

Using the BayStack 450 Switch

Part No. 302401-A Rev 00
June 1998



Copyright © 1998 Bay Networks, Inc.

All rights reserved. Printed in the USA. June 1998.

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

Trademarks

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

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 350 10/100 Autosense Switch is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class A (CISPR 22).

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

EC Declaration of Conformity

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

Japan/Nippon Requirements Only

Voluntary Control Council for Interference (VCCI) Statement

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

Voluntary Control Council for Interference (VCCI) Statement

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

Canada Requirements Only

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (BayStack 350 10/100 Autosense Switch) does not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (BayStack 350 10/100 Autosense Switch) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

Bay Networks, Inc. Software License Agreement

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

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

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

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse.

The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence.

THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

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

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

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

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

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

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

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

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

Contents

Preface

Audience	xix
Organization	xx
Conventions	xx
Special Message Formats	xxi
Use of Enter, Type, and Press	xxi
Other Conventions	xxi
Bay Networks Technical Publications	xxii
Bay Networks Customer Service	xxii
How to Get Help	xxiii

Safety Messages

Safety Alert Message Format	xxv
Safety Alert Messages Used in This Guide	xxvii

Chapter 1

Introduction to the BayStack 450 Switch

Physical Description	1-1
Front-Panel	1-2
Comm Port	1-3
Uplink/Expansion Slot	1-3
10BASE-T/100BASE-TX Port Connectors	1-3
LED Display Panel	1-4
Back-Panel	1-7
AC Power Receptacle	1-7
RPSU Connector	1-9
Filler Panel	1-9
Cooling Fans	1-9
Features	1-9
Autosensing and Autonegotiation	1-12

IEEE 802.1Q VLANs	1-12
IGMP Snooping Feature	1-13
IEEE 802.1p Prioritizing	1-13
MultiLink Trunking	1-13
Port Mirroring	1-13
Flash Memory Storage	1-14
BootP Automatic IP Configuration	1-14
SNMP MIB Support	1-15
Configuration and Switch Management	1-15
Network Configuration	1-15
Desktop Switch Application	1-16
Segment Switch Application	1-17
High-Density Switched Workgroup Application	1-18
IEEE 802.1Q VLAN Workgroups	1-19
IEEE 802.1Q Tagging	1-20
VLANs Spanning Multiple Switches	1-24
VLANs Spanning Multiple 802.1Q Tagged Switches	1-24
VLANs Spanning Multiple Untagged Switches	1-25
Shared Servers	1-26
VLAN Workgroup Summary	1-32
VLAN Configuration Rules	1-34
IGMP Snooping	1-35
IGMP Snooping Configuration Rules	1-39
IEEE 802.1p Prioritizing	1-40
MultiLink Trunks	1-44
Client/Server Configuration Utilizing MultiLink Trunks	1-45
Trunk Configuration Screen Examples	1-47
Trunk Configuration Screen for Switch S1	1-47
Trunk Configuration Screen for Switch S2	1-50
Trunk Configuration Screen for Switch S3	1-52
Trunk Configuration Screen for Switch S4	1-54
Before Configuring Trunks	1-56
MultiLink Trunking Configuration Rules	1-56
Spanning Tree Considerations	1-58
Additional Tips About the MultiLink Trunking Feature	1-61

Port Mirroring (Conversation Steering)	1-62
Port-Based Mirroring Configuration	1-63
Address-Based Mirroring Configuration	1-65
Port Mirroring Configuration Rules	1-68

Chapter 2

Installing the BayStack 450 Switch

Installation Requirements	2-1
Installation Procedure	2-3
Installing the BayStack 450 Switch on a Flat Surface	2-3
Installing the BayStack 450 Switch in a Rack	2-4
Attaching Devices to the BayStack 450 Switch	2-6
Connecting the 10BASE-T/100BASE-TX Ports	2-7
Connecting the Console/Comm Port	2-8
Connecting Power	2-9
Verifying the Installation	2-10
Verifying the Installation Using the LEDs	2-11
Verifying the Installation Using the Self-Test Screen	2-12
Initial Setup of the BayStack 450 Switch	2-13

Chapter 3

Using the Console Interface

Accessing the CI Menus and Screens	3-1
Using the CI Menus and Screens	3-2
Navigating the CI Menus and Screens	3-2
Screen Fields and Descriptions	3-3
Main Menu	3-4
IP Configuration/Setup	3-7
Choosing a BootP Request Mode	3-9
BootP When Needed	3-9
BootP Always	3-10
BootP Disabled	3-10
BootP or Last Address	3-10
SNMP Configuration	3-12
System Characteristics	3-14
Switch Configuration	3-16

MAC Address Table	3-18
VLAN Configuration Menu	3-20
VLAN Configuration	3-22
VLAN Port Configuration	3-24
VLAN Display by Port	3-27
Traffic Class Configuration	3-28
Port Configuration	3-30
High Speed Flow Control Configuration	3-32
Choosing a High Speed Flow Control Mode	3-34
MultiLink Trunk Configuration	3-35
MultiLink Trunk Configuration Screen	3-37
MultiLink Trunk Utilization Screen	3-39
Port Mirroring Configuration	3-42
Rate Limiting Configuration	3-45
IGMP Configuration	3-48
Port Statistics	3-51
Console/Comm Port Configuration	3-55
Spanning Tree Configuration	3-57
Spanning Tree Port Configuration	3-59
Display Spanning Tree Switch Settings	3-62
TELNET Configuration	3-65
Software Download	3-68
Display Event Log	3-71
Excessive Bad Entries	3-72
Write Threshold	3-72
Flash Update	3-73
Reset	3-74
Reset to Default Settings	3-76
Logout	3-78

Chapter 4

Troubleshooting

LED Indications	4-2
Diagnosing and Correcting the Problem	4-4
Port Connection Problems	4-5
Autonegotiation Modes	4-5

Port Interface	4-6
----------------------	-----

Appendix A
Technical Specifications

Environmental	A-1
Electrical	A-1
Physical Dimensions	A-2
Performance Specifications	A-2
Network Protocol and Standards Compatibility	A-2
Data Rate	A-2
Interface Options	A-3
Safety Agency Certification	A-3
Electromagnetic Emissions	A-3
Electromagnetic Immunity	A-3
Declaration of Conformity	A-4

Appendix B
Media Dependent Adapters (MDAs)

400-4TX MDA	B-2
400-2FX MDA	B-3
1000BASE-SX MDA	B-4
1000BASE-LX MDA	B-6
Installing an MDA	B-7

Appendix C
Quick Steps to Features

Configuring 802.1Q VLANs	C-2
Configuring MultiLink Trunks	C-5
Configuring Port Mirroring	C-6
Configuring IGMP Snooping	C-8

Appendix D
Connectors and Pin Assignments

RJ-45 (10BASE-T/100BASE-TX) Port Connectors	D-1
MDI and MDI-X Devices	D-2
MDI-X to MDI Cable Connections	D-3
MDI-X to MDI-X Cable Connections	D-4
DB-9 (RS-232-D) Console/Comm Port Connector	D-5

Appendix E
Default Settings

Appendix F
Sample BootP Configuration File

Figures

Figure 1-1.	BayStack 450 Switch Versions	1-1
Figure 1-2.	BayStack 450 Switch Front-Panel	1-2
Figure 1-3.	BayStack 450 Switch LED Display Panel	1-5
Figure 1-4.	BayStack 450 Switch Back-Panel	1-7
Figure 1-5.	BayStack 450 Switch Used as a Desktop Switch	1-16
Figure 1-6.	BayStack 450 Switch Used as a Segment Switch	1-17
Figure 1-7.	Configuring Power Workgroups and a Shared Media Hub	1-18
Figure 1-8.	Port-Based VLAN Example	1-19
Figure 1-9.	Default VLAN Settings	1-21
Figure 1-10.	802.1Q Tagging (1 of 4)	1-22
Figure 1-11.	802.1Q Tagging (2 of 4)	1-22
Figure 1-12.	802.1Q Tagging (3 of 4)	1-23
Figure 1-13.	802.1Q Tagging (4 of 4)	1-23
Figure 1-14.	VLANs Spanning Multiple 802.1Q Tagged Switches	1-24
Figure 1-15.	VLANs Spanning Multiple Untagged Switches	1-25
Figure 1-16.	Possible Problems with VLANs and Spanning Tree Protocol	1-26
Figure 1-17.	Multiple VLANs Sharing Resources	1-27
Figure 1-18.	VLAN Broadcast Domains Within the Switch	1-28
Figure 1-19.	Default VLAN Configuration Screen Example	1-29
Figure 1-20.	VLAN Configuration Screen Example	1-30
Figure 1-21.	Default VLAN Port Configuration Screen Example	1-31
Figure 1-22.	VLAN Port Configuration Screen Example	1-32
Figure 1-23.	VLAN Configuration Spanning Multiple Switches	1-33
Figure 1-24.	IP Multicast Propagation With IGMP Routing	1-36
Figure 1-25.	BayStack 450 Switch Filtering IP Multicast Streams (1 of 2)	1-37
Figure 1-26.	BayStack 450 Switch Filtering IP Multicast Streams (2 of 2)	1-38
Figure 1-27.	Prioritizing Packets	1-40
Figure 1-28.	Port Transmit Queue	1-41
Figure 1-29.	Default Traffic Class Configuration Screen Example	1-42

Figure 1-30.	Setting Port Priority Example	1-43
Figure 1-31.	Switch-to-Switch Trunk Configuration Example	1-44
Figure 1-32.	Switch-to-Server Trunk Configuration Example	1-45
Figure 1-33.	Client/Server Configuration Example	1-46
Figure 1-34.	Choosing the MultiLink Trunk Configuration Screen	1-47
Figure 1-35.	MultiLink Trunk Configuration Screen for Switch S1	1-48
Figure 1-36.	MultiLink Trunk Configuration Screen for Switch S2	1-50
Figure 1-37.	MultiLink Trunk Configuration Screen for Switch S3	1-52
Figure 1-38.	MultiLink Trunk Configuration Screen for Switch S4	1-54
Figure 1-39.	Path Cost Arbitration Example	1-58
Figure 1-40.	Example 1: Correctly Configured Trunk	1-59
Figure 1-41.	Example 2: Detecting a Misconfigured Port	1-60
Figure 1-42.	Port-Based Mirroring Configuration Example	1-63
Figure 1-43.	Port Mirroring Port-Based Screen Example	1-65
Figure 1-44.	Address-Based Mirroring Configuration Example	1-66
Figure 1-45.	Port Mirroring Address-Based Screen Example	1-67
Figure 2-1.	Package Contents	2-2
Figure 2-2.	Positioning the Chassis in the Rack	2-4
Figure 2-3.	Attaching Mounting Brackets	2-5
Figure 2-4.	Installing the BayStack 450 Switch in an Equipment Rack	2-5
Figure 2-5.	10/100 Mb/s Port Connections	2-7
Figure 2-6.	Connecting to the Console/Comm Port	2-9
Figure 2-7.	BayStack 450 Switch AC Power Receptacle	2-10
Figure 2-8.	Grounded AC Power Outlet	2-10
Figure 2-9.	Observing LEDs to Verify Proper Operation	2-11
Figure 2-10.	BayStack 450 Switch Self-Test Screen	2-12
Figure 2-11.	Bay Networks Logo Screen	2-13
Figure 2-12.	Main Menu	2-14
Figure 2-13.	IP Configuration/Setup Screen	2-15
Figure 3-1.	Map of Console Interface Screens	3-3
Figure 3-2.	Console Interface Main Menu	3-4
Figure 3-3.	IP Configuration/Setup Screen	3-7
Figure 3-4.	SNMP Configuration Screen	3-12
Figure 3-5.	System Characteristics Screen	3-14
Figure 3-6.	Switch Configuration Menu Screen	3-16

Figure 3-7.	MAC Address Table Screen	3-19
Figure 3-8.	VLAN Configuration Menu Screen	3-21
Figure 3-9.	VLAN Configuration Screen	3-22
Figure 3-10.	VLAN Port Configuration Screen	3-24
Figure 3-11.	VLAN Display by Port Screen	3-27
Figure 3-12.	Traffic Class Configuration Screen	3-29
Figure 3-13.	Port Configuration Screen (1 of 2)	3-30
Figure 3-14.	Port Configuration Screen (2 of 2)	3-31
Figure 3-15.	High Speed Flow Control Configuration Screen	3-33
Figure 3-16.	MultiLink Trunk Configuration Menu Screen	3-35
Figure 3-17.	MultiLink Trunk Configuration Screen	3-37
Figure 3-18.	MultiLink Trunk Utilization Screen (1 of 2)	3-39
Figure 3-19.	MultiLink Trunk Utilization Screen (2 of 2)	3-40
Figure 3-20.	Port Mirroring Configuration Screen	3-42
Figure 3-21.	Rate Limiting Configuration Screen (1 of 2)	3-45
Figure 3-22.	Rate Limiting Configuration Screen (2 of 2)	3-46
Figure 3-23.	IGMP Configuration Screen	3-48
Figure 3-24.	Port Statistics Screen	3-51
Figure 3-25.	Console/Comm Port Configuration Screen	3-55
Figure 3-26.	Spanning Tree Configuration Menu Screen	3-57
Figure 3-27.	Spanning Tree Port Configuration Screen (1 of 2)	3-59
Figure 3-28.	Spanning Tree Port Configuration Screen (2 of 2)	3-60
Figure 3-29.	Spanning Tree Switch Settings Screen	3-62
Figure 3-30.	TELNET Configuration Screen	3-65
Figure 3-31.	Software Download Screen	3-68
Figure 3-32.	Event Log Screen	3-71
Figure 3-33.	Sample Event Log Entry Showing Excessive Bad Entries	3-72
Figure 3-34.	Sample Event Log Event Exceeding the Write Threshold	3-73
Figure 3-35.	Sample Event Log Event Showing Flash Update Status	3-73
Figure 3-36.	Self-Test Screen After Resetting the Switch	3-74
Figure 3-37.	Bay Networks Logo Screen	3-75
Figure 3-38.	Self-Test Screen After Resetting to Factory Default Settings	3-76
Figure 3-39.	Bay Networks Logo Screen After Resetting to Factory Default Settings	3-77
Figure 3-40.	Password Prompt Screen	3-78
Figure 4-1.	BayStack 450 Switch LED Locations	4-2

Figure B-1.	400-4TX MDA Front-Panel	B-2
Figure B-2.	400-2FX MDA Front-Panel	B-3
Figure B-3.	1000BASE-SX MDA Front-Panel	B-5
Figure B-4.	1000BASE-LX MDA Front-Panel	B-6
Figure B-5.	Installing an MDA	B-8
Figure C-1.	Configuring 802.1Q VLANs (1 of 3)	C-2
Figure C-2.	Configuring 802.1Q VLANs (2 of 3)	C-3
Figure C-3.	Configuring 802.1Q VLANs (3 of 3)	C-4
Figure C-4.	Configuring MultiLink Trunks	C-5
Figure C-5.	Configuring Port Mirroring (1 of 2)	C-6
Figure C-6.	Configuring Port Mirroring (2 of 2)	C-7
Figure C-7.	Configuring IGMP Snooping (1 of 3)	C-8
Figure C-8.	Configuring IGMP Snooping (2 of 3)	C-9
Figure C-9.	Configuring IGMP Snooping (3 of 3)	C-10
Figure D-1.	RJ-45 (8-Pin Modular) Port Connector	D-1
Figure D-2.	MDI-X to MDI Cable Connections	D-3
Figure D-3.	MDI-X to MDI-X Cable Connections	D-4
Figure D-4.	DB-9 Console/Comm Port Connector	D-5

Tables

Table 1-1.	BayStack 450 Switch LED Descriptions	1-6
Table 1-2.	International Power Cord Specifications	1-8
Table 2-1.	Power-Up Sequence	2-11
Table 3-1.	Console Interface Main Menu options	3-4
Table 3-2.	IP Configuration/Setup Screen Fields	3-8
Table 3-3.	SNMP Configuration Screen Fields	3-13
Table 3-4.	System Characteristics Screen Fields	3-15
Table 3-5.	Switch Configuration Menu Screen Options	3-17
Table 3-6.	MAC Address Table Screen Fields	3-19
Table 3-7.	VLAN Configuration Menu Screen Options	3-21
Table 3-8.	VLAN Configuration Screen Fields	3-23
Table 3-9.	VLAN Port Configuration Screen Fields	3-25
Table 3-10.	VLAN Display by Port Screen Fields	3-28
Table 3-11.	Traffic Class Configuration Screen Fields	3-29
Table 3-12.	Port Configuration Screen Fields	3-31
Table 3-13.	High Speed Flow Control Configuration Screen Fields	3-33
Table 3-14.	MultiLink Trunk Configuration Menu Screen Options	3-36
Table 3-15.	MultiLink Trunk Configuration Screen Fields	3-38
Table 3-16.	MultiLink Trunk Utilization Screen Fields	3-40
Table 3-17.	Port Mirroring Configuration Screen Fields	3-43
Table 3-18.	Monitoring Modes	3-44
Table 3-19.	Rate Limiting Configuration Screen Fields	3-47
Table 3-20.	IGMP Configuration Screen Fields	3-49
Table 3-21.	Port Statistics Screen Fields	3-52
Table 3-22.	Console/Comm Port Configuration Screen Fields	3-55
Table 3-23.	Spanning Tree Configuration Menu Screen Options	3-58
Table 3-24.	Spanning Tree Port Configuration Screen Fields	3-60
Table 3-25.	Spanning Tree Switch Settings Parameters	3-63
Table 3-26.	TELNET Configuration Screen Fields	3-66

Table 3-27.	Software Download Screen Fields	3-69
Table 3-28.	LED Indications During the Software Download Process	3-70
Table 4-1.	BayStack 450 Switch LED Descriptions	4-3
Table 4-2.	Corrective Actions	4-4
Table B-1.	400-4TX MDA Components	B-2
Table B-2.	400-2FX Components	B-3
Table B-3.	1000BASE-SX Components	B-5
Table B-4.	1000BASE-LX Components	B-7
Table D-1.	RJ-45 Port Connector Pin Assignments	D-2
Table D-2.	DB-9 Console/Comm Port Connector Pin Assignments	D-5
Table E-1.	Factory Default Settings for the BayStack 450 Switch	E-1

Preface

Congratulations on your purchase of the BayStack 450 Switch, part of the Bay Networks® BayStack™ 10/100/1000 switches line of communications products.

There are two versions of the BayStack 450 switch: the BayStack 450-24 switch and the BayStack 450-12 switch. This guide describes the features, uses, and installation procedures for the two versions. (Unless otherwise specified, the terms “BayStack 450 switch” and “switch” refer to both switch versions.)

This release of the BayStack 450 switch does not include the stacking feature functionality, currently planned for a future release. Although the LED display panel and chassis show labeling related to the stacking feature, the function is not operational and is referred to as “for future release” in this manual.

Contact your Bay Networks sales representative for more information.

Audience

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

Organization

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

- Chapter 1 provides an introduction to the BayStack 450 switch and provides an overview of its key features.
- Chapter 2 explains how to install and verify the operation of the BayStack 450 switch. The chapter includes instructions for installing the switch on a flat surface or in a 19-inch equipment rack.
- Chapter 3 explains how to connect to the BayStack 450 switch Console/Comm Port and how to use the console interface (CI) menus to configure and manage the switch.
- Chapter 4 describes how to isolate and diagnose problems with the BayStack 450 switch, as indicated by the LEDs.
- Appendix A lists operational and environmental specifications that apply to the BayStack 450 switch.
- Appendix B provides an overview of optional media dependent adapters (MDAs) you can use with the BayStack 450 switch. This appendix also shows how to install an MDA to the switch.
- Appendix C provides Quick-Step flowcharts for using the BayStack 450 switch features.
- Appendix D describes the BayStack 450 switch connectors (ports) and pin assignments.
- Appendix E lists the factory default settings for the BayStack 450 switch.
- Appendix F provides a sample BootP configuration file.
- The index provides an alphabetical listing of the topics and subtopics in this guide, with cross-references to relevant information.

Conventions

This section describes the conventions used in this guide.

Special Message Formats

This guide uses the following formats to highlight special messages:



Note: A note is used to highlight information of importance or special interest.



Caution: A caution alerts the user to some action or set of conditions that could result in damage to the equipment.



Warning: A warning alerts the user to some action or set of conditions that could result in personal injury.

Use of Enter, Type, and Press

This guide uses “enter,” “type,” and “press” to describe the following actions:

- When you read “enter,” type the text and press the Enter key.
- When you read “type,” type the text, but do not press the Enter key.
- When you read “press,” press only the alphanumeric or named key.

Other Conventions

This guide uses the following typographical conventions:

<i>italics</i>	Always used for book titles. In command descriptions, italic type indicates a variable that you supply. In a body of text, italic type is sometimes used to emphasize a term or word.
monospace type	Represents examples of screen text or screen field entries you might be required to type.
[Enter]	Named keys in text are enclosed in square brackets. The notation [Enter] is used for the Enter key and the Return key.
[Ctrl]-C	Two or more keys that must be pressed simultaneously are shown in text linked with a hyphen (-) sign.

Bay Networks Technical Publications

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

Documentation sets and CDs are available through your local Bay Networks sales office or account representative.

Bay Networks Customer Service

You can purchase a support contract from your Bay Networks distributor or authorized reseller, or directly from Bay Networks Services. For information about, or to purchase a Bay Networks service contract, either call your local Bay Networks field sales office or one of the following numbers:

Region	Telephone number	Fax number
United States and Canada	800-2LANWAN; then enter Express Routing Code (ERC) 290, when prompted, to purchase or renew a service contract 978-916-8880 (direct)	978-916-3514
Europe	33-4-92-96-69-66	33-4-92-96-69-96
Asia/Pacific	61-2-9927-8888	61-2-9927-8899
Latin America	561-988-7661	561-988-7550

Information about customer service is also available on the World Wide Web at *support.baynetworks.com*.

How to Get Help

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

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

Technical Solutions Center	Telephone number	Fax number
Billerica, MA	800-2LANWAN	978-916-3514
Santa Clara, CA	800-2LANWAN	408-495-1188
Valbonne, France	33-4-92-96-69-68	33-4-92-96-69-98
Sydney, Australia	61-2-9927-8800	61-2-9927-8811
Tokyo, Japan	81-3-5402-0180	81-3-5402-0173

Safety Messages

Übersetzter Sicherheitshinweis

Traduction des Messages de Sécurité

Traducción de los mensajes de seguridad

Messaggi relativi alla sicurezza



翻訳された安全警告

This section translates the safety alert messages used in this guide. Safety alert messages notify users of unsafe actions or conditions that could lead to personal injury or equipment damage.

Safety Alert Message Format

All safety alert messages are tagged with an international alert symbol. When you see a safety alert in this guide, be sure to read and follow the instructions before continuing with the procedure.

The safety alert messages in this guide appear in the following format:

Symbol	Meaning (English, German, French, Spanish, Italian, Japanese)
	Warning: A warning alerts the user to some action or set of conditions that could result in personal injury.
	Caution: A caution alerts the user to some action or set of conditions that could result in damage to the equipment.

Symbol Meaning (English, German, French, Spanish, Italian, Japanese)



Vorsicht: Dieser Sicherheitshinweis macht den Benutzer auf Maßnahmen oder Bedingungen aufmerksam, die die Verletzung von Personen zur Folge haben können.



Achtung: Dieser Sicherheitshinweis macht den Benutzer auf Maßnahmen oder Bedingungen aufmerksam, die eine Beschädigung der Geräte zur Folge haben können.



Avertissement: La mention Avertissement attire l'attention de l'utilisateur sur une action ou un ensemble de conditions pouvant causer des blessures corporelles.



Attention: La mention Attention attire l'attention de l'utilisateur sur une action ou un ensemble de conditions pouvant endommager l'équipement visé.



Advertencia: Un mensaje de advertencia avisa al usuario sobre una acción o conjunto de condiciones que pueden causar daños personales.



Precaución: Un mensaje de precaución avisa al usuario sobre alguna acción o conjunto de condiciones que pueden dañar el equipo.



Avvertenza: L'avvertenza indica all'utente la presenza di una o più condizioni che possono causare lesioni fisiche.



Attenzione: Questo messaggio indica all'utente la presenza di una o più condizioni che possono causare danni alle apparecchiature.



警告: 「警告」は、身体に損傷を与える恐れのある操作や状況に対してユーザに警戒を促します。



注意: 「注意」は、機器の損害を招く恐れのある操作や状況に対してユーザに警戒を促します。

Safety Alert Messages Used in This Guide

The following safety alert messages are used in this guide. Please read and follow these instructions when you encounter them in the text.

Class A Product

Copyright page



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



Achtung: Dieses Gerät ist ein Produkt der Klasse A. Bei Heiminstallationen kann dieses Gerät Störungen des Rundfunkempfangs verursachen, wodurch der Benutzer gegebenenfalls entsprechende Maßnahmen ergreifen muß.



Attention: Appareil électrique de classe A pouvant causer des radio-interférences en utilisation domestique et nécessiter, le cas échéant, l'application de mesures correctives appropriées.



Precaución: Este dispositivo es un producto de la Clase A. En un entorno doméstico, este dispositivo puede producir interferencias de radio, en cuyo caso, puede exigirse al usuario que tome las medidas de corrección apropiadas.



Attenzione: Questo dispositivo è un prodotto di Classe A. Se utilizzato in ambiente domestico, può causare interferenze radio e, in tal caso, l'utente dovrà prendere le opportune precauzioni.



注意: この機器は、クラスAの製品です。国内の環境で、この機器は電波障害を引き起こす恐れがあります。この場合、ユーザは適切な対策を講じる必要があります。

Accumulated Weight (Shelf or Table Mount)

Page 2-3



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



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



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



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



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



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

Stacking Units in a Rack

Page 2-4



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



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



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



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



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



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

Turning Off Power to the Unit

Page 2-9



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



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



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



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



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



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

Reset to Default Settings Command

Page 3-4



Caution: If you choose the Reset to Default Settings command, all of your configured settings will be replaced with factory default settings when you press [Enter].



Achtung: Bei Auswahl des Befehls zur Rücksetzung auf die Standardeinstellungen werden alle von Ihnen konfigurierten Einstellungen durch die werkseitigen Standardeinstellungen ersetzt, wenn Sie die Eingabetaste drücken.



Attention: Si vous restaurez la configuration usine, votre configuration courante sera remplacée par la configuration usine dès que vous appuierez sur [Entrée].



Precaución: Si selecciona el comando Restaurar valores predeterminados, todos los valores de configuración se sustituirán por los valores predeterminados en fábrica al pulsar [Intro].



Attenzione: Nel caso in cui si selezioni la reimpostazione dei valori di default, tutte le impostazioni configurate verranno sostituite dai default di fabbrica premendo il tasto [Invio].



注意：「デフォルトの設定にリセット」コマンドを選択すると、現在のコンフィグレーションされた設定は、[Enter]を押したとき、工場出荷時の設定に変更されます。

Choosing a Baud Rate

Page 3-56



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



Achtung: Bei Auswahl einer Baudrate, die nicht mit der Baudrate des Konsolenterminals übereinstimmt, geht die Kommunikation mit der Konsolenschnittstelle verloren, wenn Sie die Eingabetaste drücken. Stellen Sie in diesem Fall das Konsolenterminal so ein, daß es mit der neuen Einstellung der Service-Schnittstelle übereinstimmt.



Attention: Si vous sélectionnez un débit différent de celui de votre terminal, vous perdrez le contact avec l'interface de votre console dès que vous appuierez sur [Entrée]. Pour restaurer la communication, alignez le débit de votre terminal sur le nouveau débit de votre port de service.



Precaución: Si selecciona una velocidad de transmisión que no coincide con la velocidad de transmisión del terminal de la consola, perderá la comunicación con el interfaz de la consola al pulsar [Intro]. Si se pierde la comunicación, ajuste el terminal de la consola para que coincida con el nuevo valor del puerto de servicio.



Attenzione: Nel caso in cui si scelga una velocità di trasmissione non corrispondente a quella del terminale della console, la comunicazione con l'interfaccia della console cadrà premendo il tasto [Invio]. Se la comunicazione cade, impostare il terminale della console in modo tale che corrisponda alla nuova impostazione della porta di servizio.



注意：コンソール・ターミナルのボー・レートに合っていないボー・レートを選択すると、[Enter]を押したときに、コンソール・インタフェイスとの通信が途切れてしまいます。この場合には、新しいサービス・ポート設定に合うようにコンソール・ターミナルを設定してください。

Changing Passwords

Page 3-57



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



Achtung: Wenn Sie die für das System standardmäßig eingestellten Paßwörter ändern, notieren Sie sich die neuen Paßwörter, und bewahren Sie sie an einem sicheren Ort auf. Falls Sie die neuen Paßwörter vergessen, können Sie nicht mehr auf die Konsolenschnittstelle zugreifen. Wenden Sie sich in diesem Fall an Bay Networks, um Unterstützung zu erhalten.



Attention: Si vous changez les mots de passe par défaut du système, assurez-vous de bien noter vos nouveaux mots de passe et de les conserver dans un endroit sûr. Si vous perdez vos nouveaux mots de passe, vous ne pourrez plus accéder à votre interface. Le cas échéant, veuillez contacter Bay Networks.



Precaución: Si modifica las contraseñas predeterminadas asignadas por el sistema, asegúrese de anotar las nuevas contraseñas y guárdelas en un lugar seguro. Si olvida las nuevas contraseñas, no podrá acceder al interfaz de la consola. En ese caso, póngase en contacto con Bay Networks para obtener ayuda al respecto.



Attenzione: In caso di modifica delle password predefinite nel sistema, assicurarsi di annotare le nuove password e di conservarle in un luogo sicuro. Nel caso in cui le nuove password vengano dimenticate, non sarà possibile accedere all'interfaccia della console. In tal caso, contattare la Bay Networks per avere assistenza.



注意：システム装備したデフォルトのパスワードを変更する場合、必ず新しいパスワードを書き留めて安全な場所に保管してください。新しいパスワードを忘れてしまうと、コンソール・インタフェイスにアクセスできません。この場合は、Bay Networksまでご連絡ください。

Interrupting a Software Download

Page 3-68



Caution: Do not interrupt power to the device during the software download process. If the power is interrupted, the firmware image can become corrupted.



Achtung: Unterbrechen Sie die Stromzufuhr zum Gerat nicht, wahrend die Software heruntergeladen wird. Bei Unterbrechung der Stromzufuhr kann das Firmware-Image beschadigt werden.



Attention: Ne pas couper l'alimentation de l'appareil pendant le chargement du logiciel. En cas d'interruption, le programme resident peut ˆtre endommage.



Precauci3n: No interrumpa la alimentaci3n del dispositivo durante el proceso de descarga del software. Si lo hace, puede alterar la imagen de la programaci3n (firmware).



Attenzione: Non interrompere l'alimentazione elettrica al dispositivo durante il processo di scaricamento del software. In caso di interruzione, l'immagine firmware potrebbe danneggiarsi.



注意: ソフトウェアをダウンロードしているとき、デバイスへの電源を切らないでください。電源を切ると、ファームウェアのイメージを損う恐れがあります。

Removing the Top Cover

Page 4-1



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



Vorsicht: Um Verletzungsgefahr durch einen elektrischen Stromschlag auszuschließen, nehmen Sie niemals die obere Abdeckung vom Gerät ab. Im Geräteinnern befinden sich keine Komponenten, die vom Benutzer gewartet werden können.



Avertissement: Pour éviter tout risque d'électrocution, ne jamais retirer le capot de l'appareil. Cet appareil ne contient aucune pièce accessible par l'utilisateur.



Advertencia: A fin de evitar daños personales por corrientes eléctricas peligrosas, no desmonte nunca la cubierta superior de este dispositivo. Los componentes internos no son reparables por el usuario.



Avvertenza: Per evitare lesioni fisiche dovute a scariche pericolose di corrente, non rimuovere mai il coperchio superiore del dispositivo. I componenti interni non possono essere manipolati dall'utente.



警告: 危険な電流から身体を保護するために、デバイスの上部カバーを決して取り外さないでください。内部には、ユーザが扱うコンポーネントはありません。

Chapter 1

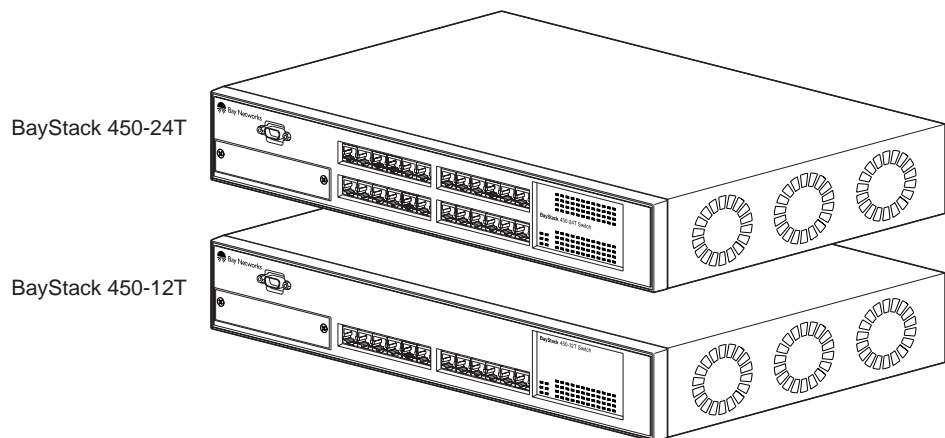
Introduction to the BayStack 450 Switch

This chapter introduces the BayStack 450 switch and covers the following topics:

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

Physical Description

There are two versions of the BayStack 450 switch: the BayStack 450-24 switch and the BayStack 450-12 switch ([Figure 1-1](#)).



8473FA

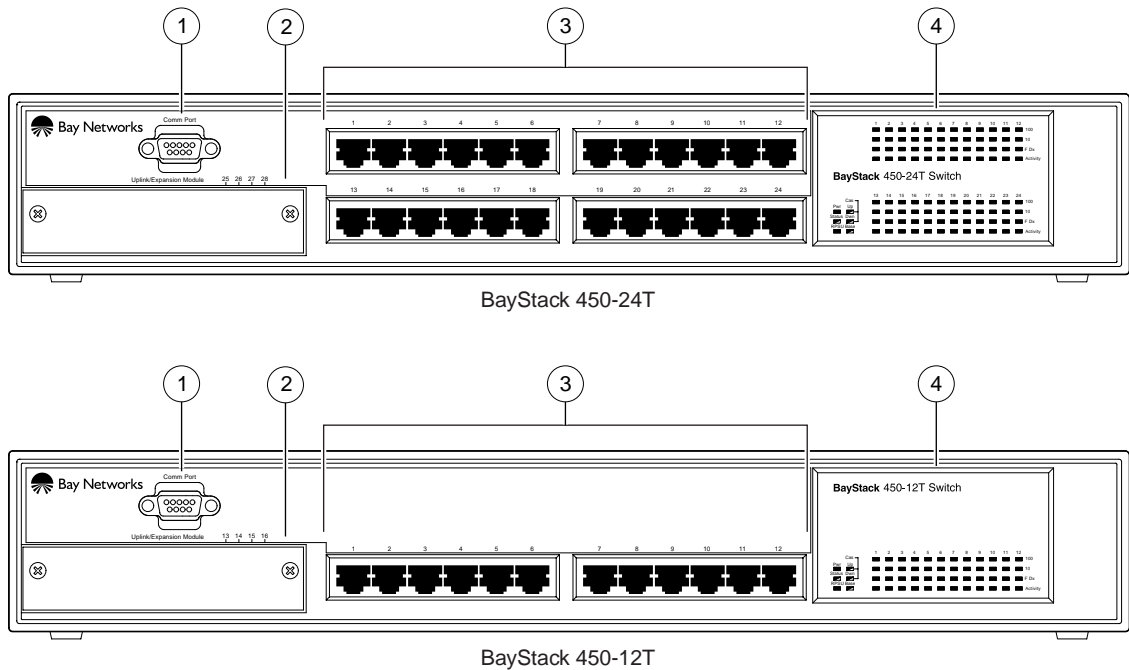
Figure 1-1. BayStack 450 Switch Versions

Front-Panel

This section describes the front-panel components of the BayStack 450 switch.

[Figure 1-2](#) shows the BayStack 450-24 switch and the BayStack 450-12 switch front-panel. Descriptions of the front-panel components follow the figures.

See [“Back-Panel”](#) for a description of the components located on the back-panel of the BayStack 450 switch.



- 1 = Comm Port
- 2 = Uplink/Expansion slot
- 3 = 10BASE-T/100BASE-TX port connectors
- 4 = LED display panel

8477EA

Figure 1-2. BayStack 450 Switch Front-Panel

Comm Port

The Comm Port (also referred to as the Console/Comm Port) allows you to access the console interface (CI) screens and customize your network using the supplied menus and screens (see Chapter 3, “Using the Console Interface”).

The Console/Comm Port is a DB-9, RS-232-D male serial port connector. You can use this connector to connect a management station or console/terminal to the switch by using a straight-through DB-9 to DB-9 standard serial port cable (see “Connecting the Console/Comm Port” on page 2-8).



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

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

Uplink/Expansion Slot

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

10BASE-T/100BASE-TX Port Connectors

The BayStack 450 switch uses 10BASE-T/100BASE-TX RJ-45 (8-pin modular) port connectors.

All BayStack 450 switches are shipped with port connectors configured as MDI-X (media-dependent interface-crossover). These ports connect over straight cables to the network interface controller (NIC) card in a node or server, similar to a conventional Ethernet repeater hub. If you are connecting to another Ethernet hub or Ethernet switch, you need a crossover cable unless an MDI connection exists on the associated port of the attached device (see “MDI and MDI-X Devices” on page D-2).

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

The switch ports also support half- and full-duplex mode operation (see “Connecting the 10BASE-T/100BASE-TX Ports” on page 2-7).

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



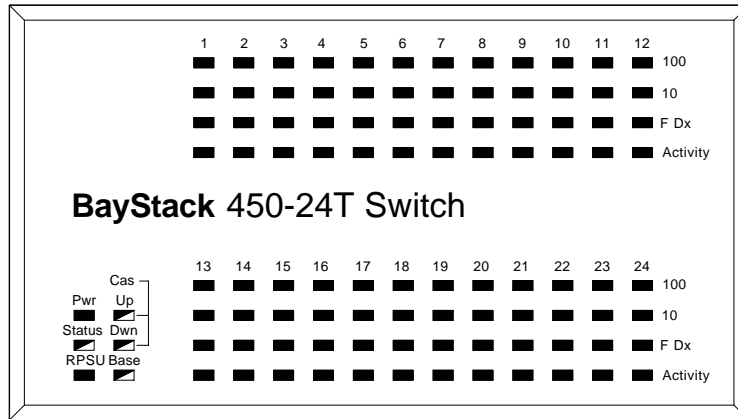
Note: Use only Category 5 copper unshielded twisted pair (UTP) cable connections when connecting 10BASE-T/100BASE-TX ports.

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

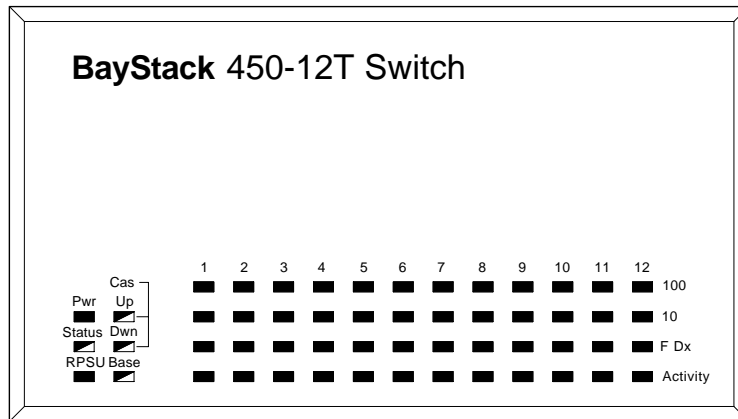
LED Display Panel

[Figure 1-3](#) shows the LED display panels used with the BayStack 450-24 switch and BayStack 450-12 switch switches.

Refer to [Table 1-1](#) for a description of the LEDs.



BayStack 450-24T



BayStack 450-12T

8487EA

Figure 1-3. BayStack 450 Switch LED Display Panel

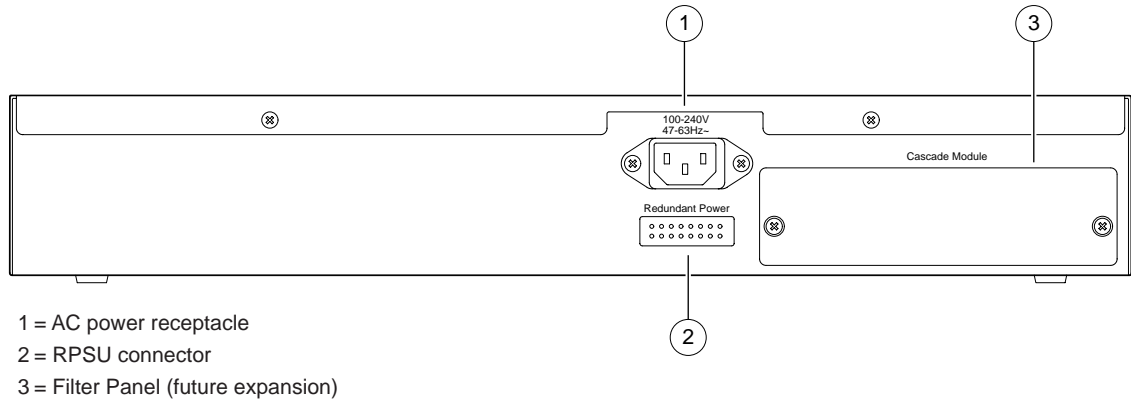
Table 1-1. BayStack 450 Switch LED Descriptions

Label	Type	Color	State	Meaning
Pwr	Power status	Green	On	DC power is available to the switch's internal circuitry.
			Off	No AC power to switch or power supply failed.
Status	System status	Green	On	Self-test passed successfully and switch is operational.
			Blinking	A nonfatal error occurred during the self-test.
			Off	The switch failed the self-test.
RPSU	RPSU status	Green	On	The switch is connected to the HRPSU and can receive power if needed.
			Off	The switch is not connected to the HRPSU or HRPSU is not supplying power.
CAS Up/ Dwn	-	-	-	For future release.
Base	-	-	-	For future release.
100	100 Mb/s port speed indicator	Green	On	The corresponding port is set to operate at 100 Mb/s and the link is good.
			Off	The link connection is bad or there is no connection to this port.
			Blinking	The corresponding port is management disabled.
10	10 Mb/s port speed indicator	Green	On	The corresponding port is set to operate at 10 Mb/s and the link is good.
			Off	The link connection is bad or there is no connection to this port.
			Blinking	The corresponding port is management disabled.
F Dx	Half/Full-duplex mode status	Green	On	The corresponding port is operating in full-duplex mode (operating at 10 Mb/s or at 100 Mb/s).
			Off	The corresponding port is operating in half-duplex mode.
Activity	Port activity	Green	Blinking	Indicates network activity for the corresponding port. A high level of network activity can cause the LEDs to appear to be on continuously.

Back-Panel

This section describes the BayStack 450 switch back-panel components ([Figure 1-4](#)).

Descriptions of the back-panel components follow the figure.



8488EA

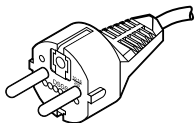
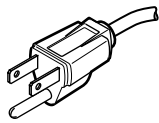
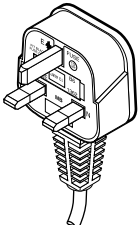
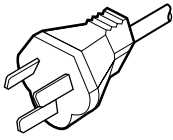
Figure 1-4. BayStack 450 Switch Back-Panel

AC Power Receptacle

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

[Table 1-2](#) lists specifications for international power cords.

Table 1-2. International Power Cord Specifications

Country/Plug description	Specifications	Typical plug
Continental Europe: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• BS1363 male plug with fuse• Harmonized cord	240 VAC 50 Hz Single phase	 229FA
Australia: <ul style="list-style-type: none">• AS3112-1981 Male plug	240 VAC 50 Hz Single phase	 230FA

RPSU Connector

The RPSU connector allows you to connect a backup power supply unit to the switch. Bay Networks provides an (optional) high-power redundant power supply unit (HRPSU) for this purpose. The HRPSU is a hot-swappable power supply unit that provides uninterrupted operation to up to four BayStack 450 switches in the event that any of the switch power supplies fail.

Bay Networks provides the HRPSU power rack (Order No. AA0002001) with four slots for power supply modules (Order No. AA0005003). Each HRPSU can support up to four BayStack 450 switches. Installation instructions are provided with the HRPSU.

Contact your Bay Networks sales representative for more information about the HRPSU.

Filler Panel

The filler panel covers an expansion slot that is reserved for future use.

Cooling Fans

The variable-speed cooling fans are located on one side of the BayStack 450 switch to provide cooling for the internal components. When you install the switch, be sure to allow enough space on *both sides* of the switch for adequate air flow.

Features

BayStack 450 switches provide wire-speed switching that allows high-performance, low-cost connections to full-duplex and half-duplex 10/100/1000 Mb/s Ethernet local area networks (LANs).

BayStack 450 switches offer the following features:

- High-speed forwarding rate: up to 3 million packets per second (peak)
- Store-and-forward switch: Full-performance forwarding at full line speed, utilizing a 2.56 Gigabit/second switch fabric
- Learning rate: 3 million addresses per second (peak)

- Address Database Size: 16,000 entries at line rate (32,000 entries without flooding)
- Spanning Tree Protocol (STP): complies with IEEE 802.1D standard. STP can be disabled on the entire switch or on a per-port basis.
- SNMP agent support for the following Management Information Bases (MIBs):
 - Bridge MIB (RFC 1493)
 - Ethernet MIB (RFC 1643)
 - RMON MIB (RFC 1757)
 - MIB-II (RFC 1213)
 - Interface MIB (RFC 1573)
 - Bay Networks proprietary MIBs:
 - s5Chass MIB
 - s5Agent MIB
 - s5ECM MIB (Ethernet Common)
 - s5emt MIB (multi-segment topology)
 - Rapid City MIB
- Rate limiting: Adjustable broadcast or IP Multicast packet-rate limits for control of broadcast and IP Multicast storms
- Console/Comm Port: Allows users to configure and manage the switch locally or remotely.
- TELNET:
 - Support for up to four simultaneous TELNET sessions
 - Optional password protection
 - Login time-out
 - Failed-login guard
 - Inactivity time-out
 - Allowed source addresses
 - Event logging

- IEEE 802.1Q Port-based virtual LANs (VLANs)
- IGMP Snooping
- IEEE 802.1p Prioritizing
- MultiLink Trunking, supporting:
 - Switch-to-switch trunks
 - Switch-to-server trunks
- Port Mirroring (Conversation Steering)
 - Port-based
 - MAC address-based
- IEEE 802.3u-compliant autonegotiation ports, with four modes:
 - 10BASE-T half-duplex
 - 10BASE-T full-duplex
 - 100BASE-TX half-duplex
 - 100BASE-TX full-duplex
- Front-panel light emitting diodes (LEDs) to monitor the following:
 - Power status
 - System status
 - Per-port status for the following:
 - 1000 Mb/s link
 - 100 Mb/s link
 - 10 Mb/s link
 - Half- and full-duplex transmission
 - Tx/Rx activity
 - Management enable/disable
- Upgradeable device firmware in nonvolatile flash memory using the Trivial File Transfer Protocol (TFTP)

- Remote monitoring (RMON), with four groups integrated:
 - Statistics
 - History
 - Alarms
 - Events

Autosensing and Autonegotiation

BayStack 450 switches are autosensing and autonegotiating devices. The term *autosense* refers to a port's ability to *sense* the speed of an attached device. The term *autonegotiation* refers to a standardized protocol (IEEE 802.3u) that exists between two IEEE 802.3u-capable devices. Autonegotiation allows the BayStack 450 switch to select the best of both speed and duplex modes.

Autosensing is used when the attached device is not capable of autonegotiation or is using a form of autonegotiation that is not compatible with the IEEE 802.3u autonegotiation standard. In this case, because it is not possible to sense the duplex mode of the attached device, the BayStack 450 switch reverts to half-duplex mode. When autonegotiation-capable devices are attached to the BayStack 450 switch, the switch ports negotiate down from 100 Mb/s speed and full-duplex mode until a supported speed and duplex mode is acknowledged by the attached device.

For more information about autosensing and autonegotiation modes, see “Autonegotiation Modes” on page 4-5.

IEEE 802.1Q VLANs

BayStack 450 switches support up to 64 port-based VLANs with IEEE 802.1Q tagging available per port. When a switch port is configured to be a member of a VLAN, it is added to a group of ports (workgroup) that belong to one broadcast domain. You can assign different ports (and therefore the devices attached to these ports) to different broadcast domains. This feature allows network flexibility because you can reassign VLANs to accommodate network moves, additions, and changes, eliminating the need to change physical cabling.

For more information about 802.1Q VLANs, see [“IEEE 802.1Q VLAN Workgroups”](#) on [page 1-19](#).

IGMP Snooping Feature

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

For more information about the IGMP Snooping feature, see [“IGMP Snooping”](#) on [page 1-35](#).

IEEE 802.1p Prioritizing

The BayStack 450 switch can prioritize the order in which packets are forwarded, on a per-port basis.

For more information about the 802.1p prioritizing feature, see [“IEEE 802.1p Prioritizing”](#) on [page 1-40](#).

MultiLink Trunking

The MultiLink Trunking feature allows a user to group multiple ports (up to four) together when forming a link to another switch or server, thus increasing aggregate throughput of the interconnection between two devices, up to 800 Mb/s in full-duplex mode. BayStack 450 switches can be configured with up to six MultiLink Trunks.

For more information about the MultiLink Trunking feature, see [“MultiLink Trunks”](#) on [page 1-44](#).

Port Mirroring

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

For more information about the port mirroring feature, see [“Port Mirroring \(Conversation Steering\)”](#) on [page 1-62](#).

Flash Memory Storage

The BayStack 450 switch uses flash memory to store the switch software image. Flash memory allows you to update the software image with a newer version without changing the switch hardware.

An in-band connection between the switch and the TFTP load host is required to download the software image (see “Software Download” on page 3-68).

For information about connecting a console terminal for this procedure, see “Connecting the Console/Comm Port” on page 2-8.



Note: If a BootP server is set up properly on the network and the BayStack 450 switch detects a corrupted software image during the self-test, the switch automatically uses TFTP to download a new software image.

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

BootP Automatic IP Configuration

The BayStack 450 switch has a unique 48-bit hardware address, or MAC address, that is printed on a label on the back panel. You use this MAC address when you configure the network BootP server to recognize the BayStack 450 switch BootP requests. A properly configured BootP server enables the switch to automatically learn its assigned IP address, subnet mask, IP address of the default router (default gateway), and software image file name.

For an example of a BootP configuration file, see Appendix F, “Sample BootP Configuration File.”

SNMP MIB Support

The BayStack 450 switch supports an SNMP agent with industry standard MIBs, as well as private MIB extensions, which ensures compatibility with existing network management tools. The BayStack 450 switch supports MIB-II (RFC 1213) and the RMON MIB (RFC 1757), which provide access to detailed management statistics. With SNMP management, you can configure SNMP traps (on individual ports) to be generated automatically for conditions such as an unauthorized access attempt or changes in a port's operating status.

Configuration and Switch Management

The BayStack 450 switch is shipped directly from the factory ready to operate in any 10BASE-T or 100BASE-TX standard network. You can manage the switch using the Bay Networks Optivity[®] network management software or any generic SNMP-based network management software; however, you must assign an IP address to the switch. You can set the switch's IP address by using the Console/Comm Port or BootP, which resides on the switch.

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

Network Configuration

You can use BayStack 450 switches to connect workstations, personal computers (PCs), and servers to each other by connecting these devices directly to the switch, through a shared media hub that is connected to the switch, or by creating a virtual LAN (VLAN) through the switch.

This section provides three network configuration examples using BayStack 450 switches:

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

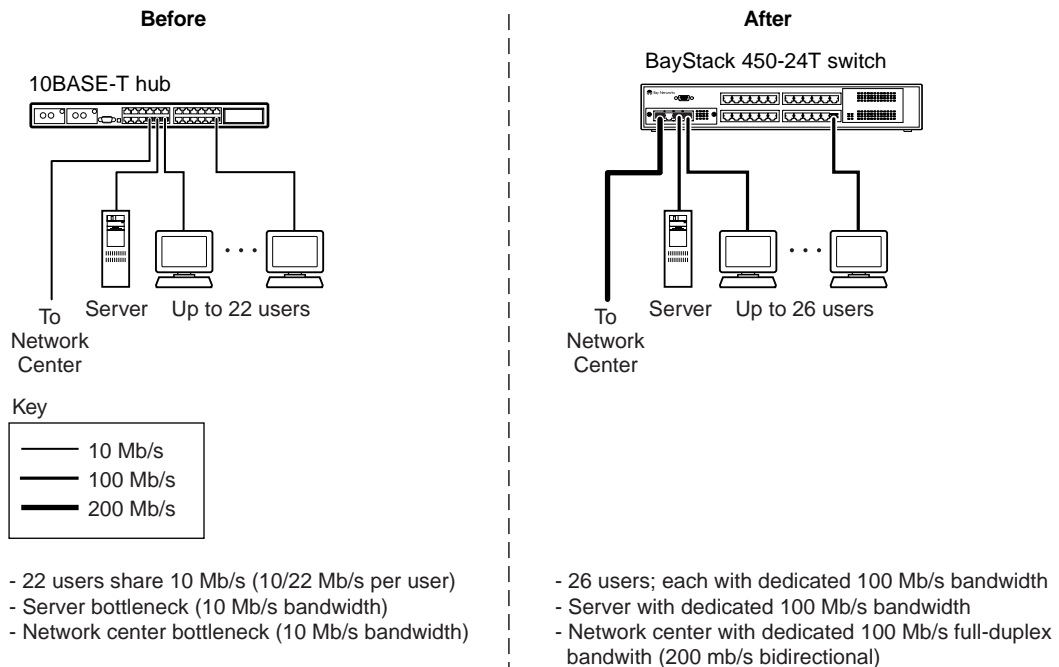


Note: All of the BayStack 450 switch models can be used interchangeably in the following network configuration examples.

Desktop Switch Application

[Figure 1-5](#) shows the BayStack 450-24 switch used as a desktop switch, where desktop workstations are connected directly to switch ports.

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

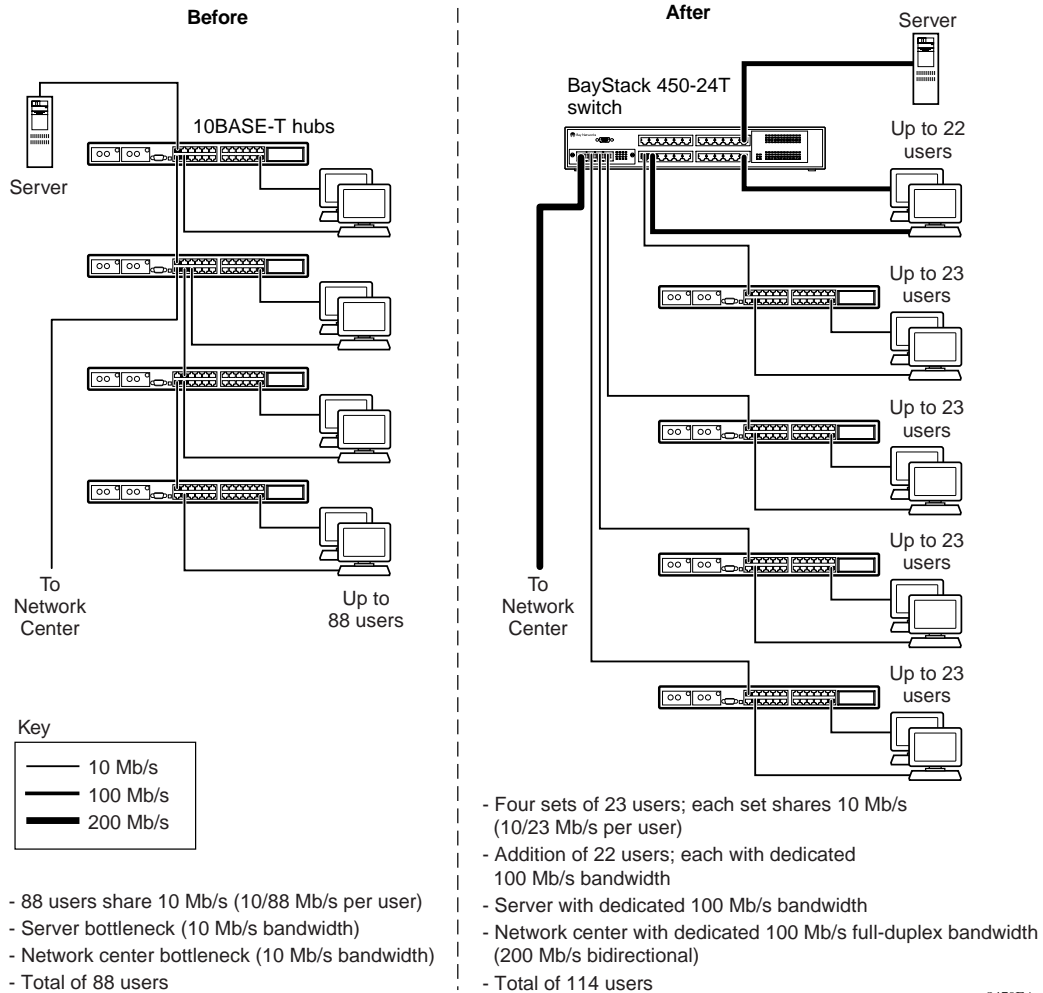


8478EA

Figure 1-5. BayStack 450 Switch Used as a Desktop Switch

Segment Switch Application

[Figure 1-6](#) shows the BayStack 450-24 switch used as a segment switch to alleviate user contention for bandwidth and eliminate server and network bottlenecks. Before segmentation, 88 users had a total bandwidth of only 10 Mb/s available. After segmentation, 92 users have 40 Mb/s, four times the previous bandwidth, while adding 22 dedicated 100 Mb/s connections. This configuration can be extended to add more segments without degrading performance.



8479EA

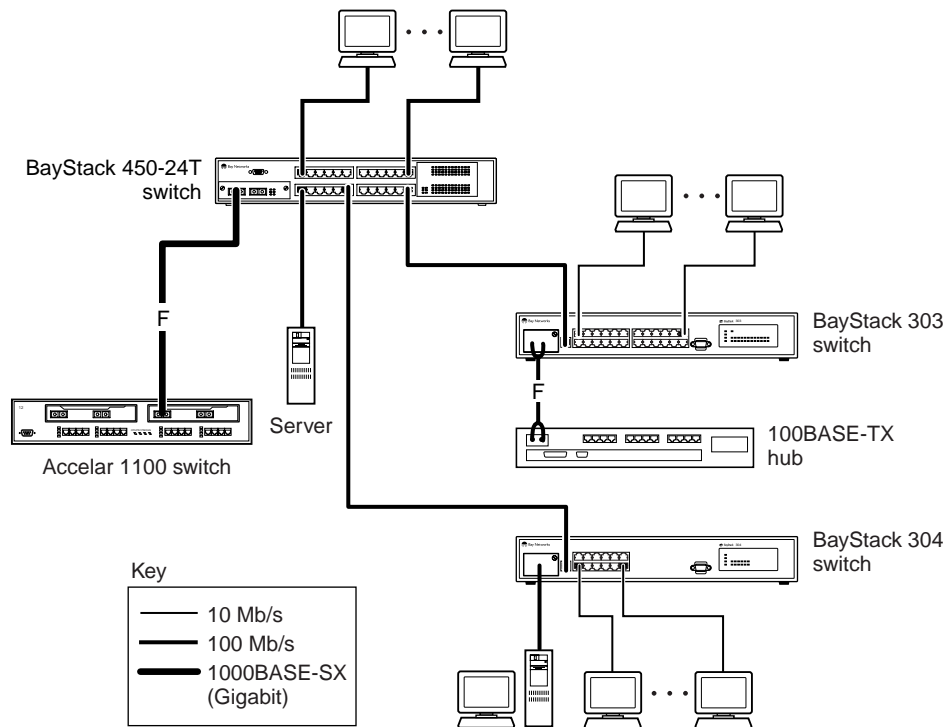
Figure 1-6. BayStack 450 Switch Used as a Segment Switch

High-Density Switched Workgroup Application

[Figure 1-7](#) shows an example of using a BayStack 450 switch with a high-speed (gigabit) connection to a Bay Networks Accelar™ 1100 switch. BayStack 303 and 304 switches are also shown in this example of a high-density switched workgroup.

As shown in [Figure 1-7](#), the Accelar 1100 switch is used as a backbone switch, connecting to the BayStack 450 switch with an optional gigabit (1000BASE-SX) MDA for maximum bandwidth. The BayStack 303 and 304 switches have 100 Mb/s connections to the BayStack 450 switch, a 100BASE-TX hub, and a 100 Mb/s server and 10 Mb/s connections to DTE (data terminal equipment).

See the Bay Networks library Web page: support.baynetworks.com/library/ for online documentation about the Bay Networks Accelar 1100 switch and the BayStack 303 and 304 switches.



8480EA

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

IEEE 802.1Q VLAN Workgroups

BayStack 450 switches support up to 64 port-based VLANs with 802.1Q tagging available per port. Ports are grouped into broadcast domains by assigning them to the same VLAN. Frames received in one VLAN can only be forwarded within that VLAN, and IP Multicast frames and unknown unicast frames are flooded only to ports in the same VLAN.

Setting up virtual LANs (VLANs) is a way to segment networks to increase network capacity and performance without changing the physical network topology ([Figure 1-8](#)). With network segmentation, each switch port connects to a segment that is a single broadcast domain. When a switch port is configured to be a member of a VLAN, it is added to a group of ports (workgroup) that belong to one broadcast domain.

The BayStack 450 switch allows you to assign ports to VLANs using the console or TELNET; VLAN assignment is not currently available through SNMP. You can assign different ports (and therefore the devices attached to these ports) to different broadcast domains. This feature allows network flexibility because you can reassign VLANs to accommodate network moves, additions, and changes, eliminating the need to change physical cabling.

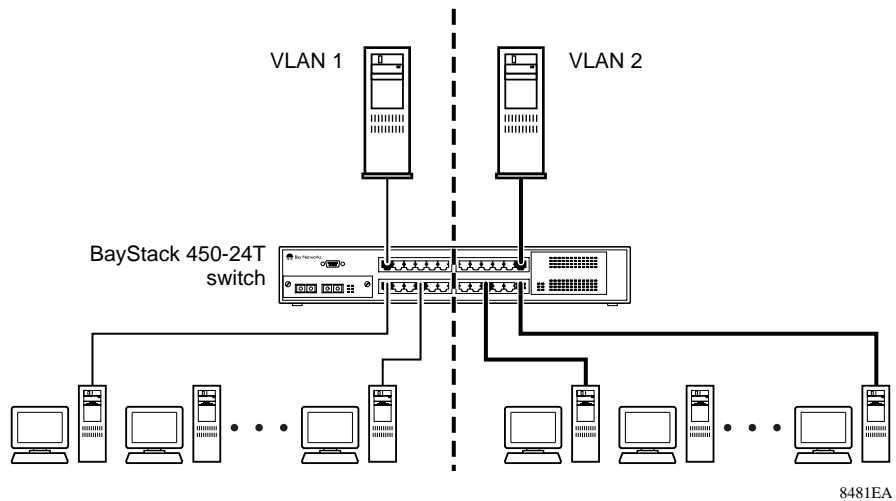


Figure 1-8. Port-Based VLAN Example

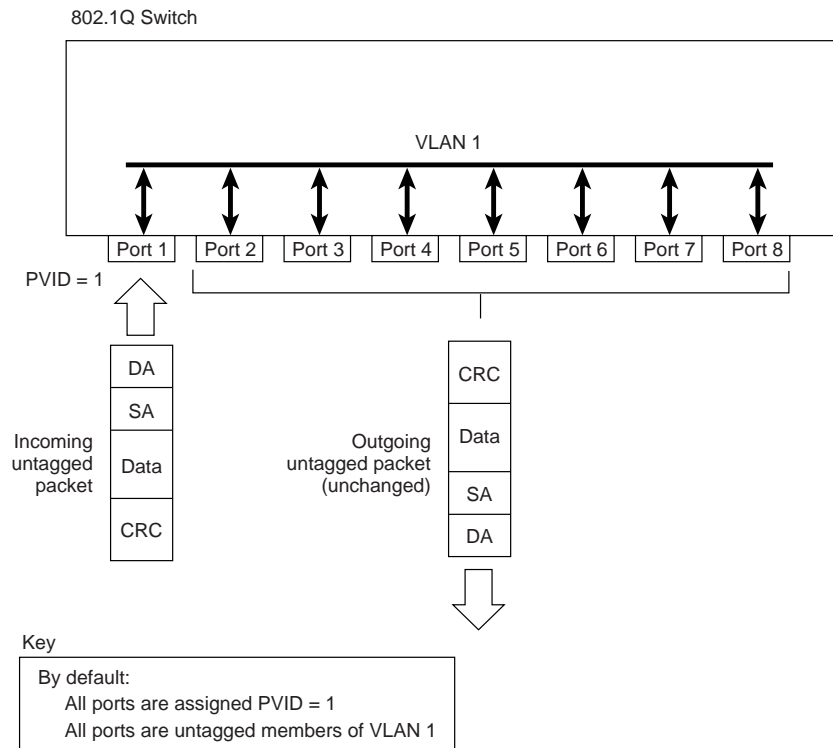
IEEE 802.1Q Tagging

BayStack 450 switches operate in accordance with the IEEE 802.1Q tagging rules. Some important terms used with the 802.1Q tagging feature are:

- VLAN Identifier (VID) --- the 12-bit portion of the VLAN tag in the frame header that identifies an explicit VLAN.
- Port VLAN Identifier (PVID) --- a classification mechanism that associates a port with a specific VLAN. For example, a port with a PVID of 3 (PVID =3) assigns all untagged frames received on this port to VLAN 3.
- Tagged frame --- the 32-bit field (VLAN tag) in the frame header that identifies the frame as belonging to a specific VLAN. Untagged frames are marked (tagged) with this classification as they leave the switch through a port that is configured as a tagged port.
- Untagged frame --- a frame that does not carry any VLAN tagging information in the frame header.
- VLAN port members --- a set of ports that form a broadcast domain for a specific VLAN. A port can be a member of one or more VLANs.
- Untagged member --- a port that has been configured as an untagged member of a specific VLAN. When an untagged frame exits the switch through an untagged member port, the frame header remains unchanged. When a tagged frame exits the switch through an untagged member port, the tag is stripped and the tagged frame is changed to an untagged frame.
- Tagged member --- a port that has been configured as a member of a specific VLAN. When an untagged frame exits the switch through a tagged member port, the frame header is modified to include the 32-bit tag associated with the PVID. When a tagged frame exits the switch through a tagged member port, the frame header remains unchanged (original VID remains).
- User_priority --- a three-bit field in the header of a tagged frame. The field is interpreted as a binary number, therefore has a value of 0 -7. This field allows the tagged frame to carry the user-priority across bridged LANs where the individual LAN segments may be unable to signal priority information.
- Port priority --- the priority level assigned to *untagged* frames received on a port. This value becomes the user_priority for the frame. *Tagged* packets get their user_priority from the value contained in the 802.1Q frame header.
- Unregistered packet --- a tagged frame which contains a VID where the receiving port is not a member of that VLAN.

- Filtering Database Identifier (FID) --- the specific filtering/forwarding database within the BayStack 450 switch that is assigned to each VLAN. The current version of software assigns *all VLANs* to the same FID. This is referred to as Shared VLAN Learning in the IEEE 802.1Q specification.

The default configuration settings for BayStack 450 switches have all ports set as untagged members of VLAN 1 with all ports configured as PVID = 1. Every VLAN is assigned a unique VLAN identifier (VID) which distinguishes it from all other VLANs. In the default configuration example shown in [Figure 1-9](#), all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID = 1). Untagged packets enter and leave the switch unchanged.

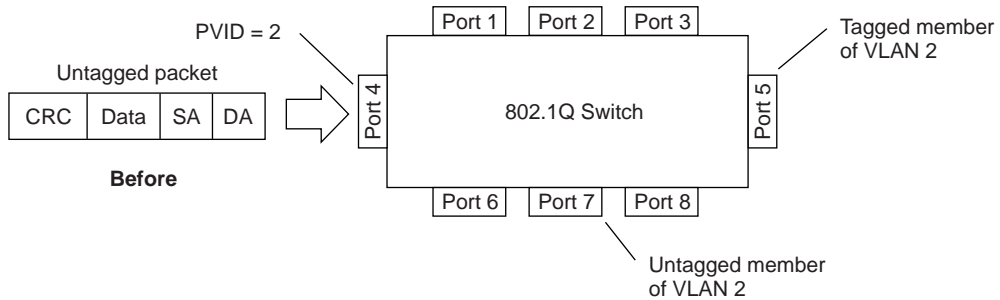


8474EA

Figure 1-9. Default VLAN Settings

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

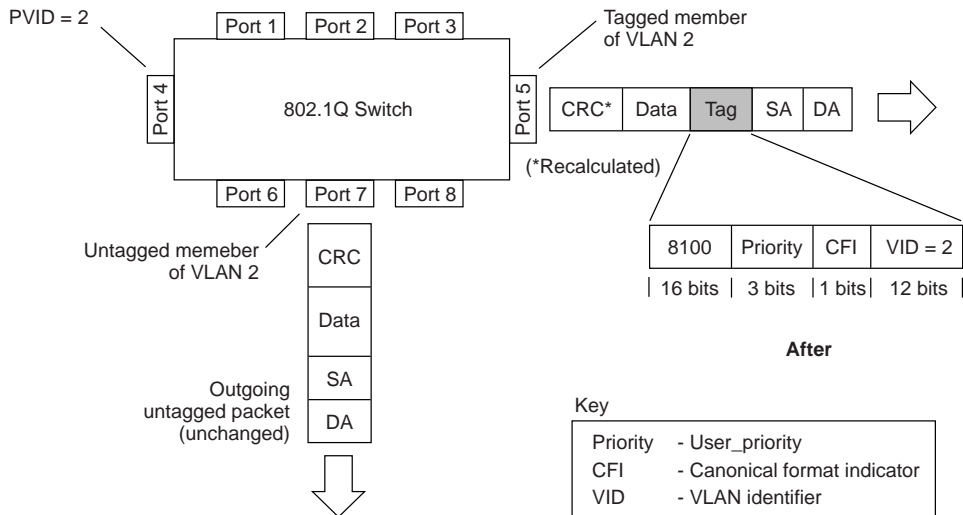
In [Figure 1-10](#), untagged incoming packets are assigned directly to VLAN 2 (PVID = 2). Port 5 is configured as a *tagged* member of VLAN 2, and port 7 is configured as an *untagged* member of VLAN 2.



8544EA

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

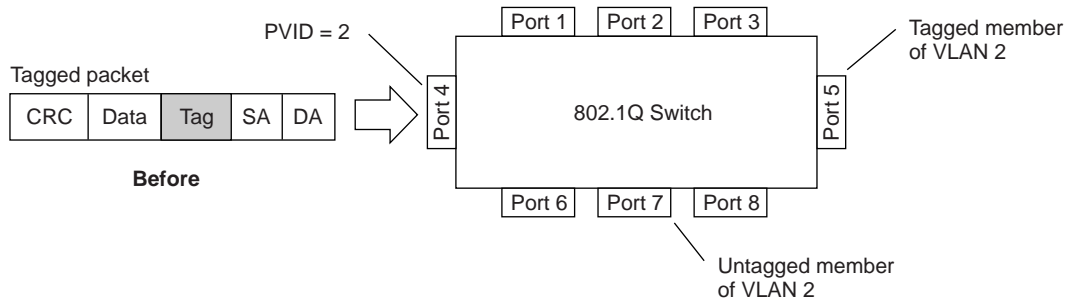
As shown in [Figure 1-11](#), the untagged packet is marked (tagged) as it leaves the switch through port 5, which is configured as a tagged member of VLAN 2. The untagged packet remains unchanged as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.



8545EA

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

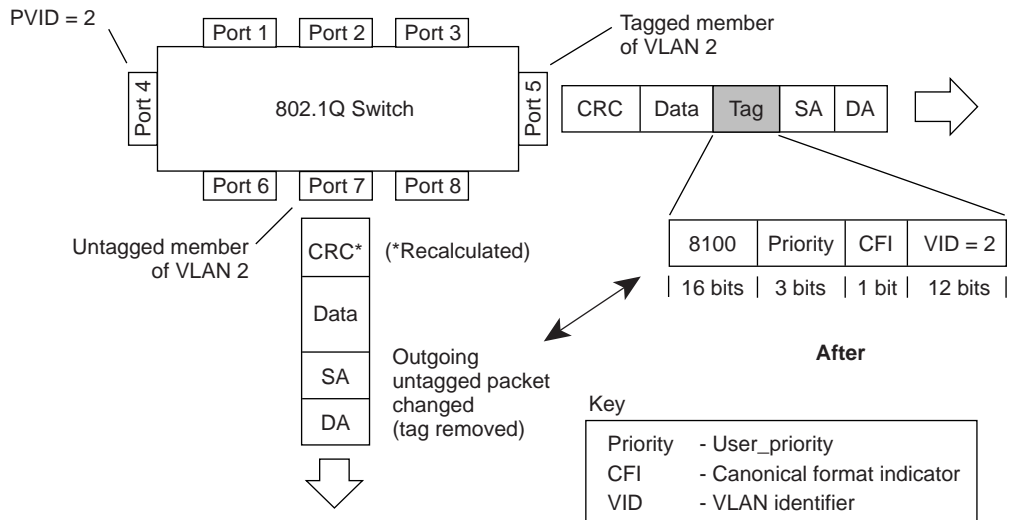
In [Figure 1-12](#), tagged incoming packets are assigned directly to VLAN 2 because of the tag assignment in the packet. Port 5 is configured as a *tagged* member of VLAN 2, and port 7 is configured as an *untagged* member of VLAN 2.



8546EA

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

As shown in [Figure 1-13](#), the tagged packet remains unchanged as it leaves the switch through port 5, which is configured as a tagged member of VLAN 2. However, the tagged packet is stripped (untagged) as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.



8547EA

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

VLANs Spanning Multiple Switches

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

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

VLANs Spanning Multiple 802.1Q Tagged Switches

[Figure 1-14](#) shows VLANs spanning two BayStack 450 switches. 802.1Q tagging is enabled on S1, port 13 and on S2, port 1 for VLAN 1 and VLAN 2. Both ports are tagged members of VLAN 1 and VLAN 2.

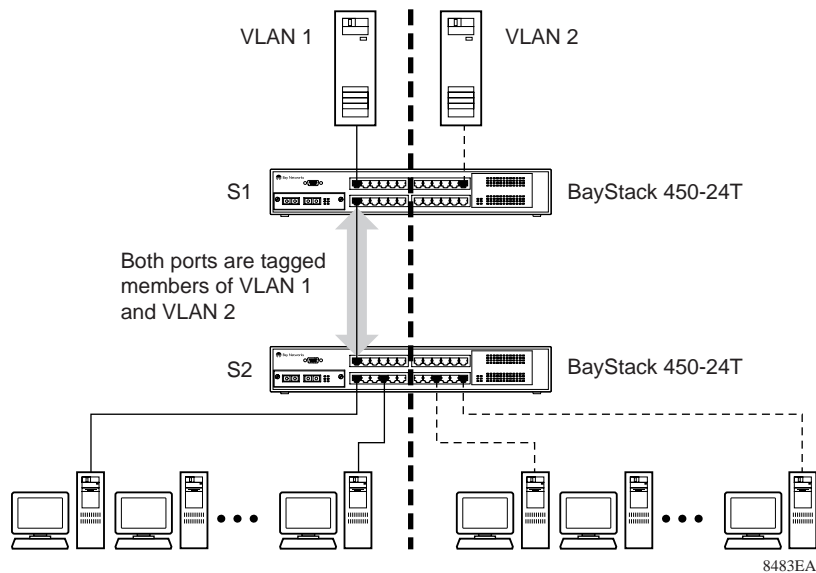


Figure 1-14. VLANs Spanning Multiple 802.1Q Tagged Switches

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

VLANS Spanning Multiple Untagged Switches

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

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

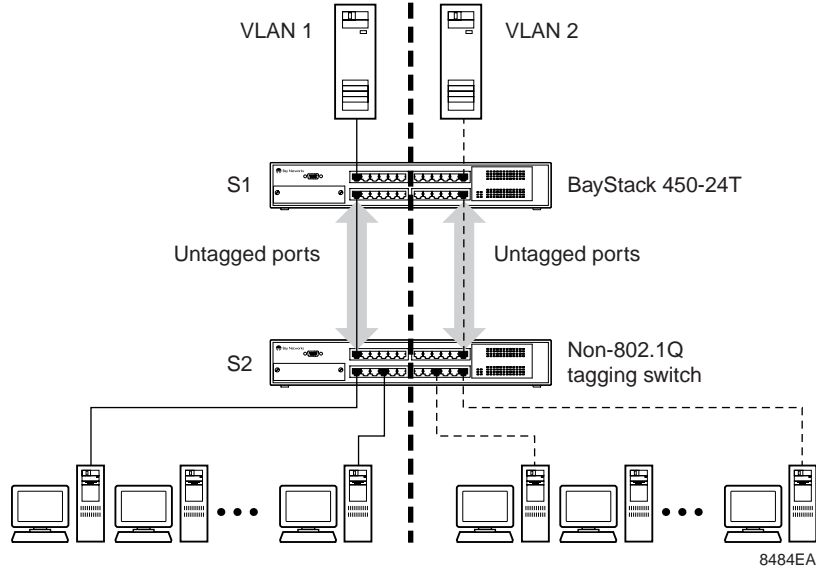


Figure 1-15. VLANs Spanning Multiple Untagged Switches

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

To connect multiple VLANs across switches with redundant links, the STP must be disabled on all participating switch ports. [Figure 1-16](#) shows possible consequences of enabling the STP when using VLANs between untagged (non-802.1Q tagged) switches.

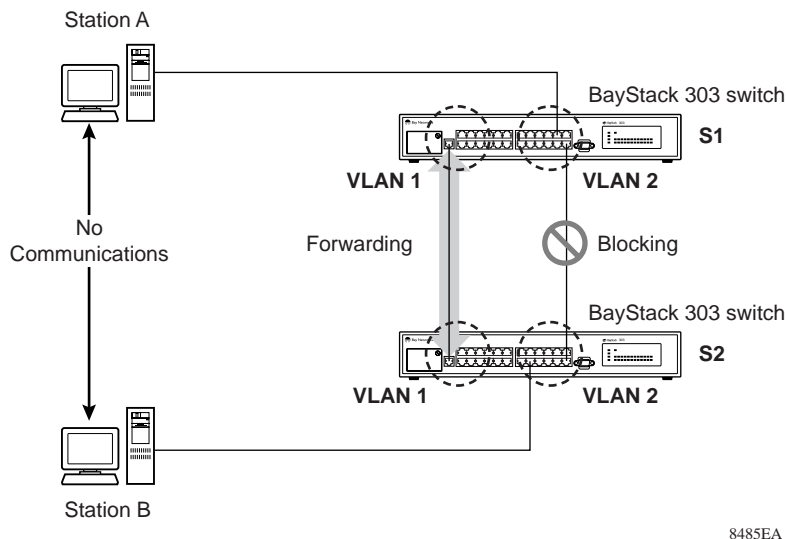


Figure 1-16. Possible Problems with VLANs and Spanning Tree Protocol

As shown in [Figure 1-16](#), with STP enabled, only one connection between S1 and S2 is forwarding at any time. Communications failure occurs between VLAN 2 of S1 and VLAN 2 of S2, blocking communications between Stations A and B.

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

Shared Servers

BayStack 450 switches allow ports to exist in multiple VLANs for shared resources, such as servers, printers, and switch-to-switch connections. It is also possible to have resources exist in multiple VLANs on one switch as shown in [Figure 1-17](#).

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

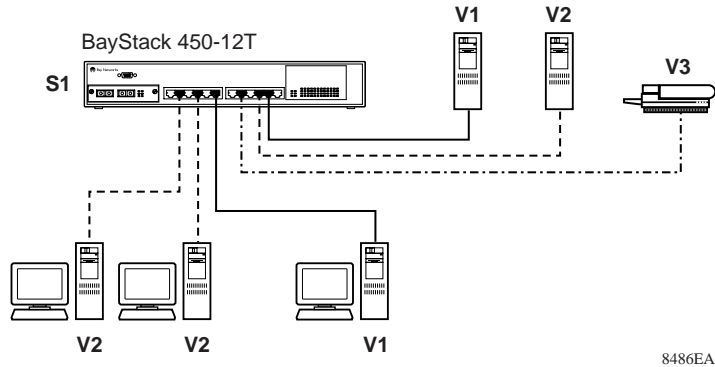
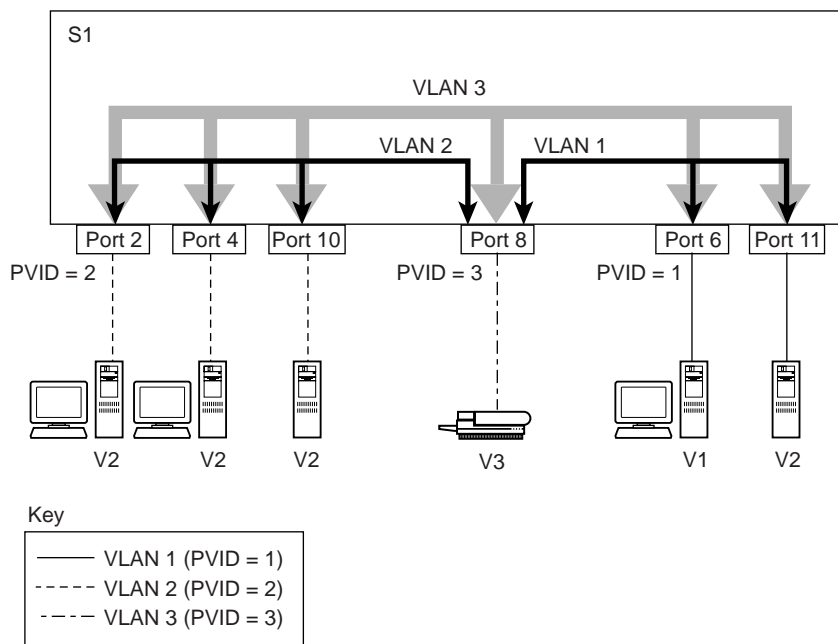


Figure 1-17. Multiple VLANs Sharing Resources

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



8476EA

Figure 1-18. VLAN Broadcast Domains Within the Switch

The broadcast domain for each of the VLANs shown in [Figure 1-18](#) are created by configuring VLAN port memberships for each VLAN and then configuring each of the ports with the appropriate PVID/VLAN association.

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

The following steps show how to use the VLAN configuration screens to configure the VLAN 3 broadcast domain shown in [Figure 1-18](#).

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

1. **Select Switch Configuration from the BayStack 450-12T Main Menu (or press w).**
2. **From the Switch Configuration Menu, select VLAN Configuration (or press v).**
3. **From the VLAN Configuration Menu select VLAN Configuration (or press v).**

The default VLAN Configuration screen opens ([Figure 1-19](#)):

```

                                VLAN Configuration

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

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

```

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

Figure 1-19. Default VLAN Configuration Screen Example

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

[Figure 1-20](#) shows the VLAN Configuration screen after it is configured to support the VLAN 3 broadcast domain shown in [Figure 1-18](#) (VLAN Name is optional).

Ports 2, 4, 6, 8, 10, and 11 are now untagged members of VLAN 3 as shown in [Figure 1-18](#) on [page 1-28](#).

```
VLAN Configuration

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

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

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

Figure 1-20. VLAN Configuration Screen Example

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

- 1. From the VLAN Configuration screen, press [Ctrl]-R to return to the VLAN Configuration Menu.**
- 2. From the VLAN Configuration Menu, select VLAN Port Configuration (or press c).**

The default VLAN Port Configuration screen opens ([Figure 1-21](#)).

The VLAN Port Configuration screen settings shown in [Figure 1-21](#) are default settings.

VLAN Port Configuration

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

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

Figure 1-21. Default VLAN Port Configuration Screen Example

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

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

```
VLAN Port Configuration

Port:                               [ 8 ]
Filter Tagged Frames:               [ No ]
Filter Untagged Frames:             [ No ]
Filter Unregistered Frames:         [ No ]
Port Name:                          [ Library Sharing ]
PVID:                                [ 3 ]
Port Priority:                       [ 0 ]

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

Figure 1-22. VLAN Port Configuration Screen Example

VLAN Workgroup Summary

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

As shown in [Figure 1-23](#), switch S1 (a BayStack 450 switch) is configured with multiple VLANs:

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

Because S4 (a BayStack 350 switch) does not support 802.1Q tagging, a single switch port on each switch must be utilized for each VLAN (see “[VLANS Spanning Multiple Untagged Switches](#)” on [page 1-25](#)).

The connection to S2 requires only one link between the switches because S1 and S2 are both BayStack 450 switches that support 802.1Q tagging (see “[VLANs Spanning Multiple 802.1Q Tagged Switches](#)” on [page 1-24](#)).

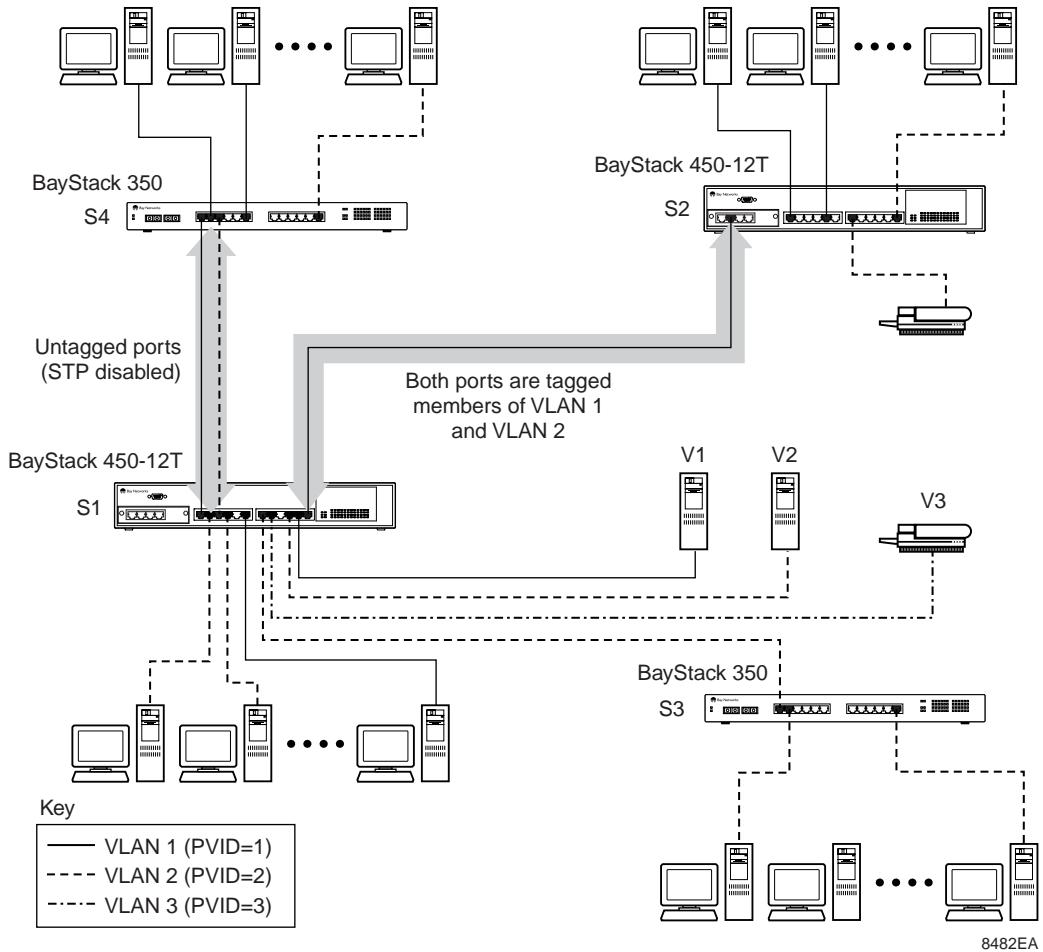


Figure 1-23. VLAN Configuration Spanning Multiple Switches

VLAN Configuration Rules

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

- All ports involved in port mirroring must be on the same VLANs. If a port is involved in port mirroring (monitor, X, or Y), the port cannot be configured on a VLAN.
- If a port is a trunk group member, all trunk members are added or deleted from the VLAN.
- VLANs are not dependent on STP settings.
- All ports involved in trunking and port mirroring must have the same VLAN configuration. If a port is on a trunk with a mirroring port, the VLAN configuration does not change.
- VLANs are not dependent on Rate Limiting settings.
- If a port is an IGMP member on any VLAN, and is removed from a VLAN, the port's IGMP membership is also removed.
- If a port is added to a different VLAN, and it is already configured as an IGMP Router port, the port is configured as an IGMP member on that specific VLAN.
- The following gigabit MDA restriction applies for VLAN configurations: tagging is restricted on secondary VLANs to either *all* tagged or *all* untagged.

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

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

IGMP Snooping

BayStack 450 switches can sense IGMP Host Membership Reports from attached stations and can use this information to set up a dedicated path between the requesting station and a local IP Multicast router. Once the pathway is established, the BayStack 450 switch blocks the IP Multicast stream from exiting any other port that does not connect to another Host Member, thus conserving bandwidth. The following describes how BayStack 450 switches provide the same benefit as IP Multicast routers, but in the local area:

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

[Figure 1-24](#) shows how IGMP is used to set up the path between the client and server. As shown in this example, the IP Multicast source provides an IP Multicast stream to designated routers which only forward the IP Multicast stream on their local network if there is a recipient.

The client/server path is set up as follows:

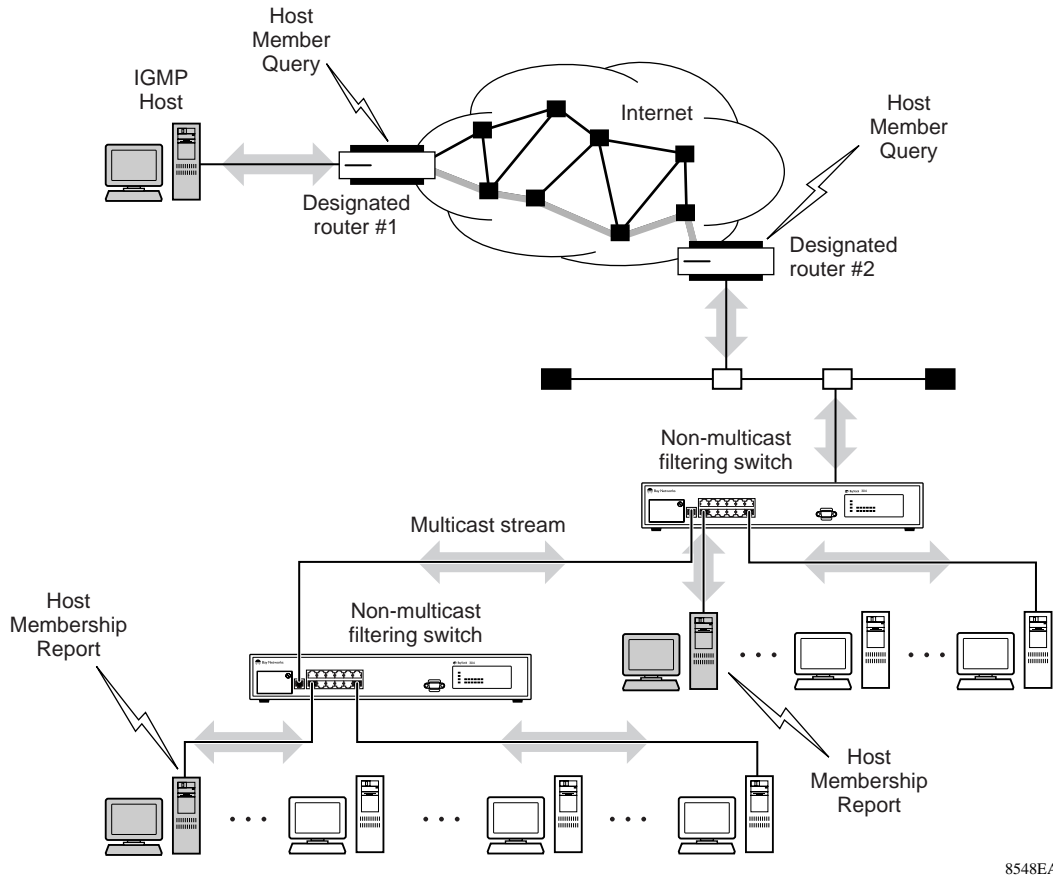
1. The designated router sends out a *Host Member Query* to the subnet and receives *Host Membership Reports* from end stations on the subnet.
2. The designated routers then set up a path between the IP Multicast stream source and the end stations.
3. Periodically, the router continues to query end stations on whether to continue participation.
4. As long as any client continues to participate, all clients, including non-participating endstations on that subnet, receive the IP Multicast stream.



Note: Although the non-participating endstations can filter the IP Multicast traffic, the IP Multicast still exists on the subnet and consumes bandwidth.

IP Multicast can be optimized in a LAN by using *IP Multicast filtering switches*, such as the BayStack 450 switch.

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



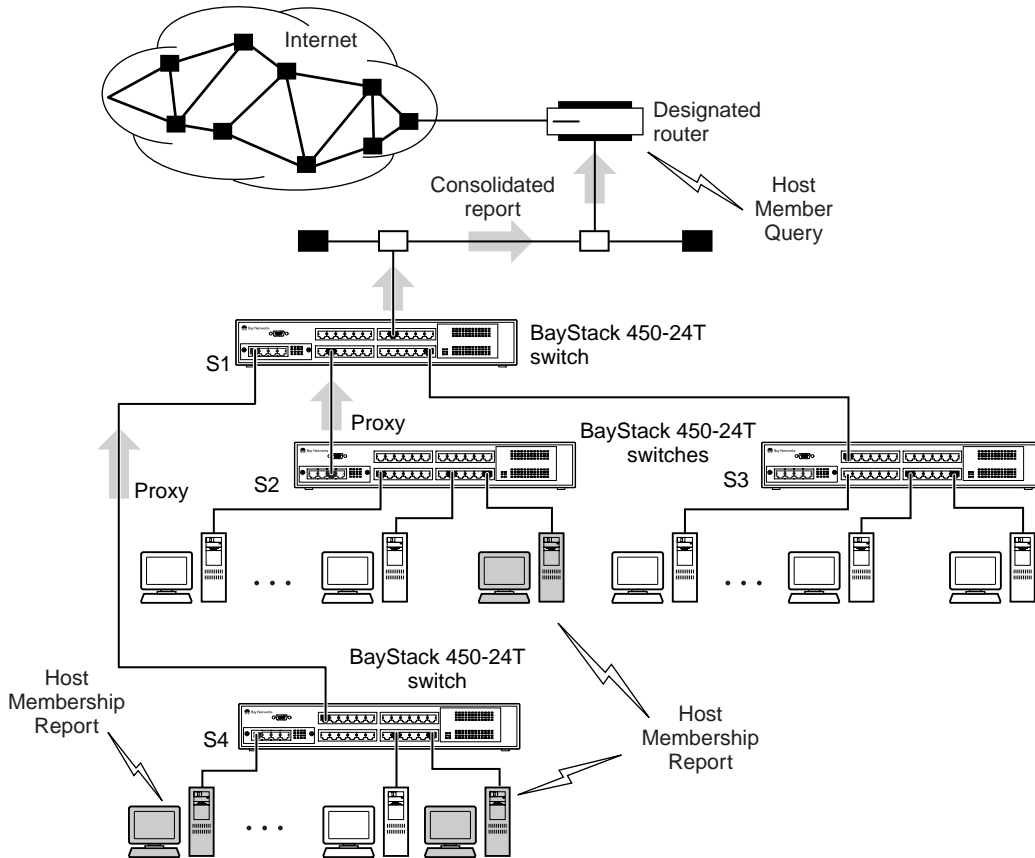
8548EA

Figure 1-24. IP Multicast Propagation With IGMP Routing

The BayStack 450 switch can automatically set up IP Multicast filters so the IP Multicast traffic is only directed to the participating end nodes (see [Figure 1-25](#)).

In [Figure 1-25](#), switches S1 to S4 represent a LAN connected to a IP Multicast router. The router periodically sends Host Member Queries to the LAN and listens for a response from end stations. All of the clients connected to switches S1 to S4 are aware of the queries from the router.

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

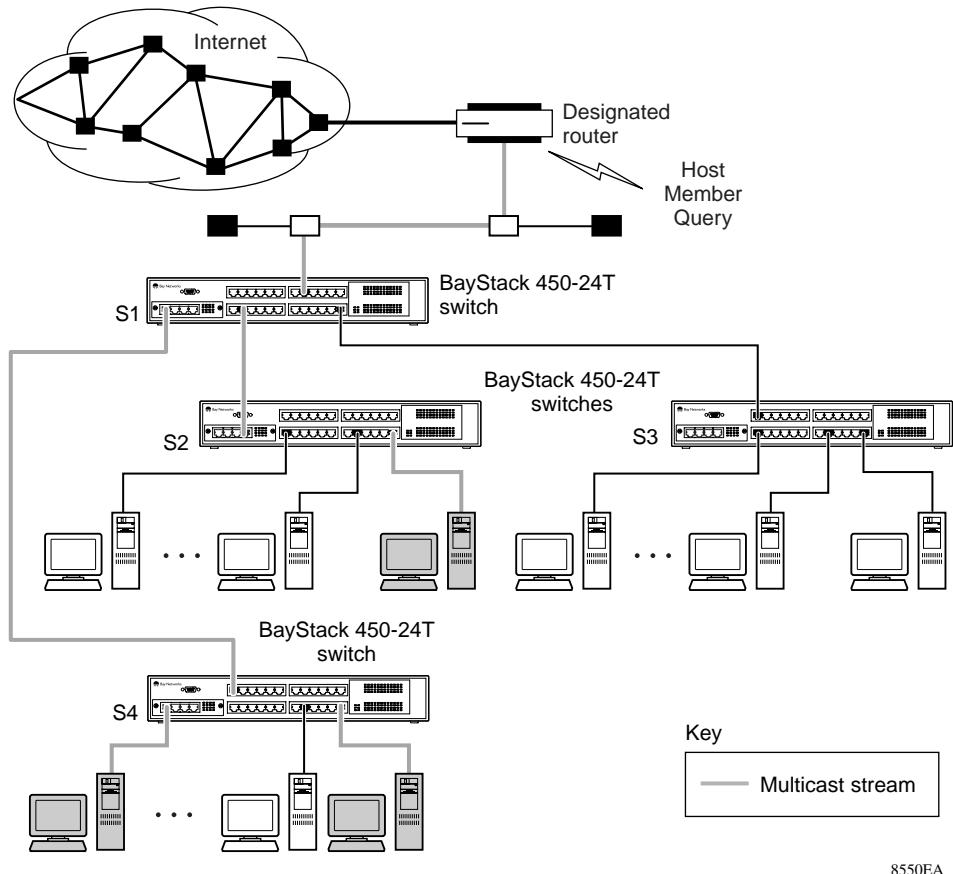


8549EA

Figure 1-25. BayStack 450 Switch Filtering IP Multicast Streams (1 of 2)

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

After the switches learn which ports are requesting access to the IP Multicast stream, all other ports not responding to the queries are blocked from receiving the IP Multicast (see [Figure 1-26](#)).



8550EA

Figure 1-26. BayStack 450 Switch Filtering IP Multicast Streams (2 of 2)

IGMP Snooping Configuration Rules

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

- A port cannot be configured as an IGMP Router port if it is already configured as a Port Mirroring monitor port.
- If a port that is a member of a MultiLink trunk is configured as an IGMP port, all ports on the MultiLink trunk are configured as IGMP Router ports. Also, if an IGMP Router port is removed, and it is a MultiLink trunk member, all trunk members are removed as IGMP Router members, automatically.
- IGMP Router ports must be VLAN port members.
- If a port is configured as an IGMP Router port, it is configured as an IGMP Router port for all VLANs on that port. The IGMP configuration is propagated through all VLANs of that port.
- If an IGMP Router port is removed, the IGMP Router membership for that port is also removed from all VLANs of that port.
- The IGMP Snooping feature is not STP dependent.
- The IGMP Snooping feature not Rate Limiting dependent.
- Proxy is only valid if snooping is enabled.
- IGMP is configured per VLAN and per IGMP Version.



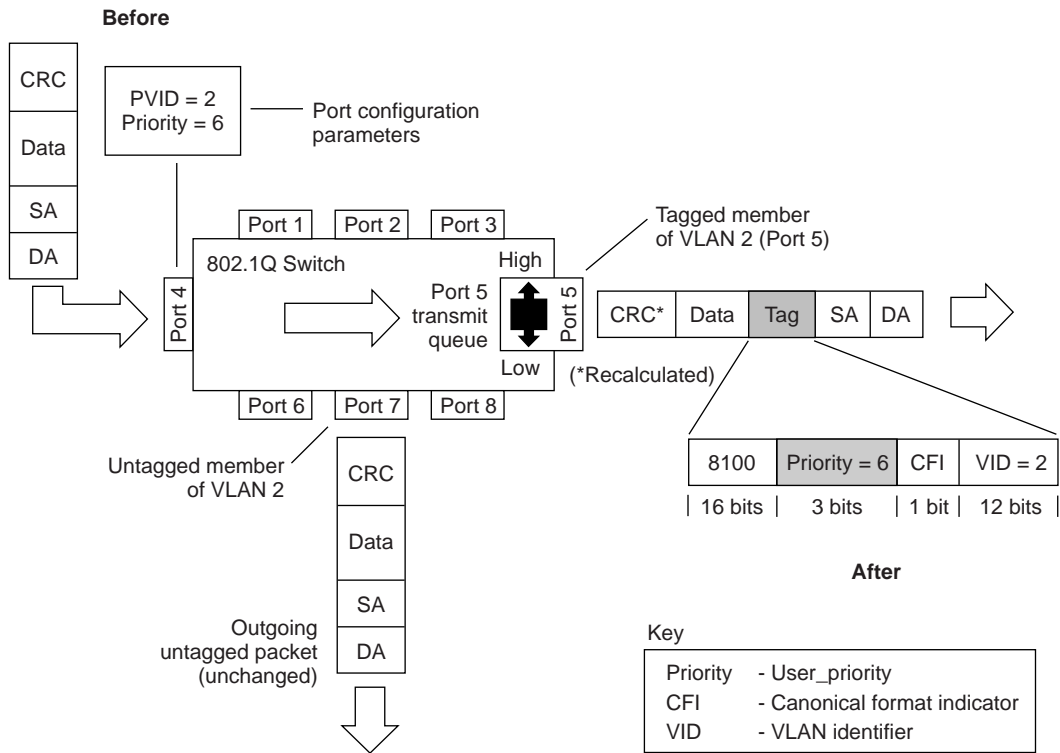
Note: Because IGMP Snooping is set up per VLAN, all IGMP changes are implemented according to the VLAN configuration for the specified ports.

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

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

IEEE 802.1p Prioritizing

You can use the VLAN Configuration screens to prioritize the order in which the switch forwards packets, on a per-port basis. For example, if messages from a specific segment are crucial to your operation, you can set the switch port connected to that segment to a higher priority level (by default, all switch ports are set to Low priority). Untagged packets received by the switch on that port are tagged according to the priority level you assign to the port (see [Figure 1-27](#)).



8551EA

Figure 1-27. Prioritizing Packets

The newly tagged frame is read within the switch and sent to the port's high or low transmit queue for disposition (see [Figure 1-28](#)). The port transmit queue example shown in [Figure 1-28](#) applies to all ports on the BayStack 450 switch.

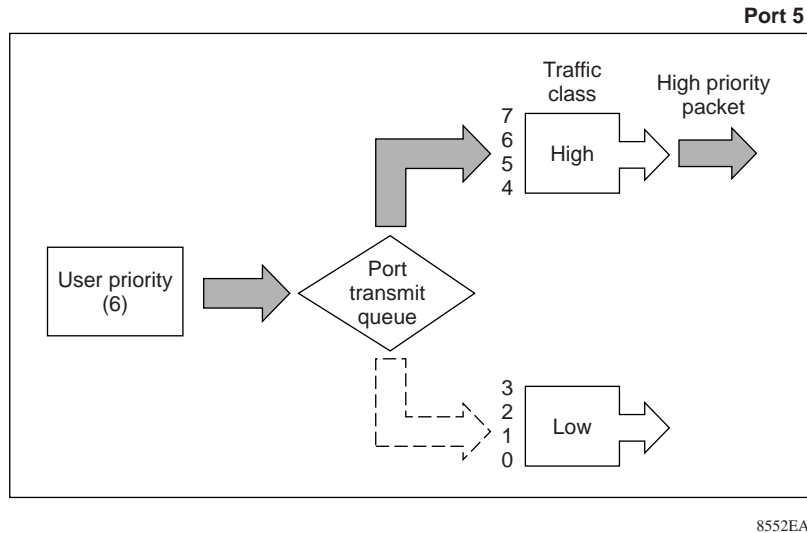


Figure 1-28. Port Transmit Queue

As shown in [Figure 1-28](#), the switch provides two transmission queues, a High transmission queue and a Low transmission queue, for any given port. Frames are assigned to one of these queues on the basis of user_priority using a *traffic class table*. This table is managed by using the Traffic Class Configuration screen ([Figure 1-29](#)). The table indicates the corresponding traffic class that is assigned to the frame, for each possible user_priority value. If the frame leaves the switch formatted as a tagged packet, the traffic class assigned to the frame is carried forward to the next 802.1p capable switch. This allows the packet to carry the assigned traffic class priority through the network until it reaches its destination.

The following steps show how to use the Traffic Class Configuration screen to configure the port priority level shown in the example [Figure 1-27](#).

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

To configure the port priority level, follow these steps:

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

User Priority levels are assigned default settings in all BayStack 450 switches. The range is from 0 to 7. The traffic class table can be modified, therefore, view the settings shown in the Traffic Class Configuration screen before setting the port priority in the VLAN Port Configuration screen.

2. Select Switch Configuration from the BayStack 450-12T Main Menu (or press w).

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

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

The Traffic Class Configuration screen opens ([Figure 1-29](#)).

```

                                Traffic Class Configuration

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

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

Figure 1-29. Default Traffic Class Configuration Screen Example

5. **Select a priority level from the range shown in the Traffic Class Configuration screen (or modify the Traffic Class parameters to suit your needs).**
6. **Assign the priority level to ports using the VLAN Port Configuration screen:**
 - a. **Press [Ctrl]-R to return to the VLAN Configuration Menu.**
 - b. **From the VLAN Configuration Menu, select VLAN Port Configuration (or press c).**

The VLAN Port Configuration screen opens ([Figure 1-30](#)).

[Figure 1-30](#) shows the VLAN Port Configuration screen setup for port 4 in [Figure 1-27](#) on [page 1-40](#).

```
VLAN Port Configuration

Port:                               [ 4 ]
Filter Tagged Frames:               [ No ]
Filter Untagged Frames:             [ No ]
Filter Unregistered Frames:         [ No ]
Port Name:                           [ High Anxiety ]
PVID:                                [ 2 ]
Port Priority:                        [ 6 ]

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

Figure 1-30. Setting Port Priority Example

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

MultiLink Trunks

MultiLink trunks allow you to group up to four switch ports together to form a link to another switch or server, thus increasing aggregate throughput of the interconnection between the devices (up to 800 Mb/s in full-duplex mode). BayStack 450 switches can be configured with up to six MultiLink Trunks. MultiLink Trunking software detects misconfigured (or broken) trunk links and redirects traffic on the misconfigured or broken trunk link to other trunk members within that trunk.

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

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

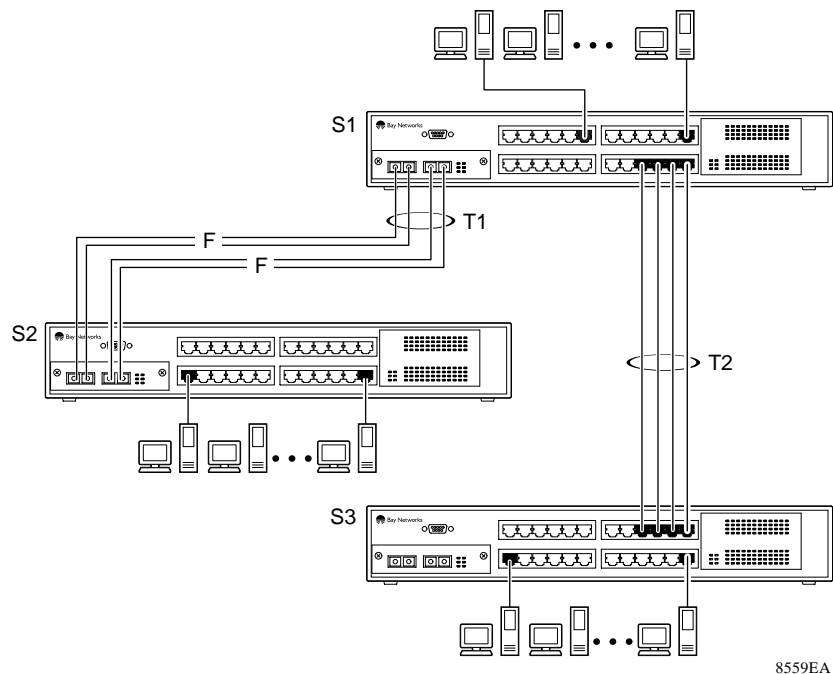


Figure 1-31. Switch-to-Switch Trunk Configuration Example

Each of the trunks shown in [Figure 1-31](#) can be configured with up to four switch ports to provide up to 800 Mb/s aggregate bandwidth through each trunk, in full-duplex mode. As shown in this example, when traffic between switch-to-switch connections approaches single port bandwidth limitations, creating a MultiLink trunk can supply the additional bandwidth required to improve the performance.

[Figure 1-32](#) shows a typical switch-to-server trunk configuration. In this example, file server FS1 utilizes dual MAC addresses, using one MAC address for each Network interface controller (NIC). For this reason, FS1 does not require a trunk assignment. FS2 is a single MAC server (with a four-port NIC) and is set up as trunk configuration T1.

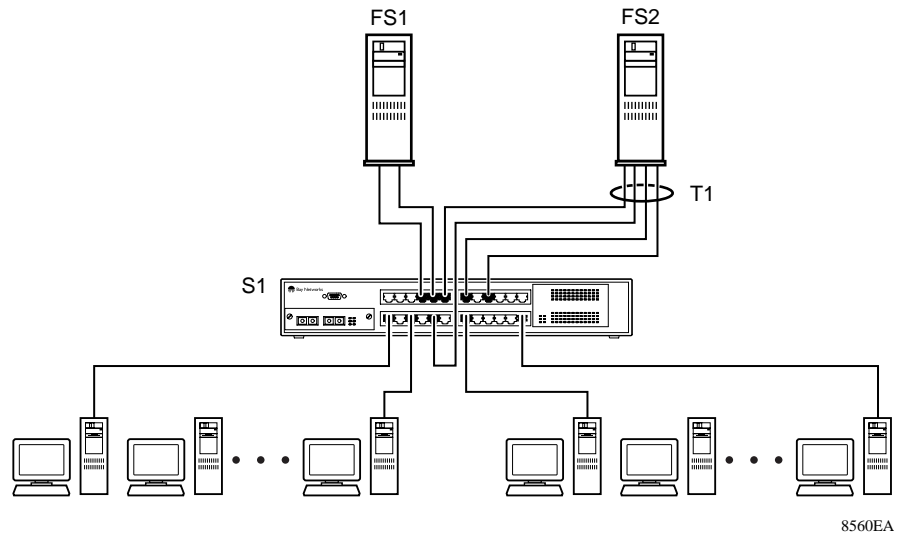


Figure 1-32. Switch-to-Server Trunk Configuration Example

Client/Server Configuration Utilizing MultiLink Trunks

[Figure 1-33](#) shows an example of how MultiLink trunking can be used in a client/server configuration. In this example, both servers are connected directly to switch S1. FS2 is connected through a trunk configuration (T1). The switch-to-switch connections are through trunks (T2, T3, T4, and T5).

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

With spanning tree *enabled*, one of the trunks (T2 or T3) acts as a redundant (backup) trunk to switch S2. With spanning tree *disabled*, trunks T2 and T3 must be configured into separate VLANs for this configuration to function properly (see “[IEEE 802.1Q VLAN Workgroups](#)” on [page 1-19](#)).

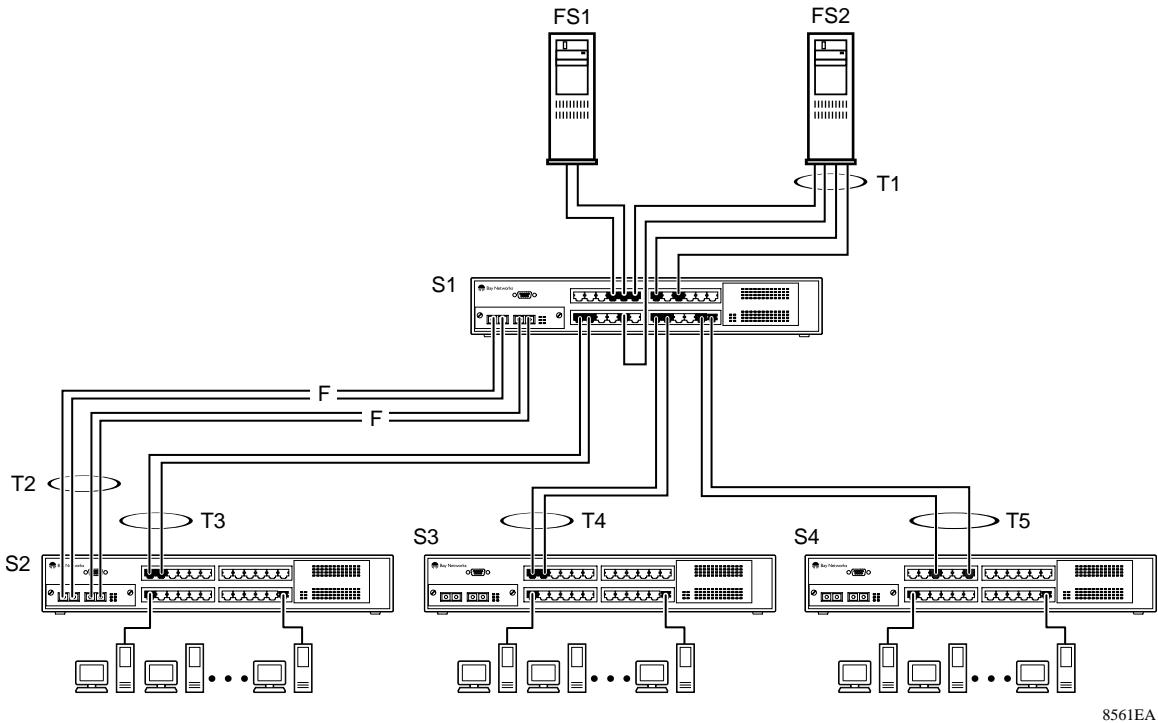


Figure 1-33. Client/Server Configuration Example

The Trunk Configuration screens for switches S1 to S4 are shown in “[Trunk Configuration Screen Examples](#)” following this section. For detailed information about configuring trunks, see “MultiLink Trunk Configuration” on page 3-35.

Trunk Configuration Screen Examples

This section shows examples of the MultiLink Trunk Configuration screens for the client/server configuration example shown in [Figure 1-33](#) on [page 1-46](#). The screens show how you could set up the trunk configuration screens for switches S1 to S4. See “[Spanning Tree Considerations](#)” on [page 1-58](#), and “MultiLink Trunk Configuration” on page 3-35 for more information.

Trunk Configuration Screen for Switch S1

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

Setting up the Trunk Configuration For S1:

To set up the trunk configuration, choose MultiLink Trunk Configuration (or press t) from the MultiLink Trunk Configuration Menu screen ([Figure 1-34](#)).

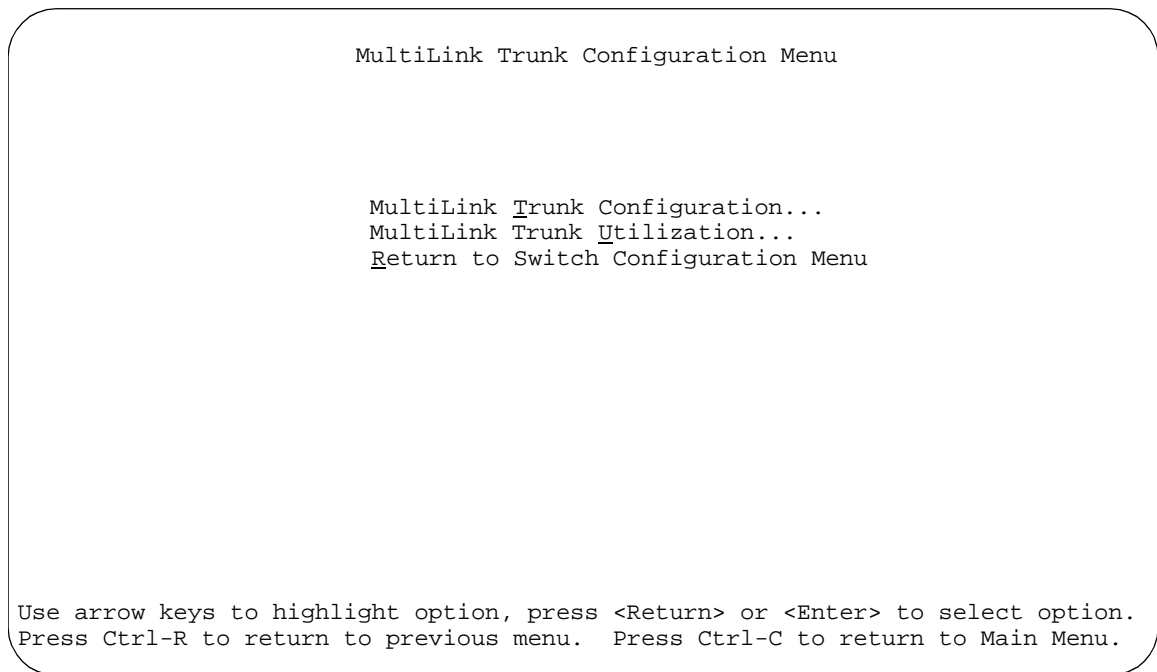


Figure 1-34. Choosing the MultiLink Trunk Configuration Screen

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

```

MultiLink Trunk Configuration

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

Trunk      Trunk Name
-----
 1 [ S1:T1 to FS2 ]
 2 [ S1:T2 to S2 ]
 3 [ S1:T3 to S2 ]
 4 [ S1:T4 to S3 ]
 5 [ S1:T5 to S4 ]
 6 [ Trunk #6 ]

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

```

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

The MultiLink Trunk Configuration screen for switch S1 is configured as follows:

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

Ports 6, 7, 9, and 17 are assigned as trunk members of trunk 1.

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

Ports 13 and 14 are assigned as trunk members of trunk 3.

Ports 19 and 20 are assigned as trunk members of trunk 4.

Ports 22 and 23 are assigned as trunk members of trunk 5.

- **STP Learning** indicates the spanning tree participation setting for each of the trunks:
Trunks 1 through 4 are enabled for Normal STP Learning.
Trunk 5 is enabled for Fast STP Learning.
- **Trunk Mode (read only)** indicates the Trunk Mode for each of the trunks:
The Trunk Mode fields for trunks 1 to 5 are set to Basic, by default. Source MAC addresses are statically assigned to specific trunk members for flooding and forwarding. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.
- **Trunk Status** indicates the Trunk Status for each of the trunks. When set to Enabled, the configuration settings for that specific trunk are activated.
- **Trunk Name** indicates optional fields for assigning names to the corresponding configured trunks.
The names chosen for this example provide meaningful information to the user of this switch (for example, S1:T1 to FS2 indicates that Trunk 1, in switch S1, connects to File Server 2).

Trunk Configuration Screen for Switch S2

As shown in [Figure 1-33](#) on [page 1-46](#), switch S2 is set up with two trunk configurations (T2 and T3). Both trunks connect directly to switch S1.

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

[Figure 1-36](#) shows the MultiLink Trunk Configuration screen for switch S2.

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

Trunk	Trunk Name
1	[S2:T2 to S1]
2	[S2:T3 to S1]
3	[Trunk #3]
4	[Trunk #4]
5	[Trunk #5]
6	[Trunk #6]

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

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

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

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

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

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

- **STP Learning** indicates the spanning tree participation setting for each of the trunks:

Trunk 1 and 2 are enabled for Normal STP Learning.

- **Trunk Mode (read only)** indicates the Trunk Mode for each of the trunks:

The Trunk Mode fields for trunks 1 and 2 are set to Basic, by default. Source MAC addresses are statically assigned to specific trunk members for flooding and forwarding. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.

- **Trunk Status** indicates the Trunk Status for each of the trunks. When set to Enabled, the configuration settings for that specific trunk are activated.
- **Trunk Name** indicates optional fields for assigning names to the corresponding configured trunks.

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

Trunk Configuration Screen for Switch S3

As shown in [Figure 1-33](#) on [page 1-46](#), switch S3 is set up with one trunk configuration (T4). This trunk connects directly to switch S1.

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

[Figure 1-37](#) shows the MultiLink Trunk Configuration screen for switch S3.

MultiLink Trunk Configuration						
Trunk	Trunk Members			STP Learning	Trunk Mode	Trunk Status
1	[1]	[2]	[]	[Normal]	Basic	[Enabled]
2	[]	[]	[]	[Normal]	Basic	[Disabled]
3	[]	[]	[]	[Normal]	Basic	[Disabled]
4	[]	[]	[]	[Normal]	Basic	[Disabled]
5	[]	[]	[]	[Normal]	Basic	[Disabled]
6	[]	[]	[]	[Normal]	Basic	[Disabled]

Trunk	Trunk Name
1	[S3:T4 to S1]
2	[Trunk #2]
3	[Trunk #3]
4	[Trunk #4]
5	[Trunk #5]
6	[Trunk #6]

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

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

The MultiLink Trunk Configuration screen for switch S3 is configured as follows:

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

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

- **STP Learning** indicates the spanning tree participation setting for each of the trunks:

Trunk 1 is enabled for Normal STP Learning.

- **Trunk Mode (read only)** indicates the Trunk Mode for each of the trunks:

The Trunk Mode field for trunk 1 is set to Basic, by default. Source MAC addresses are statically assigned to specific trunk members for flooding and forwarding. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.

- **Trunk Status** indicates the Trunk Status for each of the trunks. When set to Enabled, the configuration settings for that specific trunk are activated.
- **Trunk Name** optional fields for assigning names to the corresponding configured trunks.

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

Trunk Configuration Screen for Switch S4

As shown in [Figure 1-33](#), switch S4 is set up with one trunk configuration (T5). This trunk connects directly to switch S1.

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

[Figure 1-38](#) shows the MultiLink Trunk Configuration screen for switch S4.

MultiLink Trunk Configuration						
Trunk	Trunk Members			STP Learning	Trunk Mode	Trunk Status
1	[3]	[6]	[]	[Normal]	Basic	[Enabled]
2	[]	[]	[]	[Normal]	Basic	[Disabled]
3	[]	[]	[]	[Normal]	Basic	[Disabled]
4	[]	[]	[]	[Normal]	Basic	[Disabled]
5	[]	[]	[]	[Normal]	Basic	[Disabled]
6	[]	[]	[]	[Normal]	Basic	[Disabled]
Trunk	Trunk Name					
1	[S4:T5 to S1]					
2	[Trunk #2]					
3	[Trunk #3]					
4	[Trunk #4]					
5	[Trunk #5]					
6	[Trunk #6]					

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

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

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

- **Trunk field (read only)** --- indicates the trunk (1 to 6) that corresponds to the switch ports specified in the Trunk Members fields.
- **Trunk Members fields** --- indicates the ports that can be configured, in each row, to create the corresponding trunk:
 - Ports 3 and 6 are assigned as trunk members of trunk T1.
- **STP Learning field** --- indicates the spanning tree participation setting for each of the trunks:
 - Trunk 1 --- indicates that trunk 1 is enabled for Normal STP Learning.
- **Trunk Mode field (read only)** --- indicates the Trunk Mode for each of the trunks:
 - Trunk 1 --- Read-only Trunk Mode fields for trunk 1 is set to Basic, by default. Source MAC addresses are statically assigned to specific trunk members for flooding and forwarding. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.
- **Trunk Status field** --- indicates the Trunk Status for each of the trunks. When set to Enabled, the configuration settings for that specific trunk are activated.
- **Trunk Name field** --- optional fields for assigning names to the corresponding configured trunks. The names chosen for this example provide meaningful information to the user (for example, S4:T5 to S1 indicates that Trunk 1, in switch S4, connects to Switch 1).

Before Configuring Trunks

When you create and enable a trunk, the trunk members (switch ports) take on certain settings necessary for correct operation of the MultiLink Trunking feature. These settings, along with specific configuration rules, must be considered before configuring your MultiLink trunk.

Before configuring any MultiLink trunk, follow these steps:

1. **Read the configuration rules provided in the next section, “[MultiLink Trunking Configuration Rules](#).”**
2. **Determine which switch ports (up to four) are to become *trunk members* (the specific ports making up the trunk):**
 - a. **A minimum of two ports are required for each trunk.**
 - b. **Ensure that the chosen switch ports are set to Enabled, using the Port Configuration screen (see “Port Configuration” on page 3-30) or through network management.**
 - c. **Trunk member ports must be in the same VLAN.**
3. **All network cabling should be complete and stable before configuring any trunks, to avoid configuration errors.**
4. **Consider how the existing spanning tree will react to the new trunk configuration (see “[Spanning Tree Considerations](#)” on [page 1-58](#)).**
5. **Consider how existing VLANs will be affected by the addition of a trunk.**
6. **After completing the above steps, see “MultiLink Trunk Configuration” on page 3-35 for screen examples and field descriptions that will help you configure your MultiLink trunks.**

MultiLink Trunking Configuration Rules

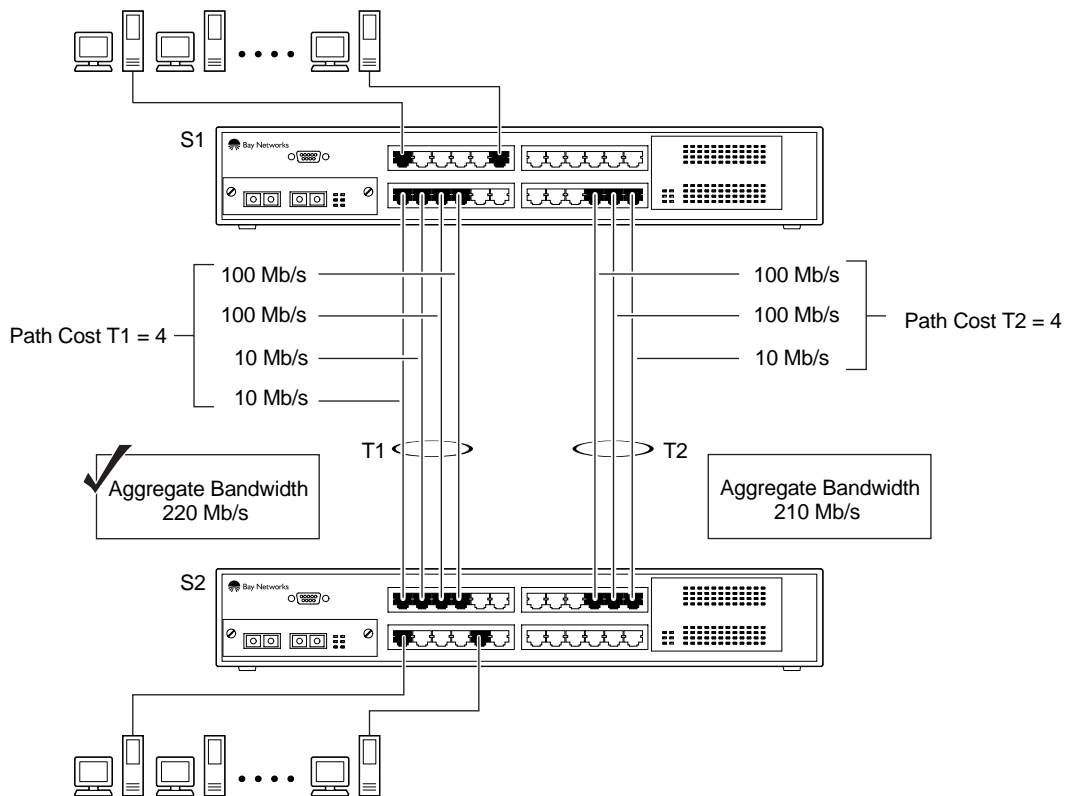
The MultiLink Trunking feature is deterministic; that is, it operates according to specific configuration rules. When creating trunks, consider the following rules that determine how the MultiLink trunk reacts in any network topology:

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

- All trunk members must be configured into the same VLAN before the Trunk Configuration screen's Trunk Status field can be set to Enabled (See ““VLAN Configuration” on page 3-22).
- When an active port is configured in a trunk, the port becomes a *trunk member* as soon as the Trunk Status field is set to Enabled. After the Trunk Status field is set to Enabled, the spanning tree parameters for the port will change to reflect the new trunk settings.
- If spanning tree participation of any trunk member is changed (enabled or disabled), the spanning tree participation of all members of that trunk is changed similarly (see “[Spanning Tree Considerations](#)” on [page 1-58](#)).
- When a trunk is enabled, the trunk spanning tree participation setting takes precedence over that of any trunk member. When a trunk is active, the trunk STP setting can be changed from either the Trunk Configuration screen or the Spanning Tree Configuration screen.
- If the VLAN settings of any trunk member are changed, the VLAN settings of all members of that trunk are changed similarly.
- When any trunk member is set to Disabled (not active) through the Port Configuration screen or through network management, the trunk member is removed from the trunk. The removed trunk member has to be reconfigured through the Trunk Configuration screen to rejoin the trunk. A screen prompt precedes this action. A trunk member cannot be disabled if there are only two trunk members on the trunk.
- A trunk member cannot be configured as a monitor port (see “Port Mirroring Configuration” on page 3-42).
- Trunks cannot be monitored by a monitor port; however, trunk members can be monitored (see “[Port-Based Mirroring Configuration](#)” on [page 1-63](#)).
- All trunk members must have identical IGMP Snooping configurations.
- If the IGMP Snooping configuration for any trunk member is changed, the IGMP Snooping settings for all trunk members are changed.

Spanning Tree Considerations

The spanning tree Path Cost parameter is recalculated based on the aggregate bandwidth of the trunk. For example, [Figure 1-39](#) shows a four port trunk (T1) with two port members operating at 100 Mb/s and the other two port members operating at 10 Mb/s. Trunk T1 provides an aggregate bandwidth of 220 Mb/s. The Path Cost for T1 is 4 (Path Cost = 1000/LAN speed, in Mb/s). If a second three port trunk (T2) is configured with an aggregate bandwidth of 210 Mb/s, with a comparable Path Cost of 4, the switch software chooses the trunk with the larger bandwidth (T1) to determine the most efficient path.



8553EA

Figure 1-39. Path Cost Arbitration Example

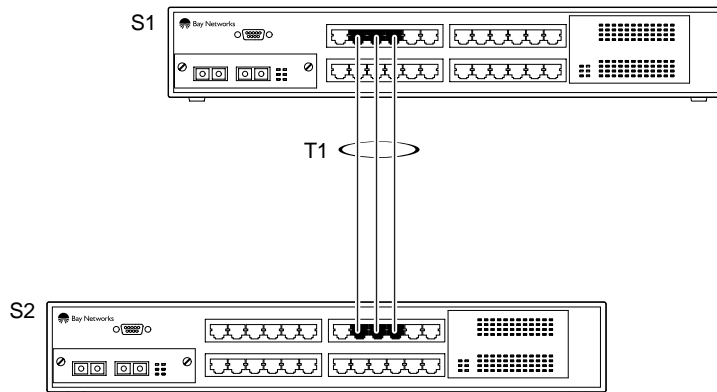
The switch can also detect trunk member ports that are physically misconfigured. For example, in [Figure 1-40](#), trunk member ports 2, 3, and 4 of switch S1 are configured *correctly* to trunk member ports 8, 9, and 10 of switch S2. The Spanning Tree Port Configuration screen for each switch shows the port State field for each port in the Forwarding state.

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

More...

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

S1 Port Configuration screen



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

More...

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

S2 Port Configuration screen

8557EA

Figure 1-40. Example 1: Correctly Configured Trunk

If switch S2's trunk member port 10 is physically disconnected and then reconnected to port 12, the Spanning Tree Port Configuration screen for switch S1 changes to show port 4 in the Blocking state (Figure 1-41).

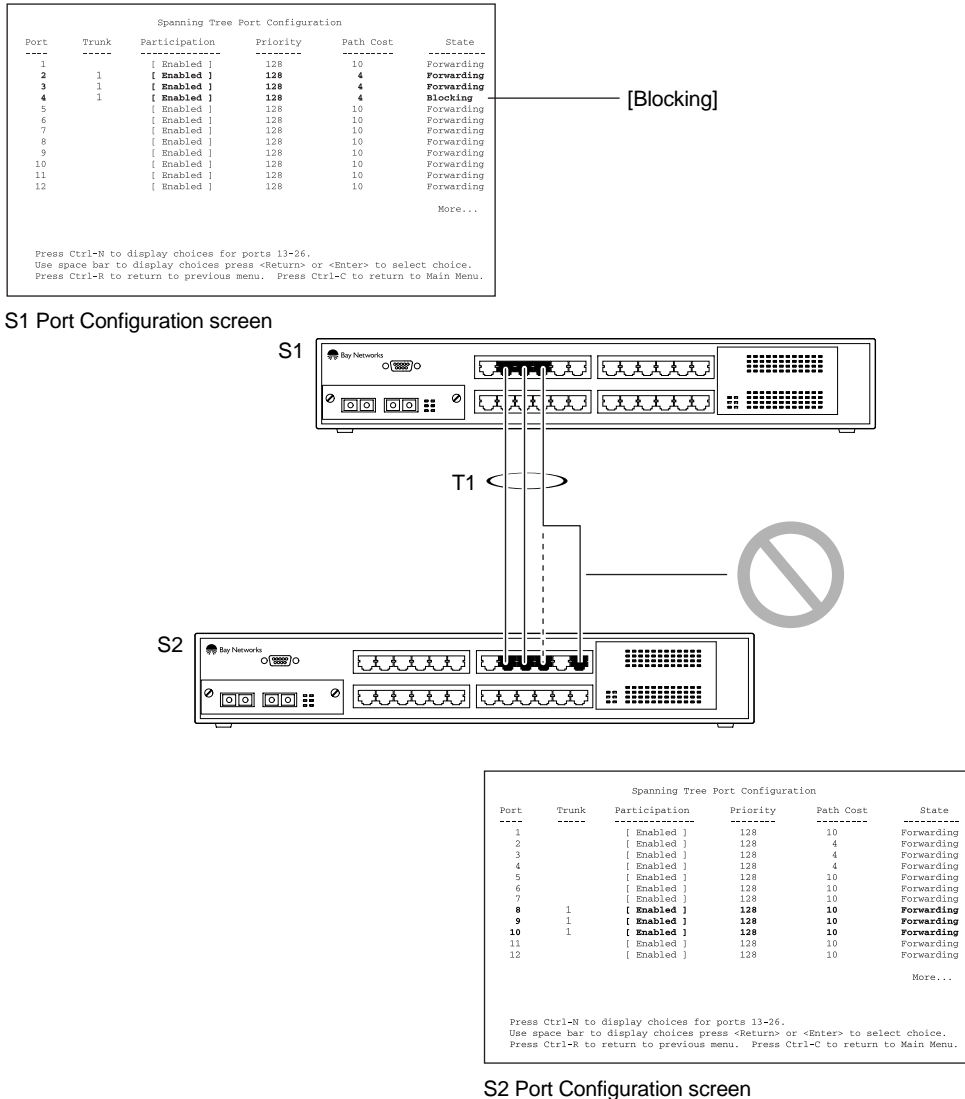


Figure 1-41. Example 2: Detecting a Misconfigured Port

Additional Tips About the MultiLink Trunking Feature

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

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

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

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

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

For more information about using the MultiLink Trunking feature, see "MultiLink Trunk Configuration" on page 3-35.

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

Port Mirroring (Conversation Steering)

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



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

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

- Port-based Mirroring
- Address-based Mirroring

A sample of the Port Mirroring Configuration screen is provided with each of the examples to support the network configuration example.

Note that in the following examples, the displayed screens do not show all of the screen prompts that precede some actions. For example, when you configure a switch for port mirroring or when you modify an existing port mirroring configuration, the new configuration does not take effect until you respond [Yes] to the following screen prompt:

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

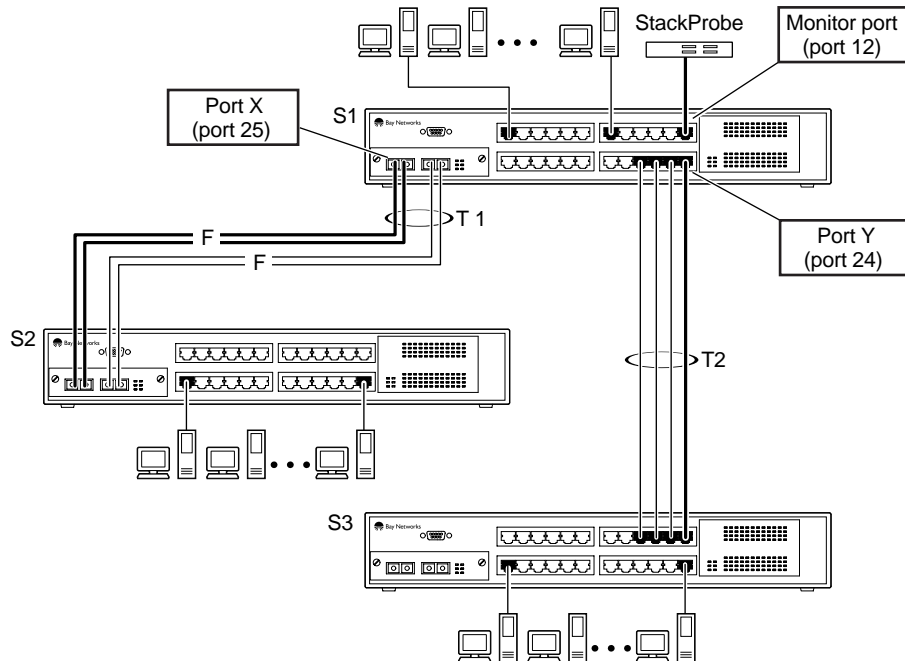
Port-Based Mirroring Configuration

[Figure 1-42](#) shows an example of a port-based mirroring configuration where port 12 is designated as the monitor port for ports 24 and 25 of switch S1. Although this example shows ports 24 and 25 monitored by the monitor port (port 12), any of the trunk members of T1 and T2 can also be monitored.



Note: Trunks cannot be monitored and trunk members cannot be configured as monitor ports (see [“MultiLink Trunking Configuration Rules”](#) on [page 1-56](#)).

[Figure 1-43](#) shows the Port Mirroring Configuration screen setup for this example.



8554EA

Figure 1-42. Port-Based Mirroring Configuration Example

In the configuration example shown in [Figure 1-42](#), the designated monitor port (port 12) can be set to monitor traffic in any of the following modes:

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

As shown in the Port Mirroring Configuration screen example ([Figure 1-43](#)), a user has designated port 12 as the Monitor Port for ports 24 and 25 in switch S1.

The Monitoring Mode field [- > Port X or Port Y - >] indicates that all traffic received by port X *or* all traffic transmitted by port Y is currently being monitored by the StackProbe attached to Monitor Port 12.

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

```

Port Mirroring Configuration

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

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

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

Port mirroring configuration has taken effect.

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

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

```

Figure 1-43. Port Mirroring Port-Based Screen Example

Address-Based Mirroring Configuration

[Figure 1-44](#) shows an example of an address-based mirroring configuration where port 12, the designated monitor port for switch S1, is monitoring traffic occurring between address A and address B.

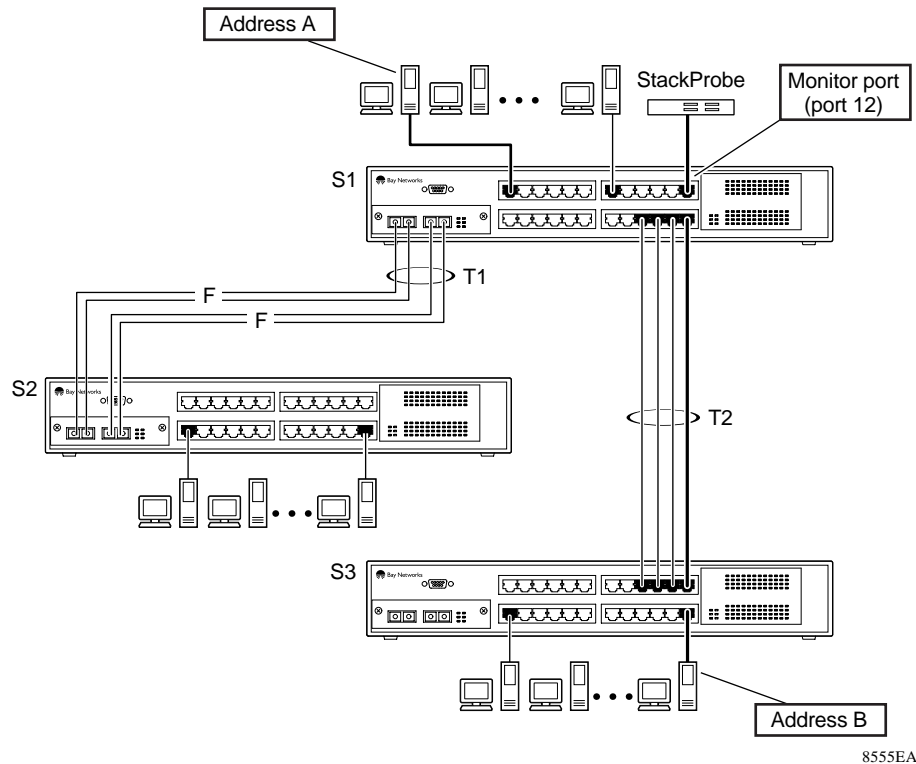


Figure 1-44. Address-Based Mirroring Configuration Example

In this configuration, the designated monitor port (port 12) can be set to monitor traffic in any of the following modes:

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

[Figure 1-45](#) shows the Port Mirroring Configuration screen setup for this example.

In this example, port 12 becomes the designated Monitor Port for switch S1 when you press [Enter] in response to the [Yes] screen prompt. The screen data displayed at the bottom of the screen will change to show the *new* currently active port mirroring configuration when you press Return.

The Monitoring Mode field [Address A -> Address B] indicates that all traffic transmitted by address A to address B will be monitored by the StackProbe attached to Monitor Port 12.



Note: When you enter MAC addresses in this screen, they are also displayed in the MAC Address Table screen (see “MAC Address Table” on page 3-18).

```

Port Mirroring Configuration

Monitoring Mode:      [ Address A  ->  Address B  ]
Monitor Port:        [ 12  ]

Port X:              [      ]
Port Y:              [      ]

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

Is your Port mirroring configuration complete?      [ Yes ]

-----
Currently Active Port Mirroring Configuration
-----
Monitoring Mode:      Address A  <->  Address B      Monitor Port:      1
Address A:  00-11-22-33-44-55                Address B:  22-33-44-55-66-77

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

```

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

Port Mirroring Configuration Rules

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

- A monitor port cannot be configured as a trunk member or IGMP member, and cannot be used for normal switch functions.
- When a port is configured and enabled as a monitor port, the port is automatically disabled from participating in the spanning tree. When the port is reconfigured as a standard switch port (no longer a monitor port), the port becomes enabled for spanning tree participation.
- When creating a *port-based* port mirroring configuration, be sure that the monitor port and both of the mirrored ports, port X and port Y, have the same configuration. Use the VLAN Configuration screen to configure the VLAN (see “VLAN Configuration” on page 3-22).
- VLAN configuration settings for any ports configured for port-based mirroring cannot be changed. Use the Port Mirroring Configuration screen to disable port mirroring (or reconfigure the port mirroring ports), then change the VLAN configuration settings. See also rule 3.
- For port-based monitoring of traffic, use one of the following modes for monitoring broadcast, IP Multicast, or unknown DA frames:
 - Monitor all traffic received by port X.
 - Monitor all traffic transmitted by port X.
 - Monitor all traffic received and transmitted by port X.
 - Monitor all traffic received by port X or transmitted by port Y.

For more information about using the Port Mirroring feature, see “Port Mirroring Configuration” on page 3-42.

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

Chapter 2

Installing the BayStack 450 Switch

This chapter provides the following information about the BayStack 450 switch:

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

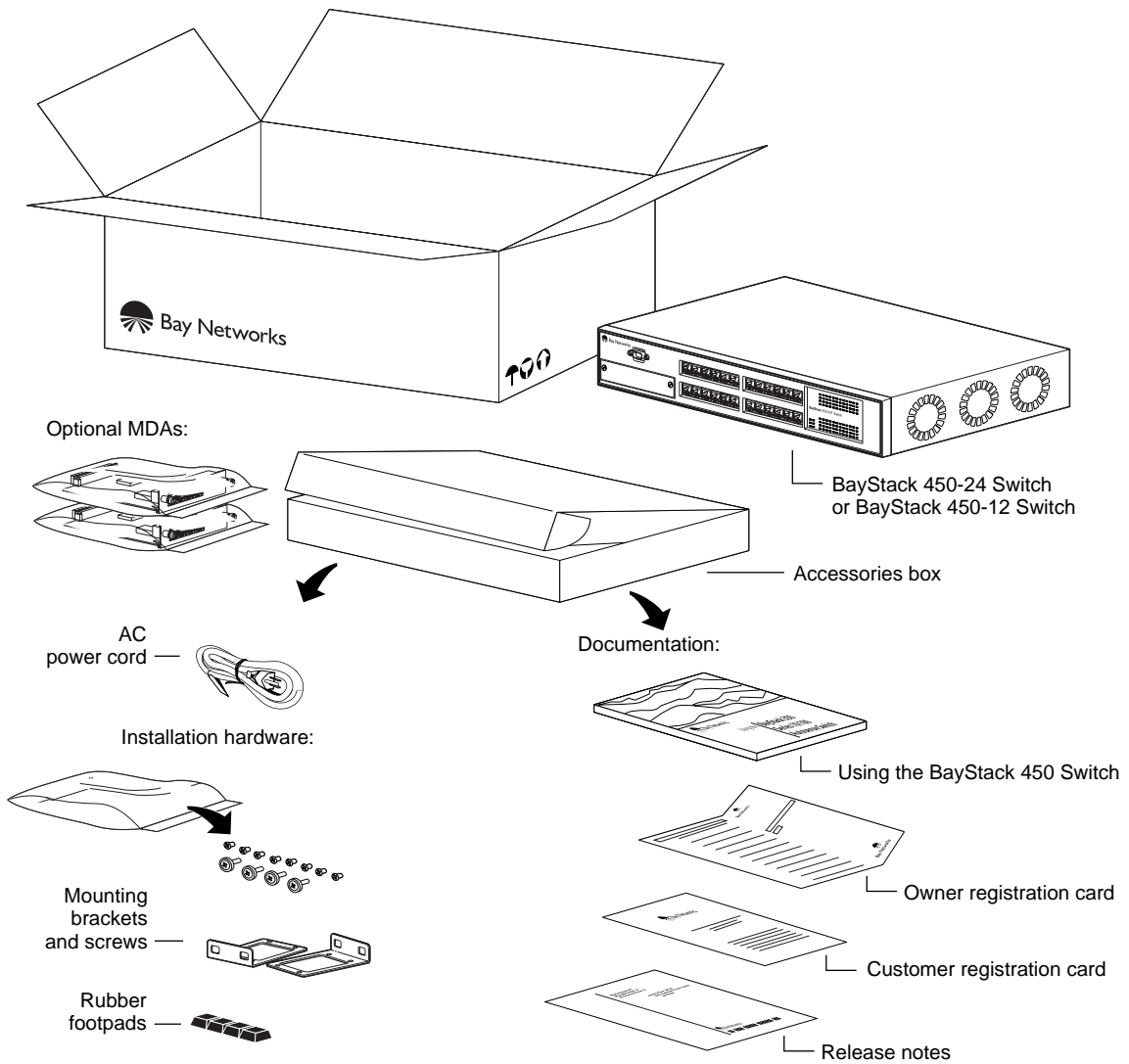
Refer to Chapter 3, “Using the Console Interface,” to further configure your BayStack 450 switch.

Installation Requirements

Before installing the BayStack 450 switch, verify that the package contains the following items in addition to this guide (see [Figure 2-1](#)):

- A BayStack 450-24 switch or a BayStack 450-12 switch
- Power cable for operating country; see “AC Power Receptacle” on page 1-7
- Rack-mounting kit
- Registration card
- Release Notes (optional)

Install the BayStack 450 switch in a ventilated area that is dust free and away from heat vents, warm air exhaust from other equipment, and direct sunlight. Avoid proximity to large electric motors or other electromagnetic equipment. When choosing a location, observe the environmental guidelines listed in Appendix A, “Technical Specifications.”



8524FA

Figure 2-1. Package Contents

If any items are missing or damaged, contact the sales agent or the customer service representative from whom you purchased the BayStack 450 switch. You will need a Phillips screwdriver for the installation.

Installation Procedure

This section provides the requirements and instructions for installing the BayStack 450 switch on a flat surface or in a standard 19-inch utility rack. If you install the switch in a rack, ground the rack to the same grounding electrode used by the power service in the area. The ground path must be permanent and must not exceed 1 ohm of resistance from the rack to the grounding electrode.

Installing the BayStack 450 Switch on a Flat Surface

The BayStack 450 switch can be mounted onto any appropriate flat, level surface that can safely support the weight of a switch and its attached cables, as long as there is adequate space around the unit for ventilation and access to cable connectors.



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

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

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

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

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

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

3. Attach all devices to the ports.

See “[Attaching Devices to the BayStack 450 Switch](#)” on [page 2-6](#).

Installing the BayStack 450 Switch in a Rack

The BayStack 450 switch occupies a 1.6-unit (1.6u) rack space and can be installed in most standard 19-inch racks. The rack must be grounded to the same grounding electrode used by the power service in the area. The ground path must be permanent and must not exceed 1 ohm of resistance from the rack to the grounding electrode.

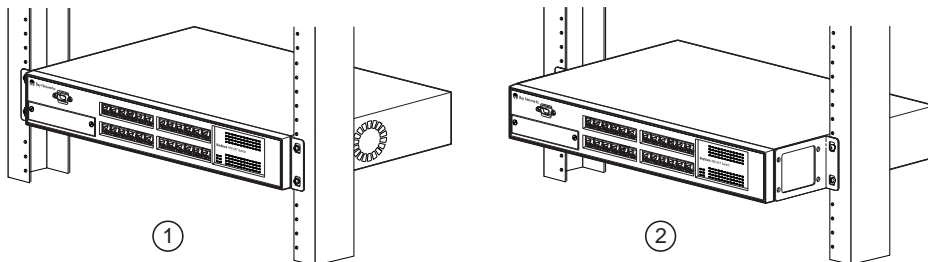


Caution: When mounting this device in a rack, do not stack units directly on top of one another in the rack. Each unit must be secured to the rack with appropriate mounting brackets. Mounting brackets are not designed to support multiple units.

To install the BayStack 450 switch in a rack, follow these steps:

1. Determine how far you want the switch to protrude in front of the rack.

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

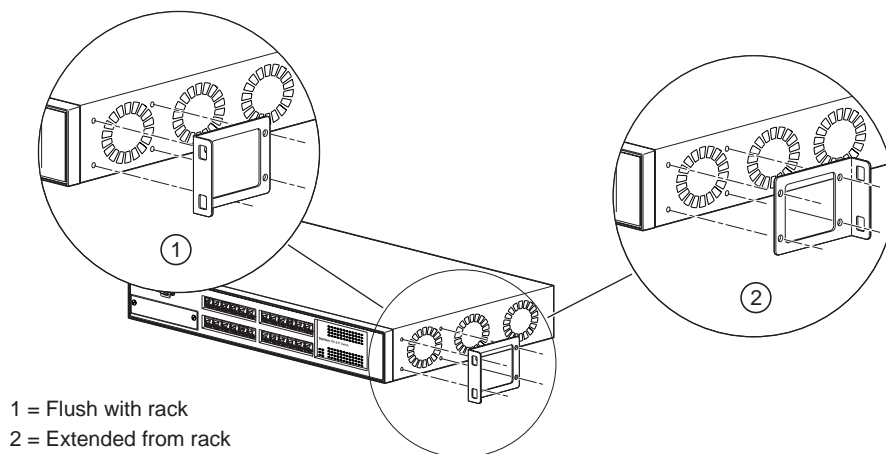


- 1 = Flush with rack
2 = Extended from rack

8530FA

Figure 2-2. Positioning the Chassis in the Rack

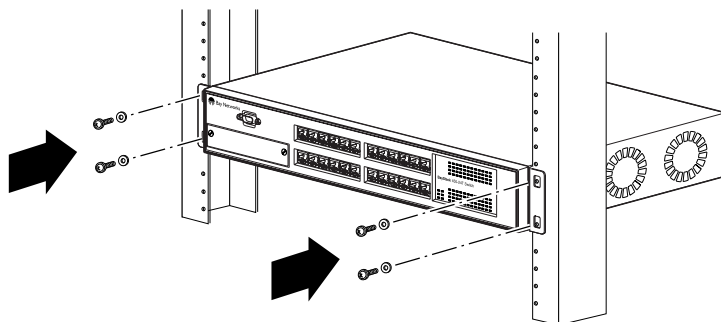
2. Using a Phillips screwdriver, attach a mounting bracket to each side of the switch using the supplied screws ([Figure 2-3](#)).



8535FA

Figure 2-3. Attaching Mounting Brackets

3. Position the switch in the rack and align the holes in the mounting bracket with the holes in the rack (see [Figure 2-4](#)).
4. Insert two screws, appropriate for your 19-inch rack, into each of the mounting brackets and tighten.



8536FA

Figure 2-4. Installing the BayStack 450 Switch in an Equipment Rack

5. After the switch is secured in the rack, proceed to the next section, [“Attaching Devices to the BayStack 450 Switch”](#) on [page 2-6](#).

Attaching Devices to the BayStack 450 Switch

This section describes how to attach devices to the BayStack 450 switch ports and how to connect a console terminal to the switch Console/Comm port. You can use the console terminal to observe the power on self-test results and setup the switch, if required, as described later in this chapter.

The BayStack 450 switch also has an Uplink/Expansion slot that allows you to attach optional media dependent adapters (MDAs). The MDAs support a range of media types (see Appendix B, “Media Dependent Adapters (MDAs)” for more information about MDA types available from Bay Networks).



Note: Refer to the documentation that came with your specific MDA for information about its cabling and LED indications.

Depending on your network configuration requirements, you connect the RJ-45 port cables, the console port, and any optional MDA port cables.

After attaching the devices to the BayStack 450 switch, proceed to [“Connecting Power”](#) on [page 2-9](#) to connect the AC power cord and power up the switch.

You can connect the BayStack 450 switch to any equipment that conforms to the IEEE 802.3 standard, such as the following devices:

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

The F Dx LED on the LED display panel indicates whether the switch is operating in half- or full-duplex mode. When the F Dx LED is on, the port is operating in full-duplex mode (meaning the port is operating at either 20 Mb/s or at 200 Mb/s, depending on the connecting device). When the F Dx LED is off, the port is operating in half-duplex mode, which is 10 Mb/s or 100 Mb/s.

For more information about half-duplex and full-duplex modes, see “10BASE-T/100BASE-TX Port Connectors” on page 1-3.

For more information on autonegotiation, see “Autosensing and Autonegotiation” on page 1-12. For troubleshooting possible related problems, see “Autonegotiation Modes” on page 4-5.

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

The BayStack 450 switch 10BASE-T/100BASE-TX ports are configured with RJ-45 connectors that are wired as MDI-X ports. As in conventional Ethernet repeater hubs, the BayStack 450 switch ports connect via straight-through cables to the network interface card (NIC) in a node or server. When connecting to an Ethernet hub or to another switch, you must use a crossover cable. See Appendix D, “Connectors and Pin Assignments,” for more information.



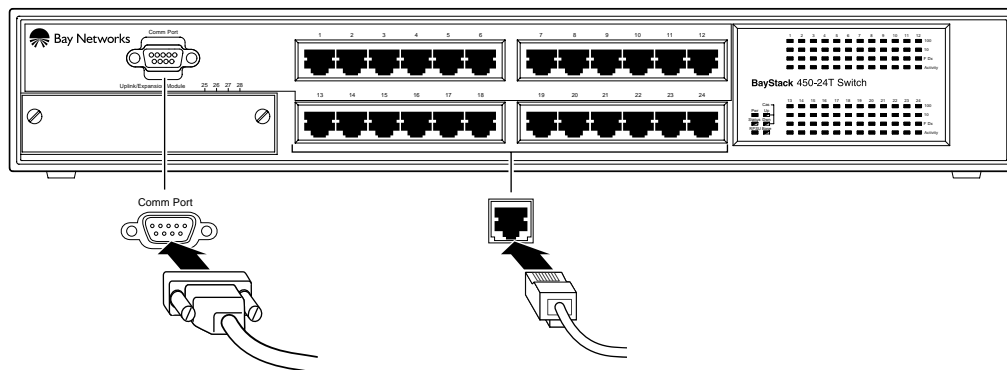
Note: By default, all BayStack 450 switch 10BASE-T/100BASE-TX switch ports are set with the autonegotiation feature enabled. This feature allows any port to match the best service provided by the connected station, up to 100 Mb/s in full-duplex mode.

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



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

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



8537EA

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

Connecting the Console/Comm Port

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

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

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

The terminal should have the following settings:

- 9600 baud
 - No parity
 - 8 bits
 - 1 stop bit
 - Window Terminal Emulator option set to NO
 - Terminal Preferences: Function, Arrow, and Control keys active
 - Buffer size set to 24
- A UL-listed straight-through RS-232 cable with a female DB-9 connector for the console port on the switch

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

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

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

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

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

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

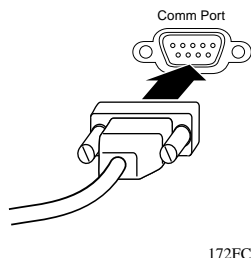


Figure 2-6. Connecting to the Console/Comm Port

4. **Connect the other end of the cable to a terminal or the serial connector of a personal computer running communications software.**
5. **Proceed to the next section, “[Connecting Power](#),” to connect the AC power cord and power up the BayStack 450 switch.**

Connecting Power

The BayStack 450 switch does not have a power on/off switch. When you connect the AC power cord to a suitable AC power outlet, the switch powers up immediately.



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

To connect the AC power cord, follow these steps:

1. Plug one end of the AC power cord into the AC power receptacle on the switch back panel ([Figure 2-7](#)).

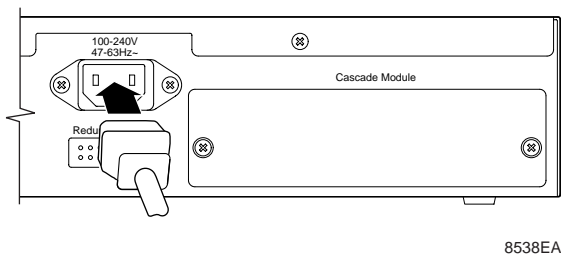


Figure 2-7. BayStack 450 Switch AC Power Receptacle

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

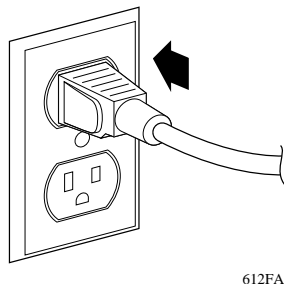


Figure 2-8. Grounded AC Power Outlet

3. Proceed to the next section, [“Verifying the Installation,”](#) to verify proper operation.

Verifying the Installation

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

You can verify proper operation of the BayStack 450 switch by observing the front-panel LEDs or by viewing the self-test results as displayed in the BayStack 450 switch Self-Test screen.

Verifying the Installation Using the LEDs

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

Table 2-1. Power-Up Sequence

Stage	Description	LED indication
1	Immediately after AC power is applied to the switch, DC power is available to the switch's internal circuitry.	<p>The Power LED turns on within 5 seconds (Figure 2-9).</p> <p>If the Power LED does not turn on, verify that power is available at the AC power outlet and that the power cable is fastened securely at both ends.</p> <p>If the Power LED remains off, contact the sales agent or the customer service representative from whom you purchased the switch.</p>
2	The switch initiates a self-test.	<p>As subroutines are initiated by the self-test, the port status LEDs flash various patterns. When the switch passes the self-test (within 10 seconds), the Status LED turns on (Figure 2-9).</p> <p>If a nonfatal error occurs during the self-test, the Status LED blinks.</p> <p>If the switch fails the self-test, the Status LED remains off. Contact the sales agent or the customer service representative from whom you purchased the switch.</p>

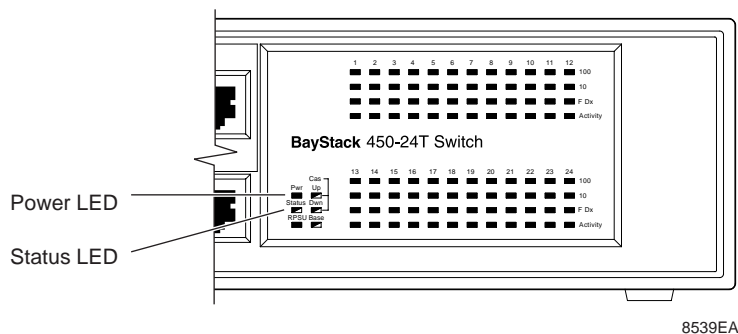


Figure 2-9. Observing LEDs to Verify Proper Operation

Verifying the Installation Using the Self-Test Screen

If a monitor is connected to the switch (see [“Connecting the Console/Comm Port”](#) on [page 2-8](#)), you can observe the BayStack 450 switch Self-Test screen ([Figure 2-10](#)).

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



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

```
BayStack 450-24T Self-Test

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

Self-test complete.
```

Figure 2-10. BayStack 450 Switch Self-Test Screen

```
*****
* Bay Networks, Inc. *
* Copyright (c) 1996,1998 *
* All Rights Reserved *
* BayStack 450-24T *
* Versions: HW:RevA FW:V1.00 SW:V1.0.0.0 *
*****
```

Enter Ctrl-Y to begin.

Figure 2-11. Bay Networks Logo Screen

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

To access the BayStack 450 Main Menu, press [Ctrl]-Y.

Initial Setup of the BayStack 450 Switch

In most cases the BayStack 450 switch can be installed and made operational using the system default settings (see Appendix E, “Default Settings” for a list of default setting for the BayStack 450 switch).

The BayStack 450 switch is designed for plug-and-play operation; however, certain parameters must be configured for the switch management function to become fully operational. A minimal configuration is required when you plan on remote management or TFTP operations.

In that case, you need to enter the IP address of the switch, the subnet mask, and the gateway address (refer to Chapter 3, “Using the Console Interface” for more information about configuring your BayStack 450 switch).

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

1. **Apply power to the switch.**
2. **After the Self-Test screen displays, press [Ctrl]-Y.**

The Main Menu is displayed ([Figure 2-12](#)). The Main Menu hierarchy is described in “Chapter 3, “Using the Console Interface.”

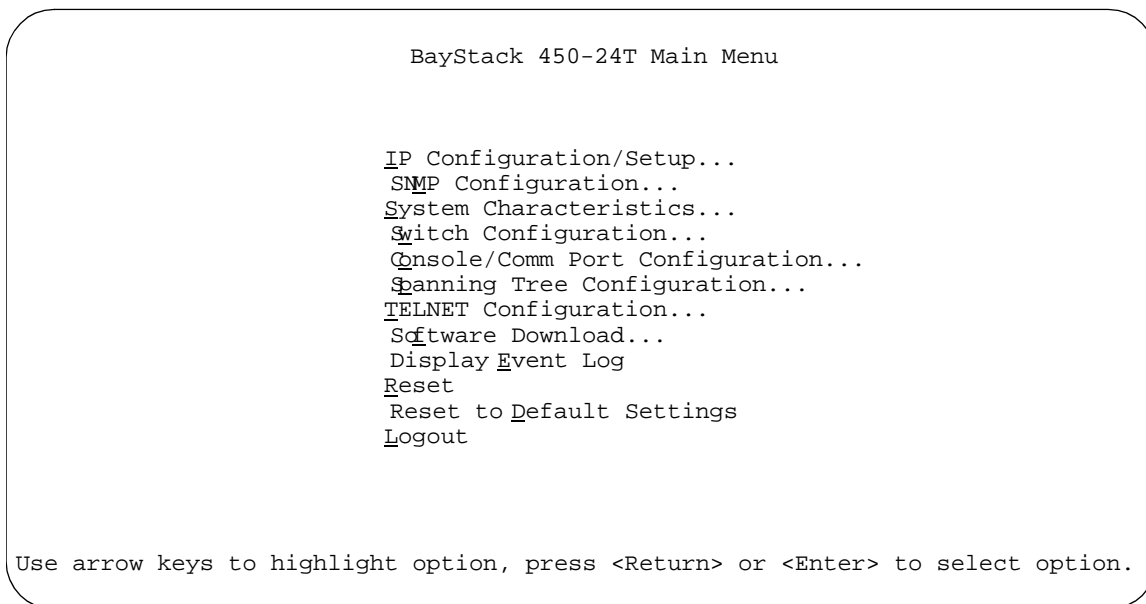


Figure 2-12. Main Menu

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

This selection displays the IP Configuration/Setup screen ([Figure 2-13](#)).



Note: The IP interface of the BayStack 450 switch is *only* on VLAN 1. You can manage the switch *only* from VLAN 1 (or via routers that connect VLAN 1 to the network management station).

```
IP Configuration/Setup

BootP Request Mode:  [ BootP When Needed      ]

                Configurable          In Use          Last BootP
                -----          -----          -----
-
In-Band IP Address:  [ 0.0.0.0 ]          0.0.0.0          0.0.0.0
In-Band Subnet Mask: [ 0.0.0.0 ]          0.0.0.0          0.0.0.0
Default Gateway:    [ 0.0.0.0 ]          0.0.0.0          0.0.0.0

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

Figure 2-13. IP Configuration/Setup Screen

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



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.

Chapter 3

Using the Console Interface

This chapter describes how to configure and manage the BayStack 450 switch using the menu-driven console interface (CI).

This chapter includes the following information:

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

Accessing the CI Menus and Screens

You can access the CI menus and screens through the Console/Comm port located on the switch front-panel (see “Connecting the Console/Comm Port” on page 2-8).

You can also manage the BayStack 450 switch using Bay Networks Optivity network management software or any generic SNMP-based management software; however, certain parameters (such as the switch IP address) must be configured for the switch management function to become fully operational (see “Initial Setup of the BayStack 450 Switch” on page 2-13).



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

For information about SNMP, see your network management documentation.

Using the CI Menus and Screens

The CI menus and screens provide options that allow you to configure and manage the BayStack 450 switch. Help prompts at the bottom of each menu and screen explain how to enter data in the highlighted field and how to navigate the menus and screens.

Some options allow you to toggle between several possible settings; other options allow you to set or modify a parameter.

Navigating the CI Menus and Screens

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

- To select a menu option:
 - a. Use the arrow keys to highlight the option name.
 - b. Press Enter.

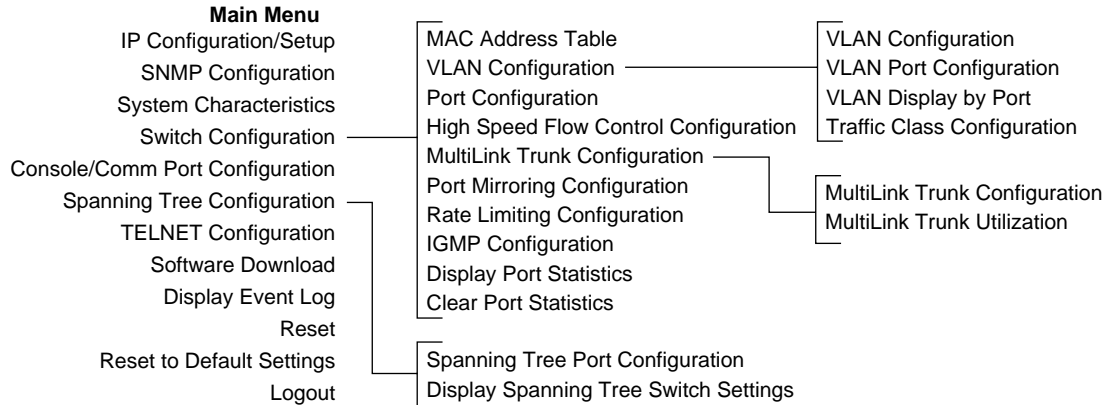
The option takes effect immediately after you press Enter.

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

- To toggle between settings in a form:
 - a. Use the spacebar to highlight the setting.
 - b. Press Enter.
- To clear a string field:
 - a. Position the cursor in the string field.
 - b. Press [Ctrl]-K.
- To return to the previous menu, press [Ctrl]-R.
- To return to the main menu at any time, press [Ctrl]-C.
- Press [Backspace] to delete entered text.

Screen Fields and Descriptions

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



614EC

Figure 3-1. Map of Console Interface Screens

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



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

Main Menu

This section describes the options available from the CI main menu ([Figure 3-2](#)). The CI screens and submenus for these options are described in the following sections.

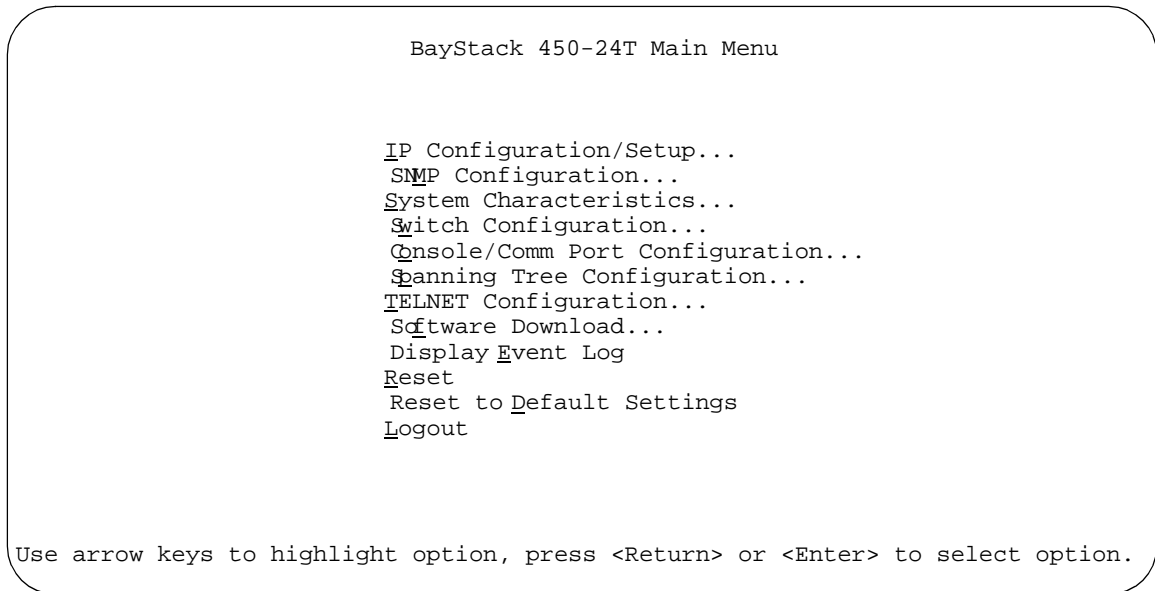


Figure 3-2. Console Interface Main Menu

[Table 3-1](#) describes the CI main menu options.

Table 3-1. Console Interface Main Menu options

Option	Description
IP Configuration/Setup...	Displays the IP Configuration/Setup screen (see " IP Configuration/Setup " on page 3-7). This screen allows you to set or modify IP configuration parameters.
SNMP Configuration...	Displays the SNMP Configuration screen (see " SNMP Configuration " on page 3-12). This screen allows you to set or modify the SNMP read-only community and read-write community strings, enable or disable the authentication trap, set the IP address of trap receivers, and set the trap community strings.


(continued)

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

Option	Description
System Characteristics...	Displays the System Characteristics screen (see “System Characteristics” on page 3-14). This screen allows you to view switch characteristics, including number of resets, power status, and the hardware and firmware version. This screen also contains three user-configurable fields: sysContact, sysName, and sysLocation.
Switch Configuration...	Displays the Switch Configuration Menu screen (see “Switch Configuration” on page 3-16). This menu provides the following configuration options: MAC Address Table, VLAN Configuration, Port Configuration, High speed Flow Control Configuration (only when a gigabit MDA is installed), MultiLink Trunk Configuration, Port Mirroring Configuration, Rate Limiting Configuration, IGMP Configuration, Display Port Statistics, and Clear All Port Statistics.
Console/Comm Port Configuration...	Displays the Console/Comm Port Configuration screen (see “Console/Comm Port Configuration” on page 3-55). This screen allows you to configure and modify the console/Comm port parameters, including the console port speed and password settings.
Spanning Tree Configuration...	Displays the Spanning Tree Configuration Menu (see “Spanning Tree Configuration” on page 3-57). This menu provides the following configuration options: Spanning Tree Port Configuration, Display Spanning Tree Switch Settings.
TELNET Configuration...	Displays the TELNET Configuration screen (see “TELNET Configuration” on page 3-65). This screen allows you to set your switch to enable a user at a remote console terminal to communicate with the BayStack 450 switch as if the console terminal were directly connected to it. You can have up to four active TELNET sessions at one time.
Software Download...	Displays the Software Download screen (see “Software Download” on page 3-68). This screen allows you to revise the BayStack 450 switch software image that is located in nonvolatile flash memory.
Display Event Log	Displays the Event Log screen (see “Display Event Log” on page 3-71).
Reset	Resets the switch with the current configuration settings. This option is followed by a screen prompt that precedes the action. Enter Yes to reset the switch; enter No to abort the option. When you select this option, the switch resets, runs a self-test, then displays the Bay Networks logo screen. Press [Ctrl]-Y to access the BayStack 450 Main Menu.

(continued)

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

Option	Description
Reset to Default Settings	Resets the switch to the factory default configuration settings. This option is followed by a screen prompt that precedes the action. Enter Yes to reset the switch to the factory default configuration settings; enter No to abort the option.
	Caution: If you choose the Reset to Default Settings option, all of your configured settings will be replaced with factory default settings when you press Enter.
Logout	When you select this option, the switch resets, runs a self-test, then displays the Bay Networks logo screen. Press [Ctrl]-Y to access the BayStack 450 Main Menu. The Logout option allows a user in a TELNET session or a user working at a password-protected console terminal to terminate the session (see "Logout" on page 3-78).

IP Configuration/Setup

The IP Configuration/Setup screen ([Figure 3-3](#)) allows you to set or modify the BayStack 450 switch IP configuration parameters. Data that you enter in the user-configurable fields takes effect as soon as you press Enter.

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



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

```

IP Configuration/Setup

BootP Request Mode: [ BootP When Needed ]

                Configurable          In Use          Last BootP
-----
In-Band IP Address: [ 0.0.0.0 ]      0.0.0.0          0.0.0.0
In-Band Subnet Mask: [ 0.0.0.0 ]      0.0.0.0          0.0.0.0
Default Gateway:    [ 0.0.0.0 ]      0.0.0.0          0.0.0.0

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

```

Figure 3-3. IP Configuration/Setup Screen

[Table 3-2](#) describes the IP Configuration/Setup screen fields.

Table 3-2. IP Configuration/Setup Screen Fields

Field	Description
BootP Request Mode	One of four modes of operation for BootP. (See “Choosing a BootP Request Mode” on page 3-9 for details about the four modes.) Default Value BootP When Needed Range BootP When Needed, BootP Always, BootP Disabled, BootP or Last Address
Configurable	Column header for the user-configurable fields in this screen.
In Use	Column header for the read-only fields in this screen. The read-only data displayed in this column represents data that is currently in use.
Last BootP	Column header for the read-only fields in this screen. The read-only data displayed in this column represents data obtained from the last BootP reply received.
In-Band IP Address	The in-band IP address of the BayStack 450 switch. Default Value 0.0.0.0 (no IP address assigned) Range Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
In-Band Subnet Mask	The subnet address mask associated with the in-band IP address shown on the screen. Network routers use the subnet mask to determine the network or subnet address portion of a host's IP address. The bits in the IP address that contain the network address (including the subnet) are set to 1 in the address mask, and the bits that contain the host identifier are set to 0. Default Value 0.0.0.0 (no subnet mask assigned) Range Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
Default Gateway	The IP address of the default gateway. Default Value 0.0.0.0 (no IP address assigned) Range Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point

Choosing a BootP Request Mode

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

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



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

BootP When Needed

Allows the switch to request an IP address if one has not already been set from the console terminal.

When selected, this mode operates as follows:

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

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

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

BootP Always

Allows the switch to be managed only when configured with the IP address obtained from the BootP server.

When selected, this mode operates as follows:

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

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

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

BootP Disabled

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

When selected, this mode operates as follows:

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

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

BootP or Last Address

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

When selected, this mode operates as follows:

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

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

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

SNMP Configuration

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

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

```
SNMP Configuration

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

Trap #1 IP Address:         [ 0.0.0.0 ]
      Community String:     [   ]
Trap #2 IP Address:         [ 0.0.0.0 ]
      Community String:     [   ]
Trap #3 IP Address:         [ 0.0.0.0 ]
      Community String:     [   ]
Trap #4 IP Address:         [ 0.0.0.0 ]
      Community String:     [   ]

Authentication Trap:       [ Enabled ]

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

Figure 3-4. SNMP Configuration Screen

[Table 3-3](#) describes the SNMP Configuration screen fields.

Table 3-3. SNMP Configuration Screen Fields

Field	Description
Read-Only Community String	The community string used for in-band read-only SNMP operations. Default Value public Range Any ASCII string of up to 32 printable characters
Read-Write Community String	The community string used for in-band read-write SNMP operations. Default Value private Range Any ASCII string of up to 32 printable characters
Trap #1 IP Address¹	Number one of four trap IP addresses. Successive trap IP address fields are numbered 2, 3, and 4. Each trap address has an associated community string (see Community String). Default Value 0.0.0.0 (no IP address assigned) Range Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
Community String	The community string associated with one of the four trap IP addresses (see Trap #1 IP Address). Default Value Zero-length string Range Any ASCII string of up to 32 printable characters
Authentication Trap	Determines whether a trap will be sent when there is an SNMP authentication failure. Default Value Enabled Range Enabled, Disabled

¹ The Trap IP Address and Community String fields can be set using a MIB table (in a Bay Networks proprietary MIB). The status of the row in the MIB table can be set to Ignore. If the row status is set to Ignore, the fields appear to be set when viewed from the console terminal; however, no traps will be sent to that address until the row status is set to Valid.

System Characteristics

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

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

```
System Characteristics

MAC Address:      00-60-FD-77-A1-AC
Reset Count:     9
Last Reset Type: Software Download
Power Status:    Primary Power

sysDescr:        BayStack 450-24T HW:RevA  FW:V1.00 SW:V1.0.0.0
sysObjectID:     1.3.6.1.4.1.45.3.35.2
sysUpTime:       02:20:06
sysServices:     3
sysContact:      [ Mario Lento ]
sysName:         [ Documentation ]
sysLocation:     [ Building 5, Floor 10 ]

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

Figure 3-5. System Characteristics Screen

[Table 3-4](#) describes the System Characteristics screen fields.

Table 3-4. System Characteristics Screen Fields

Field	Description
MAC Address	The MAC address of the BayStack 450 switch.
Reset Count	A read-only field that indicates the number of resets since the operational firmware was first loaded on the switch. Default Value 1 Range 0 to 2 ³² -1
Last Reset Type	A read-only field that indicates the last type of reset. Default Value Power Cycle Range Power Cycle, Software Download, Management Reset, Management Factory Reset
Power Status	A read-only field that indicates the current power source (primary, RPSU, or both). Default Value Primary Power Range Primary Power, Redundant Power, Primary and Redundant Power
sysDescr	A read-only field that specifies the hardware and software version.
sysObjectID	A read-only field that provides a unique identification of the switch, which contains the vendor's private enterprise number.
sysUpTime	A read-only field that shows the length of time since the last reset. Note that this field is updated when the screen is redisplayed.
sysServices	A read-only field that indicates the switch's physical and data link layer functionality.
sysContact	The name and phone number of the person responsible for the switch. Default Value Zero-length string Range Any ASCII string of up to 56 printable characters ¹
sysName	A name that uniquely identifies the switch. Default Value Zero-length string Range Any ASCII string of up to 56 printable characters ¹
sysLocation	The physical location of the switch. Default Value Zero-length string Range Any ASCII string of up to 56 printable characters

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

Switch Configuration

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



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

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

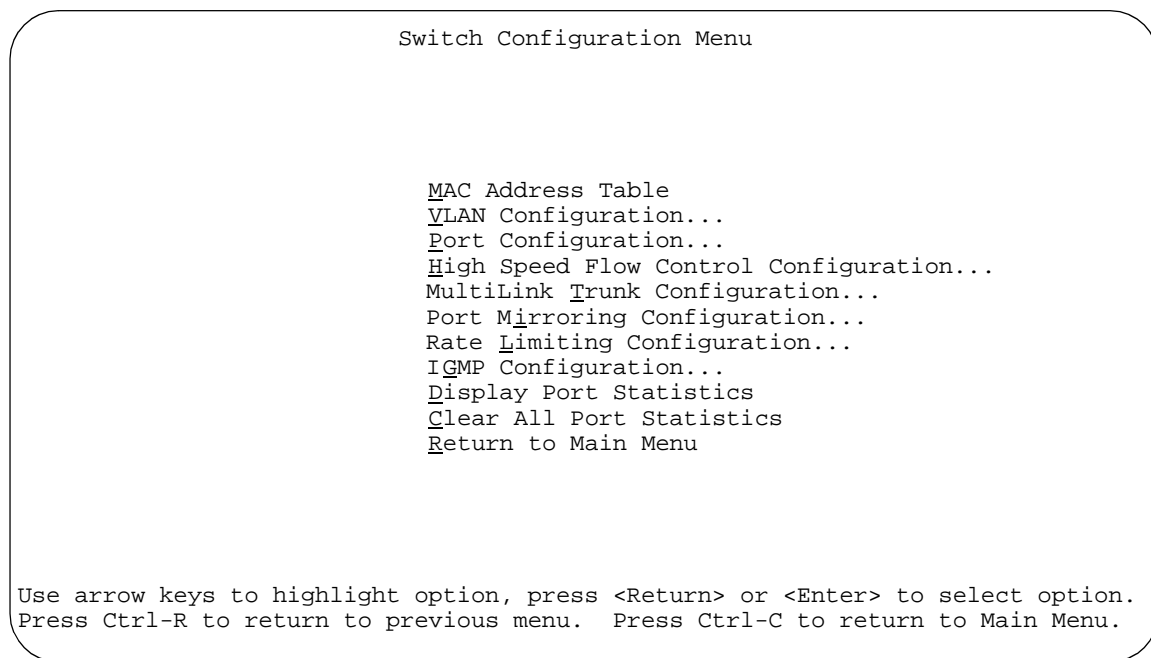


Figure 3-6. Switch Configuration Menu Screen

[Table 3-5](#) describes the Switch Configuration Menu screen options.

Table 3-5. Switch Configuration Menu Screen Options

Option	Description
MAC Address Table	Displays the MAC Address Table screen (see “MAC Address Table” on page 3-18). This screen allows you to view all MAC addresses and their associated port or trunk that the switch has learned, or to search for a particular MAC address (to see if the switch has learned the address).
VLAN Configuration...	Displays the VLAN Configuration Menu (see “VLAN Configuration Menu” on page 3-20). This menu provides the following options: VLAN Configuration, VLAN Port Configuration, VLAN Display by Port, Traffic Class Configuration, and Return to Switch Configuration Menu screen. This menu allows you to create and modify VLANs.
Port Configuration...	Displays the Port Configuration screen (see “Port Configuration” on page 3-30). This screen allows you to configure a specific switch port or all switch ports.
High Speed Flow Control Configuration...	This menu selection only appears when an optional gigabit MDA is installed in the Uplink Module slot. When the gigabit MDA is installed, selecting this option displays the High Speed Flow Control Configuration screen (see “High Speed Flow Control Configuration” on page 3-32).
MultiLink Trunk Configuration...	Displays the MultiLink Trunk Configuration Menu (see “MultiLink Trunk Configuration” on page 3-35). This menu provides the following options: MultiLink Trunk Configuration, MultiLink Trunk Utilization, and Return to Switch Configuration Menu screen. This menu allows you to create and modify trunks, and to monitor the bandwidth utilization of configured trunks.
Port Mirroring Configuration...	Displays the Port Mirroring Configuration screen (see “Port Mirroring Configuration” on page 3-42). This screen allows you to designate a single switch port as a traffic monitor for up to two specified ports or addresses.
Rate Limiting Configuration...	Displays the Rate Limiting Configuration screen (see “Rate Limiting Configuration” on page 3-45). This screen allows you to limit the forwarding rate of broadcast and multicast packets.
IGMP Configuration...	Displays the IGMP Configuration screen (see “IGMP Configuration” on page 3-48). This screen allows you to optimize multicast traffic by setting up IGMP port memberships that filter multicast on a per port basis (see “IGMP Snooping” on page 1-35 for more information about this feature).

(continued)

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

Option	Description
Display Port Statistics	Displays the Port Statistics screen (see “Port Statistics” on page 3-51). This screen allows you to view detailed information about any switch port.
Clear All Port Statistics	Allows you to clear all port statistics for all switch ports. This option is followed by a screen prompt that precedes the action. Enter Yes to clear all port statistics; enter No to abort the option.
Return to Main Menu	Exits the Switch Configuration Menu screen and displays the main menu.

MAC Address Table

The MAC Address Table screen ([Figure 3-7](#)) allows you to view MAC addresses that the switch has learned or to search for a specific MAC address.

The MAC Address screen also operates in conjunction with the Port Mirroring Configuration screen. When you configure a switch for MAC address-based port mirroring, you can use the MAC Address Table screen to find an address, and enter the address directly from this screen. You can enter addresses from either screen, but you must return to the Port Mirroring Configuration screen to activate the feature (see [“Port Mirroring Configuration”](#) on [page 3-42](#)).

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



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

```

MAC Address Table

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

00-60-FD-00-02-30
00-00-A2-85-BB-26      Port: 1
00-60-FD-12-02-15      Port: 1
00-08-C7-1D-4F-38      Trunk:3

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

```

Figure 3-7. MAC Address Table Screen

[Table 3-6](#) describes the MAC Address Table screen fields.

Table 3-6. MAC Address Table Screen Fields

Field	Description
Aging Time	Specifies how long a learned MAC address remains in the switch's forwarding database. If an entry is inactive for a period of time that exceeds the specified aging time, the address is removed. Default Value 300 seconds Range 10 to 1,000,000 seconds
Find an Address	Allows the user to search for a specific MAC address. Default Value 00-00-00-00-00-00 (no MAC address assigned) Range 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF

(continued)

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

Field	Description
Port Mirroring Address A	<p>This field only appears when any of the five <i>address-based</i> monitoring modes are selected from the Port Mirroring Configuration screen. When you enter a MAC address in this field, it is also configured into the Port Mirroring Configuration screen. Conversely, when you enter the MAC address from the Port Mirroring Configuration screen, it also displays in this screen. See “Port Mirroring Configuration” on page 3-42 for more information.</p> <p>Default Value 00-00-00-00-00-00 (no MAC address assigned)</p> <p>Range 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF</p>
Port Mirroring Address B	<p>This field only appears when any of the two <i>address-based</i> monitoring modes that use Address B are selected from the Port Mirroring Configuration screen. When you enter a MAC address in this field, it is also configured into the Port Mirroring Configuration screen. Conversely, when you enter the MAC address from the Port Mirroring Configuration screen, it also displays in this screen. See “Port Mirroring Configuration” on page 3-42 for more information.</p> <p>Default Value 00-00-00-00-00-00 (no MAC address assigned)</p> <p>Range 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF</p>

VLAN Configuration Menu

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

See “IEEE 802.1Q VLAN Workgroups” on page 1-19, for detailed information about configuring VLANs.

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

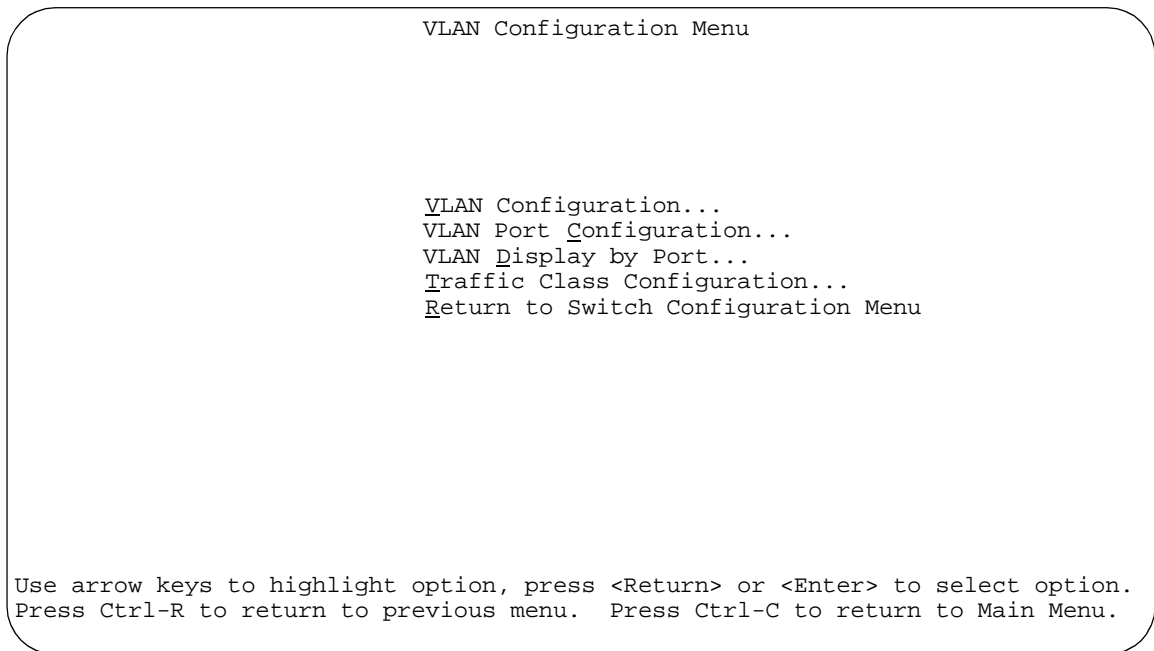


Figure 3-8. VLAN Configuration Menu Screen

[Table 3-7](#) describes the VLAN Configuration Menu screen options.

Table 3-7. VLAN Configuration Menu Screen Options

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

VLAN Configuration

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

VLAN port members can be assigned attributes that allow the individual ports to operate in accordance with the IEEE 802.1Q tagging rules. You can assign each VLAN port member as *tagged* or *untagged* port members (see “IEEE 802.1Q Tagging” on page 1-20, for a description of important terms used with 802.1Q VLANs).

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

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

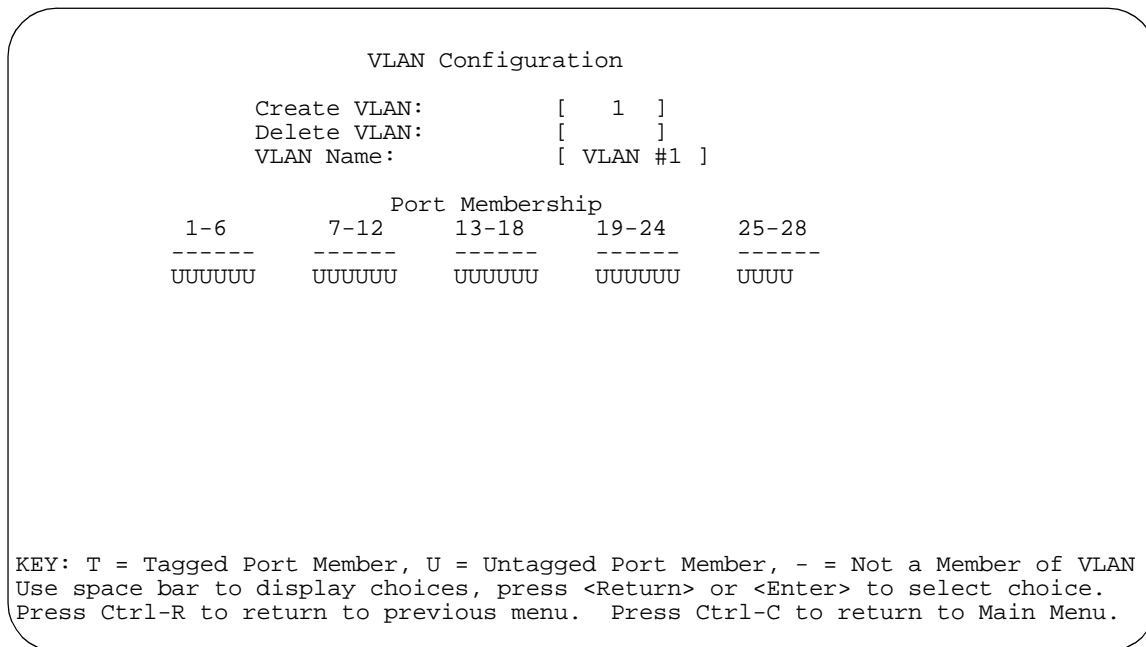


Figure 3-9. VLAN Configuration Screen

[Table 3-8](#) describes the VLAN Configuration screen fields.

Table 3-8. VLAN Configuration Screen Fields

Field	Description
Create VLAN	<p>Allows you to set up or view configured VLAN workgroups. Enter the number of the new VLAN you want to create or view, then press [Return]. The Port Membership fields indicate the corresponding VLAN workgroup configuration, if configured, or all dashes (-), indicating no VLAN Members configured. Alternatively, you can use the space bar to toggle through the various configured VLAN workgroups. You can only create up to 64 different VLANs.</p> <p>Default 1</p> <p>Range 1 to 4094</p>
Delete VLAN	<p>Allows you to delete specified VLANs. Enter the number of the VLAN you want to delete, then press [Return], or use the space bar to toggle through the selection until you reach the VLAN you want to delete, then press [Return].</p> <p>The selected VLAN is deleted as soon as you press [Return]. The software does not prompt you to reconsider this action.</p> <p>You cannot delete VLAN 1. By default, all switch ports are assigned as untagged members of VLAN 1 with all ports configured as PVID = 1). See “IEEE 802.1Q VLAN Workgroups” on page 1-19 for more information.</p> <p>Default blank field</p> <p>Range 2 to 4094</p>
VLAN Name	<p>Allows you to assign a name field to configured VLANs.</p> <p>Default VLAN # (<i>VLAN number</i>)</p> <p>Range Any ASCII string of up to 16 printable characters</p>
Port Membership	<p>Allows you to assign switch ports as a tagged port member (T), untagged port member (U), or as a non-VLAN port member (-). Switch ports can be configured in one or more VLANs. An exception to this rule applies to the gigabit MDAs (see note).</p> <hr/> <p>Note: The gigabit MDAs restrict the configuration of VLAN tagging. The gigabit MDA ports can be set up as tagged VLAN members or as untagged VLAN members for a VLAN that has a VID which is equal to the port’s PVID. For all other VLANs configured on that port the VLAN port membership will be <i>all tagged</i> or <i>all untagged</i> (see “VLAN Port Configuration” on page 3-24).</p> <hr/> <p>The Port Membership fields are displayed in six-port groups (for example, 1-6, 7-12, 13-18). The number of ports displayed depends on the switch model or type of optional MDA installed in the Uplink Module slot.</p> <p>Default U (All ports are assigned as untagged members of VLAN 1.)</p> <p>Range U, T, and -</p>

VLAN Port Configuration

The VLAN Port Configuration screen ([Figure 3-10](#)) allows you to configure specified switch ports with the appropriate PVID/VLAN association that enables the creation of broadcast domains (see “Shared Servers” on page 1-26 for more information about setting up broadcast domains). You can configure specified switch ports to filter (discard) all received tagged frames, untagged frames, or unregistered frames (see “IEEE 802.1Q Tagging” on page 1-20). You can also prioritize the order in which the switch forwards packets, on a per-port basis (see “IEEE 802.1p Prioritizing” on page 1-40).

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

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

```
VLAN Port Configuration

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

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

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

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

Figure 3-10. VLAN Port Configuration Screen

[Table 3-9](#) describes the VLAN Port Configuration screen fields.

Table 3-9. VLAN Port Configuration Screen Fields

Field	Description
Port	Allows you to select the number of the port you want to view or configure. To view another port, type its port number and press Enter, or press the spacebar on your keyboard to toggle the port numbers.
Filter Tagged Frames	Allows you to set this port to filter (discard) all received tagged packets. Default No Range No, Yes
Filter Untagged Frames	Allows you to set this port to filter (discard) all received untagged packets. Default No Range No, Yes
Filter Unregistered Frames	Allows you to set this port to filter (discard) all received unregistered packets. Default No Range No, Yes
Port Name	Allows you to assign a name to this port. Default Port # (<i>port number</i>) Range Any ASCII string of up to 16 printable characters
PVID	Port VLAN identifier field. Allows you to associate this port with a specific VLAN. For example, a port with a PVID of 3 assigns all untagged frames received on this port to VLAN 3. Default 1 Range 1 to 4094
Port Priority	Allows you to prioritize the order in which the switch forwards packets received on specified ports (see “IEEE 802.1p Prioritizing” on page 1-40). Default 0 Range 0 to 7

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

(continued)

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

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

Assigning Tagging to Gigabit MDA Ports



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

This section shows how a user could assign the gigabit MDA port (port 25 shown in [Figure 3-10](#)) as a Tagged VLAN member. In this example, the MDA port in the example is configured with a PVID of 1. This means that the port-to-VLAN association for port 25 is VLAN 1 (see “IEEE 802.1Q Tagging” on page 1-20). If the PVID for port 25 is changed to another number (for example, PVID 7), port 25 becomes associated with VLAN 7. This is important to note because the rules applying to the gigabit MDA configuration only allow for one (primary) VLAN for the gigabit port. All other VLANs configured on that port are considered secondary VLANs, and the *secondary* VLAN memberships can only be *all* tagged or *all* untagged.

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

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

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

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

VLAN Display by Port

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

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

```

                                VLAN Display by Port
                                Port:           [ 1 ]
                                PVID:          1
                                Port Name:     Port #1

    VLANs      VLAN Name          VLANs      VLAN Name
    -----
    1          VLAN #1
  
```

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

Figure 3-11. VLAN Display by Port Screen

[Table 3-10](#) describes the VLAN Display by Port screen fields.

Table 3-10. VLAN Display by Port Screen Fields

Field	Description
Port	Allows you to select the number of the port you want to view. To view another port, type its port number and press Enter, or press the spacebar on your keyboard to toggle the port numbers.
PVID	Read-only field that indicates the PVID setting for the specified port.
Port Name	Read-only field that indicates the port name assigned to the specified port.
VLANs	Column header for the read-only fields listing the VLANs associated with the specified port.
VLAN Name	Column header for the read-only fields listing the VLAN Names associated with the specified port.

Traffic Class Configuration

The Traffic Class Configuration screen ([Figure 3-12](#)) allows you to assign a Low or High traffic classification to any of eight (0 to 7) user_priority values assigned to a received frame on specified switch ports.

See “IEEE 802.1p Prioritizing” on page 1-40 for more information about this screen.

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

```

                                Traffic Class Configuration

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

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

```

Figure 3-12. Traffic Class Configuration Screen

[Table 3-11](#) describes the Traffic Class Configuration screen fields.

Table 3-11. Traffic Class Configuration Screen Fields

Field	Description
User Priority	Column header for the read-only fields that indicate the user-priority values from priority 0 to priority 7. These values are derived from the three-bit field in the header of 802.1Q tagged frames (see “IEEE 802.1Q Tagging” on page 1-20).
Traffic Class	Column header for the eight user-configurable fields that correspond to the adjacent user priority levels.
	Default Low
	Range Low, High

Port Configuration

The Port Configuration screen ([Figure 3-13](#) and [Figure 3-14](#)) allows you to configure a specific switch port or all switch ports. You can set the switch ports to autonegotiate for the highest available speed of the connected station, or you can set the speed for selected switch ports.

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



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

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

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

More...

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

Figure 3-13. Port Configuration Screen (1 of 2)

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

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

Figure 3-14. Port Configuration Screen (2 of 2)



Note: When a gigabit MDA is installed, only the Status field for that MDA port is configurable. See [“High Speed Flow Control Configuration”](#) on [page 3-32](#) to set the autonegotiation field for the gigabit MDA port. The gigabit MDA only supports 1000 Mb/s in full-duplex mode.

[Table 3-12](#) describes the Port Configuration screen fields.

Table 3-12. Port Configuration Screen Fields

Field	Description
Port	Indicates the switch port numbers that correspond to the field settings in that row of the screen (for example, the field settings in row 2 apply to switch port 2). Note that the settings applied in the All row (bottom row) affect all switch ports (except the gigabit MDA port, when installed).

(continued)

Table 3-12. Port Configuration Screen Fields (*continued*)

Field	Description
Trunk	The read-only data displayed in this column indicates the trunk (1 to 4) that corresponds to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen (see “MultiLink Trunk Configuration” on page 3-35).
Status	Allows you to disable any of the switch ports. You can also use this field to control access to any switch port. Default Value Enabled Range Enabled, Disabled
Link	A read-only field that indicates the current link state of the corresponding port, as follows: <ul style="list-style-type: none"> • Up: The port is connected and operational. • Down: The port is not connected or is not operational.
Autonegotiation	When enabled, sets the corresponding port speed to match the best service provided by the connected station, up to 100 Mb/s in full-duplex mode. This field is disabled for all fiber optic ports. Default Value Enabled Range Enabled, Disabled
Speed/Duplex	Allows you to manually configure any port to support an Ethernet speed of 10 Mb/s or 100 Mb/s, in half- or full-duplex mode. This field is set (by default) to 1000 Mb/s, full-duplex for gigabit MDA ports only. Default Value 100Mbps/Half (when Autonegotiation is Disabled) Range 10Mbps/Half, 10Mbps/Full, 100Mbps/Half, 100Mbps/Full

High Speed Flow Control Configuration

The High Speed Flow Control Configuration screen ([Figure 3-15](#)) allows you to set the port parameters for installed gigabit MDAs.



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

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


```

High Speed Flow Control Configuration

Autonegotiation:          [ Enabled ]
Flow Control:            [ Disabled ]

Preferred Phy            [ Right ]
Active Phy               None

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

```

Figure 3-15. High Speed Flow Control Configuration Screen

[Table 3-13](#) describes the High Speed Flow Control Configuration screen fields.

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

Field	Description
Autonegotiation	When enabled, the port advertises support for 1000 Mb/s operation, in full-duplex mode. Default Value Enabled Range Enabled, Disabled
Flow Control	Allows you to control traffic and avoid congestion on the gigabit MDA port. Two modes are available (see “Choosing a High Speed Flow Control Mode” on page 3-34 for details about the two modes). Autonegotiation must be disabled for this port when using this feature. Default Value Disabled Range Disabled, Symmetric, Asymmetric

(continued)

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

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

Choosing a High Speed Flow Control Mode

The High Speed Flow Control feature allows you to control traffic and avoid congestion on the gigabit full-duplex link. If the receive port buffer becomes full, the BayStack 450 switch issues a flow-control signal to the device at the other end of the link to suspend transmission. When the receive buffer is no longer full, the switch issues a signal to resume the transmission.

You can choose Symmetric or Asymmetric flow control mode:

Symmetric Mode:

This mode allows both the gigabit MDA port and its link partner to send flow control *pause* frames to each other.

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

Asymmetric:

This mode allows the link partner to send flow control pause frames to the gigabit MDA port. When a pause frame is received, the receiving port suspends transmission of frames for a number of slot times specified in the control frame or until a pause-release control frames is received.

In this mode the gigabit MDA port is disabled from transmitting pause frames to its link partner. This mode can be used if the gigabit MDA port is connected to a buffered repeater device.

MultiLink Trunk Configuration

The MultiLink Trunk Configuration Menu screen ([Figure 3-16](#)) allows you to select the appropriate screen to configure up to six MultiLink trunks. You can group up to four switch ports together to form each trunk, and you can use the trunks to link to another switch or to a server. Bandwidth utilization can be monitored for the trunk member ports within each trunk.

For more information about configuring MultiLink Trunks, see “MultiLink Trunks” on page 1-44.



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

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

```
MultiLink Trunk Configuration Menu
```

```
MultiLink Trunk Configuration...  
MultiLink Trunk Uttilization...  
Return to Switch Configuration Menu
```

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

Figure 3-16. MultiLink Trunk Configuration Menu Screen

[Table 3-14](#) describes the MultiLink Trunk Configuration Menu screen options.

Table 3-14. MultiLink Trunk Configuration Menu Screen Options

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

MultiLink Trunk Configuration Screen

The MultiLink Trunk Configuration screen allows you to configure two to four switch ports together as members of a trunk. Up to six trunks can be created for each BayStack 450 switch. [Figure 3-17](#) shows an example of the MultiLink Trunk Configuration screen. In this screen example (previously discussed on page 1-47), five trunks are shown: one trunk is configured with four trunk members and the remaining four trunks are each configured with two trunk members. When a configured trunk is enabled, the trunk members (the specified switch ports) take on default settings necessary for correct operation of the MultiLink Trunking feature. These default settings can affect the correct operation of your configured network. See “MultiLink Trunks” on page 1-47 for more information.



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

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

```

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

Trunk      Trunk Name
-----
 1 [ S1:T1 to FS2 ]
 2 [ S1:T2 to S2 ]
 3 [ S1:T3 to S2 ]
 4 [ S1:T4 to S3 ]
 5 [ S1:T5 to S4 ]
 6 [ Trunk #6 ]

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

```

Figure 3-17. MultiLink Trunk Configuration Screen

[Table 3-15](#) describes the MultiLink Trunk Configuration screen fields.

Table 3-15. MultiLink Trunk Configuration Screen Fields

Field	Description
Trunk	Column header for the read-only fields in this screen. The read-only data displayed in the Trunk column indicates the trunk (1 to 6) that corresponds to the switch ports specified in the user-configurable Trunk Members fields.
Trunk Members	<p>The Trunk Members column contains fields in each row that can be configured to create the corresponding trunk. Each switch port can only be a member of a single trunk. The appropriate trunk number for each trunk member configured within this field is shown adjacent to the corresponding switch port in the following screens: Port Configuration screen, and Spanning Tree Configuration screen. Gigabit ports cannot be configured as trunk members.</p> <p>Default Value blank field</p> <p>Range 1 to 28 (depending on model type)</p>
STP Learning	<p>The STP Learning column contains a single field for each row that, when enabled, allows the specified trunk to participate in the spanning tree. This setting overrides those of the individual trunk members.</p> <p>Fast is the same as Normal, except that the state transition timer is shortened to two seconds.</p> <p>Default Value Normal</p> <p>Range Normal, Fast, Disabled</p>
Trunk Mode	<p>The Trunk Mode column contains a single read only field for each row that indicates the default operating mode for the switch.</p> <p>Basic: Basic mode is the default mode for the switch. When in this mode, source MAC addresses are dynamically assigned to specific trunk members for flooding and forwarding. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.</p> <p>Default Value Basic</p>
Trunk Status	<p>The Trunk Status column contains a single field for each row that allows users to enable or disable any of the trunks.</p> <p>Default Value Enabled</p> <p>Range Enabled, Disabled</p>
Trunk Name	The Trunk Name column contains a single optional field in each row that can be used to assign names to the corresponding configured trunks. The names chosen for this example can provide meaningful information to the user (for example, S1:T1 to FS2 indicates Trunk 1, in switch S1 connects to File Server 2)

MultiLink Trunk Utilization Screen

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

[Figure 3-18](#) shows an *example* of bandwidth utilization rates for the trunk member ports configured in [Figure 3-17](#). Because two screens are required to show all of the configured trunks (up to six), the screen prompts users to Press [Ctrl]-N to view trunks five and six.

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

MultiLink Trunk Utilization					
Trunk	Traffic Type	Port	Last 5 Minutes	Last 30 Minutes	Last Hour
1	[Rx and Tx]	6	90.0%	70.0%	90.0%
		7	20.0%	55.0%	80.0%
		9	35.0%	45.0%	45.0%
		17	85.0%	35.0%	20.0%
2	[Rx and Tx]	25	45.0%	45.0%	50.0%
		26	25.0%	70.0%	35.0%
3	[Rx and Tx]	13	35.0%	35.0%	50.0%
		14	30.0%	80.0%	70.0%
4	[Rx and Tx]	19	40.0%	35.0%	75.0%
		20	25.0%	70.0%	85.0%

More...

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

Figure 3-18. MultiLink Trunk Utilization Screen (1 of 2)

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

Press Ctrl-P to display utilization for trunks 1-4.
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

Figure 3-19. MultiLink Trunk Utilization Screen (2 of 2)

[Table 3-16](#) describes the MultiLink Trunk Utilization screen fields.

Table 3-16. MultiLink Trunk Utilization Screen Fields

Field	Description
Trunk	Column header for the read-only fields in this screen. The read-only data displayed in this column indicates the trunk (1 to 6) that corresponds to the switch ports specified in the Port field.
Traffic Type	Allows you to choose the traffic type to be monitored for percent of bandwidth utilization (see Range). Default Value Rx and Tx Range Rx and Tx, Rx, Tx
Port	This field lists the trunk member ports that correspond to the trunk specified in the Trunk column.

(continued)

Table 3-16. MultiLink Trunk Utilization Screen Fields *(continued)*

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

Port Mirroring Configuration

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

For more information about the port mirroring feature, see “Port Mirroring (Conversation Steering)” on page 1-62.

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

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

```

Port Mirroring Configuration

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

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

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

Port mirroring configuration has taken effect.

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

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

```

Figure 3-20. Port Mirroring Configuration Screen

[Table 3-17](#) describes the Port Mirroring Configuration screen fields.

Table 3-17. Port Mirroring Configuration Screen Fields

Field	Description
Monitoring Mode	<p>This field allows a user to select any one of six port-based monitoring modes or any one of five address-based monitoring modes (see Table 3-18). Selecting any one of the six <i>port-based modes</i> activates the port X and port Y screen fields, where a user can choose up to two ports to monitor. Selecting any one of the five <i>address-based modes</i> activates the Address A and Address B screen fields, where a user can specify MAC addresses to monitor.</p> <p>Default Value Disabled</p> <p>Range See Table 3-18</p>
Monitor Port	<p>Indicates the switch port designated as the monitor port.</p> <p>Default Value Zero-length string</p> <p>Range 1 to 28 (Model dependent)</p>
Port X	<p>Indicates one of the switch ports that will be monitored by the designated port monitor when one of the port-based monitoring modes is selected. This port will be monitored according to the value X in the Monitoring Mode field (see Table 3-18).</p> <p>Default Value Zero-length string</p> <p>Range 1 to 28 (Model dependent)</p>
Port Y	<p>Indicates one of the switch ports that will be monitored by the designated port monitor when one of the port-based monitoring modes is selected. This port will be monitored according to the value Y in the Monitoring Mode field (see Table 3-18).</p> <p>Default Value Zero-length string</p> <p>Range 1 to 28 (Model dependent)</p>
Address A	<p>Indicates the MAC addresses that will be monitored by the designated port monitor when one of the address-based monitoring modes is selected. This port will be monitored according to the value "Address A" in the selected Monitoring Mode field (see Table 3-18). Users can enter the MAC address from this screen or from the MAC Address Table screen. The entry is displayed and can be modified by either screen (see "MAC Address Table" on page 3-18).</p> <p>Default Value 00-00-00-00-00-00 (no MAC address assigned)</p> <p>Range 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF</p>

(continued)

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

Field	Description
Address B	Indicates the MAC addresses that will be monitored by the designated port monitor when one of the address-based monitoring modes is selected. This port will be monitored according to the value "Address B" in the selected Monitoring Mode field (see Table 3-18). Users can enter the MAC address from this screen or from the MAC Address Table screen. The entry is displayed and can be modified by either screen (see " MAC Address Table " on page 3-18).
Default Value	00-00-00-00-00-00 (no MAC address assigned)
Range	00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF

[Table 3-18](#) describes the various monitoring modes available from the Port Mirroring Configuration screen.

Table 3-18. Monitoring Modes

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

Rate Limiting Configuration

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

[Figure 3-21](#) and [Figure 3-22](#) show sample rate limiting settings for the two Rate Limiting Configuration screens.



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

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

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

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

Figure 3-21. Rate Limiting Configuration Screen (1 of 2)

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

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

Figure 3-22. Rate Limiting Configuration Screen (2 of 2)

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

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

[Table 3-19](#) describes the Rate Limiting Configuration screen fields.

Table 3-19. Rate Limiting Configuration Screen Fields

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

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

IGMP Configuration

The IGMP Configuration screen allows you to set your switch ports to optimize IP multicast packets in a bridged Ethernet environment (see “IGMP Snooping” on page 1-35). [Figure 3-23](#) shows an example of the IGMP Configuration screen with switch ports 8 and 14 set to receive/transmit multicast from the local multicast router. The configured ports are VLAN port members of VLAN 5.

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

```

                                IGMP Configuration

                                VLAN:           [ 5 ]
                                Snooping:        [ Enabled ]
                                Proxy:           [ Enabled ]
                                Robust Value:     [ 2 ]
                                Query Time:      [ 125 seconds ]
                                Set Router Ports: [ Version 1 ]

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

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

```

Figure 3-23. IGMP Configuration Screen

[Table 3-20](#) describes the IGMP Configuration screen fields.

Table 3-20. IGMP Configuration Screen Fields

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

(continued)

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

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

Port Statistics

The Port Statistics screen ([Figure 3-24](#)) allows you to view detailed information about a switch port. The screen is divided into two sections (Received and Transmitted) so that you can compare and evaluate throughput or other port parameters. All screen data is updated approximately every two seconds.

You can use the Port Statistics screen to clear (reset to zero) port counters for a specific port. Alternatively, you can use the Clear All Port Statistics option to clear port counters for all ports (see “[Switch Configuration](#)” on [page 3-16](#)).

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

```

Port: [ 1 ]
                Port Statistics
                -----
                Received                               Transmitted
-----
Packets:                0   Packets:                497
Multicasts:             0   Multicasts:             497
Broadcasts:            0   Broadcasts:            0
Total Octets:          0   Total Octets:          31808
Lost Packets:          0   Lost Packets:          0
FCS Errors:            0   Collisions:            0
Frame Errors:          0   Single Collisions:     0
Undersized Packets:    0   Multiple Collisions:   0
Oversized Packets:     0   Excessive Collisions:  0
Packets 64 bytes:      0   Packets 64 bytes:      497
   65-127 bytes         0       65-127 bytes         0
   128-255 bytes        0       128-255 bytes        0
   256-511 bytes        0       256-511 bytes        0
   512-1023 bytes       0       512-1023 bytes       0
   1024-1518 bytes      0       1024-1518 bytes      0
Filtered Packets:      0   Deferred Packets:      0
Flooded Packets:       0   Late Collisions:       0

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

```

Figure 3-24. Port Statistics Screen

[Table 3-21](#) describes the Port Statistics screen fields.



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

Table 3-21. Port Statistics Screen Fields

Field	Description
Port	Allows you to select the number of the port you want to view or reset to zero. To view another port, type its port number and press Enter, or press the spacebar on your keyboard to toggle the port numbers.
Packets	Received column: Indicates the total number of packets received on this port, including bad packets, broadcast packets, and multicast packets. Transmitted column: Indicates the total number of packets transmitted successfully on this port, including broadcast packets and multicast packets.
Multicasts	Received column: Indicates the total number of good multicast packets received on this port, excluding broadcast packets. Transmitted column: Indicates the total number of multicast packets transmitted successfully on this port, excluding broadcast packets.
Broadcasts	Received column: Indicates the total number of good broadcast packets received on this port. Transmitted column: Indicates the total number of broadcast packets transmitted successfully on this port.
Total Octets	Received column: Indicates the total number of octets of data (including data in bad packets) received on this port, excluding framing bits but including FCS octets. Transmitted column: Indicates the total number of octets of data transmitted successfully on this port, including FCS octets.
Lost Packets	Received column: Indicates the total number of packets lost (discarded) when the capacity of the port receive buffer was exceeded. Transmitted column: Indicates the total number of packets lost (discarded) when the capacity of the port transmit buffer was exceeded.
FCS Errors	Indicates the total number of valid-size packets that were received with proper framing but discarded because of cyclic redundancy check (CRC) errors.
Frame Errors	Indicates the total number of valid-size packets that were received but discarded because of CRC errors and improper framing.

(continued)

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

Field	Description
Undersized Packets	Indicates the total number of packets received on this port with fewer than 64 bytes and with proper CRC and framing (also known as short frames or runts).
Oversized Packets	Indicates the total number of packets received on this port with more than 1518 bytes and with proper CRC and framing (also known as oversized frames).
Collisions	Indicates the total number of collisions detected on this port.
Single Collisions	Indicates the total number of packets that were transmitted successfully on this port after a single collision.
Multiple Collisions	Indicates the total number of packets that were transmitted successfully on this port after more than one collision.
Excessive Collisions	Indicates the total number of packets lost on this port due to excessive collisions.
Packets 64 bytes	Received column: Indicates the total number of 64-byte packets received on this port. Transmitted column: Indicates the total number of 64-byte packets transmitted successfully on this port.
65-127 bytes	Received column: Indicates the total number of 65-byte to 127-byte packets received on this port. Transmitted column: Indicates the total number of 65-byte to 127-byte packets transmitted successfully on this port.
128-255 bytes	Received column: Indicates the total number of 128-byte to 255-byte packets received on this port. Transmitted column: Indicates the total number of 128-byte to 255-byte packets transmitted successfully on this port.
256-511 bytes	Received column: Indicates the total number of 256-byte to 511-byte packets received on this port. Transmitted column: Indicates the total number of 256-byte to 511-byte packets transmitted successfully on this port.
512-1023 bytes	Received column: Indicates the total number of 512-byte to 1023-byte packets received on this port. Transmitted column: Indicates the total number of 512-byte to 1023-byte packets transmitted successfully on this port.
1024-1518 bytes	Received column: Indicates the total number of 1024-byte to 1518-byte packets received on this port. Transmitted column: Indicates the total number of 1024-byte to 1518-byte packets transmitted successfully on this port.

(continued)

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

Field	Description
Filtered Packets	Indicates the number of packets filtered (not forwarded) by this port.
Flooded Packets	Indicates the total number of packets flooded (forwarded) through this port because the destination address was not in the address database.
Deferred Packets	Indicates the total number of frames that were delayed on the first transmission attempt, but never incurred a collision.
Late Collisions	Indicates the total number of packet collisions that occurred after a total length of time that exceeded 512 bit-times of packet transmission.

Console/Comm Port Configuration

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

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

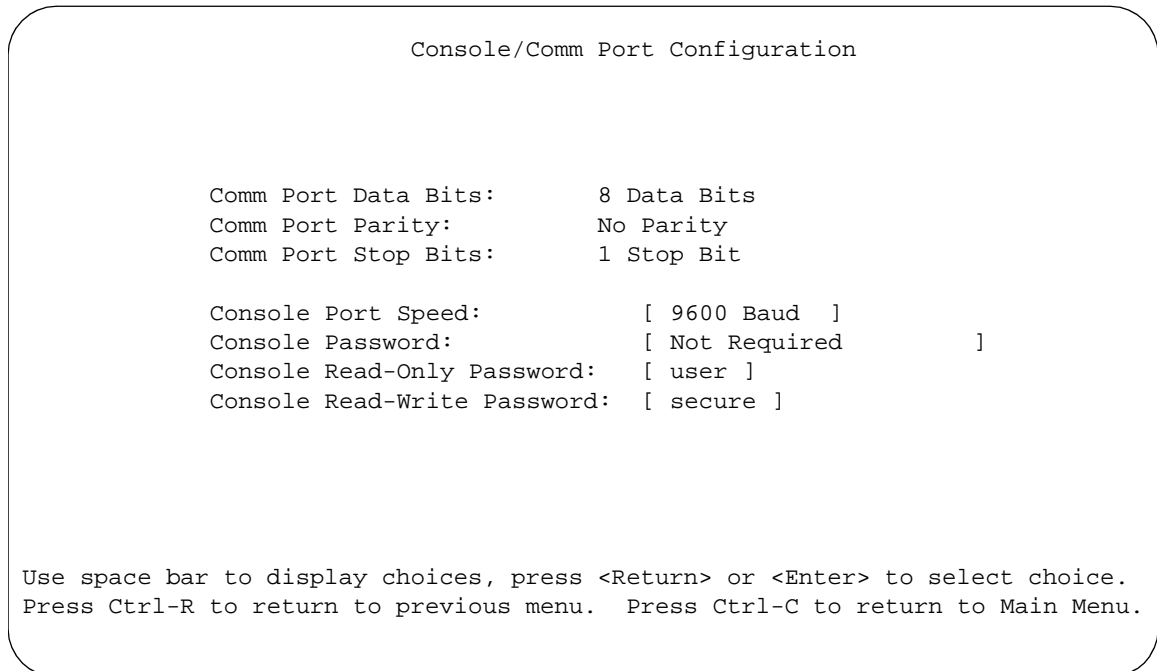


Figure 3-25. Console/Comm Port Configuration Screen


[Table 3-22](#) describes the Console/Comm Port Configuration screen fields.

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

Field	Description
Comm Port Data Bits	A read-only field that indicates the current console/comm port data bit setting.
Comm Port Parity	A read-only field that indicates the current console/comm port parity setting.


(continued)

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

Field	Description
Comm Port Stop Bits	A read-only field that indicates the current console/comm port stop bit setting.
Console Port Speed	Allows you to set the console/comm port baud rate to match the baud rate of the console terminal.
	 Caution: If you choose a baud rate that does not match your console terminal baud rate, you will lose communication with the configuration interface when you press Enter. If communication is lost, set your console terminal to match the new console/comm port setting.
	Default Value 9600 Baud Range 2400 Baud, 4800 Baud, 9600 Baud, 19200 Baud, 38400 Baud
Console Password	Enables password protection for accessing the console interface (CI) through a TELNET session, a console terminal, or both. If you set this field to Required, you can use the Logout option to restrict access to the CI. Thereafter, you will need to specify the correct password at the console-terminal prompt. See Console Read-Only Password and Console Read-Write Password for more information. Default Value Not Required Range Not Required, Required for TELNET, Required for Console, Required for Both
Console Read-Only Password	When the Console Password field is set to Required (for TELNET, for Console, or for Both), this field allows read-only password access to the CI. Users can access the CI using the correct password (see Default Value), but cannot change any parameters or use the Reset option or Reset to Default option. Default Value user Range An ASCII string of up to 15 printable characters
Console Read-Write Password	When the Console Password field is set to Required (for TELNET, for Console, or for Both), this field allows read-write password access to the CI. Users can log in to the CI using the correct password (see Default Value), and can change any parameters. Note that you can change the default passwords for read-only access and read-write access to a private password.

(continued)

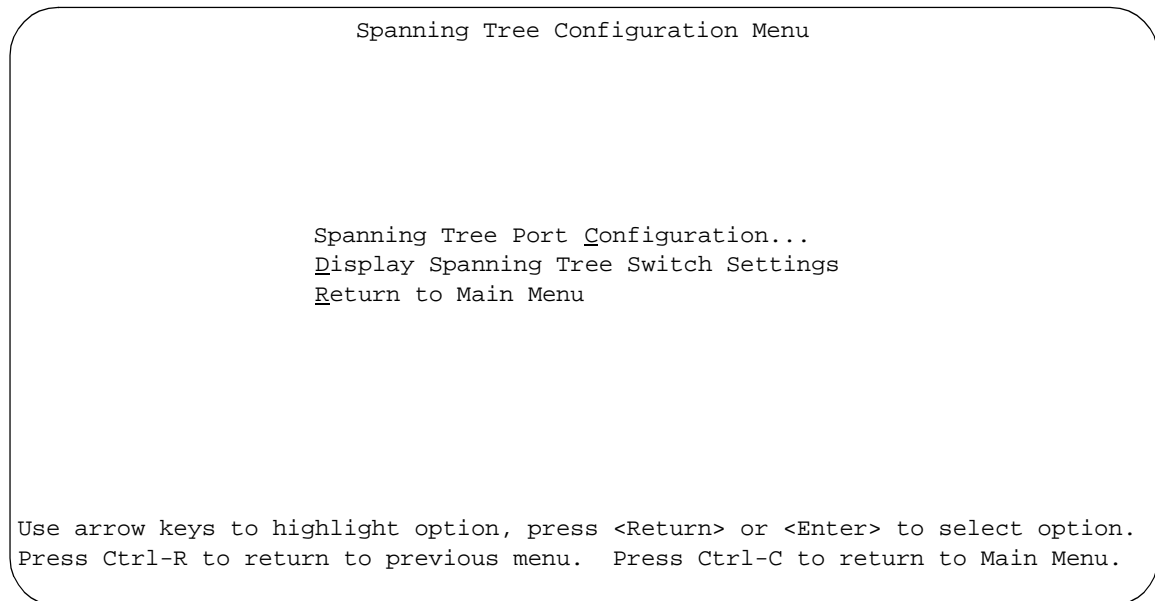
Table 3-22. Console/Comm Port Configuration Screen Fields (*continued*)

Field	Description
	Caution: If you change the system-supplied default passwords, be sure to write the new passwords down and keep them in a safe place. If you forget the new passwords, you cannot access the console interface. In that case, contact Bay Networks for help.
Default Value	secure
Range	Any ASCII string of up to 15 printable characters

Spanning Tree Configuration

The Spanning Tree Configuration Menu screen ([Figure 3-26](#)) allows you to view spanning tree parameters and configure individual switch ports to participate in the spanning tree algorithm (STA). To modify any of the spanning tree parameters, see your SNMP documentation.

Choose Spanning Tree Configuration (or press p) from the main menu to open the Spanning Tree Configuration Menu screen.

**Figure 3-26. Spanning Tree Configuration Menu Screen**

[Table 3-23](#) describes the Spanning Tree Configuration Menu screen options:

Table 3-23. Spanning Tree Configuration Menu Screen Options

Option	Description
Spanning Tree Port Configuration...	Displays the Spanning Tree Port Configuration screen (see “Spanning Tree Port Configuration” on page 3-59).
Display Spanning Tree Switch Settings	Displays the Spanning Tree Switch Settings screen (see “Display Spanning Tree Switch Settings” on page 3-62).
Return to Main Menu	Exits the Spanning Tree Configuration Menu and displays the main menu.

Spanning Tree Port Configuration

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



Note: If spanning tree participation of any trunk member is changed (enabled or disabled), the spanning tree participation of all members of that trunk is changed similarly.

[Figure 3-27](#) and [Figure 3-28](#) show sample port configurations for the two Spanning Tree Port Configuration screens.

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

Spanning Tree Port Configuration					
Port	Trunk	Participation	Priority	Path Cost	State
1		[Normal Learning]	128	10	Forwarding
2		[Normal Learning]	128	10	Forwarding
3		[Normal Learning]	128	10	Forwarding
4		[Normal Learning]	128	10	Forwarding
5		[Normal Learning]	128	10	Forwarding
6	1	[Normal Learning]	128	10	Forwarding
7	1	[Normal Learning]	128	10	Forwarding
8		[Normal Learning]	128	10	Forwarding
9	1	[Normal Learning]	128	10	Forwarding
10		[Normal Learning]	128	10	Forwarding
11		[Normal Learning]	128	10	Forwarding
12		[Normal Learning]	128	10	Forwarding
13	3	[Normal Learning]	128	10	Forwarding
14	3	[Normal Learning]	128	10	Forwarding
More...					

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

Figure 3-27. Spanning Tree Port Configuration Screen (1 of 2)

Spanning Tree Port Configuration					
Port	Trunk	Participation	Priority	Path Cost	State
15		[Normal Learning]	128	5	Forwarding
16		[Normal Learning]	128	5	Forwarding
17	1	[Normal Learning]	128	10	Forwarding
18		[Normal Learning]	128	10	Forwarding
19	4	[Normal Learning]	128	10	Forwarding
20	4	[Normal Learning]	128	10	Forwarding
21		[Normal Learning]	128	10	Forwarding
22	5	[Normal Learning]	128	10	Forwarding
23	5	[Normal Learning]	128	10	Forwarding
24		[Normal Learning]	128	10	Forwarding
25	2	[Normal Learning]	128	10	Forwarding
26	2	[Normal Learning]	128	10	Forwarding
27		[Normal Learning]	128	10	Forwarding
28		[Normal Learning]	128	10	Forwarding
All		[Normal Learning]			

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

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

[Table 3-24](#) describes the Spanning Tree Port Configuration screen fields.

Table 3-24. Spanning Tree Port Configuration Screen Fields

Field	Description
Port	Indicates the switch port numbers that correspond to the field settings in that row of the screen (for example, the field settings in row 2 apply to switch port 2). Note that the settings in the All row (bottom row) affect all switch ports.
Trunk	The read-only data displayed in this column indicates the trunks that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen (see “MultiLink Trunk Configuration” on page 3-35).

(continued)

Table 3-24. Spanning Tree Port Configuration Screen Fields (*continued*)

Field	Description
Participation	<p>Allows you to configure any (or all) of the switch ports for Spanning tree participation.</p> <p>When an individual port is a trunk member (see Trunk field), changing this setting for one of the trunk members changes the setting for all members of that trunk. You should consider how this can change your network topology before you change this setting (see "MultiLink Trunking Configuration Rules" on page 1-56).</p> <p>The Fast Learning parameter is the same as Normal Learning, except that the state transition timer is shortened to two seconds.</p> <p>Default Value Normal Learning</p> <p>Range Normal Learning, Fast Learning, Disabled</p>
Priority	<p>This read-only field is a bridge spanning tree parameter that prioritizes the port's lowest path cost to the root. When one or more ports have the same path cost, the STA selects the path with the highest priority (lowest numerical value). See also Path Cost.</p> <p>Default Value 128</p> <p>Range 0 to 255</p>
Path Cost	<p>This read-only field is a bridge spanning tree parameter that determines the lowest path cost to the root.</p> <p>Default Value 10 or 100 (1 for gigabit port)</p> <p> Path Cost = 1000/LAN speed (in Mb/s)</p> <p> The higher the LAN speed, the lower the path cost.</p> <p> See also Priority.</p> <p>Range 1 to 65535</p>
State	<p>This read-only field indicates the current port state within the spanning tree network. Each port can transition to various states, as determined by the Participation field setting. For example, when the Participation field is set to Disabled, the port does not participate in the STA and transitions to the Forwarding state (the default). When the Participation field is set to Enabled, the port transitions from the Disabled state through the Blocking, Listening, and Learning states before entering the Forwarding state.</p> <p>Default Value Topology dependent</p> <p>Range Disabled, Blocking, Listening, Learning, Forwarding</p>

Display Spanning Tree Switch Settings

The Spanning Tree Switch Settings screen ([Figure 3-29](#)) allows you to view spanning tree parameter settings for the BayStack 450 switch.

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

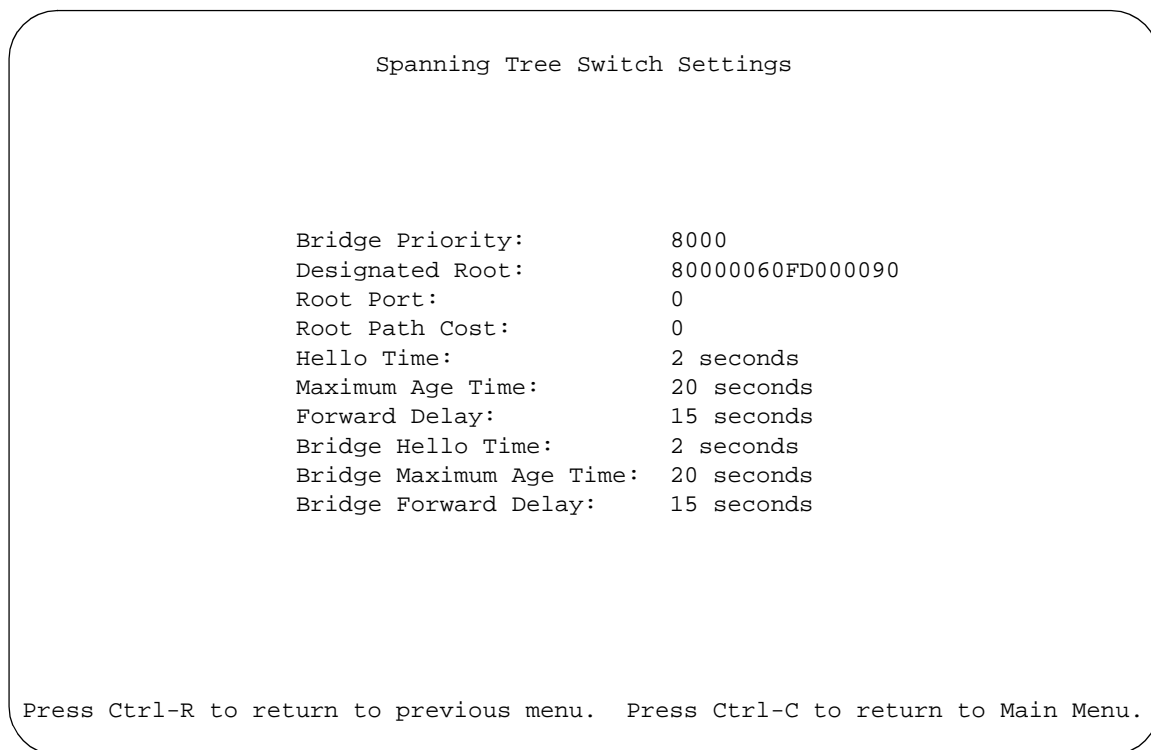


Figure 3-29. Spanning Tree Switch Settings Screen

[Table 3-25](#) describes the Spanning Tree Switch Settings parameters.

Table 3-25. Spanning Tree Switch Settings Parameters

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

(continued)

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

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

TELNET Configuration

The TELNET Configuration screen ([Figure 3-30](#)) allows a user at a remote console terminal to communicate with the BayStack 450 switch as if the console terminal were directly connected to it. You can have up to four active TELNET sessions at one time.

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

```

                                TELNET Configuration

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

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

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

```

Figure 3-30. TELNET Configuration Screen

[Table 3-26](#) describes the TELNET Configuration screen fields.

Table 3-26. TELNET Configuration Screen Fields

Field	Description
TELNET Access	Allows a user remote access to the CI through a TELNET session. Default Value Enabled Range Enabled, Disabled
Login Timeout	Specifies the amount of time a user has to enter the correct password at the console-terminal prompt. Default Value 1 minute Range 0 to 10 minutes (0 indicates "no timeout")
Login Retries	Specifies the number of times a user can enter an incorrect password at the console-terminal prompt before terminating the session. Default Value 3 Range 1 to 100
Inactivity Timeout	Specifies the amount of time the session can be inactive before it is terminated. Default Value 15 minutes Range 0 to 60 minutes (0 indicates "no timeout")
Event Logging	Specifies the types of events that will be displayed in the Event Log screen (see " Display Event Log " on page 3-71). Default Value All Range All, None, Accesses, Failures Description: All: Logs the following TELNET events to the Event Log screen: <ul style="list-style-type: none"> • TELNET connect: Indicates the IP address and access mode of a TELNET session. • TELNET disconnect: Indicates the IP address of the remote host and the access mode, due to either a logout or inactivity. • Failed TELNET connection attempts: Indicates the IP address of the remote host whose IP address is not on the list of allowed addresses, or indicates the IP address of the remote host that did not supply the correct password. None: Indicates that no TELNET events will be logged in the Event Log screen. Accesses: Logs only TELNET connect and disconnect events in the Event Log screen. Failures: Logs only failed TELNET connection attempts in the Event Log screen.

(continued)

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

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

Software Download

The Software Download screen ([Figure 3-31](#)) allows you to revise the BayStack 450 switch software image that is located in nonvolatile flash memory. To download the BayStack 450 switch software image, a properly configured Trivial File Transfer Protocol (TFTP) server must be present in your network, and the switch must have an IP address. (See “IP Configuration” on [page 3-7](#) to learn how to configure the switch’s IP address.)

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

You can monitor the software download process by observing the BayStack 450 switch LEDs (see “[LED Indications During the Download Process](#)” on [page 3-69](#)).



Caution: Do not interrupt power to the device during the software download process. If the power is interrupted, the firmware image can become corrupted.

```
Software Download

Image Filename:           [ b450_100.img ]
TFTP Server IP Address:   [ 192.0.1.12 ]

Start TFTP Load of New Image: [ Yes ]


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

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

Figure 3-31. Software Download Screen

[Table 3-27](#) describes the Software Download screen fields.

Table 3-27. Software Download Screen Fields

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

LED Indications During the Download Process

The software download process is automated so that it runs to completion without user intervention. The download process erases the contents of flash memory and replaces it with a new software image; therefore, it is important that the download process not be interrupted once initiated. When the download process is complete, the switch is reset automatically and the new software image initiates a self-test. The self-test results are displayed briefly in the BayStack 450 switch Self-Test screen, which is followed by the console interface screens.

During the download process, the BayStack 450 switch is not operational. You can monitor the progress of the download process by observing the LED indications.

[Table 3-28](#) describes the LED indications during the software download process.

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

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

Display Event Log

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



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

Choose Display Event Log (or press e) from the main menu to open the Event Log screen.

```
Event Log

Entry Number: 4          sysUpTime: 00:14:36          Reset Count: 2
Connection logout, IP address: 38.227.40.8, access mode: no security.

Entry Number: 3          sysUpTime: 00:13:35          Reset Count: 2
Connection logout, IP address: 38.227.40.8, access mode: no security.

Entry Number: 2          sysUpTime: 00:00:53          Reset Count: 2
Successful connection from IP address: 38.227.40.8, access mode: no security.

Entry Number: 1          sysUpTime: 00:00:00          Reset Count: 1
Software downloaded to BayStack Model 450-24T HW:RevA FW:V1.00 SW:V1.0.0.0

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

Figure 3-32. Event Log Screen

The Event Log screen provides the following information:

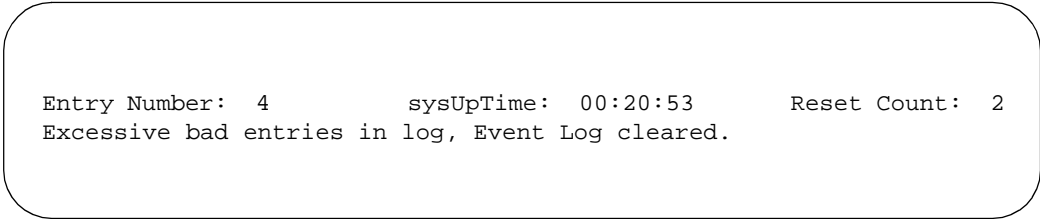
- **Software download:** Indicates the new software version.
- **Authentication failure:** Indicates any attempted SNMP **get** or **set** access that specified an invalid community string.

- **TELNET session status:** Indicates various TELNET events. (For details on configuring this feature, see [“TELNET Configuration”](#) on [page 3-65](#).)
- **Operational exception:** Indicates that the microprocessor has received an exception at the specified vector number and dumps stack registers.
- **Excessive bad entries:** displays excessive bad entries detected by firmware.
- **Write threshold:** displays event entries that exceeded the write threshold.
- **Flash update:** displays status of flash updates.

Excessive Bad Entries

If the firmware detects excessive bad entries in the event log’s flash memory (errors exceeding 75 percent of the memory buffer), the event log is cleared (all entries are discarded) and an event entry is displayed in the Event Log screen.

[Figure 3-33](#) shows an example of the event log entry for this type of event.



```
Entry Number: 4          sysUpTime: 00:20:53      Reset Count: 2
Excessive bad entries in log, Event Log cleared.
```

Figure 3-33. Sample Event Log Entry Showing Excessive Bad Entries

Write Threshold

To extend the lifetime of the event log’s flash memory, a write threshold is set for each event entered in flash memory. The write threshold is 20 entries for each event. If any event exceeds the write threshold, an event entry is displayed in the Event Log screen.

[Figure 3-34](#) shows an example of the event log entry for this type of event.


```
Entry Number: 3          sysUpTime: 02:29:44 Reset Count: 2
The last event exceeded the write threshold. Further write attempts
by this event are blocked. The write threshold will be cleared when
the switch is reset or when the Event Log is compressed.
```

Figure 3-34. Sample Event Log Event Exceeding the Write Threshold

The write threshold is reset when either of the following occurs:

- The BayStack 450 switch is reset.
- The firmware determines that compression is required for maintenance of the event log's flash memory.

Flash Update

[Figure 3-35](#) shows an example of the event log entry for this type of event.

```
Entry Number: 13          sysUpTime: 12:20:38 Reset Count: 2
Flash configuration update operation (write or erase) failed.
Configuration information may be lost.
```

Figure 3-35. Sample Event Log Event Showing Flash Update Status

Reset

The Reset option (accessed from the main menu) allows you to reset the BayStack 450 switch without erasing any configured switch parameters.

Resetting the switch takes approximately five seconds to complete. During this time, the switch initiates a self-test that comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

The results of the self-test are displayed briefly (5 or 10 seconds) in the Self-Test screen ([Figure 3-36](#)), which is followed by the Bay Networks Logo screen ([Figure 3-37](#)).



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

```
BayStack 450-24T Self-Test
CPU RAM test                ... Pass
ASIC addressing test        ... Pass
ASIC buffer RAM test       ... Pass
Port internal loopback test ... Pass
Self-test complete.
```

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

```
*****  
* Bay Networks, Inc. *  
* Copyright (c) 1996,1998 *  
* All Rights Reserved *  
* BayStack 450-24T *  
* Versions: HW:RevA FW:V1.00 SW:V1.0.0.0 *  
*****
```

Enter Ctrl-Y to begin.

Figure 3-37. Bay Networks Logo Screen

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

To access the BayStack 450 Main Menu, press [Ctrl]-Y.

Reset to Default Settings

The Reset to Default Settings option (accessed from the main menu) allows you to reset the BayStack 450 switch and replace all configured switch parameters with the factory default settings. For a list of the factory default settings, see Appendix E, “Default Settings.”



Caution: If you choose this option, all of your configured settings will be replaced with factory default settings when you press Enter.

The Reset to Default Settings option takes approximately five seconds to complete. During this time, the switch initiates a self-test that comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

The results of the self-test are displayed briefly (5 or 10 seconds) in the Self-Test screen ([Figure 3-38](#)), which is followed by the Bay Networks Logo screen ([Figure 3-39](#)).

```
BayStack 450-24T Self-Test

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

Self-test complete.
```

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

```
*****
* Bay Networks, Inc. *
* Copyright (c) 1996,1998 *
* All Rights Reserved *
* BayStack 450-24T *
* Versions: HW:RevA FW:V1.00 SW:V1.0.0.0 *
*****

Enter Ctrl-Y to begin.
```

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



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

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

To access the BayStack 450 Main Menu, press [Ctrl]-Y.

Logout

The Logout option (accessed from the main menu) allows a user working at a password-protected console terminal or in an active TELNET session to terminate the session.

The Logout option works as follows:

- If the user is accessing the BayStack 450 switch through a TELNET session, the Logout option terminates the TELNET session.
- If the user is accessing the BayStack 450 switch through a password-protected console terminal (connected to the console/comm port on the switch), the Logout option displays the console-terminal password prompt ([Figure 3-40](#)). The user must enter the correct password to access the CI screens.

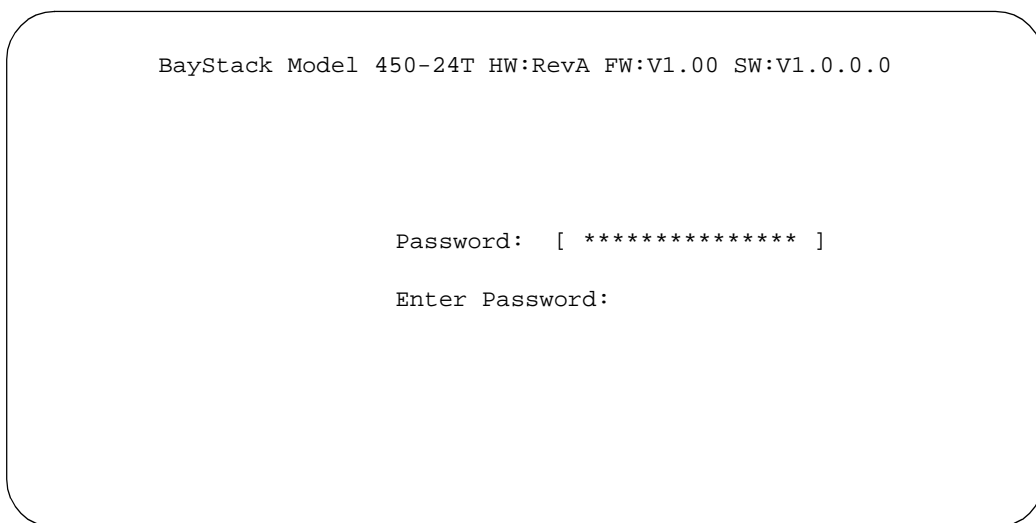


Figure 3-40. Password Prompt Screen

You can specify whether a password is required for the TELNET session or the console terminal using the Console/Comm Port Configuration screen (see [“Console/Comm Port Configuration”](#) on [page 3-55](#)).

If the console terminal is not password protected, the system ignores the Logout option.

Chapter 4

Troubleshooting

This chapter explains how to isolate and diagnose problems with the BayStack 450 switch.

This chapter includes the following information:

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



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

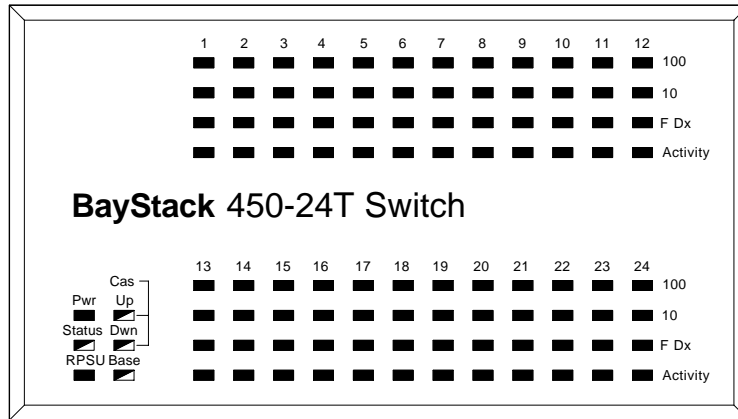
This chapter is organized to help lead you through a logical process for troubleshooting the BayStack 450 switch. For example, because the LEDs provide visual indications of problems, the section [“LED Indications”](#) on [page 4-2](#) helps you to understand the various states that each LED can exhibit during operation.

If you need more help in determining the problem, the section [“Diagnosing and Correcting the Problem”](#) on [page 4-4](#) provides a table that lists symptoms and corrective actions you can perform to resolve specific problems. Subsequent sections provide step-by-step procedures for correcting the problems listed in the table.

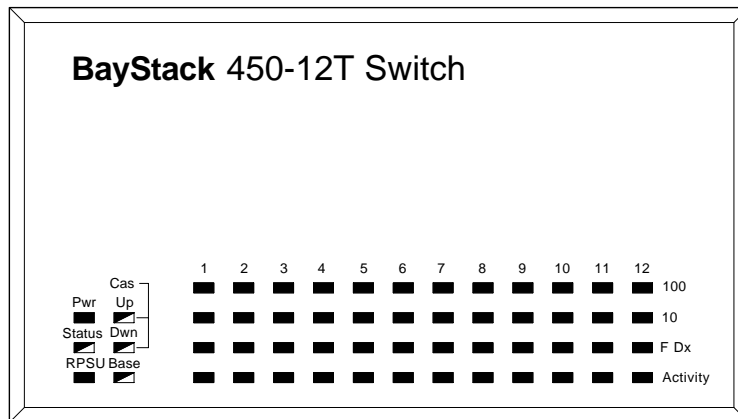
LED Indications

[Figure 4-1](#) shows the LED display panels used with the BayStack 450 switch.

Refer to [Table 4-1](#) for a description of the LEDs.



BayStack 450-24T



BayStack 450-12T

8487EA

Figure 4-1. BayStack 450 Switch LED Locations

Table 4-1. BayStack 450 Switch LED Descriptions

Label	Type	Color	State	Meaning
Pwr	Power status	Green	On	DC power is available to the switch's internal circuitry.
			Off	No AC power to switch or power supply failed.
Status	System status	Green	On	Self-test passed successfully and switch is operational.
			Blinking	A nonfatal error occurred during the self-test.
			Off	The switch failed the self-test.
RPSU	RPSU status	Green	On	The switch is connected to the HRPSU and can receive power if needed.
			Off	The switch is not connected to the HRPSU or HRPSU is not supplying power.
CAS Up/ Dwn	-	-	-	For future release.
Base	-	-	-	For future release.
100	100 Mb/s port speed indicator	Green	On	The corresponding port is set to operate at 100 Mb/s and the link is good.
			Off	The link connection is bad or there is no connection to this port.
			Blinking	The corresponding port is management disabled.
10	10 Mb/s port speed indicator	Green	On	The corresponding port is set to operate at 10 Mb/s and the link is good.
			Off	The link connection is bad or there is no connection to this port.
			Blinking	The corresponding port is management disabled.
F Dx	Half/Full-duplex mode status	Green	On	The corresponding port is operating in full-duplex mode (operating at 10 Mb/s or at 100 Mb/s).
			Off	The corresponding port is operating in half-duplex mode.
Activity	Port activity	Green	Blinking	Indicates network activity for the corresponding port. A high level of network activity can cause the LEDs to appear to be on continuously.

Diagnosing and Correcting the Problem


Before you perform the problem-solving steps in this section, cycle the power to the BayStack 450 switch (disconnect and then reconnect the AC power cord); then, verify that the switch follows the normal power-up sequence.

Normal Power-Up Sequence

In a normal power-up sequence, the LEDs display as follows:

1. After power is applied to the switch, the Pwr (Power) LED turns on within five seconds.
2. The switch initiates a self-test, during which the port LEDs display various patterns to indicate the progress of the self-test.
3. Upon successful completion of the self-test (within 10 seconds after power is applied), the Status LED turns on.
4. The remaining port LEDs indicate their operational status, as described in [Table 4-2](#).

Table 4-2. Corrective Actions

Symptom	Probable cause	Corrective action
All LEDs are off.	The switch is not receiving AC power.	Verify that the AC power cord is fastened securely at both ends and that power is available at the AC power outlet.
	The fans are not operating or the airflow is blocked, causing the unit to overheat.	Verify that there is sufficient space for adequate airflow on both sides of the switch.
The Activity LED for a connected port is off or does not blink (and you have reason to believe that traffic is present).	The switch is experiencing a port connection problem.	 Note: Operating temperature for the switch must not exceed 40°C (104°F). The switch should not be placed in the direct sunlight or near warm air exhausts or heaters.
	The switch's link partner is not autonegotiating properly.	

(continued)

Table 4-2. Corrective Actions (*continued*)

Symptom	Probable cause	Corrective action
The Status LED is off.	A fatal error was detected by the self-test.	Cycle the power to the switch (disconnect and then reconnect the AC power cord). If the problem persists, replace the switch.
The Status LED is blinking.	A nonfatal error occurred during the self-test.	Cycle the power to the switch (disconnect and then reconnect the AC power cord). If the problem persists, contact the Bay Networks Technical Solutions Center.

Port Connection Problems

Port connection problems can usually be traced to a poor cable connection or an improper connection of the port cables at either end of the link. These types of problems can be remedied by making sure that the cable connections are secure and that the cables are connected to the correct ports at both ends of the link.

Port connection problems can also be traced to the autonegotiation mode or the port interface.

Autonegotiation Modes

Port connection problems can occur when a port (or station) is connected to another port (or station) that is not operating in a compatible mode (for example, connecting a full-duplex port on one station to a half-duplex port on another station).

The BayStack 450 switch negotiates port speeds according to the IEEE 802.3u autonegotiating standard. The switch adjusts (autonegotiates) its port speed and duplex mode to match the best service provided by the connected station, up to 100 Mb/s in full-duplex mode.

- If the connected station uses a form of autonegotiation that is not compatible with the IEEE 802.3u autonegotiating standard, the BayStack 450 switch cannot negotiate a compatible mode for correct operation.
- If the autonegotiation feature is not present or is not enabled at the connected station, the BayStack 450 switch may not be able to determine the correct duplex mode.

In both situations, the BayStack 450 switch “autosenses” the speed of the connected station and, by default, reverts to half-duplex mode. If the connected station is operating in full-duplex mode, it cannot communicate with the switch.

To correct this mode mismatch problem, follow these steps:

1. **Use the Port Configuration screen to disable autonegotiation for the suspect port (see “Port Configuration” on page 3-30).**
2. **Manually set the Speed/Duplex field to match the speed/duplex mode of the connected station (see Table 3-12 on page 3-31).**

You may have to try several settings before you find the correct speed/duplex mode of the connected station.

If the problem persists, follow these additional steps:

1. **Disable the autonegotiation feature at the connected station.**
2. **Manually set the speed/duplex mode of the connected station to the same speed/duplex mode you have manually set for the BayStack 450 switch port.**



Note: Bay Networks recommends that you manually set the BayStack 450 switch port to the desired speed/duplex mode when connecting to any of the following Bay Networks products:

- Bay Networks 28000 product family
 - Bay Networks 58000 product family
 - BayStack Model 302T switch (100 Mb/s port)
-

Port Interface

Ensure that the devices are connected using the appropriate crossover or straight-through cable (see Appendix D, “Connectors and Pin Assignments”).

Appendix A

Technical Specifications

This appendix lists the technical specifications for the BayStack 450 switch.

Environmental

Parameter	Operating Specification	Storage Specification
Temperature:	0° to 40°C (32° to 104°F)	-25° to 70°C (-13° to 158°F)
Humidity:	85% maximum relative humidity, noncondensing	95% maximum relative humidity, noncondensing
Altitude:	3024 m (10,000 ft)	3024 m (10,000 ft)

Electrical

Parameter	Model 450-24	Model 450-12
Input Voltage:	100 to 240 VAC @ 50 to 60 Hz	100 to 240 VAC @ 50 to 60 Hz
Input Power Consumption:	150 W maximum	120 W maximum
Input Volt Amperes Rating:	200 VA maximum	150 VA maximum
Input Current:	2.0 A @ 100 VAC	1.5 A @ 100 VAC
Maximum Thermal Output	500 BTU/hr	400 BTU/hr

Physical Dimensions

Parameter	Model 450-24	Model 450-12
Height	7.03 cm (2.77 in.)	7.03 cm (2.77 in.)
Width	44.07 cm (17.55 in.)	44.07 cm (17.55 in.)
Depth	38.1 cm (15.0 in)	38.1 cm (15.0 in)
Weight	5.26 kg (11.60 lb)	5.26 kg (11.60 lb)

Performance Specifications

Frame Forward Rate (64-byte packets):	Up to 3 million packets per second (pps) maximum, learned unicast traffic
Port Forwarding/Filtering Performance (64-byte packets):	For 10 Mb/s: 14,880 pps maximum For 100 Mb/s: 148,810 pps maximum
Address Database Size:	16,000 entries at line rate (32,000 entries without flooding)
Addressing:	48-bit MAC address
Frame Length:	64 to 1518 bytes (IEEE 802.1Q Untagged) 64 to 1522 bytes (IEEE 802.1Q Tagged)

Network Protocol and Standards Compatibility

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

Data Rate

- 10 Mb/s Manchester encoded or 100 Mb/s 4B/5B encoded

Interface Options

- RJ-45 (8-pin modular) connectors for MDI-X interface
- 100BASE-FX SC connectors for supporting switched 100 Mb/s (100BASE-FX) connections over 50/125 and 62.5/125 micron multimode fiber optic cable

Safety Agency Certification

- UL Listed (UL 1950)
- IEC 950/EN60950
- C22.2 No. 950 (cUL)
- UL-94-V1 flammability requirements for PC board

Electromagnetic Emissions

- US. CFR47, Part 15, Subpart B, Class A
- Canada. ICES-003, Issue 2, Class A
- Australia/New Zealand. AS/NZS 3548:1995, Class A
- Japan. V-3/97.04:1997, Class A
- Taiwan. CNS 13438, Class A
- EN55022:1995, Class A
- EN61000-3-2:1995
- EN61000-3-3:1994

Electromagnetic Immunity

- EN50082-1:1997

Declaration of Conformity

The Declaration of Conformity for the BayStack 450 switches complies with ISO/IEC Guide 22 and EN45014. The declaration identifies the product models, the Bay Networks name and address, and the specifications recognized by the European community.

As stated in the Declaration of Conformity, the BayStack 450 switches comply with the provisions of Council Directives 89/336/EEC and 73/23/EEC.

Appendix B

Media Dependent Adapters (MDAs)

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

The following MDA versions are available for the BayStack 450 switch:

- 400-4TX MDA --- 10BASE-T/100BASE-TX MDA (4-port copper)
- 400-2FX MDA --- 100BASE-FX MDA (2-port fiber)
- 450-1SR MDA --- 1000BASE-SX MDA (1-port shortwave gigabit fiber, with 1-redundant port)
- 450-1SX MDA --- 1000BASE-SX MDA (1-port shortwave gigabit fiber)
- 450-1LR MDA --- 1000BASE-LX MDA (1-port longwave gigabit fiber, with 1-redundant port)
- 450-1LX MDA --- 1000BASE-LX MDA (1-port longwave gigabit fiber)

Bay Networks is constantly adding new models and features to existing product lines; see your Bay Networks sales representative for a full range of available MDAs that may have been added after the release of this manual. Each MDA shipment comes with installation instructions.



Note: Installing or removing an MDA from an operating switch (hot-swapping) causes the switch to auto-reset as soon as the insertion or removal of the device is sensed by the switch software. Although the switch is hot-swap survivable, data integrity during the reset will be compromised.

Use the installation procedure provided in this appendix in the event that the original installation instructions are misplaced or lost.

400-4TX MDA

The 400-4TX MDA ([Figure B-1](#)) uses a standard RJ-45 connector to attach an Ethernet device. This MDA is capable of operating at either 10 Mb/s or 100 Mb/s speed. The speed is determined through autonegotiation with its connecting device.

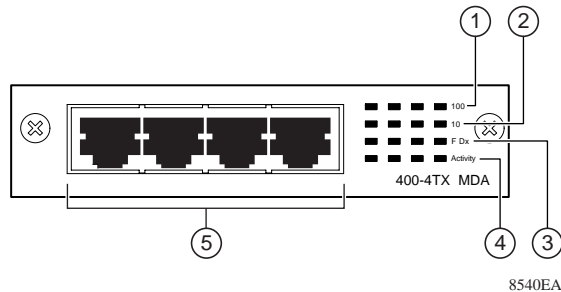


Figure B-1. 400-4TX MDA Front-Panel

[Table B-1](#) describes the 400-4TX MDA components and LEDs.

Table B-1. 400-4TX MDA Components

Item	Label	Description
1	100	100BASE-TX port status LEDs (green): On: The corresponding port is set to operate at 100 Mb/s. Off: The link connection is bad or there is no connection to this port. Blinking: The corresponding port is management disabled.
2	10	10BASE-T port status LEDs (green): On: The corresponding port is set to operate at 10 Mb/s. Off: The link connection is bad or there is no connection to this port. Blinking: The corresponding port is management disabled.
3	F Dx	Full-duplex port status LEDs (green): On: The corresponding port is in full-duplex mode. Off: The corresponding port is in half-duplex mode.

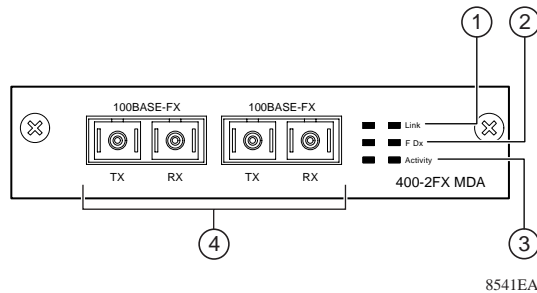
(continued)

Table B-1. 400-4TX MDA Components (*continued*)

Item	Label	Description
4	Activity	Port activity LEDs (green): Blinking: Indicates the network activity level for the corresponding port. A high level of network activity can cause LEDs to appear to be on continuously
5		10BASE-T/100BASE-TX RJ-45 (8-pin modular) port connectors.

400-2FX MDA

The 400-2FX MDA ([Figure B-2](#)) is used to attach a fiber-based 100 Mb/s connection to the switch. This MDA accepts standard SC connections using 62.5/125 μm fiber optic cable. The 400-2FX MDA is not supported on single-mode fiber cabling.

**Figure B-2. 400-2FX MDA Front-Panel**

[Table B-2](#) describes the 400-2FX MDA components and LEDs.

Table B-2. 400-2FX Components

Item	Label	Description
1	Link	Communications link LEDs (green): On: Valid communications link established. Off: The communications link connection is bad or there is no connection to this port. Blinking: The corresponding port is management disabled.

(*continued*)

Table B-2. 400-2FX Components *(continued)*

Item	Label	Description
2	F Dx	Full-duplex port status LEDs (green): On: The corresponding port is in full-duplex mode. Off: The corresponding port is in half-duplex mode.
3	Activity	Port activity LEDs (green): Blinking: Indicates the network activity level for the corresponding port. A high level of network activity can cause LEDs to appear to be on continuously.
4		100BASE-FX SC port connectors.

1000BASE-SX MDA

There are two versions of the 1000BASE-SX (shortwave gigabit) MDAs:

- The 450-1SR MDA is a single MAC MDA with a separate redundant Phy (backup Phy port).
- The 450-1SX MDA is a single Phy MDA.

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

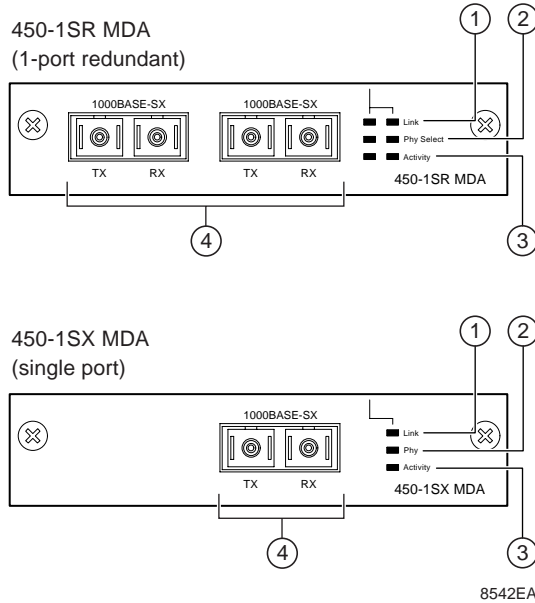


Figure B-3. 1000BASE-SX MDA Front-Panel

[Table B-3](#) describes the 1000BASE-SX MDA components and LEDs.

Table B-3. 1000BASE-SX Components

Item	Label	Description
1	Link	Communication link LEDs (green): On: Valid communications link. Off: The communications link connection is bad or there is no connection to this port. Blinking: The corresponding port is management disabled.
2	Phy Select	Phy Selection LEDs(green): On: The corresponding Phy port is selected. Off: The corresponding Phy port is in backup mode.
3	Activity	Port activity LEDs (green): Blinking: Indicates network activity level for the corresponding port. A high level of network activity can cause LEDs to appear to be on continuously.
4		1000BASE-FX SC port connectors.

1000BASE-LX MDA

There are two versions of the 1000BASE-LX (longwave gigabit) MDAs:

- The 450-1LR MDA is a single MAC MDA with a separate redundant Phy (backup Phy port).
- The 450-1LX MDA is a single Phy MDA.

Both versions ([Figure B-4](#)) use longwave 1300 nm fiber optic connectors to connect devices over single-mode (3 kilometer) or multimode (550 meters) fiber optic cable.

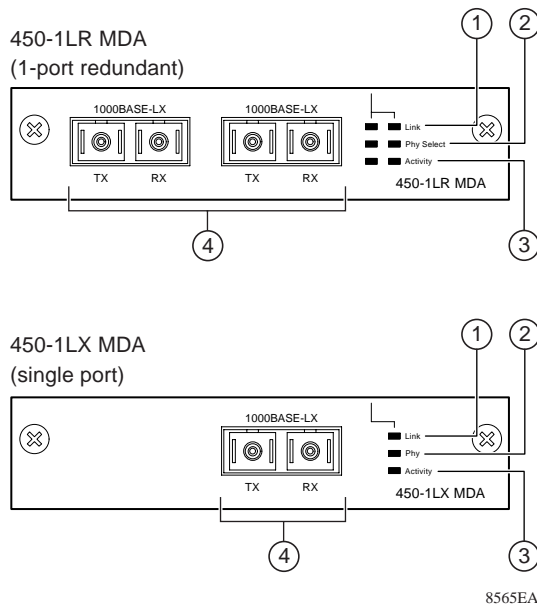


Figure B-4. 1000BASE-LX MDA Front-Panel

[Table B-4](#) describes the 1000BASE-LX MDA components and LEDs.

Table B-4. 1000BASE-LX Components

Item	Label	Description
1	Link	<p>Communication link LEDs (green):</p> <p>On: Valid communications link.</p> <p>Off: The communications link connection is bad or there is no connection to this port.</p> <p>Blinking: The corresponding port is management disabled.</p>
2	Phy Select	<p>Phy Selection LEDs(green):</p> <p>On: The corresponding Phy port is selected.</p> <p>Off: The corresponding Phy port is in backup mode.</p>
3	Activity	<p>Port activity LEDs (green):</p> <p>Blinking: Indicates network activity level for the corresponding port. A high level of network activity can cause LEDs to appear to be on continuously.</p>
4		1000BASE-FX SC port connectors.

Installing an MDA

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



Note: Installing or removing an MDA from an operating switch (hot-swapping) causes the switch to auto-reset as soon as the insertion or removal of the device is sensed by the switch software. Although the switch is hot-swap survivable, data integrity during the reset will be compromised.

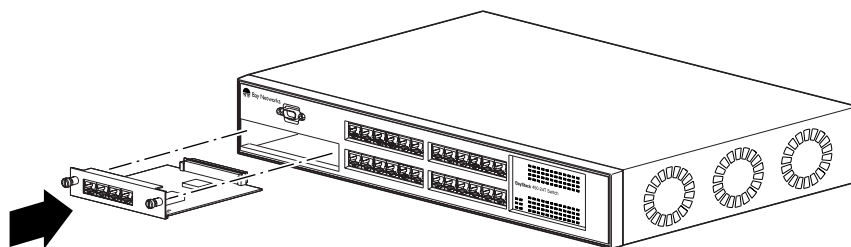
To install an MDA into the Uplink Module slot, follow these steps:

1. **Unplug the AC power cord from the back of the switch.**
2. **Loosen the thumbscrews and remove the filler panel (or previously installed MDA) from the Uplink Module slot.**

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



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



8531FA

Figure B-5. Installing an MDA

4. Press the MDA *firmly* into the chassis slot. Be sure that the MDA is fully seated into the mating connector.
5. Secure the MDA in the chassis by tightening the thumb screws on the MDA front panel.
6. Attach devices to the MDA ports (refer to “Attaching Devices to the BayStack 450 Switch” on page 2-6).



Note: The IEEE 802.3u specification requires that all ports operating at 100 Mb/s use only Category 5 unshielded twisted pair (UTP) cabling.

Appendix C

Quick Steps to Features

This appendix provides Quick Steps for using the BayStack 450 switch features. It is intended for system administrators who are familiar with the BayStack 450 switch features described in this manual.

If you have experience in configuring the BayStack 450 switch features (such as VLANs, MultiLink Trunking, Port Mirroring, IGMP Snooping, and more) you can use the configuration flowcharts provided in this appendix to guide you through the steps necessary to configure your switch. References to additional information about configuring the specific feature are provided within the steps of the flowcharts as required.

This appendix provides Quick Step flowcharts for the following features:

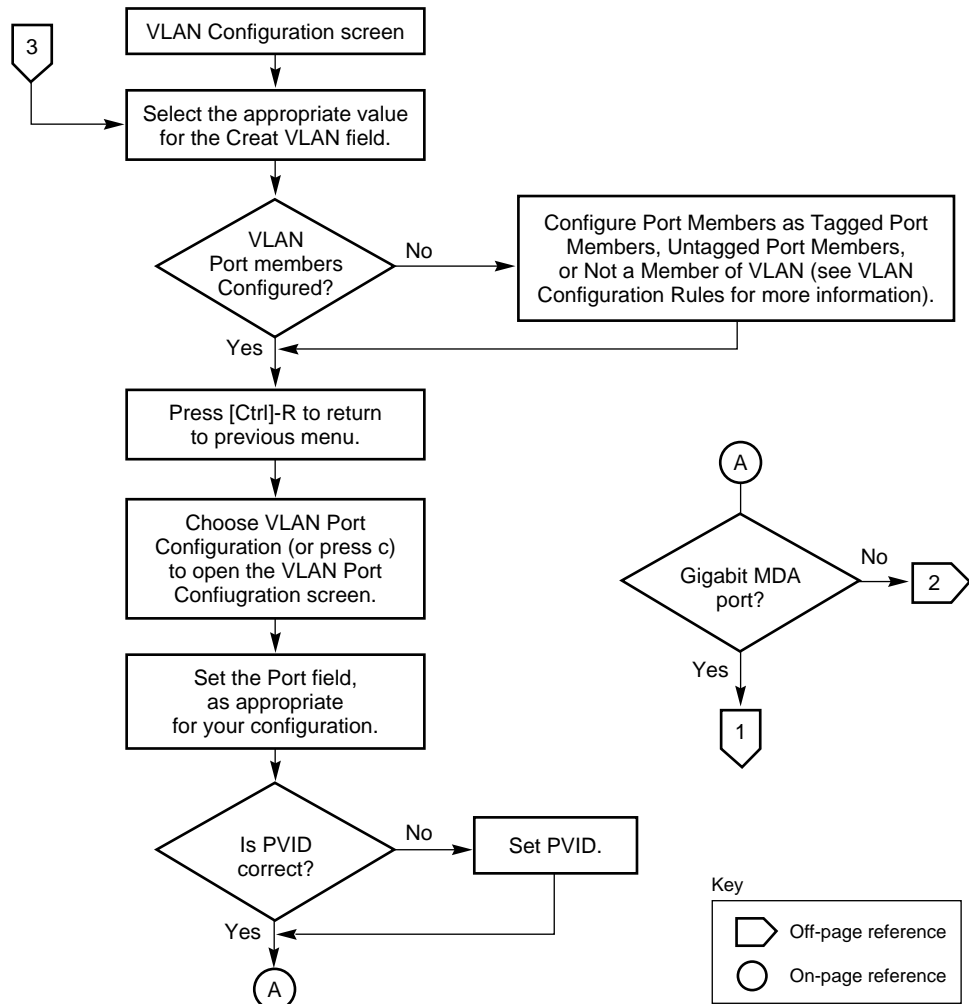
- 802.1Q VLANs
- MultiLink Trunks
- Port Mirroring
- IGMP Snooping

To learn more about:	Refer to this section:
802.1Q VLANs	"IEEE 802.1Q VLAN Workgroups" on page 1-19.
MultiLink Trunks	"MultiLink Trunks" on page 1-44.
Port Mirroring	"Port Mirroring (Conversation Steering)" on page 1-62.
IGMP Snooping	"IGMP Snooping" on page 1-35.

Configuring 802.1Q VLANs

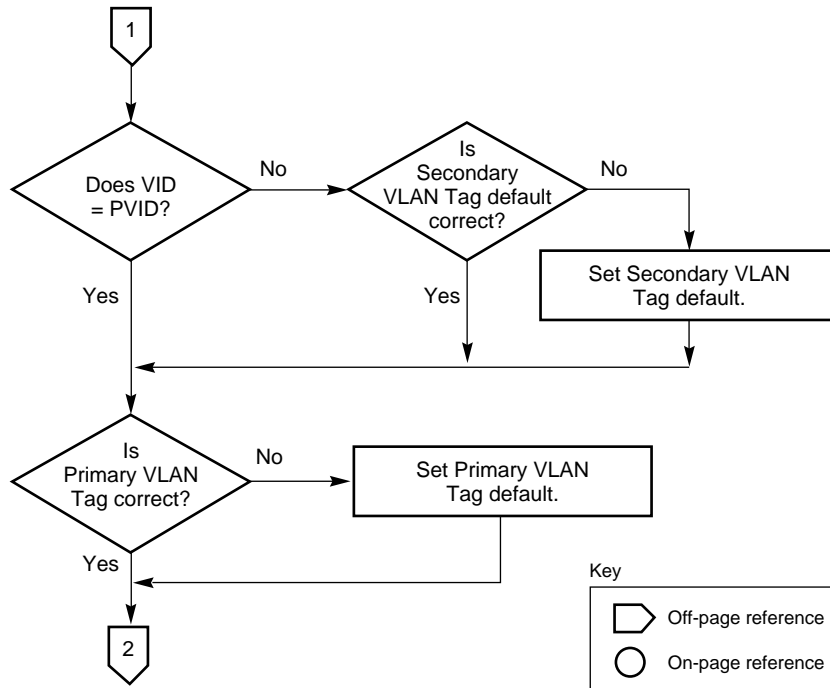
This section shows how to create a new VLAN or to modify an existing VLAN (see [Figure C-1](#) to [Figure C-3](#)).

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



8579EA

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



8580EA

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

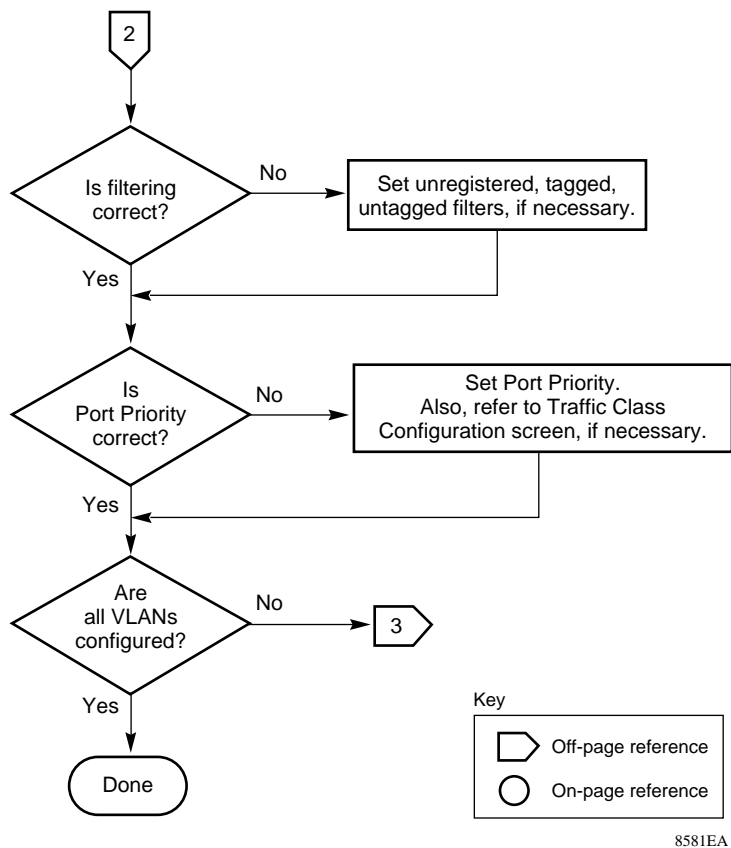
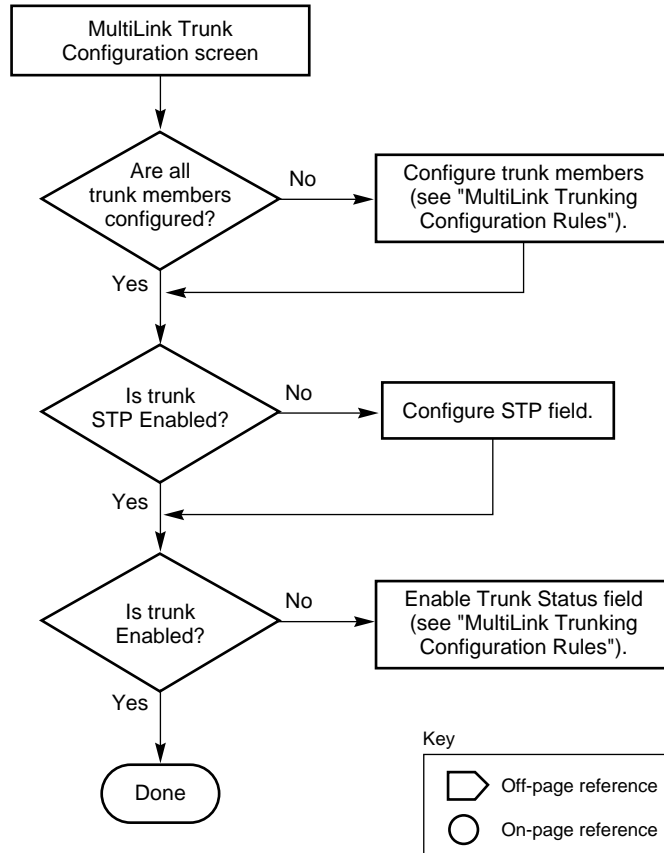


Figure C-3. Configuring 802.1Q VLANs (3 of 3)

Configuring MultiLink Trunks

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

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



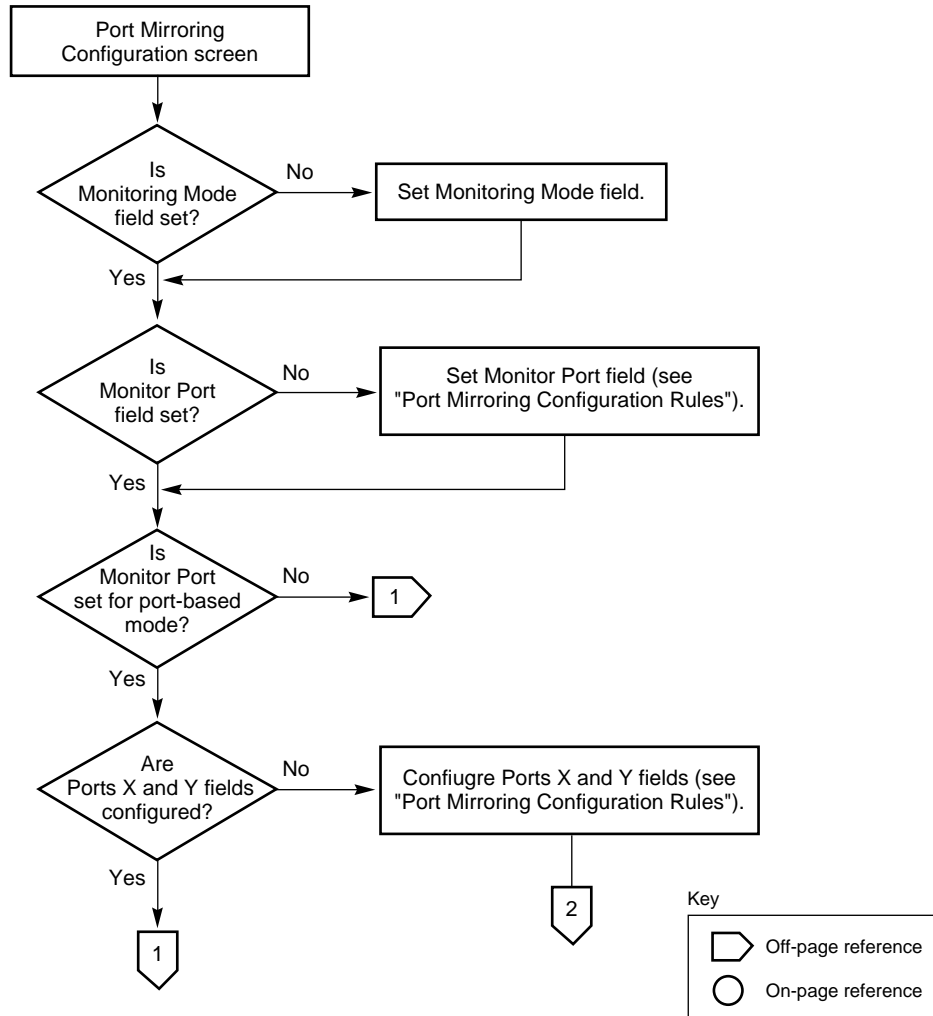
8582EA

Figure C-4. Configuring MultiLink Trunks

Configuring Port Mirroring

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

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



8583EA

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

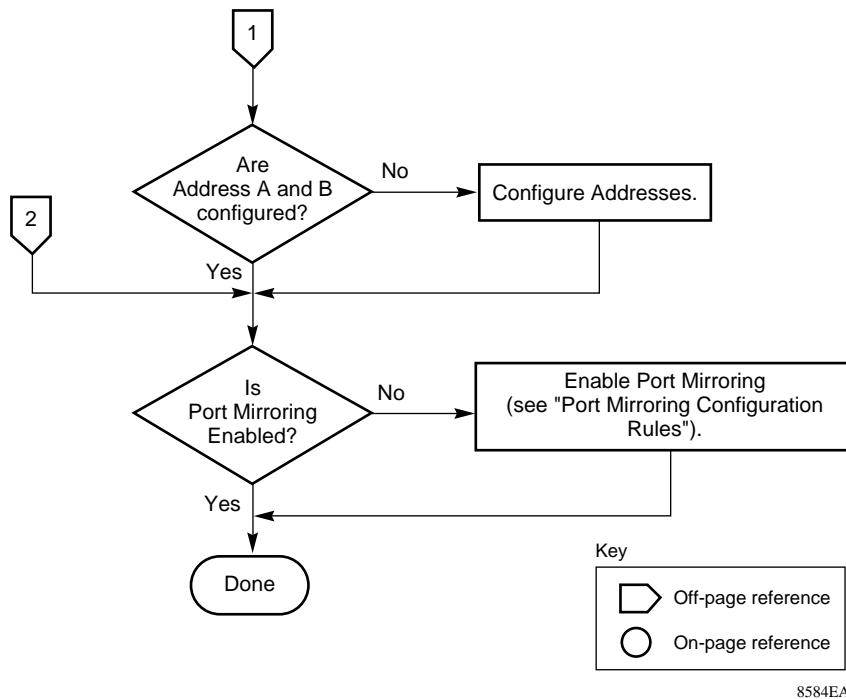
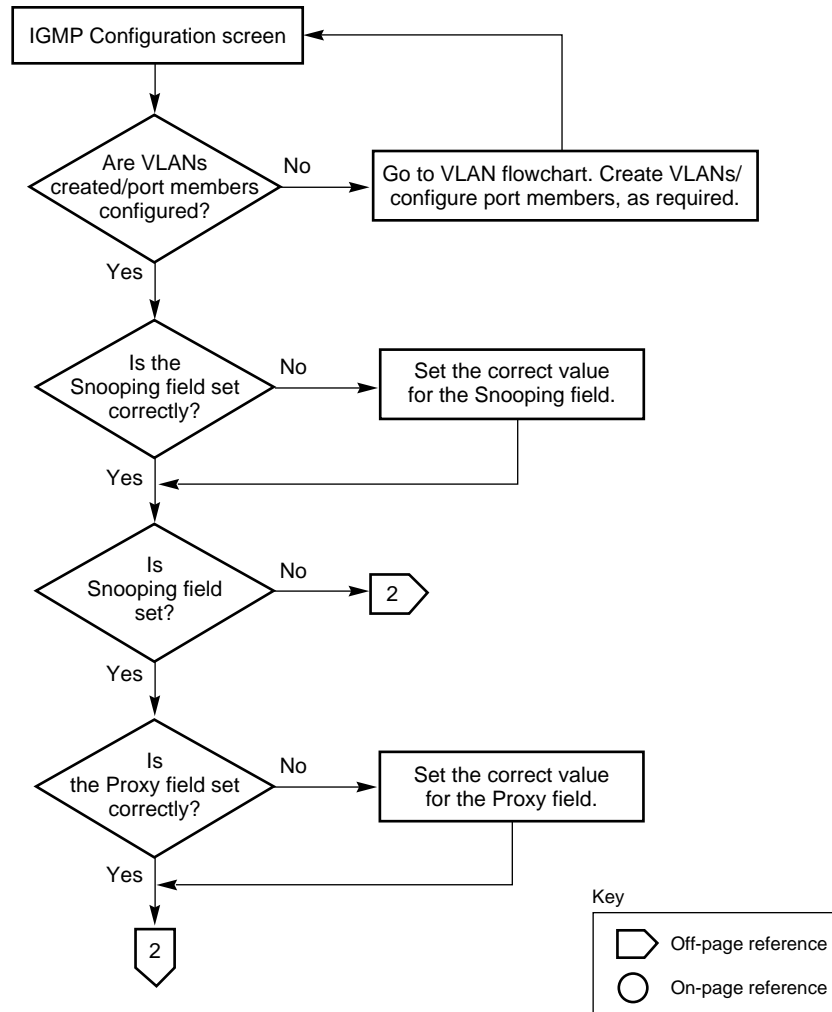


Figure C-6. Configuring Port Mirroring (2 of 2)

Configuring IGMP Snooping

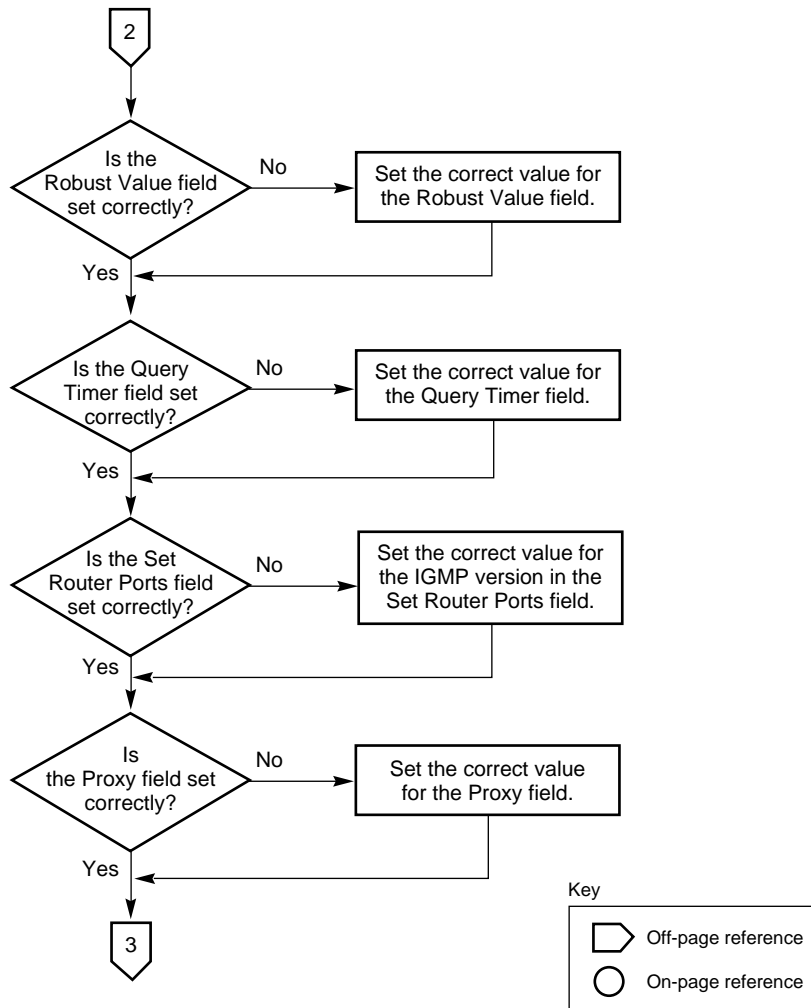
This section shows how to configure switch ports for IGMP Snooping or to modify existing IGMP Snooping ports (see [Figure C-7](#) to [Figure C-9](#)).

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



8585EA

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



8586EA

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

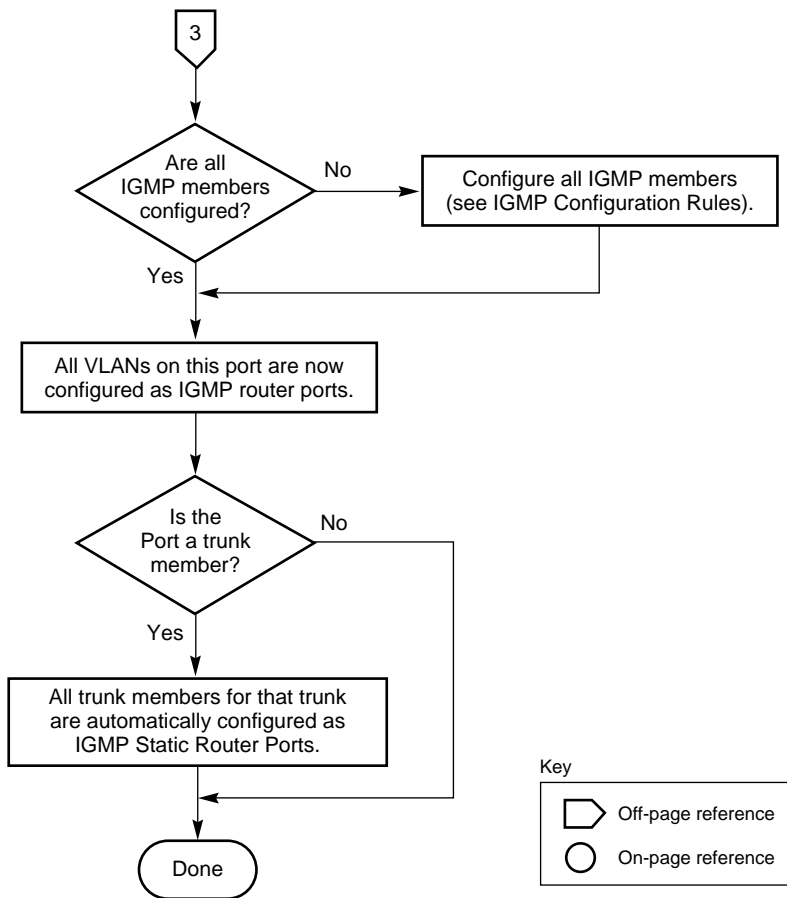


Figure C-9. Configuring IGMP Snooping (3 of 3)

Appendix D

Connectors and Pin Assignments

This appendix describes the BayStack 450 switch port connectors and pin assignments.

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

The RJ-45 port connectors ([Figure D-1](#)) are wired as MDI-X ports to connect end stations without using crossover cables. (See [“MDI and MDI-X Devices”](#) on [page D-2](#) for information about MDI-X ports.) For 10BASE-T connections, use Category 3 (or higher) UTP cable. For 100BASE-TX connections, use only Category 5 UTP cable.

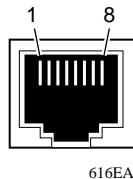


Figure D-1. RJ-45 (8-Pin Modular) Port Connector

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

Table D-1. RJ-45 Port Connector Pin Assignments

Pin	Signal	Description
1	RX+	Receive Data +
2	RX-	Receive Data -
3	TX+	Transmit Data +
4	Not applicable	Not applicable
5	Not applicable	Not applicable
6	TX-	Transmit Data -
7	Not applicable	Not applicable
8	Not applicable	Not applicable

MDI and MDI-X Devices

Media dependent interface (MDI) is the IEEE standard for the interface to unshielded twisted pair (UTP) cable.

For two devices to communicate, the transmitter of one device must connect to the receiver of the other device. The connection is established through a crossover function, which can be a crossover cable or a port that implements the crossover function internally.

Ports that implement the crossover function internally are known as MDI-X ports, where X refers to the crossover function.

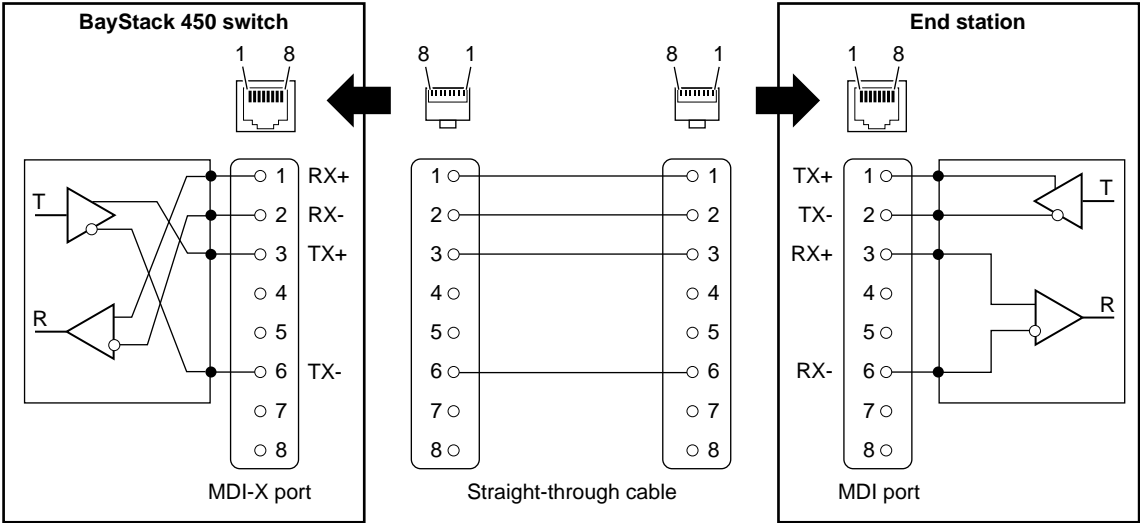


Note: For the transmitter of one device to connect to the receiver of another device, the total number of crossovers must always be an odd number.

The following sections describe the use of straight-through and crossover cables for connecting MDI and MDI-X devices.

MDI-X to MDI Cable Connections

BayStack 450 switches use MDI-X ports that allow you to connect directly to end stations without using crossover cables ([Figure D-2](#)).

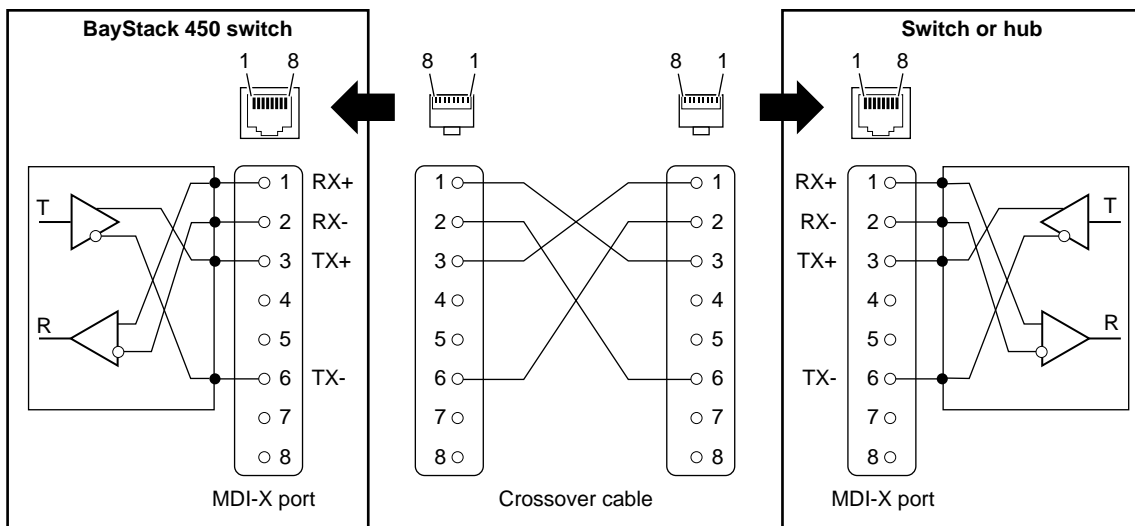


617EA

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

MDI-X to MDI-X Cable Connections

If you are connecting the BayStack 450 switch to a device that also implements MDI-X ports, use a crossover cable ([Figure D-3](#)).



618EA

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

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

The DB-9 Console/Comm Port connector ([Figure D-4](#)) is configured as a data communications equipment (DCE) connector. The DSR and CTS signal outputs are always asserted; the CD, DTR, RTS, and RI signal inputs are not used. This configuration enables a management station (a PC or console terminal) to connect directly to the switch using a straight-through cable.

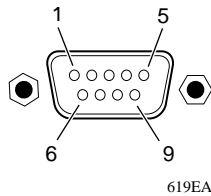


Figure D-4. DB-9 Console/Comm Port Connector

[Table D-2](#) lists the DB-9 Console/Comm Port connector pin assignments.

Table D-2. DB-9 Console/Comm Port Connector Pin Assignments

Pin	Signal	Description
1	CD	Carrier detect (not used)
2	TXD	Transmit data (output)
3	RXD	Receive data (input)
4	DTR	Data terminal ready (not used)
5	GND	Signal ground
6	DSR	Data set ready (output always asserted)
7	RTS	Request to send (not used)
8	CTS	Clear to send (output always asserted)
9	RI	Ring indicator (not used)
Shell		Chassis ground

Appendix E

Default Settings

[Table E-1](#) lists the factory default settings for the BayStack 450 switch.

Table E-1. Factory Default Settings for the BayStack 450 Switch

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

(continued)

Table E-1. Factory Default Settings for the BayStack 450 Switch *(continued)*

Field	Default setting	Appears in this CI screen
Aging Time	300 seconds	MAC Address Table
Find an Address	00-00-00-00-00-00 (no MAC address assigned)	
Port Mirroring Address A:	00-00-00-00-00-00 (no MAC address assigned)	
Port Mirroring Address B:	00-00-00-00-00-00 (no MAC address assigned)	
Create VLAN	1	VLAN Configuration
Delete VLAN	blank field	
VLAN Name	VLAN # (<i>VLAN number</i>)	
Port Membership	U (all ports assigned as untagged members of VLAN 1)	
Port	1	VLAN Port Configuration
Filter Tagged Frames	No	
Filter Untagged Frames	No	
Filter Unregistered Frames	No	
Port Name	Port # (<i>port number</i>)	
PVID	1	
Port Priority	0	
Note: The following two fields only appear when the port selected in the Port field is configured with an optional gigabit MDA.		
Primary VLAN Tagging	Untagged	
Secondary VLAN Tagging	Tagged	
Port	1	VLAN Display by Port
PVID	1 (read only)	
Port Name	Port # 1 (read only)	
Traffic Class	Low	Traffic Class Configuration
Status	Enabled (for all ports)	Port Configuration
Autonegotiation	Enabled (for all ports)	
Speed/Duplex	100Mbps/Half (when Autonegotiation is Disabled)	

(continued)

Table E-1. Factory Default Settings for the BayStack 450 Switch *(continued)*

Field	Default setting	Appears in this CI screen
Autonegotiation	Enabled	High Speed Flow Control Configuration
Flow Control	Disabled	
Note: The following two fields only appear when a single Phy MDA with a separate redundant Phy port is installed.		
Preferred Phy	Right	
Active Phy	Read-only field indicating the operational Phy port (Right, Left, or None)	
Trunk Members	blank field	MultiLink Trunk Configuration
STP	Normal	
Trunk Mode	Basic	
Trunk Status	Enabled	
Trunk Name	Trunk #1 to Trunk #6	
Traffic Type	Rx and Tx	Trunk Utilization
Monitoring Mode	Disabled	Port Mirroring Configuration
Monitor Port	Zero-length string	
Port X	Zero-length string	
Port Y	Zero-length string	
Address A	00-00-00-00-00-00 (no MAC address assigned)	
Address B	00-00-00-00-00-00 (no MAC address assigned)	
Packet Type	Both	Rate Limiting Configuration
Limit	None	
VLAN	1	IGMP Configuration
Snooping	Enabled	
Proxy	Enabled	
Robust Value	2	
Query Time	125 seconds	
Set Router Ports	Version 1	
Static Router Ports	- (for all ports)	

(continued)

Table E-1. Factory Default Settings for the BayStack 450 Switch *(continued)*

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

(continued)

Table E-1. Factory Default Settings for the BayStack 450 Switch *(continued)*

Field	Default setting	Appears in this CI screen
Event Logging	All	
Allowed Source IP Address (10 user-configurable fields)	First field: 0.0.0.0 (no IP address assigned) Remaining nine fields: 255.255.255.255 (any address is allowed)	
Allowed Source Mask (10 user-configurable fields)	First field: 0.0.0.0 (no IP address assigned) Remaining nine fields: 255.255.255.255 (any address is allowed)	
For details about this field, see Table 3-26 on page 3-66.		
Image Filename	Zero-length string	Software Download
TFTP Server IP Address	0.0.0.0 (no IP address assigned)	
Start TFTP Load of New Image	No	

Appendix F

Sample BootP Configuration File

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

A sample BootP configuration file follows:

```
# The following is a sample of a BootP configuration file that was extracted
# from a Bay Networks EZ LAN network management application. Note that other
# BootP daemons can use a configuration file with a different format.
#
# Before using your switch BootP facility, you must customize your BootP
# configuration file with the appropriate data.
#
# Blank lines and lines beginning with '#' are ignored.
#
# Legend:
#
#     first field -- hostname
#             ht -- hardware type
#             ha -- host hardware address
#             tc -- template host (points to similar host entry)
#             ip -- host IP address
#             hd -- bootfile home directory
#             bf -- bootfile
# EZ         dt -- device type
# EZ         fv -- firmware version
# EZ         av -- agent version
#
# Fields are separated with a pipe (|) symbol. Forward slashes (//) are
# required to indicate that an entry is continued to the next line.
#
```

```
# Caution
#
#   Omitting a Forward slash (/) when the entry is continued to the next
#   line, can cause the interruption of the booting process or the
#   incorrect image file to download. Always include forward slashes
#   where needed.
#
# Important Note:
#
#   If a leading zero (0) is used in the IP address it is calculated as an
#   octal number. If the leading character is "x" (upper or lower case),
#   it is calculated as a hexadecimal number. For example, if an IP address
#   with a base 10 number of 45 is written as .045 in the BOOTPTAB.TXT file,
#   the Bootp protocol assigns .037 to the client.
#
# Global entries are defined that specify the parameters used by every device.
# Note that hardware type (ht) is specified first in the global entry.
#
# The following global entry is defined for an Ethernet device. Note that this
# is where a client's subnet mask (sm) and default gateway (gw) are defined.
#
global|/
    |ht=ethernet|/
    |hd=c:\opt\images|/
    |sm=255.255.255.0|/
    |gw=192.0.1.0|
#
# The following sample entry describes a BootP client:

bay1|ht=ethernet|ha=0060fd000000|ip=192.0.0.1|hd=c:\ezlan\images|bf=b450_100.img

# Where:
#   host name:                bay1
#   hardware type:           Ethernet
#   MAC address:             00-60-FD-00-00-00
#   IP address:              192.0.0.1
#   home directory of boot file: c:\ezlan\images
#   boot file:               b450_100.img
```


Numbers

1000BASE-LX MDA
450-1LR MDA, B-6
450-1LX MDA, B-6
1000BASE-SX MDA
450-1SR MDA, B-4
450-1SX MDA, B-4
100BASE-FX MDA
400-2FX, B-4
10BASE-T/100BASE-TX MDA
400-4TX MDA, B-4

A

Actual Hello Interval, 3-63
Aging Time field, 3-19
Allowed Source IP Address field, 3-67
Allowed Source Mask field, 3-67
Authentication Trap field, 3-13
Autonegotiation
field, 3-32
autonegotiation
description, 1-12
autonegotiation modes
description, 1-11
troubleshooting, 4-5
Autosensing, 1-12

B

BayStack 450 switch
connectors, D-1
default port settings for VLANs, 1-21
features, 1-9 to 1-11
BootP Request Mode field, 3-8

BootP. *See* Bootstrap Protocol
Bootstrap Protocol (BootP)
Always setting, 3-10
automatic IP configuration, 1-14
BOOTPTAB.TXT file, F-1
choosing a request mode, 3-9
Disabled setting, 3-10
Last Address setting, 3-10
sample configuration file, F-1
setting IP address with, 1-15
When Needed setting, 3-9

Bridge Forward Delay field, 3-64
Bridge Hello Time field, 3-64
Bridge Maximum Age Time field, 3-64
Bridge Priority field, 3-63
Broadcasts field, 3-52

C

cable
for console/comm port, 2-8
Clear All Port Statistics option, 3-18
Collisions field, 3-53
Comm Port Data Bits field, 3-55
Comm Port Parity field, 3-55
Comm Port Stop Bits, 3-56
Community String field, 3-13
Configurable field, 3-8
Configuration rules
IGMP Snooping, 1-39
MultiLink Trunking, 1-56
Port Mirroring, 1-68
VLANs, 1-34
connectors, D-1

- AC power receptacle, 1-7
- DB-9 console/comm port connector, D-5
- RJ-45 port connector, D-1
- console interface
 - connection, 2-8
- console interface (CI)
 - main menu, 3-4
 - menus, using, 3-2
- Console Password field, 3-56
- Console Port Speed field, 3-56
- Console Read-Only Password field, 3-56
- Console Read-Write Password field, 3-56
- console/comm port
 - connecting to terminal, 2-8
 - illustration, D-5
 - pin assignments, D-5
- Console/Comm Port Configuration options, 3-5
- Console/Comm Port Configuration screen, 3-55
- conversation steering, 1-13
- cooling fans, 1-9
- crossover cable, D-4
- customer support
 - programs, xxii
 - Technical Solutions Centers, xxiii

D

E

- Event Log screen, 3-71
 - authentication failure, 3-71
 - event log flash memory, 3-72
 - excessive bad entries, 3-72
 - operational exception, 3-72
 - software download, 3-71
 - TELNET session status, 3-72
 - write threshold, 3-72
- Event Logging field, 3-66
- Excessive Collisions field, 3-53

F

- FCS Errors field, 3-52
- feet, chassis, 2-3
- Filtered Packets field, 3-54
- Find an Address field, 3-19
- flash memory for software image upgrades, 1-14
- flat surface, installing on, 2-3
- Flooded Packets field, 3-54
- Forward Delay field, 3-64
- forwarding rate (packets per second), 1-9
- Frame Errors field, 3-52

G

- gateway address setting, 2-14
- grounding the switch, 2-3, 2-4

H

- Hello Interval, 3-63, 3-64
- Hello Time field, 3-63

I

- IEEE 802.1p Prioritizing
 - feature, 1-13
- IEEE 802.1Q Tagging
 - important terms, 1-20
- IEEE 802.3u standard, 1-12

IEEE 802.3u-compliant autonegotiation, 1-11

IGMP Snooping

configuration rules, 1-39

feature, 1-13

Image Filename field, 3-69

In Use field, 3-8

Inactivity Timeout field, 3-66

In-Band IP Address field, 3-8

In-Band Subnet Mask field, 3-8

installation

chassis in a rack, 2-4

flat surface, 2-3

grounding, 2-3

LED verification, 2-11

requirements, 2-1

tools, 2-2

verifying, 2-10

IP address

format of, 2-15

setting

startup, 2-14

IP address, automatic configuration, 1-14

IP Configuration option, 3-4

IP Configuration screen, 3-7

IP subnet mask address, setting

startup, 2-14

L

Last BootP field, 3-8

Last Reset Type field, 3-15

Late Collisions field, 3-54

learning rate, addresses per second, 1-9

LEDs

indications during software download process, 3-70

status monitors, 1-11

verifying installation with, 2-11

Link field, 3-32

Login Retries field, 3-66

Login Timeout field, 3-66

Logout option, 3-6, 3-78

logout, password-protected, 3-78

Lost Packets field, 3-52

M

MAC address

location, 1-14

when configuring the BootP server, 1-14

MAC Address field, 3-15

MAC Address Table option, 3-17

MAC Address Table screen, 3-18

Main Menu

illustration, 2-14

main menu, console interface, 3-4

Management Information Base (MIB), 1-10

Maximum Age Time field, 3-63

MDAs

Installing, B-7

MDI-X to MDI cable connections, D-3

MDI-X to MDI-X cable connections, D-4

MIB. *See* Management Information Base

Multicasts field, 3-52

MultiLink Trunk Configuration option, 3-17

MultiLink Trunk Configuration screen, 3-35

MultiLink Trunking

configuration example, 1-44

configuration rules, 1-56

MultiLink Trunking description, 1-13

Multiple Collisions field, 3-53

N

network configuration

configuring power workgroups and a shared media hub, 1-18

network interface card (NIC)

connecting to, 2-7

network management, 1-14

network protocol/standards compatibility, A-2

O

options

- Clear All Port Statistics, 3-18
- Console/Comm Port Configuration, 3-5
- Display Event Log, 3-5
- Display Port Statistics, 3-18
- Display Spanning Tree Switch Settings, 3-58
- IP Configuration, 3-4
- Logout, 3-6
- MAC Address Table, 3-17
- MultiLink Trunk Configuration, 3-17
- Port Configuration, 3-17
- Port Mirroring Configuration, 3-17
- Rate Limiting Configuration, 3-17
- Reset, 3-4
- Reset to Default Settings, 3-6
- SNMP Configuration, 3-4
- Software Download, 3-5
- Spanning Tree Configuration, 3-5
- Spanning Tree Port Configuration, 3-58
- Switch Configuration, 3-5
- System Characteristics, 3-5
- TELNET Configuration, 3-5
- VLAN Configuration, 3-17
- Oversized Packets field, 3-53

P

- package contents, 2-1
- Packets field, 3-52
- Participation field, 3-61
- password prompt screen, 3-78
- Path Cost field, 3-61
- port cables, connecting, 2-7
- Port Configuration option, 3-17
- Port Configuration screen, 3-30
- port connections, troubleshooting, 4-5
- Port field, 3-31, 3-52, 3-60
- Port Mirroring
 - address-based, 1-65
 - Bay Networks StackProbe, 1-13
 - configuration rules, 1-68
 - conversation steering, 1-13
 - description, 1-13
 - monitoring modes, 3-44
 - port-based, 1-63
- Port Mirroring Configuration option, 3-17

- Port Mirroring Configuration screen, 3-42
- Port Statistics screen, 3-51
- port status LEDs, 2-11
- ports
 - connecting the console port, 2-8
 - IEEE 802.3u-compliant autonegotiation, 1-11
 - modes, 1-11
- power cords, 1-8
- Power LED, 2-11
- power on self tests, 2-10
- power, connecting, 2-9
- power-up sequence, 4-4
- Priority field, 3-61

R

- rack, standard, installing in, 2-4
- Rate limiting, 1-10
 - broadcast and multicast storms, 3-46
 - configuration, 3-45
- Rate Limiting Configuration option, 3-17
- Rate Limiting Configuration screen, 3-45
- Read-Only Community String field, 3-13
- Read-Write Community String field, 3-13
- remote monitoring (RMON), 1-12
- request mode, choosing, 3-9
- requirements
 - console terminal, 2-8
 - power cords, 1-8
- Reset Count field, 3-15
- Reset option, 3-5, 3-74
- Reset to Default Settings option, 3-6, 3-76
- RJ-45 port connector
 - illustration, D-1
 - pin assignments, D-2
- RMON. *See* remote monitoring
- Root Path Cost field, 3-63
- Root Port field, 3-63
- RS-232 console port, 2-8

S

- safety alert messages, xxv
- Self-Test screen
 - during software download process, 3-69
- settings, default, E-1
- Simple Network Management Protocol (SNMP)
 - MIB support, 1-10, 1-15
 - using to manage the switch, 1-15
- Single Collisions field, 3-53
- SNMP Configuration option, 3-4
- SNMP Configuration screen, 3-12
- SNMP. *See* Simple Network Management Protocol
- software
 - download process, 3-69
 - image upgrades, 1-14
- Software Download option, 3-5
- Software Download screen, 3-68
- Spanning Tree Configuration Menu, 3-57
- Spanning Tree Configuration option, 3-5
- Spanning Tree Port Configuration option, 3-58
- Spanning Tree Port Configuration screen, 3-59
- Spanning Tree Switch Settings screen, 3-62
- Speed/Duplex field, 3-32
- Start TFTP Load of New Image field, 3-69
- State field, 3-61
- Status field, 3-32
- switch
 - initial setup, 2-14
- Switch Configuration Menu, 3-16
 - options, 3-17
- Switch Configuration option, 3-5
- sysContact field, 3-15
- sysDescr field, 3-15
- sysLocation field, 3-15
- sysName field, 3-15
- sysObjectID field, 3-15
- sysServices field, 3-15
- System Characteristics option, 3-5
- System Characteristics screen, 3-14

- sysUpTime field, 3-15

T

- Technical Solutions Centers, xxiii
- technical specifications, A-1
- Technical terms
 - filtering database identifier (FID), 1-21
 - port priority, 1-20
 - Port VLAN Identifier (PVID), 1-20
 - tagged frame, 1-20
 - tagged member, 1-20
 - unregistered packet/frame, 1-20
 - untagged frame, 1-20
 - untagged member, 1-20
 - user_priority, 1-20
 - VLAN Identifier (VID), 1-20
 - VLAN port members, 1-20
- TELNET
 - event log operational exception, 3-72
 - event log session status, 3-72
 - Logout option, 3-78
 - supported features, 1-10
 - See also* Console/Comm Port Configuration screen
 - See also* TELNET Configuration screen
- TELNET Access field, 3-66
- TELNET Configuration option, 3-5
- TELNET Configuration screen, 3-65
- terminal requirements, 2-8
- TFTP Server IP Address field, 3-69
- TFTP. *See* Trivial File Transfer Protocol
- Total Octets field, 3-52
- Trap IP Address fields, 3-13
- traps, 1-15
- Trivial File Transfer Protocol (TFTP)
 - software download, 3-68
 - using to upgrade firmware, 1-11
- troubleshooting
 - port interface, 4-5
 - power-up sequence, 4-4
- Tutorial
 - IEEE 802.1Q tagging, 1-20
 - IEEE 802.1Q VLAN workgroups, 1-19

U

Undersized Packets field, 3-53

utility rack, 2-3

V

virtual LAN (VLAN), 1-15

- configuration rules, 1-34

- network example, 1-15

VLAN Configuration option, 3-17

VLAN Configuration screen, 3-21

VLANs

- IEEE 802.1Q VLANs feature, 1-12