP configuration of the switch.

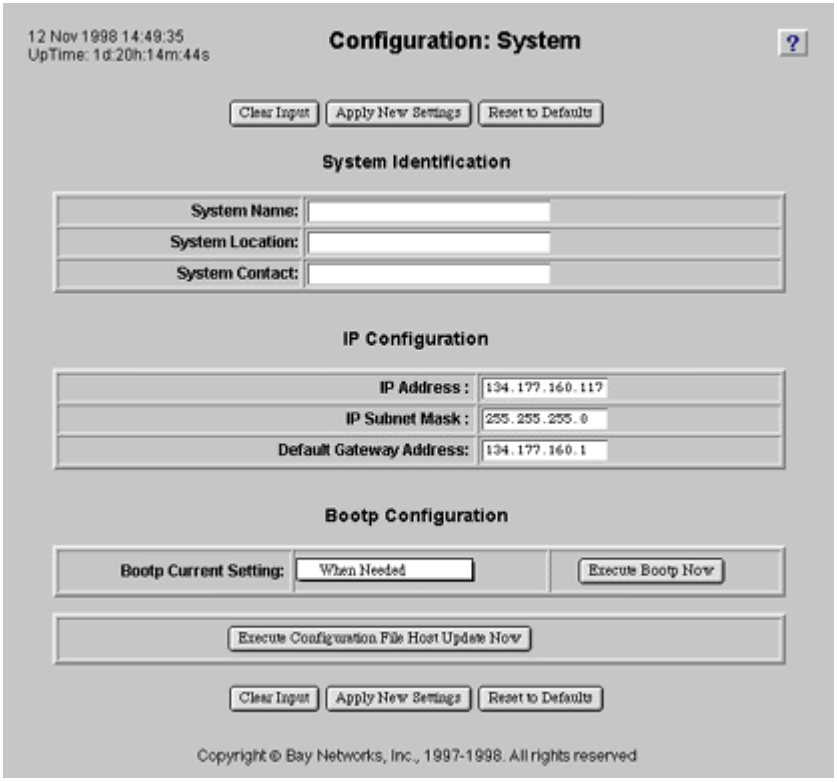


Figure E-9. System Page

This page contains the parameter fields and buttons shown in Table E-1.

Table E-1. Parameters and Buttons on the System Page

Area	Item	Type	Meaning
System Identification	System Name	Parameter	A string of characters that identify the switch, for example Finance Group.
	System Location	Parameter	A string of characters that identifies the switch location, for example 1st floor.
	System Contact	Parameter	A string that identifies the person to be contacted concerning switch operation. To operate correctly with the Web interface, the System Contact should be in the format of an Internet e-mail address.
IP Configuration	IP Address	Parameter	The Internet Protocol (IP) address of the unit. The IP address must be a unique address for initiating a Telnet session or managing the BayStack 310-24T switch using SNMP. The factory default setting of the IP address is 127.0.0.2. Any change takes effect at the next reset only.
	IP Subnet Mask	Parameter	The subnet mask that indicates which bits are used for network/subnet identification and which are used for end nodes or stations. The subnet mask is written in the form of an IP address, with all network/subnet bits set to one. The default subnet mask is 0.0.0.0. Any change takes effect at the next reset only.
	Default Gateway Address	Parameter	The address of the IP gateway during normal switch operation. The default gateway address is 0.0.0.0. This address is set separately from the TFTP gateway address used for downloading software upgrades. The TFTP gateway address is set from the Software Load page as described on page E-11.

Table E-1. Parameters and Buttons on the System Page (continued)

Area	Item	Type	Meaning
Bootp Configuration	Bootp Current Setting	Parameter	Specifies the conditions under which the switch uses BootP configuration. Choices are: • When Needed (default setting) The switch sends a BootP request when the switch IP address stored in nonvolatile memory is the factory default value. If the stored IP address is different from the factory default value, the switch uses the stored network parameters. If the switch cannot find a BootP server, it tries five more times to find one and then defaults to the factory settings. • Always Each time the switch boots, it ignores any stored network parameters and sends a BootP request. If the BootP request fails, the switch boots with the factory default IP configuration. This setting disables remote management if no BootP server is set up for the switch, but it allows the switch to boot normally. • Disable The switch boots using the IP configuration parameters stored in nonvolatile memory. If a BootP configuration is in progress when you issue this command, the BootP configuration stops • Last Address At startup, the switch tries to obtain its IP configuration using BootP. If the BootP request fails, the switch uses the network parameters stored in its nonvolatile memory. **Note:** Valid parameters obtained using BootP always replace current information stored in the nonvolatile memory
	Execute Bootp Now	Task Button	Initiates an immediate BootP download.
	Execute Configuration File Update Now	Task Button	Updates a configuration file with the current settings for switch parameters.

Table E-1. Parameters and Buttons on the System Page (continued)

Area	Item	Type	Meaning
General	Clear Input	Task Button	Returns settings on this page to their previous values.
	Apply New Settings	Task Button	Applies new parameter settings.
	Reset to Defaults	Task Button	Resets the switch to all the factory default settings. A dialog box asks for confirmation before the switch is reset. **Caution:** When the switch resets, all of your configuration settings are replaced with factory default settings. The default [0.0.0.0] takes effect and you lose your connection with the switch. You must reenter the IP address, IP subnet address, and default gateway address from the console and reset the switch before you can open another Web session.

Reset/Upgrade

The Reset/Upgrade page (Figure E-10) allows you to reset software, download software upgrades, or schedule a delayed system reset or download in the future.

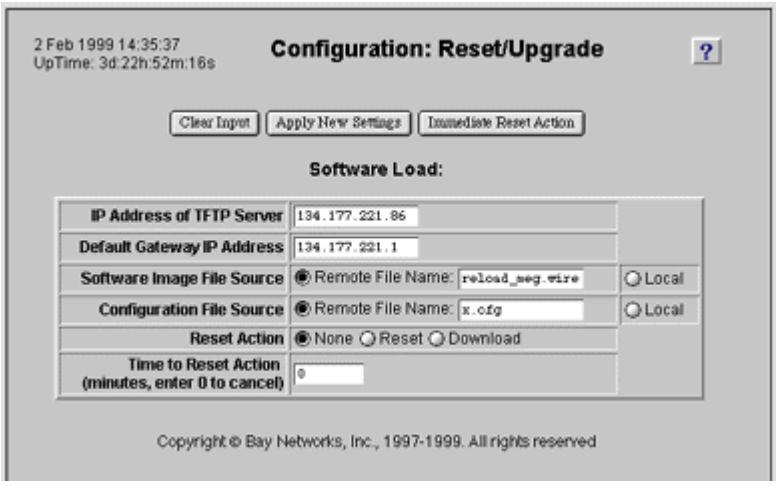


Figure E-10. Reset/Upgrade Page

This page contains the parameter fields and buttons shown in Table E-2.

Table E-2. Parameters and Buttons on the Reset/Upgrade Page

Item	Type	Meaning
Clear Input	Task Button	Returns settings on this page to their previous values.
Apply New Settings	Task Button	Applies new parameter settings.
Immediate Reset Action	Task Button	Initiates an immediate switch reset or software download. Clicking this button overrides any settings in the Time to Reset field.
IP address of TFTP server	Parameter	For software downloads only. The server location where the software upgrade can be found.
Default Gateway IP Address	Parameter	For software downloads only. The IP address of the gateway used for downloading upgrades.
Software Image File Name	Parameter	For software downloads only. The name of the software upgrade file. Click the radio button to specify a local or remote file download.
Configuration File Name	Parameter	The name of the configuration file that the switch requests during a BootP download. Click the radio button to specify a local or remote file download.
Reset Action	Radio Button	Type of reset action. Choices are: • None (no reset action) • Reset performs a switch reset. • Download upgrades the software from the selected server with the selected file name. **Note:** When you download software, the switch resets twice. Do not power down the switch before the process is completed (approximately 10 minutes).
Time to Reset Action	Parameter	Number of minutes before the specified reset action will happen. Enter 0 to cancel the previously specified timer value.

SNMP

The SNMP page (Figure E-11) allows you to set SNMP parameters for the switch.

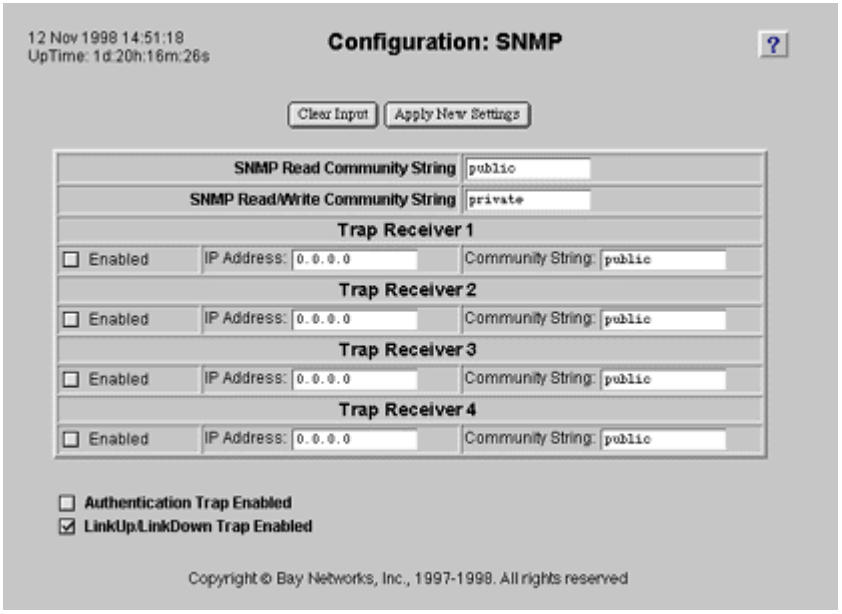


Figure E-11. SNMP Page

This page includes the items shown in Table E-3.

Table E-3. Parameters, Buttons, and Check Boxes in the SNMP Page

Area	Item	Type	Meaning
General	Clear Input	Task Button	Returns settings on this page to their previous values.
	Apply New Settings	Task Button	Applies new parameter settings.
SNMP Community Strings	SNMP Read Community String	Parameter	The community string used for in-band read-only SNMP operations. The maximum number of alphanumeric characters is 20. The default is “public.”
	SNMP Read/ Write Community String	Parameter	The community string used for in-band read/write SNMP operations. The maximum number of alphanumeric characters is 20. The default is “private.”
Trap Receivers 1 through 4	Enabled	Check Box	Enables or disables this trap receiver. The default setting is disabled (box not checked).
	IP Address	Parameter	IP address to which the trap is sent.
	Community String	Parameter	Community string for this trap receiver. The default is “public.”
Traps	Authentication Trap Enabled	Check Box	Enables or disables sending a trap on an SNMP authentication failure. The default is disabled (box not checked).
	LinkUp/ LinkDown Trap Enabled	Check Box	Enables or disables trap LinkUp/LinkDown. The default is enabled (box checked).

Spanning Tree

The Spanning Tree page (Figure E-12) allows you to set up Spanning Tree Protocol operation for the switch and indicates current settings assigned by the system software. If Spanning Tree is disabled, the current settings are all 0.

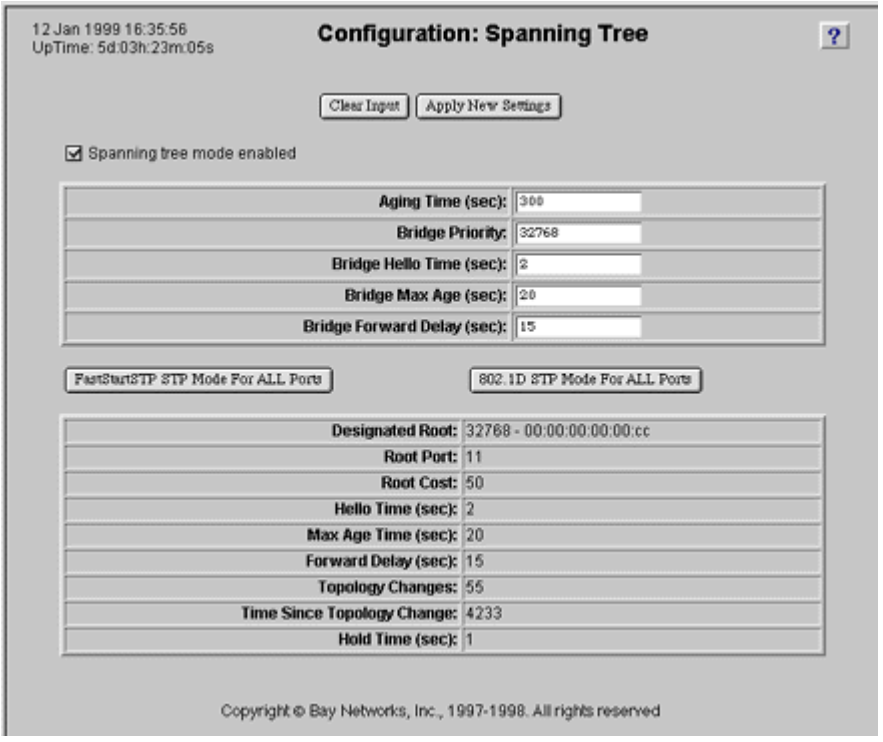


Figure E-12. Spanning Tree Page

This page includes the items shown in Table E-4.

Table E-4. Parameters, Check Boxes, and Buttons on the Spanning Tree Page

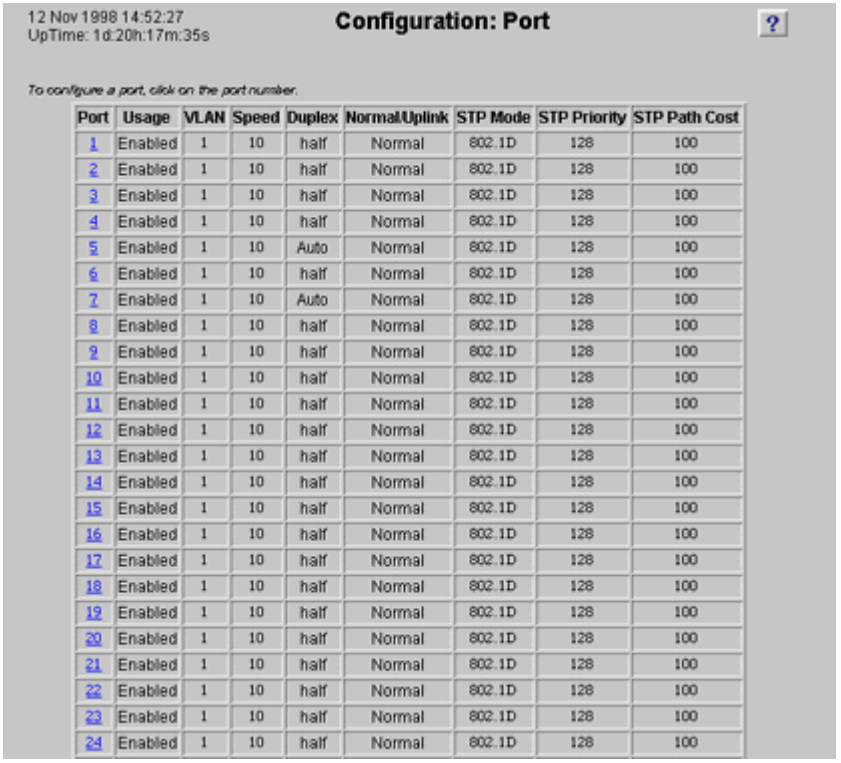
Area	Item	Type	Meaning
General	Clear Input	Task Button	Returns settings on this page to their previous values.
	Apply New Settings	Task Button	Applies new parameter settings.
Spanning Tree Parameters	Spanning tree mode enabled	Check Box	Enables or disables Spanning Tree Protocol operation for the entire switch. The default is enabled (box checked). Any change takes effect immediately and does not require resetting the switch.
	Aging Time	Parameter	Defines how many seconds a learned MAC address can be inactive before it is aged or unlearned. This value can be from 4 to 1,000,000 seconds with a default of 300 seconds.
	Bridge Priority	Parameter	Determines which bridge within the network is designated as the root bridge (bridge with the highest priority). This value can be from 0 to 65535 (where low number = high priority) with a default of 32768.
	Bridge Hello Time	Parameter	Sets the Hello interval (the amount of time between transmissions of configuration bridge PDUs) for this bridge. This parameter takes effect only when this bridge becomes the root bridge. The range is 1 to 10 seconds with a default of 2 seconds.
	Bridge Max Age	Parameter	Sets the maximum age (in seconds) that a hello message can attain before it is discarded. The set value takes effect only when this bridge becomes the root bridge. The root bridge Maximum Age Time parameter value becomes the (actual) Maximum Age Time parameter value for all bridges in the spanning tree network. The range is from 6 to 40 seconds with a default of 20 seconds.
	Bridge Forward Delay	Parameter	Sets the Forward Delay parameter value for this bridge. All bridges participating in the spanning tree network use the root bridge's Forward Delay parameter value. The range is from 4 to 30 seconds with a default of 15 seconds.

Table E-4. Parameters, Check Boxes, and Buttons on the Spanning Tree Page (continued)

Area	Item	Type	Meaning
Spanning Tree Mode	FastStartSTP STP Mode for ALL Ports	Task Button	Specifies Fast Start operation for Spanning Tree Protocol. This setting allows the port to transition to the Forwarding state faster than it does in the 802.1d mode. The probability that a loop may occur is greater with Fast Start operation than with IEEE 802.1d operation.
	802.1D STP Mode for ALL Ports	Task Button	Specifies IEEE 802.1D Spanning Tree Protocol operation. In this mode, the port operation is compliant with the IEEE standard.
Current Settings	Designated Root	Display Only	The identifier for the root bridge.
	Root Port	Display Only	The port that offers the lowest cost path from this bridge to the root bridge.
	Root Cost	Display Only	The path cost from the switch to the designated root bridge.
	Hello Time	Display Only	How many seconds (1 to 9) elapse between hello time messages that are sent from this switch to all other switches; this value is determined by the Spanning Tree Protocol root switch.
	Max Age Time	Display Only	The maximum age (in seconds) of Spanning Tree Protocol information before it is discarded. This value is learned from the network and determined by the Spanning Tree Protocol root switch.
	Forward Delay	Display Only	How many seconds the switch delays forwarding frames after a network topology change. This value is also determined by the Spanning Tree Protocol root switch.
	Topology Changes	Display Only	The total number of topology changes detected by this bridge since the management entity was last reset or initialized.
	Time Since Topology Change	Display Only	The time since the last topology change was detected by the bridge entity.
	Hold Time	Display Only	The time interval (1 to 10 seconds) during which no more than two configuration bridge PDUs will be transmitted by this node.

Port

The Port page (Figure E-13) includes a display table with information about each port. The port numbers are active links to configuration pages for each port.



12 Nov 1998 14:52:27
UpTime: 1d:20h:17m:35s

Configuration: Port

?

To configure a port, click on the port number.

Port	Usage	VLAN	Speed	Duplex	Normal/Uplink	STP Mode	STP Priority	STP Path Cost
1	Enabled	1	10	half	Normal	802.1D	128	100
2	Enabled	1	10	half	Normal	802.1D	128	100
3	Enabled	1	10	half	Normal	802.1D	128	100
4	Enabled	1	10	half	Normal	802.1D	128	100
5	Enabled	1	10	Auto	Normal	802.1D	128	100
6	Enabled	1	10	half	Normal	802.1D	128	100
7	Enabled	1	10	Auto	Normal	802.1D	128	100
8	Enabled	1	10	half	Normal	802.1D	128	100
9	Enabled	1	10	half	Normal	802.1D	128	100
10	Enabled	1	10	half	Normal	802.1D	128	100
11	Enabled	1	10	half	Normal	802.1D	128	100
12	Enabled	1	10	half	Normal	802.1D	128	100
13	Enabled	1	10	half	Normal	802.1D	128	100
14	Enabled	1	10	half	Normal	802.1D	128	100
15	Enabled	1	10	half	Normal	802.1D	128	100
16	Enabled	1	10	half	Normal	802.1D	128	100
17	Enabled	1	10	half	Normal	802.1D	128	100
18	Enabled	1	10	half	Normal	802.1D	128	100
19	Enabled	1	10	half	Normal	802.1D	128	100
20	Enabled	1	10	half	Normal	802.1D	128	100
21	Enabled	1	10	half	Normal	802.1D	128	100
22	Enabled	1	10	half	Normal	802.1D	128	100
23	Enabled	1	10	half	Normal	802.1D	128	100
24	Enabled	1	10	half	Normal	802.1D	128	100

Figure E-13. Port Page

This page includes the information listed in Table E-5.

Table E-5. Information Fields on the Port Page

Field	Meaning
Port number	The number of each port on the switch. To configure a port, click on its number. Clicking on ports 1 through 24 opens a low-speed port configuration page. Clicking on ports 25 through 27 opens a high-speed port configuration page.
Usage [Enabled/ Disabled]	Whether or not the port is enabled.
VLAN	The number of the virtual LAN (1-8) to which the port is assigned. By default, all ports are assigned to VLAN 1 when the switch is first turned on or is reset.
Speed [100 Mbps/ 10 Mbps/ Not Applicable]	The speed at which the port is transmitting and receiving data. For ports 1 through 24, the speed is always 10 Mb/s. For ports 25, 26, and 27, the speed can be either 10 Mb/s or 100 Mb/s.
Duplex [Full/ Half/Auto]	Whether the port is running in half duplex or full duplex mode or is set for autonegotiation.
Normal/Uplink [Normal/Uplink/ Not Applicable]:	Configurable for high-speed ports only (25, 26, and 27). When a port is set for Uplink, address learning is disabled on that port. This allows asymmetric MAC addressing to prevent excessive switch flooding.
STP Mode [802.1D, FastStart, none]	The operational mode for Spanning Tree Protocol.
STP Priority	The priority of each port, which is used in conjunction with the port number to create a unique port identifier. The valid range for this value is from 0 to 255. The default value is 128.
STP Path Cost	The path cost to the designated root bridge. The valid range for this value is from 1 to 65,535. Entering a value of 0 resets the parameter to the factory default setting so the switch software can automatically compute the path cost proportional to speed and duplex mode.

Low Speed Port Page

Clicking a port number 1 through 24 in the Port Page opens a configuration page for a low-speed port (Figure E-14).

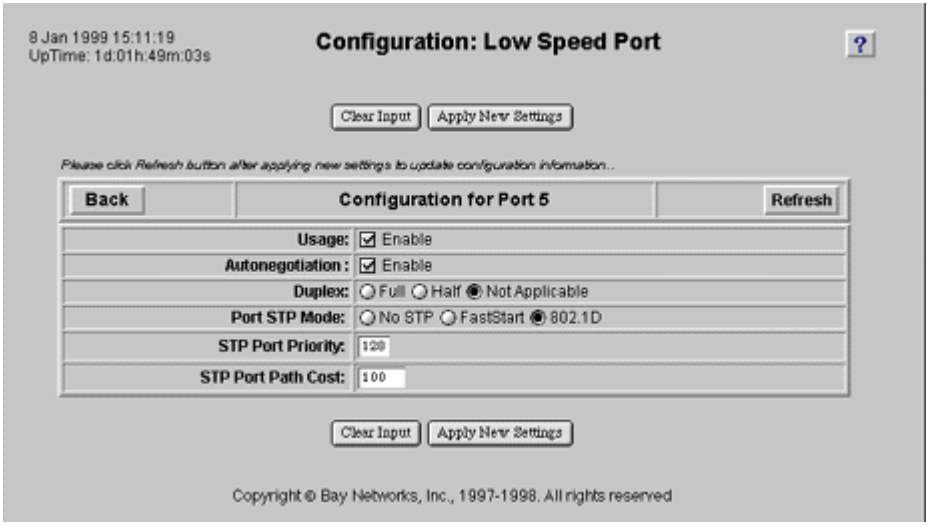


Figure E-14. Low Speed Port Page

This page shows the current parameter settings for the port and allows you to change parameter settings. It includes the items listed in Table E-6.

Table E-6. Parameters, Check Boxes, and Buttons on the Low Speed Port Page

Item	Type	Meaning
Clear Input	Task Button	Returns settings on this page to their previous values.
Apply New Settings	Task Button	Applies new parameter settings.
Back	Task Button	Returns the display to the Port page.
Refresh	Task Button	Refreshes the display and shows the latest settings for the port.
Usage	Check Box	Whether or not the port is enabled. A check indicates the port is enabled.

Table E-6. Parameters, Check Boxes, and Buttons on the Low Speed Port Page (continued)

Item	Type	Meaning
Autonegotiation	Check Box	Whether or not autonegotiation is enabled. A check indicates autonegotiation is enabled.
Duplex [Full/ Half/Not Applicable]	Radio Buttons	Whether the port is running in half-duplex or full-duplex mode. If autonegotiation is enabled for this port, this selection is disabled. The selected radio button indicates the current setting.
Port STP Mode	Radio Buttons	The operational mode for Spanning Tree Protocol. The selected radio button indicates one of the following modes: • No STP—Spanning Tree Protocol is disabled for this port. When Spanning Tree Protocol is disabled, the switch cannot detect network loops connected to this port. • FastStart—Fast Start operation for Spanning Tree Protocol is enabled for this port. This mode allows the port to transition to the Forwarding state faster than it does in the 802.1d mode. The probability that a loop may occur is greater with Fast Start operation than with IEEE 802.1d operation. • 802.1D—IEEE 802.1D-compliant Spanning Tree Protocol operation is enabled for this port. In this mode, port operation is compliant with the IEEE standard.
STP Port Priority	Parameter	The priority of each port, which is used in conjunction with the port number to create a unique port identifier. The valid range for this value is from 0 to 255. The default value is 128.
STP Port Path Cost	Parameter	The path cost to the designated root bridge. The valid range for this value is from 1 to 65,535. Entering a value of 0 will reset to the factory default setting so the switch software can automatically compute the path cost proportional to speed and duplex mode.

High Speed MLT Port Page

Clicking port 25, 26, or 27 on the Port page opens a configuration window for high-speed ports (Figure E-15). You can also open this page by clicking Configuration: Multi-Link Trunking in the navigation bar.

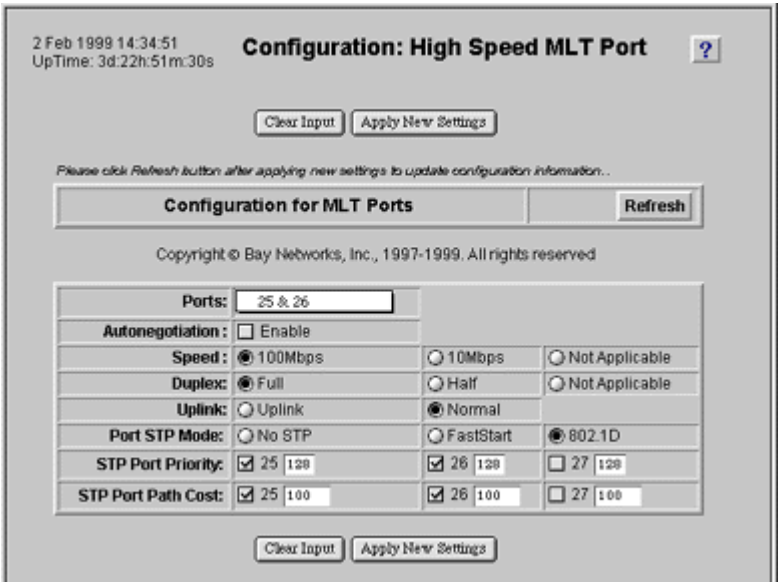


Figure E-15. High Speed MLT Port Page

This page includes the parameters and buttons listed in Table E-7.

Table E-7. Parameters and Buttons on the High Speed MLT Port Configuration Page

Item	Type	Meaning
Clear Input	Task Button	Returns settings on this page to their previous values.
Apply New Settings	Task Button	Applies new parameter settings.
Back	Task Button	Returns the display to the Port page.
Refresh	Task Button	Refreshes the display and shows the latest settings for the port.

Table E-7. Parameters and Buttons on the High Speed MLT Port Configuration Page (continued)

Item	Type	Meaning
Ports	Parameter	Selects the high-speed ports grouped into a multilink trunk. Choices are any two ports, all three ports, or none.
Autonegotiation	Check Box	Whether or not autonegotiation is enabled. A check indicates autonegotiation is enabled.
Speed	Radio Buttons	The selected radio button indicates the operating speed of the port. Choices are 100Mbps, 10Mbps, or Not Applicable. If autonegotiation is enabled, this selection is disabled, and Auto is displayed in the table on the Configuration: Port page.
Duplex [Full/ Half/Not Applicable]	Radio Buttons	Whether the port is running in half-duplex or full-duplex mode. If autonegotiation is enabled for this port, the parameter is not applicable. The selected radio button indicates the current setting.
Uplink [Uplink/ Normal]	Radio Buttons	The selected radio button indicates the setting for this port. When a port is set for Uplink, address learning is disabled on that port, allowing asymmetric MAC addressing to prevent excessive switch flooding. Selecting Normal allows address learning on the port.
Port STP Mode	Radio Buttons	The operational mode for Spanning Tree Protocol. The selected radio button indicates one of the following modes: • No STP—Spanning Tree Protocol is disabled for this port. When Spanning Tree Protocol is disabled, the switch cannot detect network loops connected to this port. • FastStart—Fast Start operation for Spanning Tree Protocol is enabled for this port. This mode allows the port to transition to the Forwarding state faster than it does in the 802.1d mode. The probability that a loop may occur is greater with Fast Start operation than with IEEE 802.1d operation. • 802.1D—IEEE 802.1D-compliant Spanning Tree Protocol operation is enabled for this port. In this mode, port operation is compliant with the IEEE standard

Table E-7. Parameters and Buttons on the High Speed MLT Port Configuration Page (continued)

Item	Type	Meaning
STP Port Priority	Parameter	The priority of each port, which is used in conjunction with the port number to create a unique port identifier. The valid range for this value is from 0 to 255. The default value is 128.
STP Port Path Cost	Parameter	The path cost to the designated root bridge. The valid range for this value is from 1 to 65,535. Entering a value of 0 will reset to the factory default setting so the switch software can automatically compute the path cost proportional to speed and duplex mode.

VLAN-ID

When you click on Configuration: VLAN in the navigation bar, the VLAN -ID configuration page (Figure E-16) opens. This page shows the VLAN assignments of the ports on the switch and allows you to designate ports as interswitch ports.

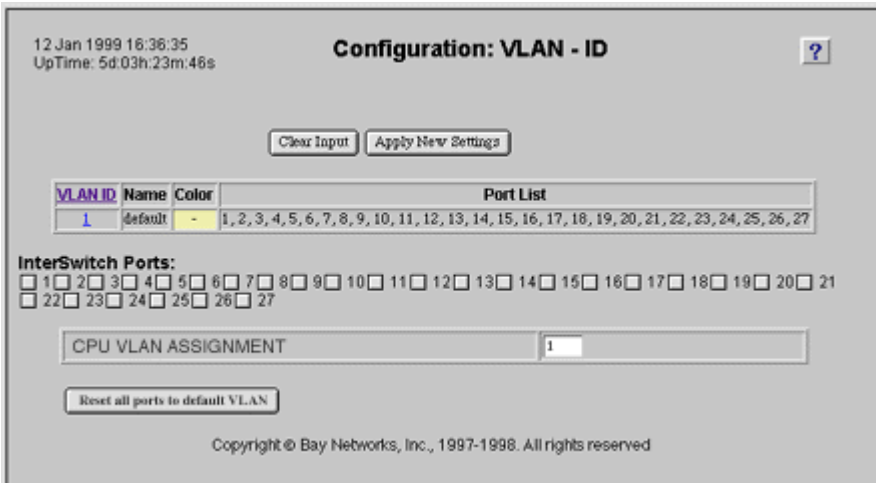


Figure E-16. VLAN-ID Page

This page includes the parameters and buttons listed in Table E-8.

Table E-8. Buttons and Parameters on the VLAN-ID Page

Item	Type	Meaning
Clear Input	Task Button	Returns settings on this page to their previous values.
Apply New Settings	Task Button	Applies new parameter settings.
VLAN ID	Link	Displays the VLAN Configuration page with the next available VLAN ID number assigned and all other fields blank. Fill in values to create a new VLAN.
VLAN number	Link	Displays the VLAN Configuration page for the specified VLAN.
Name	Display Only	A string of alphanumeric characters that identifies the VLAN. You can assign any string, such as “Finance” or “Third Floor.”
Color	Display Only	A color that has been assigned to this VLAN by system software. This color is used in graphical displays of network topology to differentiate VLANs.
Port List	Display Only	The list of ports assigned to this VLAN.
InterSwitch Ports	Check Boxes	The ports designated as interswitch ports. An interswitch port belongs to all VLANs.
CPU VLAN Assignment	Parameter Field	Allows the system administrator to specify the VLAN to which the CPU (management interface) is assigned. The network management station must also be a member of this VLAN to allow management through a Telnet or Web connection, or through SNMP management. The default assignment is VLAN 1.
Reset all ports to default VLAN	Task Button	Resets all ports to VLAN 1.

VLAN Configuration

The VLAN Configuration page (Figure E-17) is displayed when you click VLAN ID or on a number in the VLAN ID column on the VLAN-ID page. If you click VLAN ID, this page is displayed with the next available VLAN ID number and the remaining information blank. If you click a VLAN number, this page is displayed showing current settings for the specified VLAN.

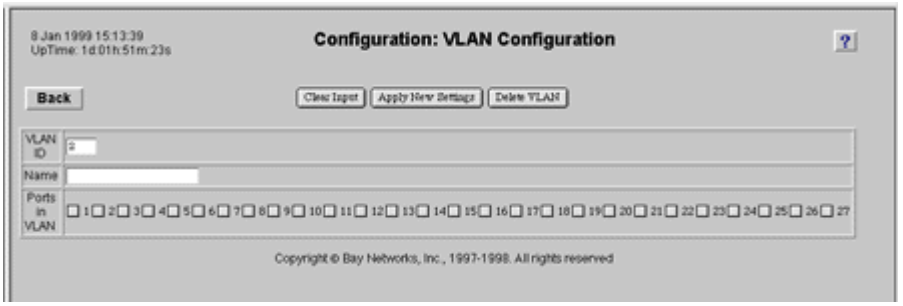


Figure E-17. VLAN Configuration Page

This page includes the items listed in Table E-9.

Table E-9. Parameters, check boxes, and buttons on the VLAN Configuration Page

Item	Type	Meaning
Clear Input	Task Button	Returns settings on this page to their previous values.
Apply New Settings	Task Button	Applies new parameter settings.
Delete VLAN	Task Button	Deletes the VLAN specified by this VLAN ID number and returns the ports to VLAN 1 (the default VLAN).
Back	Task Button	Returns the display to the VLAN-ID page.
VLAN ID	Parameter	An integer between 1 and 4094 that specifies a VLAN.
Name	Parameter	A string of alphanumeric characters that identifies the VLAN. You can assign any string, such as “Finance” or “Third Floor.”
Ports in VLAN	Check Boxes	The ports assigned to the VLAN. Click the check box to the left of the port number to assign that port to the VLAN.

Conversation Steering

The Conversation Steering page (Figure E-18) allows you to set up ports to monitor other ports as a troubleshooting technique.

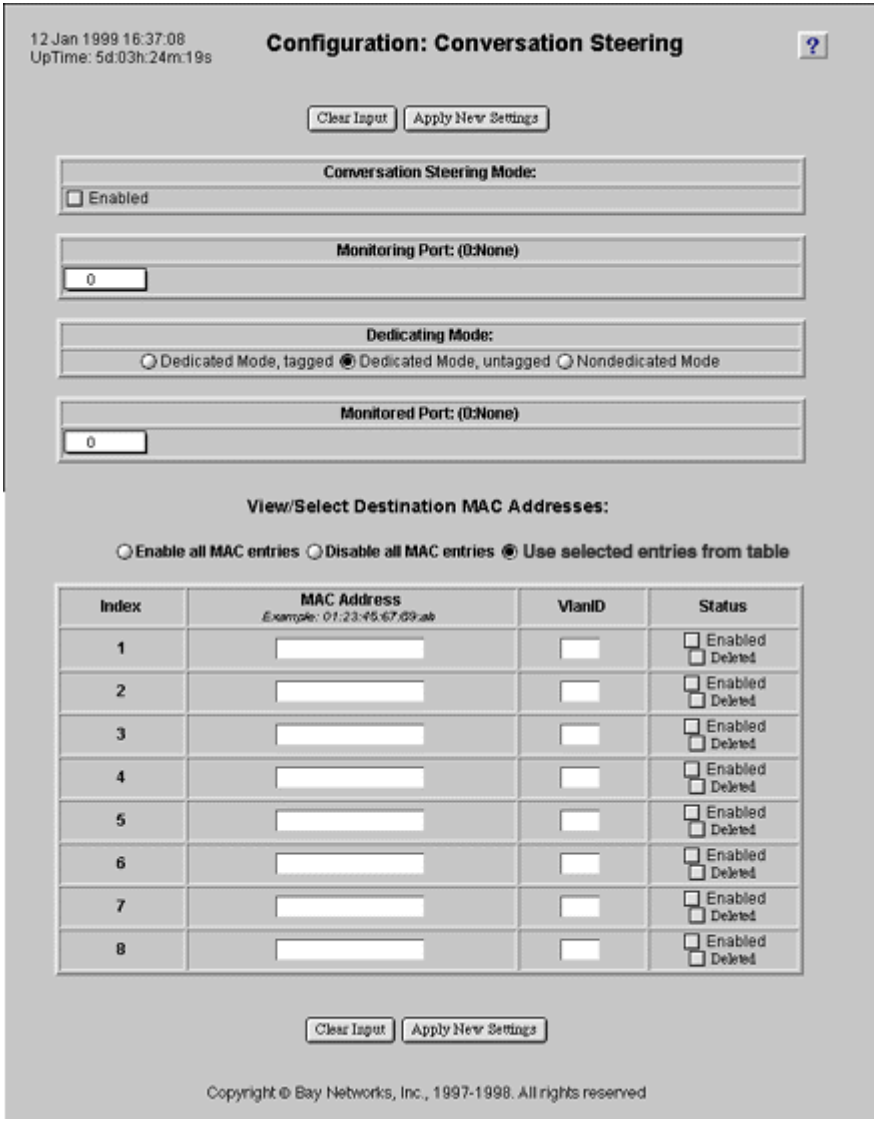


Figure E-18. Conversation Steering Page

This page includes the items listed in Table E-10.

Table E-10. Parameters, Check Boxes, and Buttons on the Conversation Steering Page

Area	Item	Type	Meaning
Port-Based Conversation Steering (Upper Half of Page)	Clear Input	Task Button	Returns settings on this page to their previous values.
	Apply New Settings	Task Button	Applies new parameter settings.
	Conversation Steering Mode Enabled	Check Box	Enables or disables conversation steering for the switch. The default is disabled (box not checked).
	Monitoring Port	Parameter	Indicates which port is specified as a monitoring port. A value of zero (0) indicates no ports are monitoring ports.
	Dedicating Mode	Radio Buttons	Specifies the dedicating mode of the monitoring port. Choices are: • Dedicated Mode, tagged An 802.1Q tag is inserted into the frame to identify the VLAN the frame is associated with. This setting allows you to use a dedicated monitoring port and a tag-aware probe. • Dedicated Mode, untagged No frames are tagged. This setting allows you to use a dedicated monitoring port and a probe that is not tag-aware. • Nondedicated Mode The monitoring port doubles as an active port. This setting allows you to another network device to share the port connection with a probe.
	Monitored Port	Parameter	The port being monitored.
MAC Address-Based Conversation Steering (Lower Half of Page)	Enable all MAC entries	Radio Button	Enables all MAC address entries on this page for traffic monitoring.
	Disable all MAC entries	Radio Button	Disables all MAC address entries on this page for traffic monitoring.
	Select Entries Use Table Below	Radio Button	Allows traffic monitoring for selected MAC addresses in the table.
	MAC Address	Parameter	The Destination address of a port to be monitored.

Table E-10. Parameters, Check Boxes, and Buttons on the Conversation Steering Page (continued)

Area	Item	Type	Meaning
	VLAN ID		The VLAN where you want to monitor this destination address.
	Enabled	Check Box	Enables or disables monitoring for the specified MAC address.
	Deleted	Check Box	Allows you to delete the specified MAC address from the table.

Filtering

The Filtering page (Figure E-19) allows you to enter up to eight MAC addresses. The switch drops (filters) all incoming packets destined to any of these addresses.

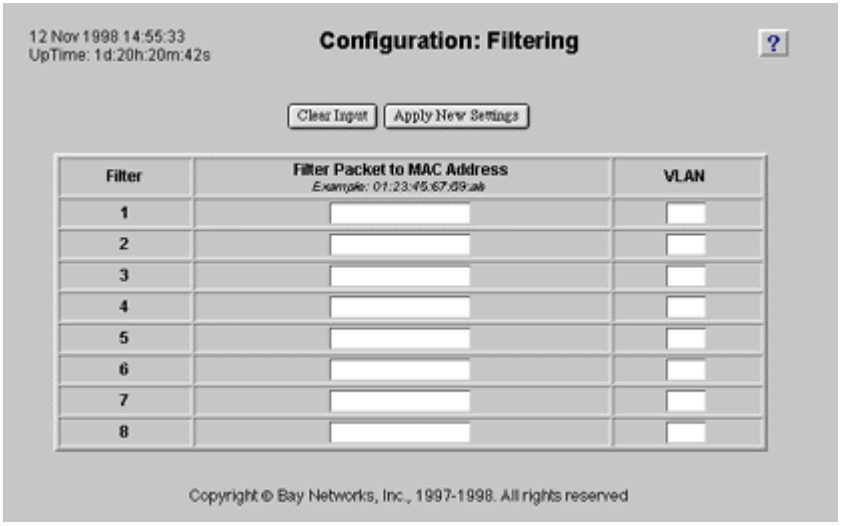


Figure E-19. Filtering Page

This page includes the parameter fields and buttons listed in Table E-11.l

Table E-11. Parameter Fields and Buttons on the Filtering Page

Item	Type	Meaning
Clear Input	Task Button	Returns settings on this page to their previous values.
Apply New Settings	Task Button	Applies new parameter settings.
Filter Packet to MAC Address	Parameter	The MAC address that appears in frames that will be dropped. This can be either a source or destination address.
VLAN	Parameter	The VLAN where you want the frame to be dropped.

Security

The following pages are listed under the Security Folder:

- Password (next section)
- Management Access (page E-32)
- Network Access (page E-34)

Password

The Password page (Figure E-20) allows you to set a password for access to the console interface and Web management interface.

Figure E-20. Password Page

This page includes the parameter fields and buttons listed in Table E-12.

Table E-12. Parameter Fields and Buttons on the Password Page

Item	Type	Meaning
Clear Input	Task Button	Returns settings on this page to their previous values.
Apply New Settings	Task Button	Applies new parameter settings.
Enter Old Password	Parameter	Allows access to this page if a password has already been set. You must enter the old password before you can change it. If no password has been set, leave this field blank.
Enter New Password	Parameter	Sets a new password.
Re-Enter New Password	Parameter	Verifies the new password.

Management Access

The Management Access page (Figure E-21) allows you to enable or disable Telnet access to the switch console interface and to set up restricted access for console, Web, and Telnet switch management.

Figure E-21. Management Access Page

This page includes the items listed in Table E-13.

Table E-13. Parameters, Check Boxes, and Buttons on the Management Access Page

Area	Item	Type	Meaning
General System	Clear Input	Task Button	Returns settings on this page to their previous values.
	Apply New Settings	Task Button	Applies new parameter settings.
Access Control	Telnet Access Control Enabled	Check Box	Enables or disables access to the console interface using a Telnet connection. The default is Enabled (box checked).
	Management Access Control Restricted	Check Box	When checked, restricts management access to only those stations with their IP addresses entered in the table. No other stations on the network can access the management functions. If management access is unrestricted, any station can access management functions. The default is unrestricted access (box not checked).
Management Access List	IP Address	Parameter	The IP address of a network station authorized to access the management functions for the switch.
	Telnet Enabled	Check Box	These check boxes individually enable or disable the specified type of access to management functions from the specified IP address. The default for each one is Enabled (box checked).
	Web Enabled	Check Box	
	SNMP Enabled	Check Box	

Network Access

The Network Access page (Figure E-22) allows you to set up the MAC address-based network access security.

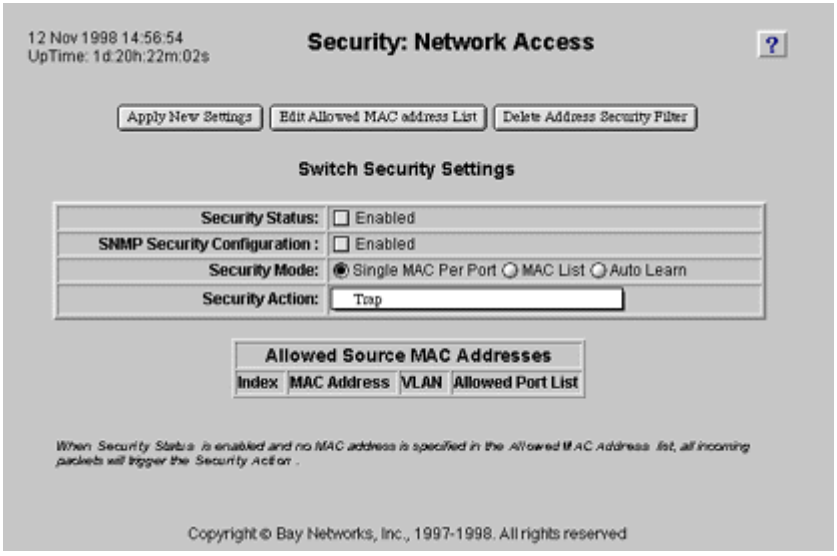


Figure E-22. Network Access Page

This page includes the items listed in Table E-14.

Table E-14. Parameters, Check Boxes, and Buttons on the Network Access Page

Area	Item	Type	Meaning
General System	Apply New Settings	Task Button	Applies new parameter settings.
	Edit Allowed MAC Address List	Task Button	Opens the Edit Allowed MAC Address List Page.
Switch Security Settings	Security Status Enabled	Check Box	Enables or disables MAC address-based security for network access. The default is disabled (box not checked).
	SNMP Security Configuration	Check Box	Enables or disables access to management functions using SNMP. The default is disabled (box not checked).
	Security Mode	Radio Buttons	The selected radio button indicates the current setting for the security mode. Choices are: • Single-MAC-per-port—Only one MAC address is allowed to access each port • MAC-list—You can specify a list of up to eight MAC addresses that are allowed to access each port. • Auto-Learn—The switch learns the first two MAC addresses that access each port and prevents access from all subsequent MAC addresses.
	Security Action	Parameter	Specifies the action to be taken if a security violation occurs. Possible choices are: • No action • Send trap to network management software • Partition the port • Partition the port and send a trap • Enable destination address filtering on the violating address • Enable destination address filtering and send a trap
Allowed MAC Addresses	Allowed Source MAC Address Table	Display Only	This table shows the MAC addresses that are allowed to access the switch, with their VLAN ID and the ports they are allowed to access.

Edit Allowed MAC Address List

The Edit Allowed MAC Address List page (Figure E-23) allows you to specify the MAC addresses that are allowed to access ports on the switch.

Figure E-23. Edit Allowed MAC Address List Page

This page includes the items listed in Table E-15.

Table E-15. Parameters, Check Boxes, and Buttons on the Edit Allowed MAC Address List Page

Item	Type	Meaning
Back to Network Access	Task Button	Returns the display to the Network Access page.
Apply New Settings	Task Button	Applies new parameter settings.
Delete Address	Task Button	Opens the Delete Address Security Filter page.
Security Configuration for MAC Address	Parameter Field	A MAC address to be added to the list or to have its access settings modified.
Allowed on Ports	Check Boxes	When checked, indicate the ports this MAC address is allowed to access.
All Ports	Task Button	Specifies this MAC address as allowed to access all ports on the switch.

Delete Address Security Filter

The Delete Address Security Filter page (Figure E-24) allows you to delete a destination address filter that has been applied in response to a security violation.

Figure E-24. Delete Address Security Filter

This page includes the items listed in Table E-16.

Table E-16. Parameters and Buttons on the Delete Address Security Filter Page

Item	Type	Meaning
Back to Network Access	Task Button	Returns the display to the Network Access page.
Delete Destination Address Filter	Task Button	Deletes the destination address filter for the specified port.
Source MAC Address	Parameter Field	Specifies the MAC address of the port for which you are deleting the destination address filter.

Fault Management Pages

The following pages are listed under the Fault Management folder:

- Port Management (this page)
- Ping/Telnet (page E-40)
- Topology (page E-41)
- MAC Address Table (page E-42)

Port Management

The Port Management page (Figure E-25) displays the current settings for high-speed ports and status information for all ports. To change any of the settings, go to the Port page.

12 Jan 1999 16:32:48
UpTime: 5d:03h:19m:58s

Fault Management: Port Management ?

High Speed Port Settings:

High Speed Port	Type	Auto-Negotiation	Operating Speed	Duplex Mode	Uplink Mode	MLT
25	100Base-TX	Disabled	100 Mbps	Full	No	Yes
26	100Base-FX	Disabled	100 Mbps	Full	No	Yes
27	100Base-TX	Enabled	10 Mbps	Half	No	No

Port Status:

Port	Usage	VLAN	InterSwitch Port	Link Status	Port Status	Monitoring	Current Utilization	Total Errors
1	Enabled	1	No	down	Disabled	-	0%	0
2	Enabled	1	No	down	Disabled	-	0%	0
3	Enabled	1	No	down	Disabled	-	0%	0
4	Enabled	1	No	down	Disabled	-	0%	0
5	Enabled	1	No	down	Disabled	-	0%	0
6	Enabled	1	No	down	Disabled	-	0%	0
7	Enabled	1	No	down	Disabled	-	0%	0
8	Enabled	1	No	down	Disabled	-	0%	0
9	Enabled	1	No	down	Disabled	-	0%	0
10	Enabled	1	No	down	Disabled	-	0%	0
11	Enabled	1	No	up	Forwarding	-	0%	17
12	Enabled	1	No	down	Disabled	-	0%	0
13	Enabled	1	No	down	Disabled	-	0%	0
14	Enabled	1	No	down	Disabled	-	0%	0

Figure E-25. Port Management Page

This page includes the information listed in Table E-17.

Table E-17. Information on the Port Management Page

Area	Parameter	Meaning
High Speed Port Settings	Port number	High-speed ports are 25, 26, and 27.
	Type	Whether the port is a 10/100BASE-TX or (for an MDA) 100BASE-FX.
	Auto-Negotiation	Whether the autonegotiation feature is enabled or disabled for the port.
	Operating Speed	Whether the port is operating at 10 or 100 Mb/s.
	Duplex Mode	Whether the port is operating in full- or half-duplex mode.
	Uplink Mode	Whether or not the port is set for Uplink mode. When a port is set for Uplink, Address Learning Mode is disabled on that port, allowing asymmetric MAC addressing to prevent excessive switch flooding.
	MLT	Whether or not the port is a member of a multilink trunk.
Port Status for Low-Speed ports	Port Number	The number of the port.
	Usage	Indicates if port usage is enabled or disabled. Clicking on an entry in this column links you to the Port Configuration page, where you can reconfigure the displayed parameters for the port.
	VLAN	The number of the VLAN the port is assigned to.
	Link Status	Indicates whether the link is active (up) or inactive (down) at the physical level.
	Port Status	Indicates if a port is disabled or, if enabled, if the spanning tree status is forwarding or blocking.
	Monitoring	Whether or not the port is set as a monitoring port.
	Current Utilization	Indicates how much of the available bandwidth on the port is being used by traffic. Port utilization is computed for the previous 5 seconds. Clicking on this column links you to the Traffic Statistics page, where more information about port utilization is displayed.
	Total Errors	Indicates the cumulative errors for that port since the switch was powered up.

Ping/Telnet

The Ping/Telnet page (Figure E-26) is comparable to the Troubleshooting selection from the console interface. It allows you to determine if a remote station is connected to the network by sending a ping signal to it.

The input field is for the Target IP address. Click the Send Ping Request task button to send the signal. The results of the ping action are displayed.

If the connection is active, clicking the Telnet task button allows you to connect to the station.

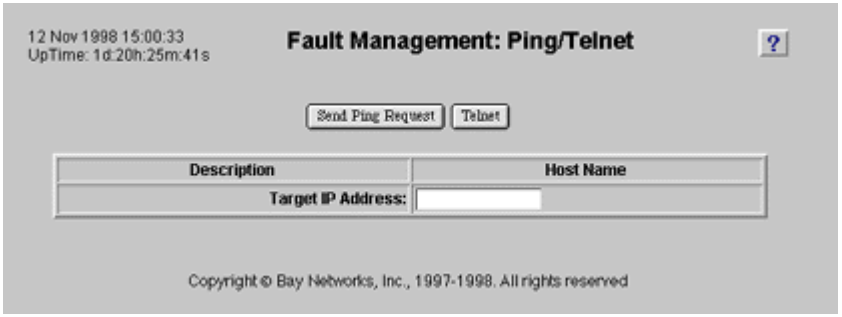


Figure E-26. Ping/Telnet Page

Topology

The Topology page (Figure E-27) allows you to display information about other Bay Networks devices discovered on the network. A topology table shows MAC addresses, IP addresses, and device types for Bay Networks devices that are directly connected to the switch. Links allow you to connect to these devices if they support Web or Telnet access.

Note: The topology table shows only those Bay Networks devices that are directly connected to the switch through an active link. Devices with a direct connection in standby mode do not appear in the table.

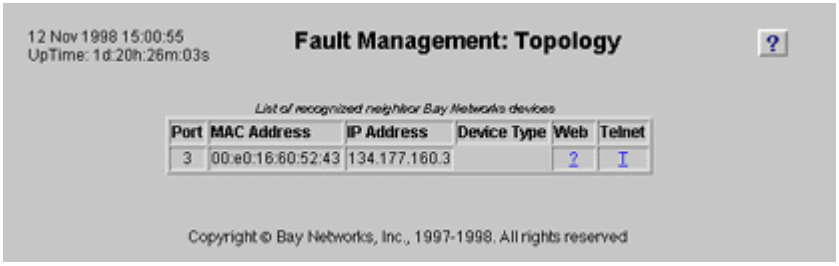


Figure E-27. Topology Page

MAC Address Table

The MAC Address Table page (Figure E-28) shows a complete list of all MAC addresses that have been learned by the switch, the ports they have been learned on, which addresses are permanent (static) and which are subject to aging (dynamic), and which addresses are subject to filtering.

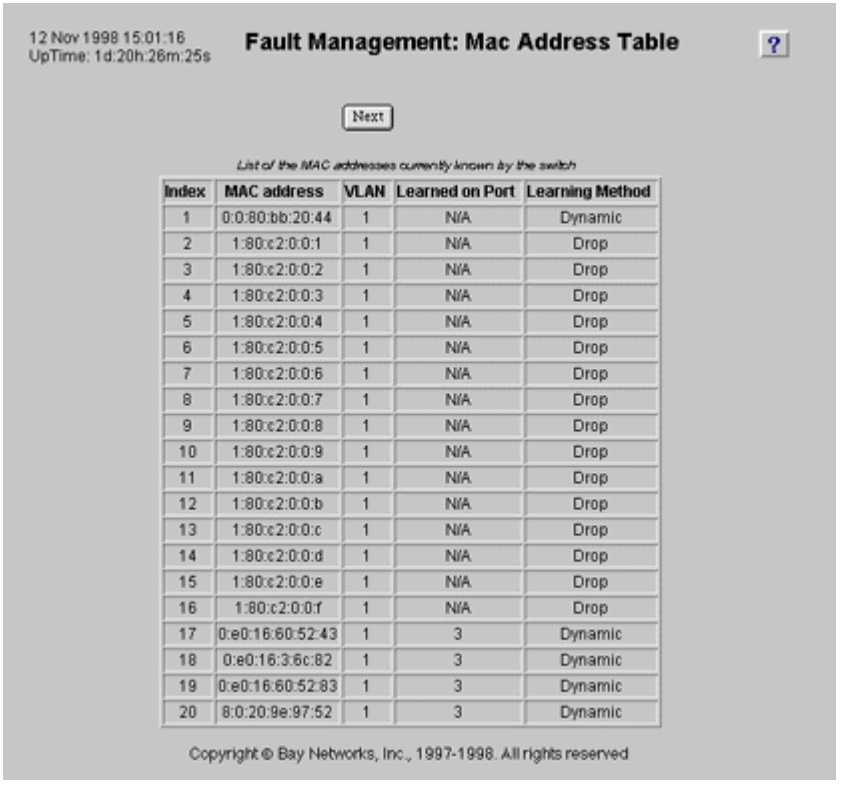


Figure E-28. MAC Address Table Page

Statistics Pages

The following pages are listed under the Statistics heading:

- Traffic (this page)
- Error (page E-45)

Traffic

The Traffic page (Figure E-29) shows current traffic statistics for the switch ports.

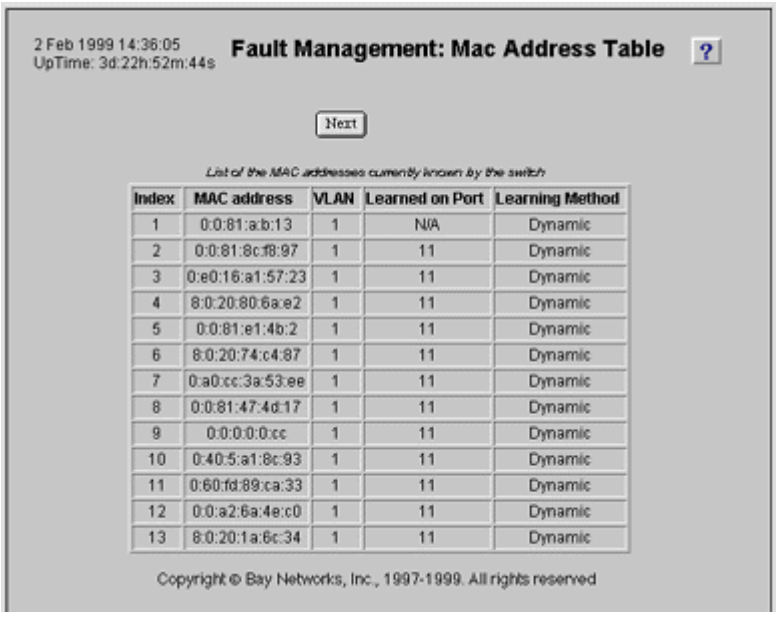


Figure E-29. Traffic Page

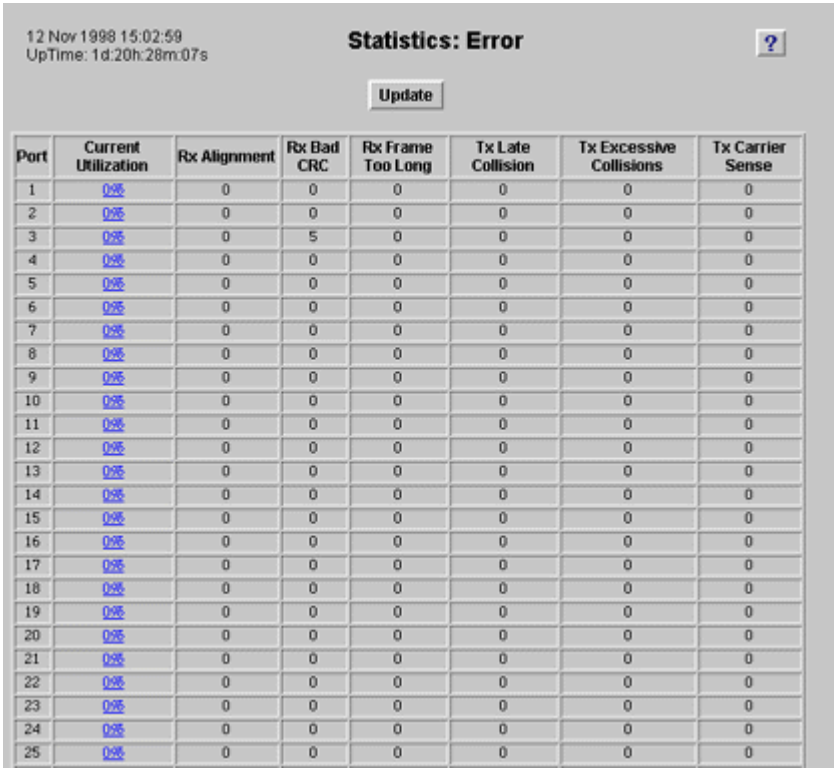
This page includes the information listed in Table E-18.

Table E-18. Information Fields on the Traffic Page

Field	Meaning
Current Utilization	Indicates how much of the available bandwidth on the port is being used by traffic. Port utilization is computed for the previous 5 seconds.
Rx Good Frames	Counters that increment whenever a frame is received successfully on the corresponding port.
Tx Good Frames	Counters that increment whenever a frame is transmitted successfully on the corresponding port.
Tx Single Collisions	Counters that increment when a frame transmitted on the port had a single collision and was transmitted successfully on the second try.
Tx Multi Collisions	Counters that increment when a frame transmitted on the port had more than one collision and was then transmitted successfully within 16 attempts. If a frame transmits successfully after only one collision, it increments the single collision counter. If there are anywhere from two to 16 tries for a successful transmission, then the multiple counter increments. If, after 16 tries, a collision is still detected, the excessive transmission counter increments and no more retries are attempted.
Tx Deferred	Counters that increment when a frame transmitted on the port was delayed because the wire was busy.
Total Errors	Counters in this column represent the sum of the receive and transmit errors on the corresponding port. Clicking on this column links you to the Error Statistics page where a breakdown of the errors is provided.

Error

The Error page (Figure E-30) shows current error statistics for the switch ports.



Port	Current Utilization	Rx Alignment	Rx Bad CRC	Rx Frame Too Long	Tx Late Collision	Tx Excessive Collisions	Tx Carrier Sense
1	0%	0	0	0	0	0	0
2	0%	0	0	0	0	0	0
3	0%	0	5	0	0	0	0
4	0%	0	0	0	0	0	0
5	0%	0	0	0	0	0	0
6	0%	0	0	0	0	0	0
7	0%	0	0	0	0	0	0
8	0%	0	0	0	0	0	0
9	0%	0	0	0	0	0	0
10	0%	0	0	0	0	0	0
11	0%	0	0	0	0	0	0
12	0%	0	0	0	0	0	0
13	0%	0	0	0	0	0	0
14	0%	0	0	0	0	0	0
15	0%	0	0	0	0	0	0
16	0%	0	0	0	0	0	0
17	0%	0	0	0	0	0	0
18	0%	0	0	0	0	0	0
19	0%	0	0	0	0	0	0
20	0%	0	0	0	0	0	0
21	0%	0	0	0	0	0	0
22	0%	0	0	0	0	0	0
23	0%	0	0	0	0	0	0
24	0%	0	0	0	0	0	0
25	0%	0	0	0	0	0	0

Figure E-30. Error Page

This page includes the information listed in Table E-19.

Table E-19. Information Fields on the Error Page

Field	Meaning
Current Utilization	Indicates how much of the available bandwidth on the port is being used by traffic. Port utilization is computed for the previous 5 seconds. Clicking on this column links you to the Traffic Statistics page.
Rx Alignment	Counters that increment when a receive frame alignment error is recorded. Misaligned frames are those that do not start or end on a byte boundary.
Rx Bad CRC	Counters that increment whenever a corrupt frame is received on the port and the integrity of the data is lost.
Rx Frame Too Long	Counters that increment whenever a frame received on the port is greater than 1,518 octets in length.
Tx Late Collision	Counters that increment when a collision on the port has been detected later than 512 bit times into the frame duration.
Tx Excessive Collisions	Counters that increment when a frame on the port is not successfully transmitted due to excessive (16 consecutive) collisions.
Tx Carrier Senses	Counters that increment each time that carrier sense was lost or not seen on the port during the transmission of a frame without a collision.

Index

Numbers

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W