

Software Release V3.0.0

Part No. 893-00992-E  
January 2000

4401 Great America Parkway  
Santa Clara, CA 95054

# Using the BayStack 350 Series 10/100 Autosense Switch

**NO**RTTEL  
NETWORKS™

---

## Copyright © 2000 Nortel Networks

All rights reserved. Printed in the USA. January 2000.

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

## Trademarks

NORTEL NETWORKS is a trademark of Nortel Networks Corporation.

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

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

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

## Statement of Conditions

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

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

## USA Requirements Only

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

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

## European Requirements Only

### EN 55 022 Statement

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

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

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

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

---

## EC Declaration of Conformity

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

## Japan/Nippon Requirements Only

### Voluntary Control Council for Interference (VCCI) Statement

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

### Voluntary Control Council for Interference (VCCI) Statement

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

## Taiwan Requirements

### Bureau of Standards, Metrology and Inspection (BSMI) Statement

警告使用者:

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

## Canada Requirements Only

### Canadian Department of Communications Radio Interference Regulations

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

### Règlement sur le brouillage radioélectrique du ministère des Communications

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

---

## Nortel Networks NA Inc. Software License Agreement

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

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

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

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

---

Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

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

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

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

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

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

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

Should you have any questions concerning this Agreement, contact Nortel Networks, 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 NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.



# Contents

## Preface

Audience .....	xix
Organization .....	xix
Text Conventions .....	xxi
Special Message Formats .....	xxii
Acronyms .....	xxii
Related Publications .....	xxiii
How to Get Help .....	xxiv

## Safety Messages

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

## Chapter 1

### Getting Started

Hardware .....	1-1
Front-Panel Components .....	1-2
Back-Panel Components .....	1-4
Cooling Fans .....	1-5
Features .....	1-5
Security .....	1-8
MAC Address-Based Security .....	1-9
RADIUS-Based and SNMP Security .....	1-9
Autosensing .....	1-10
MultiLink Trunking .....	1-10
Port Mirroring .....	1-11
Flash Memory Storage .....	1-11
BootP Automatic IP Configuration .....	1-12
SNMP MIB Support .....	1-12
Configuration and Switch Management .....	1-13

Network Configuration .....	1-13
Power Workgroups .....	1-14
Power Workgroups and Shared Media Hub .....	1-15
VLAN Workgroups .....	1-16
VLAN Configuration Screen Examples .....	1-20
Additional Tips About Configuring VLANs .....	1-23
MultiLink Trunks .....	1-24
Inter-Switch Trunk Configuration .....	1-24
Server Trunk Configuration .....	1-26
Client/Server Configuration Utilizing MultiLink Trunks .....	1-27
Trunk Configuration Screen Examples .....	1-29
Before Configuring Trunks .....	1-40
MultiLink Trunking Configuration Rules .....	1-41
Spanning Tree Considerations .....	1-42
Additional Tips About the MultiLink Trunking Feature .....	1-45
Port Mirroring (Conversation Steering) .....	1-45
Port-Based Mirroring Configuration .....	1-46
Address-Based Mirroring Configuration .....	1-49
Port Mirroring Configuration Rules .....	1-51
Quick-Start Procedures .....	1-51
Quick-Start to Installing the BayStack 350 Switch .....	1-52
Quick-Start to Managing the BayStack 350 Switch .....	1-53
Console/Service Port Interface .....	1-53
SNMP Management Applications .....	1-54

## **Chapter 2**

### **Installing the BayStack 350 Switch**

Required Tools and Materials .....	2-1
Package Contents .....	2-2
Site Preparation .....	2-3
Hardware .....	2-3
Software .....	2-4
Environment .....	2-4
Installation .....	2-5
Surface Mounting .....	2-5
Attaching the Mounting Brackets .....	2-6



Installing on a Table or Shelf .....	2-7
Wall Mounting .....	2-8
Before You Begin .....	2-8
Wall Mounting the Model 350F and Model 350T .....	2-9
Rack Mounting .....	2-10
Connecting Port Cables .....	2-13
RJ-45 Port Cables .....	2-13
100BASE-FX Port Cables .....	2-14
Connecting Power .....	2-15
Verifying the Installation .....	2-16

### Chapter 3

#### Using the Console Interface

Console Interface .....	3-1
Console/Service Port Cabling .....	3-2
Console Terminal Requirements .....	3-2
Modem Requirements .....	3-2
Connecting to the BayStack 350 Switch Console/Service Port .....	3-3
Accessing the CI Menus and Screens .....	3-3
Using the CI Menus and Screens .....	3-4
Navigating the CI Menus and Screens .....	3-5
Screen Fields and Descriptions .....	3-6
Main Menu .....	3-7
IP Configuration .....	3-10
Choosing a BootP Request Mode .....	3-12
BootP When Needed .....	3-12
BootP Always .....	3-12
BootP Disabled .....	3-13
BootP or Last Address .....	3-13
SNMP Configuration .....	3-14
SNMP Community Strings and Trap Addresses .....	3-16
<b>SNMP Port Trap Enable/Disable Options .....</b>	<b>3-18</b>
System Characteristics .....	3-20
Switch Configuration .....	3-22
MAC Address Table .....	3-24
MAC Address-Based Security .....	3-26

MAC Address Security Configuration .....	3-28
MAC Address Security Table .....	3-31
Accelerator Keys for Repetitive Tasks .....	3-32
VLAN Configuration .....	3-34
Port Configuration .....	3-36
MultiLink Trunk Configuration .....	3-39
Inter-Switch Trunk Configuration .....	3-41
Server Trunk Configuration .....	3-43
Trunk Utilization .....	3-45
Port Mirroring Configuration .....	3-48
Rate Limiting Configuration .....	3-51
Port Statistics .....	3-54
Console/Service Port Configuration .....	3-58
Setting Security Passwords .....	3-60
Spanning Tree Configuration .....	3-61
Spanning Tree Port Configuration .....	3-63
Display Spanning Tree Switch Settings .....	3-65
TELNET Configuration .....	3-68
Software Download .....	3-71
Configuration File .....	3-74
Network Security .....	3-77
Display Event Log .....	3-79
Excessive Bad Entries .....	3-80
Write Threshold .....	3-80
Reset .....	3-81
Reset to Default Settings .....	3-82
Logout .....	3-83

## **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 Susceptibility ..... A-3  
Declaration of Conformity ..... A-4

**Appendix B**  
**Server/Trunk Connections**

Optimal Server/Trunk Connections ..... B-1

**Appendix C**  
**Connectors and Pin Assignments**

RJ-45 (10BASE-T/100BASE-TX) Port Connectors ..... C-1  
MDI and MDI-X Devices ..... C-2  
    MDI-X to MDI Cable Connections ..... C-3  
    MDI-X to MDI-X Cable Connections ..... C-4  
DB-9 (RS-232-D) Console/Service Port Connector ..... C-5  
100BASE-FX Fiber Optic Port Connectors ..... C-6

**Appendix D**  
**Default Settings**

**Appendix E**  
**Sample BootP Configuration File**

**Index**



# Figures

Figure 1-1.	BayStack 350 Series Autosense Switch .....	1-1
Figure 1-2.	Front-panel components .....	1-2
Figure 1-3.	Back-panel components .....	1-4
Figure 1-4.	BayStack 350 Switch Security Feature .....	1-8
Figure 1-5.	Configuring power workgroups .....	1-14
Figure 1-6.	Configuring power workgroups and a shared media hub .....	1-15
Figure 1-7.	Port-based VLAN example .....	1-16
Figure 1-8.	VLANs spanning multiple switches .....	1-17
Figure 1-9.	Multiple VLANs sharing resources .....	1-18
Figure 1-10.	VLAN configuration spanning multiple BayStack 350 switches .....	1-19
Figure 1-11.	VLAN Configuration screen for switch SW1 .....	1-20
Figure 1-12.	VLAN Configuration screen for switch SW2 .....	1-21
Figure 1-13.	VLAN Configuration screen for switch SW3 .....	1-22
Figure 1-14.	VLAN Configuration screen for switch SW4 .....	1-23
Figure 1-15.	Inter-switch trunk configuration example .....	1-25
Figure 1-16.	Server trunk configuration example .....	1-27
Figure 1-17.	Client/server configuration example .....	1-28
Figure 1-18.	Choosing the Server Trunk Configuration screen .....	1-29
Figure 1-19.	Server Trunk Configuration screen for Switch SW1 .....	1-30
Figure 1-20.	Choosing the Inter-Switch Trunk Configuration screen .....	1-31
Figure 1-21.	Inter-Switch Trunk Configuration screen example .....	1-32
Figure 1-22.	VLAN Configuration screen example for switch SW1 (1 of 2) .....	1-34
Figure 1-23.	VLAN Configuration screen example for switch SW1 (2 of 2) .....	1-35
Figure 1-24.	Trunk Configuration screen for switch SW2 .....	1-36
Figure 1-25.	Trunk Configuration screen for switch SW3 .....	1-37
Figure 1-26.	Trunk Configuration screen for switch SW4 .....	1-39
Figure 1-27.	Path cost arbitration example .....	1-42
Figure 1-28.	Example 1: Correctly configured trunk .....	1-43
Figure 1-29.	Example 2: Detecting a misconfigured port .....	1-44

Figure 1-30.	Port-based mirroring configuration example .....	1-47
Figure 1-31.	Port Mirroring port-based screen example .....	1-48
Figure 1-32.	Address-based mirroring configuration example .....	1-49
Figure 1-33.	Port Mirroring address-based screen example .....	1-50
Figure 1-34.	Installation flowchart .....	1-52
Figure 2-1.	Package contents .....	2-2
Figure 2-2.	Attaching mounting brackets for a surface mount .....	2-6
Figure 2-3.	Attaching rubber footpads .....	2-7
Figure 2-4.	Wall mounting the Model 350F and Model 350T .....	2-9
Figure 2-5.	Attaching mounting brackets for a rack mount (standard method) .....	2-11
Figure 2-6.	Attaching mounting brackets for a rack mount (alternative method) .....	2-11
Figure 2-7.	Installing the BayStack 350 switch in an equipment rack .....	2-12
Figure 2-8.	Connecting RJ-45 port cables .....	2-13
Figure 2-9.	Connecting 100BASE-FX port cables .....	2-14
Figure 2-10.	Observing LEDs to verify proper operation .....	2-16
Figure 3-1.	Map of console interface screens .....	3-6
Figure 3-2.	Console interface main menu .....	3-7
Figure 3-3.	IP Configuration screen .....	3-10
Figure 3-4.	SNMP Configuration Screen .....	3-14
Figure 3-5.	SNMP Community Strings and Trap Addresses screen .....	3-16
Figure 3-6.	SNMP Port Link Up/Down Trap Option Screen .....	3-18
Figure 3-7.	System Characteristics screen .....	3-20
Figure 3-8.	Switch Configuration Menu screen .....	3-22
Figure 3-9.	MAC Address Table screen .....	3-24
Figure 3-10.	MAC Address Security Configuration Menu .....	3-26
Figure 3-11.	MAC Address Security Configuration Screen .....	3-28
Figure 3-12.	MAC Address Security Table Screen .....	3-31
Figure 3-13.	Model 350F-HD VLAN Configuration screen (1 of 2) .....	3-34
Figure 3-14.	Model 350F-HD VLAN Configuration screen (2 of 2) .....	3-35
Figure 3-15.	Model 350F-HD Port Configuration screen (1 of 2) .....	3-36
Figure 3-16.	Model 350F-HD Port Configuration screen (2 of 2) .....	3-37
Figure 3-17.	MultiLink Trunk Configuration Menu screen .....	3-39
Figure 3-18.	Inter-Switch Trunk Configuration screen .....	3-41
Figure 3-19.	Server Trunk Configuration screen .....	3-43
Figure 3-20.	Trunk Utilization screen (1 of 2) .....	3-45

Figure 3-21.	Trunk Utilization screen (2 of 2)	3-46
Figure 3-22.	Port Mirroring Configuration screen	3-48
Figure 3-23.	Model 350F-HD Rate Limiting Configuration screen (1 of 2)	3-51
Figure 3-24.	Model 350F-HD Rate Limiting Configuration screen (2 of 2)	3-52
Figure 3-25.	Port Statistics screen	3-54
Figure 3-26.	Console/Service Port Configuration screen	3-58
Figure 3-27.	Spanning Tree Configuration Menu screen	3-62
Figure 3-28.	Model 350T Spanning Tree Port Configuration screen	3-63
Figure 3-29.	Spanning Tree Switch Settings screen	3-65
Figure 3-30.	TELNET Configuration screen	3-68
Figure 3-31.	Software Download screen	3-71
Figure 3-32.	Configuration File Download/Upload Screen	3-74
Figure 3-33.	Radius Network Security Screen	3-77
Figure 3-34.	Event Log screen	3-79
Figure 3-35.	Sample event log entry showing excessive bad entries	3-80
Figure 3-36.	Sample event log event exceeding the write threshold	3-80
Figure 3-37.	Self-Test screen after resetting the switch	3-81
Figure 3-38.	Self-Test screen after resetting the switch to factory default settings	3-82
Figure 3-39.	Password prompt screen	3-83
Figure 4-1.	LED locations	4-2
Figure C-1.	RJ-45 (8-pin modular) port connector	C-1
Figure C-2.	MDI-X to MDI cable connections	C-3
Figure C-3.	MDI-X to MDI-X cable connections	C-4
Figure C-4.	DB-9 console/service port connector	C-5
Figure C-5.	100BASE-FX multimode fiber optic port connector	C-6





# Tables

Table 1-1.	Front-panel components .....	1-3
Table 1-2.	Back-panel components .....	1-4
Table 2-1.	Power-up sequence .....	2-16
Table 3-1.	Console interface main menu commands .....	3-7
Table 3-2.	IP Configuration screen fields .....	3-11
Table 3-3.	SNMP Configuration Menu Screen Options .....	3-15
Table 3-4.	SNMP Configuration screen fields .....	3-17
Table 3-5.	SNMP Port Link Up/Down Trap Option Screen Fields .....	3-19
Table 3-6.	System Characteristics screen fields .....	3-21
Table 3-7.	Switch Configuration Menu Options .....	3-23
Table 3-8.	MAC Address Table screen fields .....	3-25
Table 3-9.	MAC Address Security Configuration Menu Options .....	3-27
Table 3-10.	MAC Address Security Configuration Screen Fields .....	3-29
Table 3-11.	MAC Address Security Table Screen Fields .....	3-32
Table 3-12.	VLAN Configuration screen fields .....	3-35
Table 3-13.	Port Configuration screen fields .....	3-37
Table 3-14.	MultiLink Trunk Configuration Menu Options .....	3-40
Table 3-15.	Inter-Switch Trunk Configuration screen fields .....	3-42
Table 3-16.	Server Trunk Configuration screen fields .....	3-44
Table 3-17.	Trunk Utilization screen fields .....	3-46
Table 3-18.	Port Mirroring Configuration screen fields .....	3-49
Table 3-19.	Monitoring Modes .....	3-50
Table 3-20.	Rate Limiting Configuration screen fields .....	3-53
Table 3-21.	Port Statistics screen fields .....	3-55
Table 3-22.	Console/Service Port Configuration screen fields .....	3-58
Table 3-23.	Determining Console Security Requirements .....	3-60
Table 3-24.	Determining TELNET Sessions Security Requirements .....	3-60
Table 3-25.	Determining the Screen Values .....	3-61
Table 3-26.	Spanning Tree Configuration Menu Options .....	3-62

Table 3-27.	Spanning Tree Port Configuration screen fields .....	3-64
Table 3-28.	Spanning Tree Switch Settings parameters .....	3-66
Table 3-29.	TELNET Configuration screen fields .....	3-69
Table 3-30.	Software Download screen fields .....	3-72
Table 3-31.	LED indications during the software download process .....	3-73
Table 3-32.	Configuration File Download/Upload Screen Fields .....	3-75
Table 3-33.	Parameters Not Saved to the Configuration File .....	3-76
Table 3-34.	RADIUS Network Security Screen Fields .....	3-78
Table 4-1.	LED indications .....	4-3
Table 4-2.	Corrective actions .....	4-4
Table B-1.	Optimal server/trunk connections .....	B-1
Table C-1.	RJ-45 port connector pin assignments .....	C-2
Table C-2.	DB-9 console/service port connector pin assignments .....	C-5
Table D-1.	Factory default settings for the BayStack 350 switch .....	D-1

---

# Preface

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

There are four versions of the BayStack 350 Series 10/100 Autosense Switch: the Model 350F-HD, the Model 350F, the Model 350T-HD, and the Model 350T. This guide describes the features, uses, and installation procedures for the four models. (Unless otherwise specified, the terms “BayStack 350 switch” and “switch” refer to all four switch versions.)

## Audience

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

## Organization

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

---

<b>If you want to:</b>	<b>Go to:</b>
Learn about the BayStack 350 switch and its key features. This chapter also describes the Quick-Start procedures for quick access to the switch management features.	Chapter 1
Install the BayStack 350 switch on a flat surface, in a 19-inch equipment rack, on a wall, and to verify its operation	Chapter 2

*(continued)*

---

<b>If you want to:</b>	<b>Go to:</b>
Connect to the BayStack 350 switch Console/Service Port and learn how to use the console interface (CI) menus to configure and manage the switch	Chapter 3
Troubleshoot and diagnose problems with the BayStack 350 switch, as indicated by the LEDs	Chapter 4
View operational and environmental specifications that apply to the BayStack 350 switch	Appendix A
View a table that lists model-specific port groups to use when connecting MultiLink trunks to servers using a single media access control (MAC) address. (These port groups provide optimal throughput for switch to server connections.)	Appendix B
Learn more about the BayStack 350 switch connectors (ports) and pin assignments	Appendix C
View a listing of the factory default settings for the BayStack 350 switch	Appendix D
View a sample BootP configuration file	Appendix E
View an alphabetical listing of the topics and subtopics in this guide, with cross-references to relevant information	Index

---

---

## Text Conventions

This guide uses the following text conventions:

<b>bold text</b>	Indicates command names and options and text that you need to enter. Example: Enter <b>show ip {alerts   routes}</b> . Example: Use the <b>dinfo</b> command.
<i>italic text</i>	Indicates file and directory names, new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is: <b>show at &lt;valid_route&gt;</b> <i>valid_route</i> is one variable and you substitute one value for it.
screen text	Indicates system output, for example, prompts and system messages. Example: Set Trap Monitor Filters
[Enter]	Named keys in text are enclosed in square brackets. The notation [Enter] is used for the Enter key and the Return key.
[Ctrl]-C	Two or more keys that must be pressed simultaneously are shown in text linked with a hyphen (-) sign.

## 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.

---

## Acronyms

This guide uses the following acronyms:

AUI	attachment unit interface
BootP	Bootstrap Protocol
CSMA/CD	carrier sense multiple access/collision detection
IP	Internet Protocol
ISO	International Organization for Standardization
MAC	media access control
MAU	media access unit
MDI-X	medium dependent interface crossover
PPP	Point-to-Point Protocol
SNMP	Simple Network Management Protocol
STP	shielded twisted pair

## Related Publications

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

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

Describes Nortel Networks realtime security system that safeguards Ethernet networks from unauthorized surveillance and intrusion.

You can print selected technical manuals and release notes free, directly from the Internet. Go to [support.baynetworks.com/library/tpubs/](http://support.baynetworks.com/library/tpubs/). Find the 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](http://www.adobe.com).

You can purchase selected documentation sets, CDs, and technical publications through the collateral catalog. The catalog is located on the World Wide Web at [support.baynetworks.com/catalog.html](http://support.baynetworks.com/catalog.html) and is divided into sections arranged alphabetically:

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

## How to Get Help

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

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

<b>Technical Solutions Center</b>	<b>Telephone Number</b>
Billerica, MA	800-2LANWAN (800-252-6926)
Santa Clara, CA	800-2LANWAN (800-252-6926)
Valbonne, France	33-4-92-96-69-68
Sydney, Australia	61-2-9927-8800
Tokyo, Japan	81-3-5402-7041



---

# 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 (Wall Mount)

---

Page 2-1

---



**Caution:** The screws and wall composition must be able to withstand the weight of the device, plus the additional weight of the attached network cables and power cords.

---



**Achtung:** Schrauben und Wand müssen so beschaffen sein, daß sie dem Gewicht des Geräts, zuzüglich des Gewichts der angeschlossenen Netzwerk- und Netzstromkabel, standhalten können.

---



**Attention:** Les vis de fixation et le mur doivent être capables de supporter le poids du dispositif, ainsi que des câbles réseau et cordons qui y sont rattachés.

---



**Precaución:** Los tornillos y la composición de la pared deben ser capaces de sostener el peso del dispositivo más el peso adicional de los cables de red y cables de alimentación conectados.

---



**Attenzione:** Le viti e la struttura a muro devono essere in grado di sostenere il peso del dispositivo, oltre a quello dei cavi di rete e di alimentazione collegati.

---



注意：ネジや壁の材質がデバイスとこれに接続されているネットワーク・ケーブルおよび電源コードを合わせた重さに耐える必要があります。

---

---

## 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。

---

## Hazardous Electrical Current

---

Page 2-5

---



**Warning:** To avoid bodily injury from hazardous electrical current, do not connect the power cord until instructed to do so.

---



**Vorsicht:** Um Verletzungsgefahr durch einen elektrischen Stromschlag auszuschließen, schließen Sie das Netzstromkabel erst an, wenn Sie dazu angewiesen werden.

---



**Avertissement:** Pour éliminer tout risque d'électrocution, ne jamais brancher le cordon avant le moment indiqué dans le mode d'emploi.

---



**Advertencia:** A fin de evitar daños personales debidos a corrientes eléctricas peligrosas, no conecte el cable de alimentación hasta que se le indique.

---



**Avvertenza:** Per evitare lesioni fisiche dovute a scariche elettriche pericolose, non collegare il cavo di alimentazione prima del momento indicato nelle istruzioni.

---



**警告:** 危険な電流から身体を保護するために、指示が出るまで電源コードを接続しないでください。

---

---

## Stacking Units in a Rack

---

Page 2-10

---



**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。

---

## Hazardous Light Source

---

### Page 2-14

---



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

---



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

---



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

---



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

---



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

---



**警告:** 光ファイバ装置は目に有害なレーザー光や赤外線を放射することがあります。光ファイバやコネクタ・ポートを覗き込まないでください。光ファイバ・ケーブルは光源に接続されているものと思ってください。

---



---

## Turning Off Power to the Unit

---

Page 2-15

---



**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ける場所に接続してください。

---

## Reset to Default Settings Command

---

Page 3-9

---



**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、現在のコンフィギュ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 3-59

---



**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 3-60

---



**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・インタフェー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 3-71

---



**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。

---

---

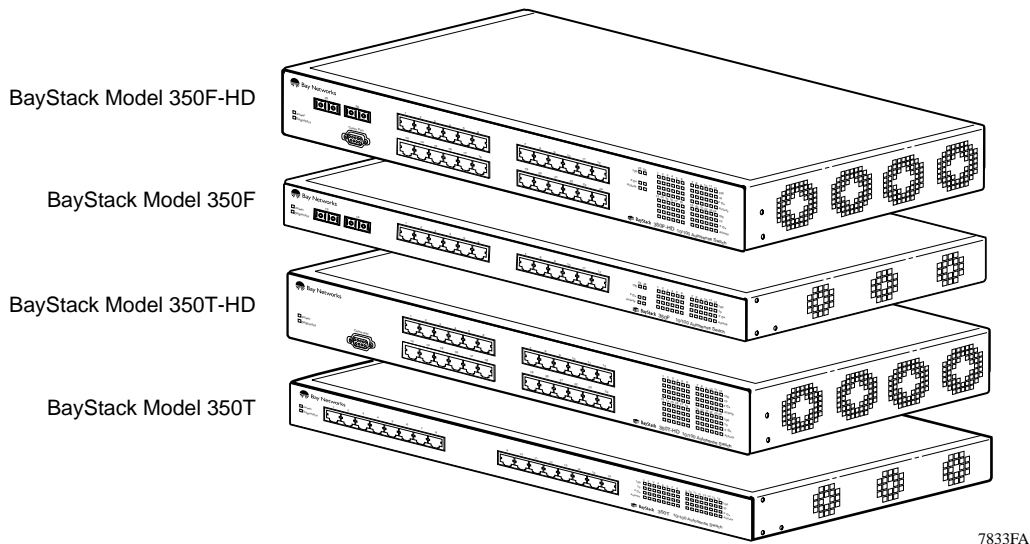
# Chapter 1

## Getting Started

This chapter introduces the BayStack 350 Series 10/100 Autosense Switch and provides network configuration examples. It also describes the Quick-Start procedures, which allow you to quickly set up parameters to manage the switch using the Simple Network Management Protocol (SNMP) or the console/service port.

### Hardware

There are four versions of the BayStack 350 switch: the Model 350F-HD, the Model 350F, the Model 350T-HD, and the Model 350T ([Figure 1-1](#)).

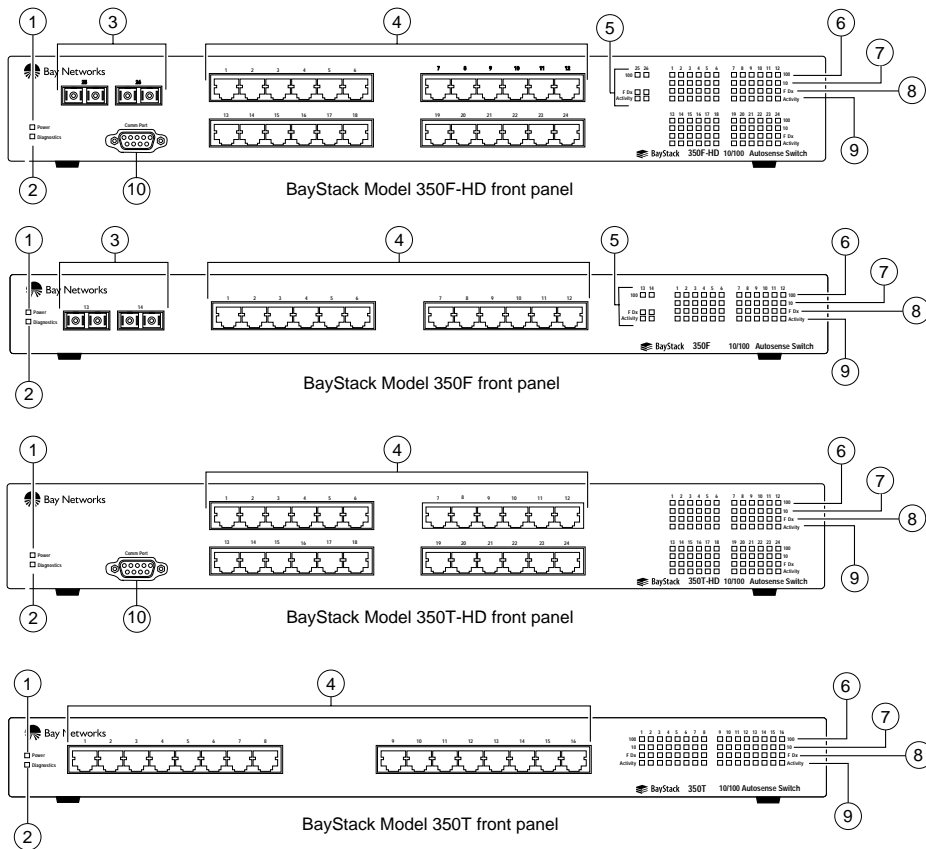


**Figure 1-1. BayStack 350 Series Autosense Switch**

## Front-Panel Components

This section describes the front-panel components of the BayStack 350 switches ([Figure 1-2](#)). For a description of each numbered component, see [Table 1-1](#).

- The Model 350F-HD provides 24 autosense 10/100BASE-TX ports and two 100BASE-FX fiber optic ports.
- The Model 350F provides 12 autosense 10/100BASE-TX ports and two 100BASE-FX fiber optic ports.
- The Model 350T-HD provides 24 autosense 10/100BASE-TX ports.
- The Model 350T provides 16 autosense 10/100BASE-TX ports.



7831EA

**Figure 1-2. Front-panel components**



**Table 1-1. Front-panel components**

Item	Icon/Label	Description
1	Power	Power LED (green): On: DC power is available to the switch's internal circuitry.
2	Diagnostics	Diagnostics LED (green): On: The switch passed the self-test. Blinking: A nonfatal error occurred during the self-test. Off: The switch failed the self-test.
3	(port numbers)	100BASE-FX fiber optic port connectors.
4	(port numbers)	10BASE-T/100BASE-TX RJ-45 (8-pin modular) port connectors. <sup>1</sup>
5	(port numbers)	100BASE-FX LED matrix.
6	100	100BASE-FX/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.
7	10 <sup>2</sup>	10BASE-T port status LEDs (yellow): 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.
8	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.
9	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.
10	Comm Port <sup>3</sup>	Console/service port DB-9 (RS-232-D) serial port connector: Allows the attachment of a console terminal device for accessing the console interface (CI) screens.

<sup>1</sup> Require 100-ohm unshielded twisted pair (UTP) cable. The RJ-45 connectors are wired as MDI-X ports to connect end stations without using crossover cables.

<sup>2</sup> Not available on the fiber optic 100BASE-FX LED matrix.

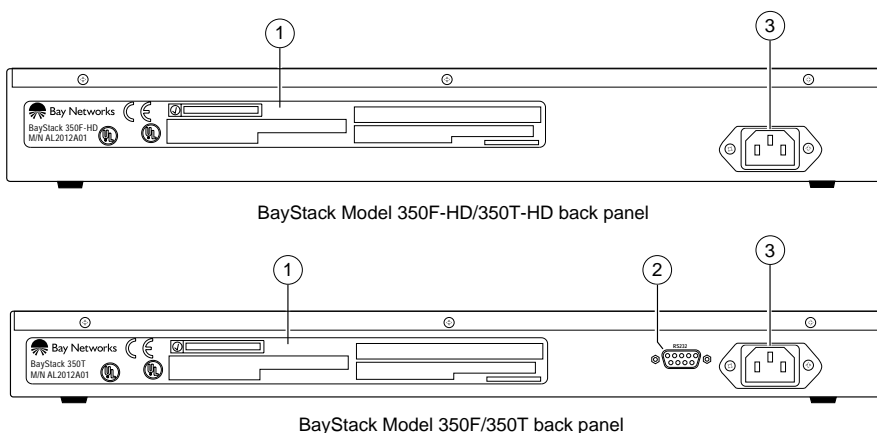
<sup>3</sup> The console/service port for the Model 350F and Model 350T, labeled RS232, is located on the back panel (see [“Back-Panel Components”](#) on [page 1-4](#)).

## Back-Panel Components

This section describes the back-panel components of the BayStack 350 switches ([Figure 1-3](#)).

- The console/service port for the Model 350F-HD and Model 350T-HD is located on the front panel (see [“Front-Panel Components”](#) on [page 1-2](#)).
- The console/service port for the Model 350F and Model 350T is located on the back panel.

For a description of each numbered component, see [Table 1-2](#).



7830EB

**Figure 1-3. Back-panel components**

**Table 1-2. Back-panel components**

Item	Icon/Label	Description
1		Manufacturing label: Lists the model number, serial number, MAC address, and voltage rating.
2	RS232 <sup>1</sup>	Console/service port DB-9 (RS-232-D) serial port connector: Allows the attachment of a console terminal device for accessing the console interface (CI) screens.
3		AC power receptacle <sup>2</sup> : Accepts the AC power cord (supplied).

<sup>1</sup> The console/service port for the Model 350F-HD, labeled Comm Port, is located on the front panel.

<sup>2</sup> The AC power receptacle is mounted with the ground pin below on some early units. Later units are configured as shown above. The receptacle is keyed and the AC power cord cannot be installed incorrectly.

## Cooling Fans

Variable-speed cooling fans in the BayStack 350 switch provide cooling for the internal components. When you install the switch, be sure to allow enough space on both sides of the switch for adequate air flow.

## Features

BayStack 350 switches provide wire-speed, 100BASE-TX/100BASE-FX (Fast Ethernet) switching that allows high-performance, low-cost connections to full-duplex and half-duplex 10 Mb/s and 100 Mb/s Ethernet local area networks (LANs).

Based on advanced application-specific integrated circuit (ASIC) technology, BayStack 350 switches can be cost effectively deployed in 10 Mb/s LANs.

BayStack 350 switches adjust (autonegotiate) their port speed and duplex mode to match the best service provided by connected stations, up to 100 Mb/s in full-duplex mode. As performance requirements increase and 100 Mb/s LANs are deployed, each port uses autosensing to support any combination of 10 Mb/s and 100 Mb/s Ethernet LANs.

One of the many benefits provided by the BayStack 350 switch is that network users can migrate from 10 Mb/s switching to 100 Mb/s switching using a single product.

The BayStack 350 switch offers the following features:

- High-speed forwarding rate: 1.6 million packets per second (peak)
- Learning rate: 1.6 million addresses per second (peak)
- Spanning Tree Protocol (STP): Complies with IEEE 802.1D standard
- SNMP agent support for the following Management Information Bases (MIBs):
  - Bridge MIB (RFC 1493)
  - Ethernet MIB (RFC 1643)
  - Proprietary MIBs
  - RMON MIB (RFC 1757)
  - MIB-II (RFC 1213)

- Configuration File download/upload support: Allows you to store your switch configuration parameters on a TFTP server. You can retrieve the configuration parameters for automatically configuring a replacement switch or other switches.
- Security:
  - MAC address-based security: Allows you to limit access to the switch based on MAC addresses.
  - RADIUS network security: Allows you to set up your switch with RADIUS-based (Remote Authentication Dial-In User Services) security, for authenticating TELNET logins.
  - SNMP security: Allows you to limit administration access to the switch via IP filtering.
- Rate limiting: Adjustable broadcast and multicast packet-rate limits for control of broadcast and multicast storms
- Store-and-forward switch: Full-performance forwarding at full line speed
- Console/service 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 802.3u-compliant autonegotiation ports, with four modes:
  - 10BASE-T half-duplex
  - 10BASE-T full-duplex
  - 100BASE-TX half-duplex
  - 100BASE-TX full-duplex

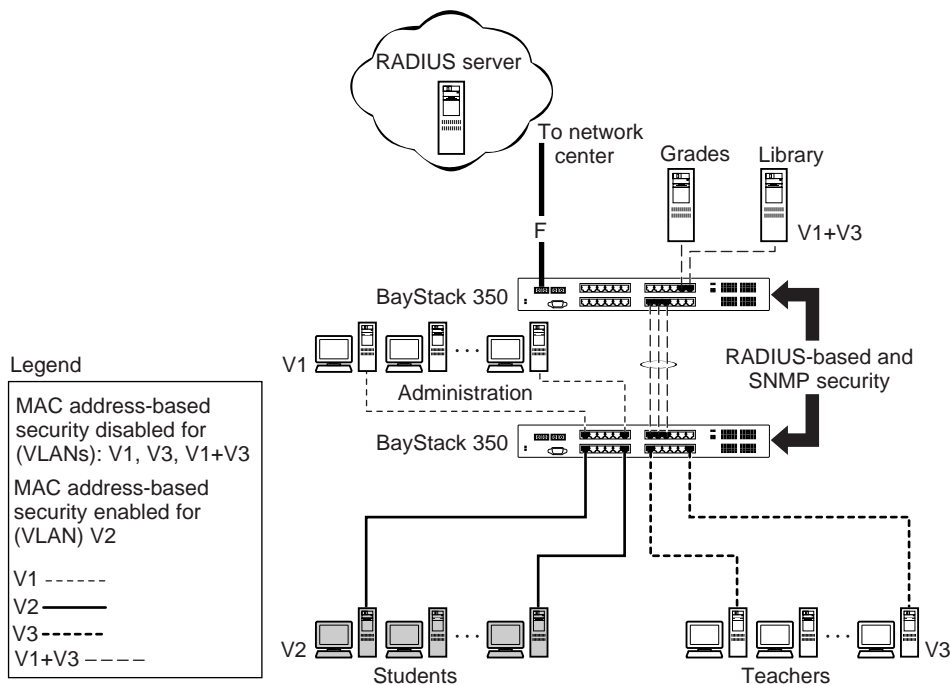
- MultiLink Trunking
  - Inter-switch trunks
  - Server based trunks
- Remote monitoring (RMON), with four groups integrated:
  - Statistics
  - History
  - Alarms
  - Events
- Port-based virtual LANs (VLANs)
- Port Mirroring
  - Port-based
  - MAC address-based
- Front-panel light emitting diodes (LEDs) to monitor the following:
  - Power status
  - System status
  - Port status for the following:
    - 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)

## Security

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

- MAC address-based security -- Limits access to the switch based on allowed source MAC addresses.
- RADIUS-based security -- Limits administrative access to the switch through user authentication.
- SNMP security -- Limits administration access via IP filtering.

[Figure 1-4](#) shows a typical campus VLAN configuration using security features. This example assumes that the administration and teachers offices (and the switches) are physically secured. In this configuration, the student VLAN (V2) is denied access to ports occupied by VLANs V1, V3, and V1 + V3. Only students who are authorized (as specified by the MAC address-based security feature) can access the switch on the secured ports.



BS35076A

**Figure 1-4. BayStack 350 Switch Security Feature**

---

## MAC Address-Based Security

The MAC address-based security feature allows you to set up network access control, based on source MAC addresses of authorized stations. You can specify a range of system responses to unauthorized access, which can range from sending a trap to disabling the intruder port. You can create a list of up to 98 MAC addresses and specify which addresses are authorized or not authorized to connect to the switch. You can also specify which of the switch ports each MAC address is allowed to access. The options for allowed port access include: NONE, ALL, and single or multiple ports that are specified in a list, for example, 1-4, 6, 9, etc.

The MAC address-based Security feature is based on Nortel Networks BaySecure LAN Access for Ethernet, a real-time security system that safeguards Ethernet networks from unauthorized surveillance and intrusion. To learn more about the Nortel Networks BaySecure LAN Access for Ethernet, refer to the *Bay Networks Guide to Implementing BaySecure LAN Access for Ethernet* (Part number 345-1106A).



**Note:** You must also include the MAC address of any router connected to any secure ports.

---

You can also specify optional actions to be exercised by the switch if the software detects a security violation. The response can be to send a trap, turn on destination address (DA) filtering, disable the specific port, or any combination of these three options. For instructions on using the console interface (CI) to set up network access control, see “MAC Address-Based Security” on page 3-26.

## RADIUS-Based and SNMP Security

The RADIUS-based and SNMP security features allows you to set up network access control, using the RADIUS (Remote Authentication Dial-In User Services) security protocol and selective IP filtering. The RADIUS-based security feature uses the RADIUS protocol to authenticate TELNET logins. SNMP-based security limits administration access to the switch, based on IP address filters.

For instructions on using the console interface (CI) to set up the RADIUS-based Security feature, see “Network Security” on page 3-77.

For instructions on using the console interface (CI) to set up SNMP Security , see “TELNET Configuration” on page 3-68.

## Autosensing

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

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

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

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

## MultiLink Trunking

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

The switch supports a load balancing function that allows the switch to spread traffic evenly across trunk members (ports that comprise a trunk), whenever possible, to achieve the highest aggregate throughput. In addition, the MultiLink Trunking software can detect misconfigured (or broken) trunk links. If this happens, the software redirects all traffic on the misconfigured or broken trunk member to other trunk members within that trunk.

The trunk members form a physical collection of ports that are treated as a single logical link of higher bandwidth by the spanning tree protocol (STP) and the learning, forwarding, and filtering functions.

For more information about the MultiLink Trunking feature, see “[MultiLink Trunks](#)” on [page 1-24](#).



## 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 Nortel Networks StackProbe™, or equivalent) to the designated monitor port. The designated port can monitor all traffic on the network segment connected to the mirrored port. Error packets can also be monitored and copied to the mirrored port for network troubleshooting.

For more information about the mirroring feature, see “[Port Mirroring \(Conversation Steering\)](#)” on [page 1-45](#).

## Flash Memory Storage

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

An in-band connection between the switch and the TFTP load host is required to download the software image (see “Software Download” on page 3-71).

For information about connecting a console terminal for this procedure, see “Console/Service Port Cabling” on page 3-2.



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

---

## **BootP Automatic IP Configuration**

The BayStack 350 switch has a unique 48-bit hardware address, or MAC address, that is printed on a label on the back panel. You use this MAC address when you configure the network BootP server to recognize the BayStack 350 switch BootP requests. A properly configured BootP server enables the switch to automatically learn its assigned IP address, subnet mask, IP address of the default router (default gateway), and software image file name.

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

## **SNMP MIB Support**

The BayStack 350 switch supports an SNMP agent with private MIB extensions, which ensures compatibility with existing network management tools. The BayStack 350 switch supports MIB-II (RFC 1213) and the RMON MIB (RFC 1757), which provide access to detailed management statistics. With SNMP management, you can configure SNMP traps (on individual ports) to be generated automatically for conditions such as an unauthorized access attempt or changes in a port's operating status.

## Configuration and Switch Management

The BayStack 350 switch is shipped directly from the factory ready to operate in any 10BASE-T or 100BASE-TX standard network. You can manage the switch using the Nortel Networks Optivity® network management software 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/service port or BootP, which resides on the switch.

For more information about using the console/service port to configure the switch, see Chapter 3, "Using the Console Interface."

## Network Configuration

You can use BayStack 350 switches to connect workstations, personal computers (PCs), and servers to each other by connecting these devices directly to the switch, through a shared media hub that is connected to the switch, or by creating a virtual LAN (VLAN) through the switch.

This section provides five network configuration examples using BayStack 350 switches:

- Power workgroups
- Power workgroups and a shared media hub
- VLAN workgroups
- MultiLink trunks
- Port mirroring

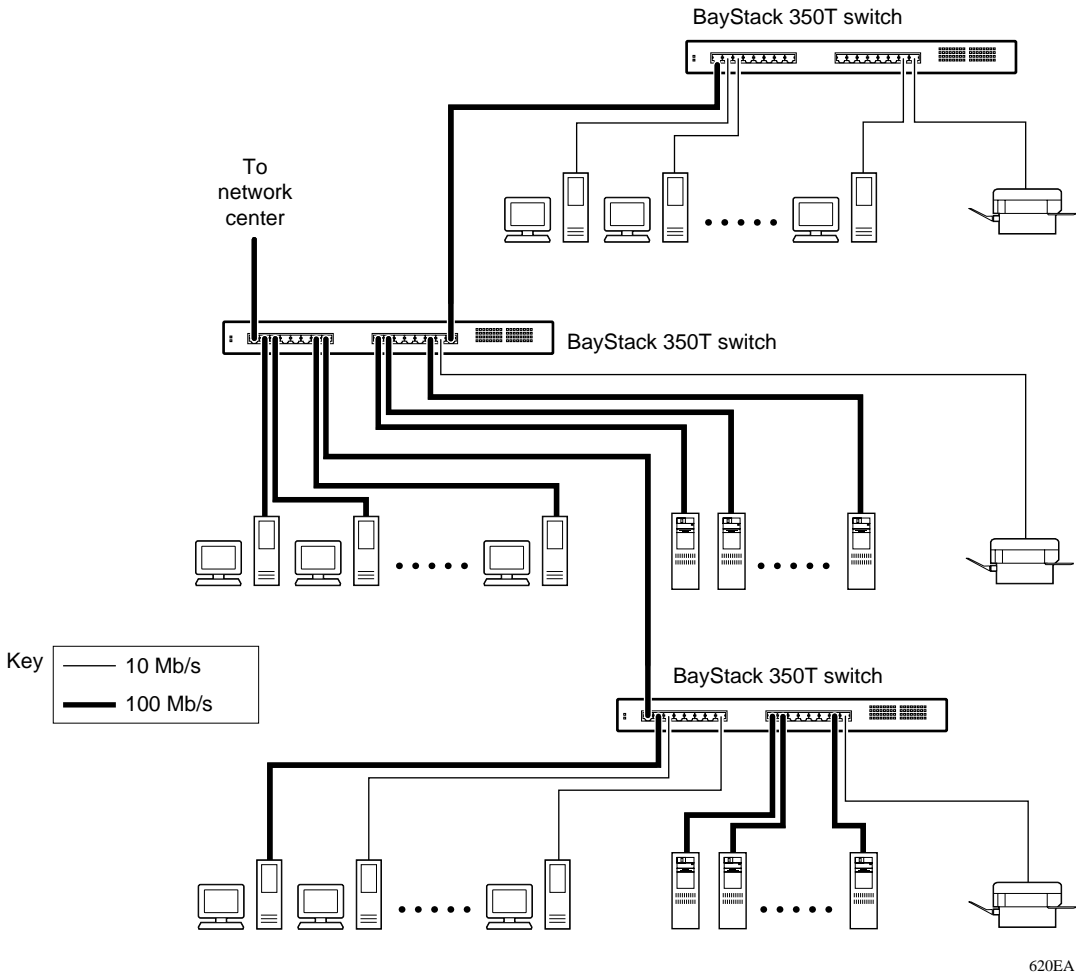


**Note:** All of the BayStack 350 switch models can be used interchangeably in the following network configuration examples.

---

## Power Workgroups

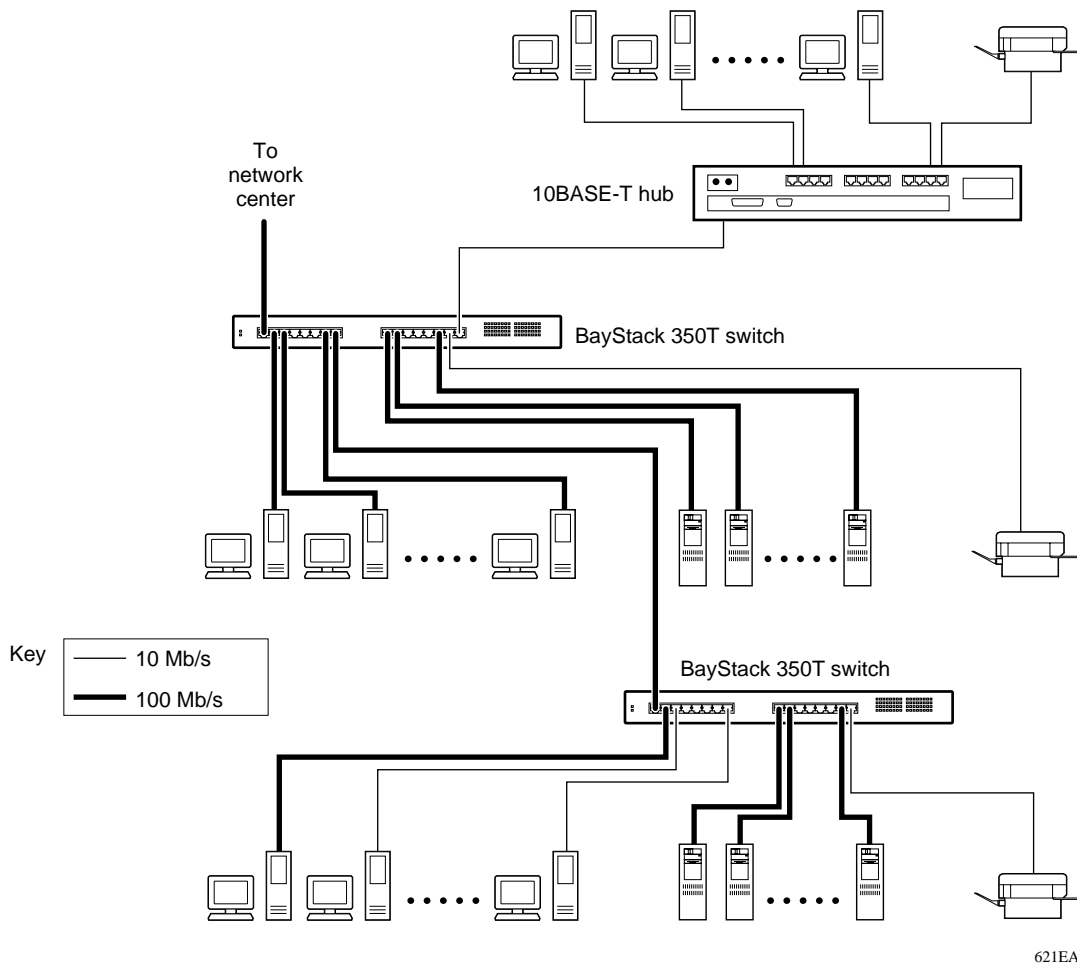
[Figure 1-5](#) shows BayStack 350 switches connecting dedicated power workgroups and standard departmental users. In this example, all users have access to 10 Mb/s bandwidth or 100 Mb/s bandwidth on any port.



**Figure 1-5. Configuring power workgroups**

## Power Workgroups and Shared Media Hub

[Figure 1-6](#) shows power workgroups connected to servers through BayStack 350 switches in a small network. Network managers who do not want to provide each end station with the full 100 Mb/s bandwidth can designate a certain number of users that share the full bandwidth provided by one of the switch ports. For example, one workgroup is connected to a 10BASE-T shared media hub and shares 10 Mb/s bandwidth provided by one of the BayStack 350 switch ports.

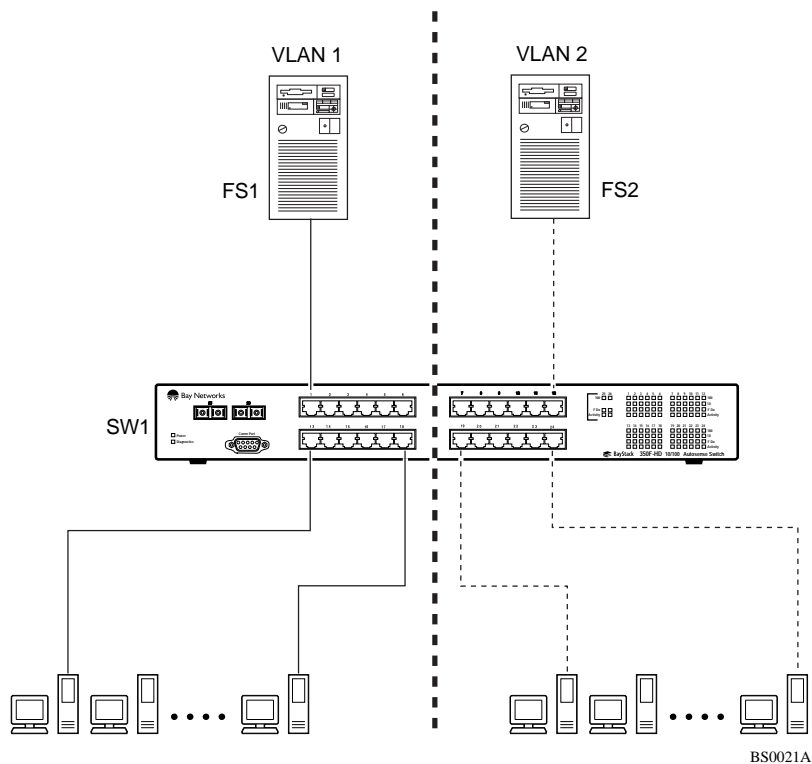


**Figure 1-6. Configuring power workgroups and a shared media hub**

## VLAN Workgroups

You can create and configure VLANs by segmenting BayStack 350 switches into logical workgroups that are independent of each other. The workgroups can be defined according to project or department.

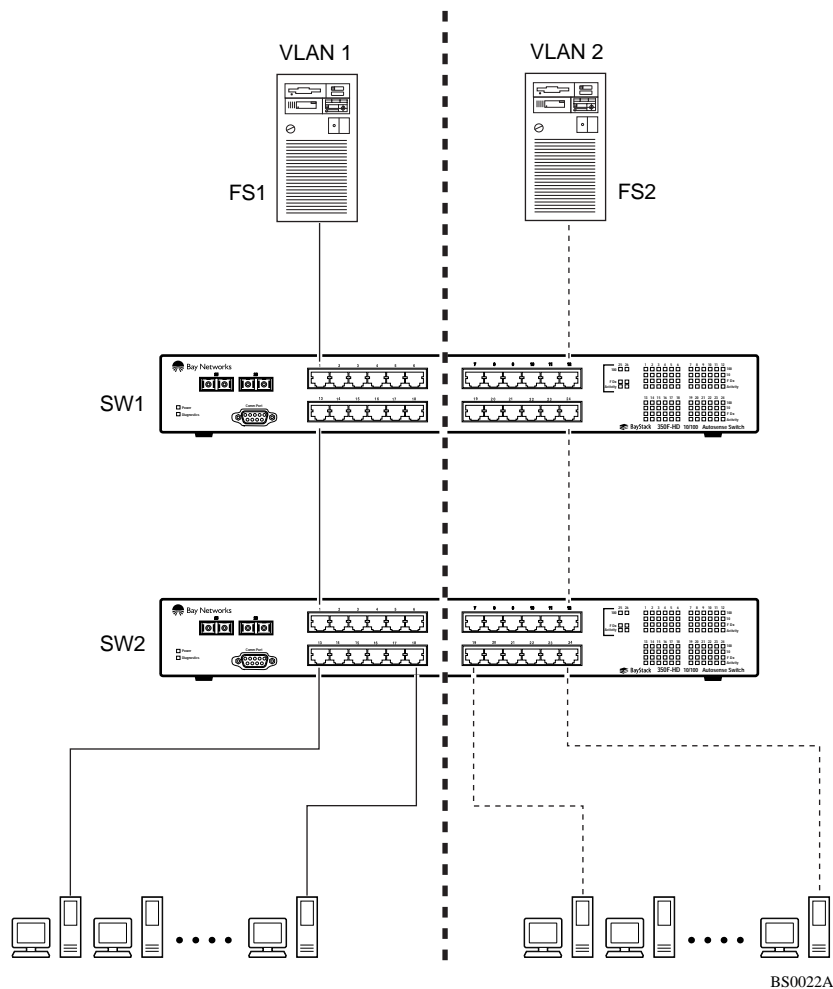
Workgroup members on VLANs share computer resources but cannot communicate with other workgroups; therefore access to specific servers is restricted to all but the assigned workgroup. Broadcast packets are also confined to a specific VLAN, which relieves traffic congestion ([Figure 1-7](#)).



**Figure 1-7. Port-based VLAN example**

This same type of segmentation can be extended to multiple switches across the network. Because BayStack 350 Series switches implement port-based VLANs, extending VLANs to another switch requires utilizing a single switch port for each VLAN ([Figure 1-8](#)).

In this example configuration ([Figure 1-8](#)), spanning tree participation must be set to Disabled because the spanning tree protocol (STP) is not supported across multiple VLANs (see “Spanning Tree Port Configuration” on page 3-63).

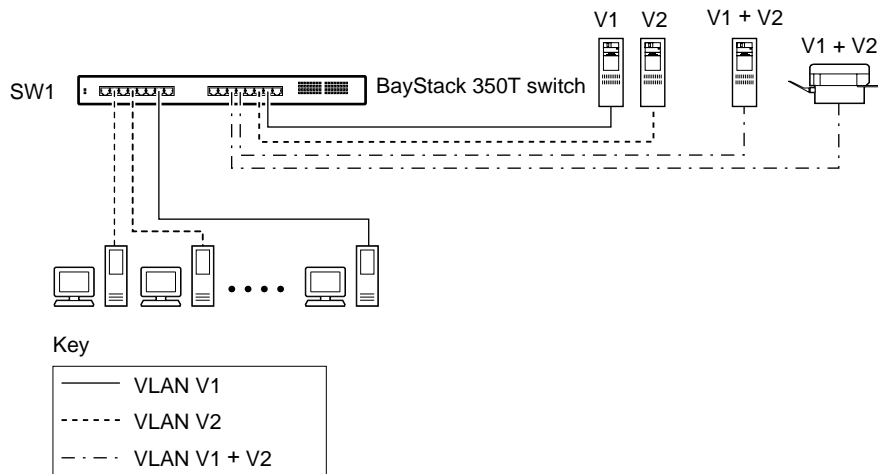


**Figure 1-8. VLANs spanning multiple switches**

BayStack 350 switches also allow ports to exist in multiple VLANs for shared resources, such as servers, printers, and switch-to-switch connections.

There are limitations when configuring multiple VLANs on a port and when configuring VLANs that cross multiple switches. For example, to have multiple VLANs that span multiple switches, no port should be configured to exist in more than one VLAN in any of the switches. This method partitions the switches into different, non-overlapping VLANs as shown previously in [Figure 1-8](#).

It is also possible to have resources exist in multiple VLANs on one switch as shown in [Figure 1-9](#). In this example, clients on different broadcast domains share resources. The broadcasts from ports configured in VLAN V1+V2 can be seen by both VLAN V1 and VLAN V2 ports. Broadcasts from VLAN V1 ports can only be seen by other VLAN V1 ports or VLAN V1+V2 ports. This analogy is also true for ports that are assigned to VLAN V2.



622EG

**Figure 1-9. Multiple VLANs sharing resources**

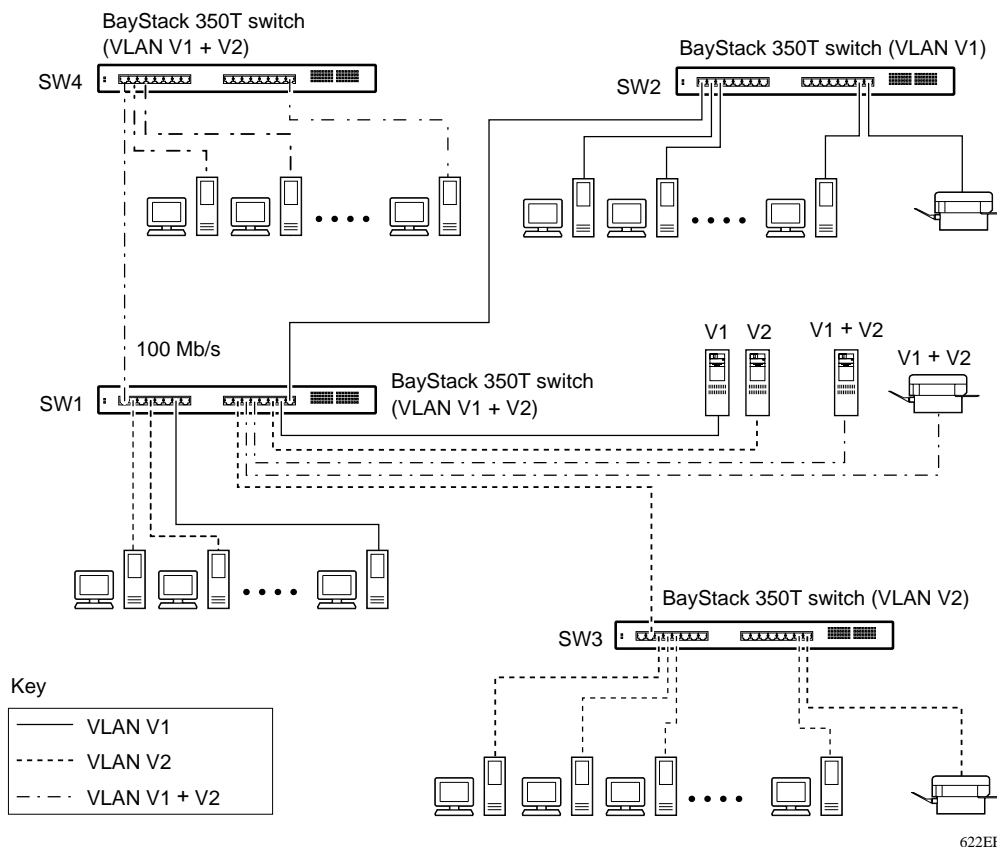
[Figure 1-10](#) shows an example of how to connect switch ports, that are configured for multiple VLANs, to other switches.



**Note:** When connecting switches that have ports configured for multiple VLANs, the multiple VLANs do not get projected across the connection. The connection is treated as a single VLAN at the other end.



As shown in [Figure 1-10](#), switch SW1 is configured with multiple VLANs: ports 7, 15, and 16 are in VLAN V1; ports 2, 4, 10, and 14 are in VLAN V2; and ports 1, 11, and 12 are in VLAN V1+V2.



622EF

**Figure 1-10. VLAN configuration spanning multiple BayStack 350 switches**

Switch SW1 can connect to switch SW2 because all of the ports on switch SW2 are configured in a single VLAN (VLAN V1). The same is true for switch SW3 where all of the ports are configured in a single VLAN (VLAN V2). In both of these cases, the connection port from switch SW1 matches the configuration of the other switch. The connection to switch SW4 is also valid because, in this case, there is no longer a distinction between VLANs V1 and V2. VLAN V1+V2 is, in effect, a single VLAN that contains both broadcast domains.

Although switch SW4 is shown with all ports configured in VLAN V1+V2, any of the ports can be assigned to additional VLANs as long as they *are all in the same VLAN membership as the connecting port (port 1)*.

### VLAN Configuration Screen Examples

Figures 1-11 to 1-14 show examples of the VLAN Configuration screen settings for switches SW1, SW2, SW3, and SW4.

The screen examples shown in this section show how the VLAN Configuration screens appear when MultiLink trunking is not active (no trunks configured).



**Note:** When MultiLink trunking is active, only five VLANs can be configured and the VLAN Configuration screen shows only five VLAN columns. For more information about the MultiLink Trunking feature, see “[MultiLink Trunks](#)” on [page 1-24](#).

VLAN Configuration									
Port	Trunk	V1	V2	V3	V4	V5	V6	V7	V8
1		[ X ]	[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
2		[ ]	[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
3		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
4		[ ]	[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
5		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
6		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
7		[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
8		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
9		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
10		[ ]	[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
11		[ X ]	[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
12		[ X ]	[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
13		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
14		[ ]	[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
15		[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
16		[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

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 1-11. VLAN Configuration screen for switch SW1

VLAN Configuration									
Port	Trunk	V1	V2	V3	V4	V5	V6	V7	V8
1		[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
2		[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
3		[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
4		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
5		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
6		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
7		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
8		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
9		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
10		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
11		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
12		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
13		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
14		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
15		[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
16		[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

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 1-12. VLAN Configuration screen for switch SW2**

VLAN Configuration									
Port	Trunk	V1	V2	V3	V4	V5	V6	V7	V8
1		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
2		[ ]	[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
3		[ ]	[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
4		[ ]	[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
5		[ ]	[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
6		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
7		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
8		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
9		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
10		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
11		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
12		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
13		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
14		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
15		[ ]	[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
16		[ ]	[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

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 1-13. VLAN Configuration screen for switch SW3**

VLAN Configuration									
Port	Trunk	V1	V2	V3	V4	V5	V6	V7	V8
1		[ X ]	[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
2		[ X ]	[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
3		[ X ]	[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
4		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
5		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
6		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
7		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
8		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
9		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
10		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
11		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
12		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
13		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
14		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
15		[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
16		[ X ]	[ X ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

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 1-14. VLAN Configuration screen for switch SW4**

### Additional Tips About Configuring VLANs

To group switch ports into logical workgroups, select the ports under the VLAN name (V1, V2, ....., or V8) in the VLAN Configuration screen. If you want users on different VLANs to share a port, select that port under each VLAN name.

You can create VLANs for one BayStack 350 switch, or you can create VLANs that span multiple switches. However, each switch that participates in the VLAN configuration must be configured individually. You can also assign multiple VLANs to a port connected to a server, which allows the server to be shared by multiple logical workgroups.

You can only create five VLANs when the MultiLink Trunking feature is active. The VLAN Configuration screen displays five VLAN columns when any trunk is enabled.

## MultiLink Trunks

BayStack 350 switches support two types of trunking configurations:

- Inter-switch trunk configuration
- Server trunk configuration

You can choose the configuration type from the MultiLink Trunk Configuration Menu screen (see “MultiLink Trunk Configuration” on page 3-39).

*Inter-switch trunk configurations* are designated as (trunks) I1 to I4 in the Inter-Switch Trunk Configuration screen. *Server trunk configurations* are designated as (trunks) S1 to S4 in the Server Trunk Configuration screen.

This trunk designation convention is also used in related screens that display trunking information (for example, the VLAN Configuration screen).

Any combination of each configuration type (server trunk and inter-switch), can be used to configure up to 16 trunk members on each switch).

### Inter-Switch Trunk Configuration

You can use the Inter-Switch Trunk Configuration screen to create switch-to-switch trunk links. This configuration type allows you to logically connect up to eight switch ports together to form up to four trunks in any of the following configurations:

- **One trunk** -- With the trunk configured with at least two trunk members, but not more than four.
- **Two trunks** -- With each trunk configured with at least two trunk members, but not more than four.
- **Three trunks** -- With each trunk configured with at least two trunk members, but not more than four; the combined trunks cannot exceed eight trunk members (see Note).



**Note:** When you create a three trunk configuration, do not configure any two of the trunks with three trunk members. That configuration is not supported.

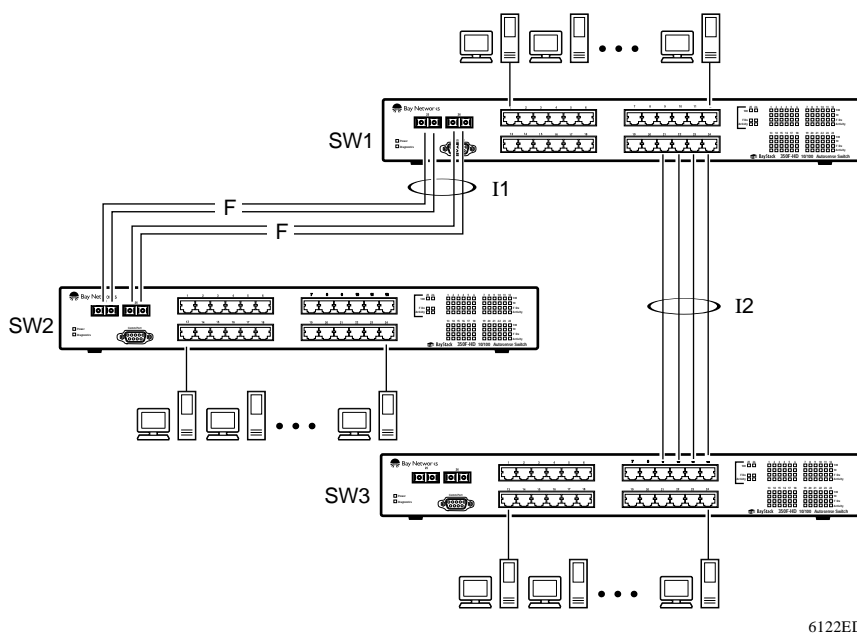
---

- **Four trunks** -- With each trunk configured with two trunk members.

You can configure individual trunks between multiple switches as shown in [Figure 1-15](#).

Although [Figure 1-15](#) shows only two inter-switch trunks (I1 and I2) connecting switch SW1 to switches SW2 and SW3, you can configure any BayStack 350 switch with up to four inter-switch trunks.

You can configure MultiLink trunks 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 [Figure 1-15](#), 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 1-15. Inter-switch trunk configuration example**

## Server Trunk Configuration

Use the Server Trunk Configuration screen to connect switches to servers that support multiport, single-MAC, network interface controllers (NICs).



**Note:** Do not use the server trunk configuration screen to create switch-to-switch trunk links. Use the inter-switch trunk configuration screen to create switch-to-switch trunk links (see [“Inter-Switch Trunk Configuration”](#) on [page 1-24](#)).

---

You can logically connect up to eight switch ports together to create up to four trunks in any of the following configurations:

- **One trunk** -- With the trunk configured with at least two trunk members, but not more than four.
- **Two trunks** -- With each trunk configured with at least two trunk members, but not more than four.
- **Three trunks** -- With each trunk configured with at least two trunk members, but not more than four; the combined trunks cannot exceed eight trunk members (see Note).



**Note:** When you create a three trunk configuration, do not configure any two of the trunks with three trunk members. That configuration is not supported.

---

- **Four trunks** -- With each trunk configured with two trunk members.



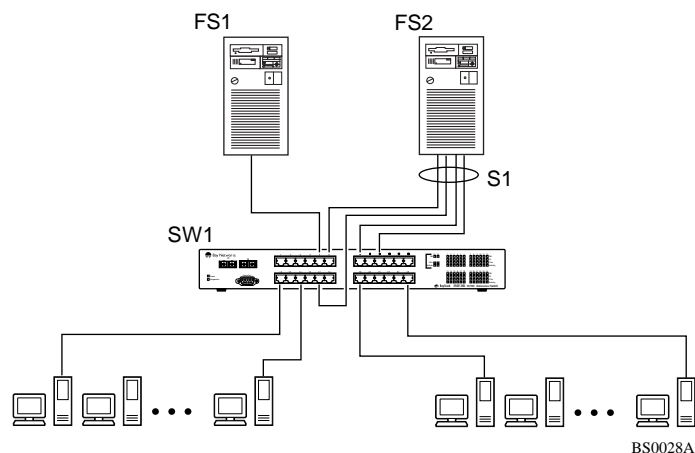
**Note:** When you use the Server Trunk Configuration screen to connect a trunk to a server that uses a single MAC address, set up your trunk members according to the information provided in Appendix B, “Server/Trunk Connections.”

---



[Figure 1-16](#) shows a typical server trunk topology utilizing the server trunk configuration. FS1 utilizes dual MAC addresses, using one MAC address for each 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 a server trunk configuration (S1).

In this configuration example, server trunk S1 is assigned trunk members that correspond to the information provided in Appendix B, “Server/Trunk Connections.” This allows the trunks to operate at optimal efficiency.



**Figure 1-16. Server trunk configuration example**

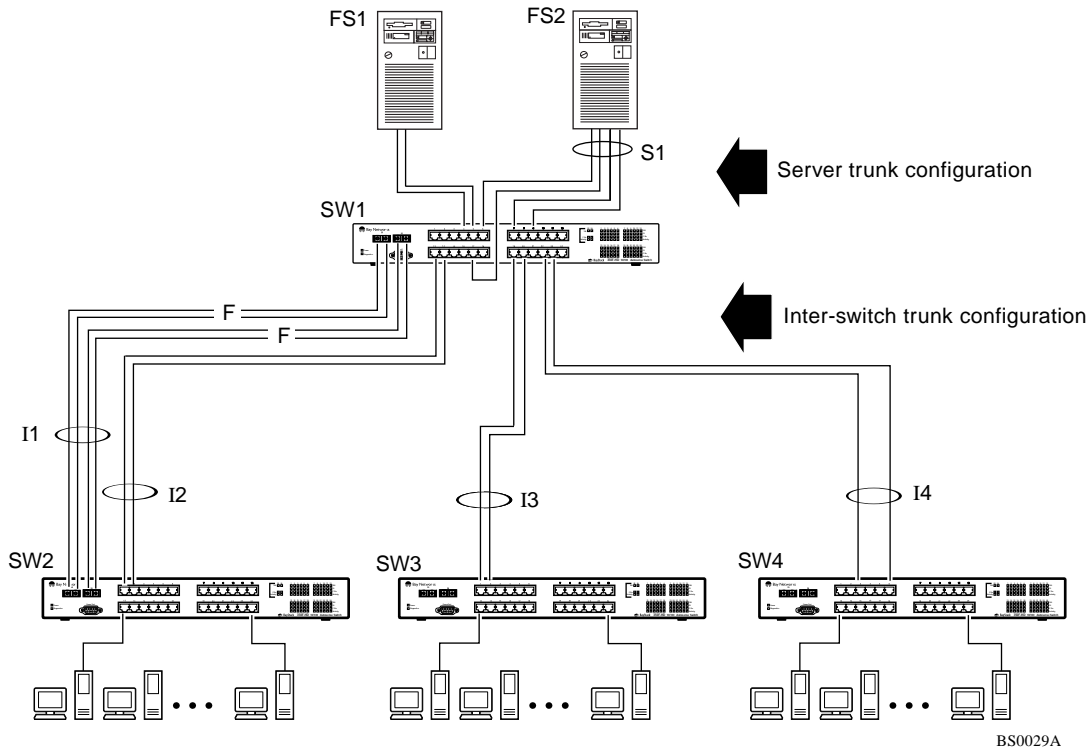
### Client/Server Configuration Utilizing MultiLink Trunks

[Figure 1-17](#) 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 SW1. FS2 is connected through a server trunk configuration (S1). The switch-to-switch connections are through inter-switch trunks (I1, I2, I3, and I4).

Clients accessing data from the servers (FS1 and FS2) are provided with maximized bandwidth through server trunk S1 and inter-switch trunks I1, I2, I3, and I4. Trunk members (the ports making up each trunk) do not have to be consecutive switch ports; they can be selected randomly, as shown by I4.

With spanning tree *enabled*, one of the trunks (I1 or I2) acts as a redundant (backup) trunk to switch SW2. With spanning tree *disabled*, trunks I1 and I2 must be configured into separate VLANs for this configuration to function properly (see “[VLAN Workgroups](#)” on [page 1-16](#)).



**Figure 1-17. Client/server configuration example**

The Trunk Configuration screens for switches SW1 to SW4 are shown in “[Trunk Configuration Screen Examples](#)” following this section. For detailed information about configuring trunks, see “[MultiLink Trunk Configuration](#)” on page 3-39.

## Trunk Configuration Screen Examples

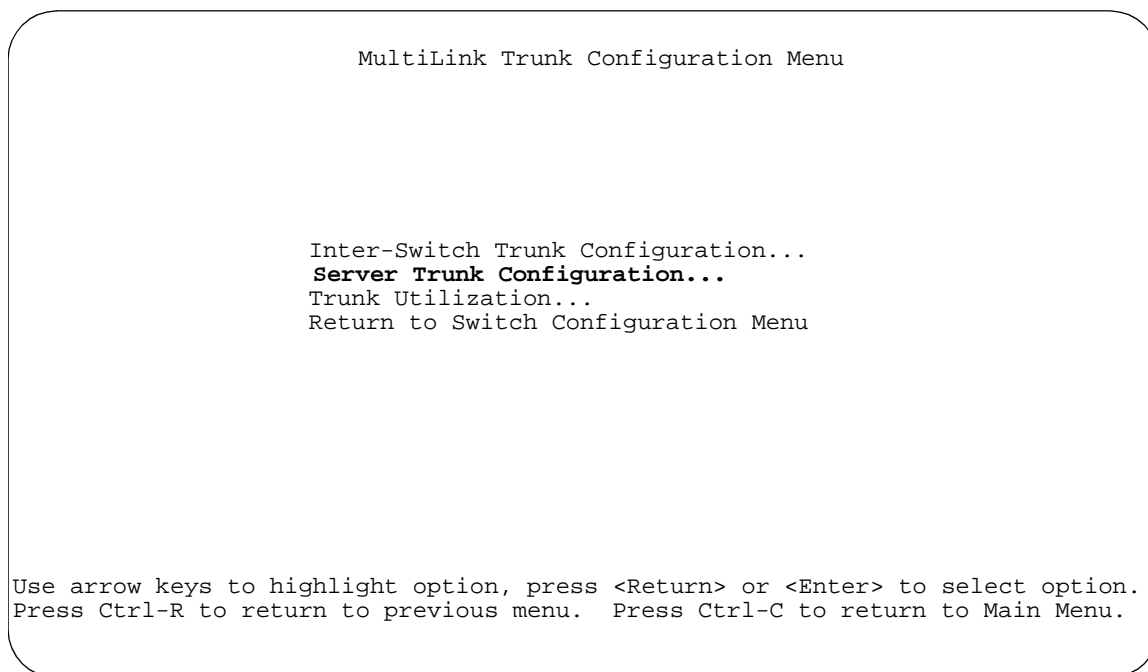
This section shows examples of the Trunk Configuration screens for the client/server configuration example shown in [Figure 1-17](#). The screens show how you could set up the trunk configuration screens for switches SW1 to SW4. For more information about configuring trunks, see “[Before Configuring Trunks](#)” on [page 1-40](#).

### *Trunk Configuration Screen for Switch SW1*

Switch SW1 is set up with one server trunk configuration (S1) and four inter-switch trunk configurations (I1, I2, I3, and I4).

#### **Setting up the Server Trunk Configuration for SW1:**

To set up the server trunk configuration, you choose **Server Trunk Configuration** from the MultiLink Trunk Configuration Menu screen ([Figure 1-18](#)).



**Figure 1-18. Choosing the Server Trunk Configuration screen**

The Server Trunk Configuration screen opens ([Figure 1-19](#)).



**Note:** The screen items shown in **boldface** type represent example configuration settings you could enter to obtain the topology configuration shown in [Figure 1-17](#).

```

Server Trunk Configuration

Trunk          Trunk Members          Trunk Status
-----
S1             [ 6 ][ 7 ][ 9 ][ 17 ]          [ Enabled ]
S2             [    ][    ][    ][    ]          [ Disabled ]
S3             [    ][    ][    ][    ]          [ Disabled ]
S4             [    ][    ][    ][    ]          [ Disabled ]

Valid server trunk configurations are:
    1 or 2 trunks of up to 4 links each
    Up to 4 trunks of 2 links each

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.
    
```

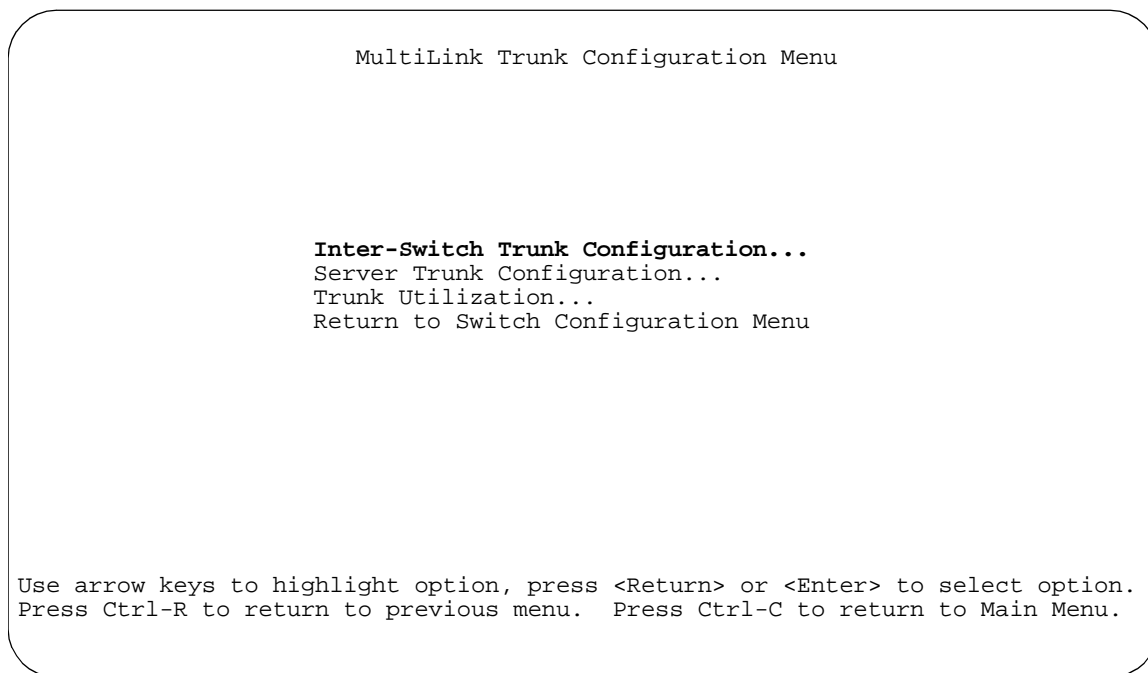
**Figure 1-19. Server Trunk Configuration screen for Switch SW1**

The Server Trunk Configuration screen for switch SW1 is configured as follows:

- **Trunk** (read only) indicates the server trunks (S1 through S4) 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 S1.
- **Trunk Status** indicates the Trunk Status for each of the trunks. When set to Enabled, the configuration settings for that specific trunk are activated.

### Setting up the Inter-switch Trunk Configuration For SW1:

To set up the inter-switch trunk configuration, choose **Inter-Switch Trunk Configuration** from the MultiLink Trunk Configuration Menu screen ([Figure 1-20](#)).



**Figure 1-20.** Choosing the Inter-Switch Trunk Configuration screen

The Inter-Switch Trunk Configuration screen opens ([Figure 1-21](#)).

```

Inter-Switch Trunk Configuration

Trunk      Trunk Members      STP      Trunk Mode      Trunk Status
-----
I1 [ 25 ][ 26 ][      ][      ] [ Enabled ] [ Enhanced ] [ Enabled ]
I2 [ 13 ][ 14 ][      ][      ] [ Enabled ] [ Enhanced ] [ Enabled ]
I3 [ 19 ][ 20 ]          [ Enabled ] [ Enhanced ] [ Enabled ]
I4 [ 22 ][ 23 ]          [ Enabled ] [ Enhanced ] [ Enabled ]

Valid inter-switch trunk configurations are:
    1 or 2 trunks of up to 4 links each
    Up to 4 trunks of 2 links each

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. Inter-Switch Trunk Configuration screen example**

The Inter-Switch Trunk Configuration screen for switch SW1 is configured as follows:

- **Trunk** (read only) indicates the trunks (I1 through I4 for this switch) that correspond to the switch ports specified in the Trunk Members fields.
- **Trunk Members** indicates the ports that can be configured, in each row, to create the corresponding trunk:
  - Ports 25 and 26 are assigned as trunk members of trunk I1.
  - Ports 13 and 14 are assigned as trunk members of trunk I2.
  - Ports 19 and 20 are assigned as trunk members of trunk I3.
  - Ports 22 and 23 are assigned as trunk members of trunk I4.
- **STP** indicates the spanning tree participation setting for each of the trunks:
  - In this example, trunks I1 to I4 are enabled for spanning tree participation.

- 
- **Trunk Mode** indicates the Trunk Mode for each of the trunks:

In this example, the Trunk Mode fields for trunks I1 through I4 are set to Enhanced. When in this mode, the switch evenly distributes source MAC addresses to the trunk members, balancing traffic throughout each trunk.



**Note:** Certain protocols, such as Local Area Transport (LAT), require proper sequencing of received packets for correct operation. Using Enhanced mode may cause some packets to be received out of sequence. If your application is using a protocol requiring proper sequencing of packets, use the Basic mode.

---

- **Trunk Status** indicates the Trunk Status for each of the trunks. When set to Enabled, the configuration settings for that specific trunk are activated.

### ***VLAN Configuration Screen for Switch SW1***

This section shows how the VLAN Configuration screen for switch SW1 displays the new trunk configuration ([Figure 1-22](#) and [Figure 1-23](#)). The addition of a trunk updates this screen and other related screens (for example the Spanning Tree Configuration screen) with the new trunking information.



**Note:** The VLAN Configuration screens for the other switches described in [Figure 1-17](#) (SW2, SW3, and SW4) are not shown here, but they also change to show the configurations for the specific switch.

---

As stated earlier in this chapter, the VLAN Configuration screen changes to allow only five VLANs when you activate the MultiLink Trunking feature. VLAN columns V6 to V8 are not displayed when any trunk is created.

If any VLANs are *already* configured in VLANs V6 to V8 when you activate the MultiLink Trunking feature, the trunk configuration screen prompts you to reconfigure VLANs V6 to V8 (for example, move those ports to any VLAN other than V6 through V8).



**Note:** All ports in a trunk must be configured in the same VLAN(s) before they can become trunk members.

[Figure 1-22](#) shows the first VLAN screen for switch SW1. It displays the settings for switch ports 1 to 16.

To display the second screen for switch ports 13 to 26 ([Figure 1-23](#)), you can press [Ctrl]+N.

VLAN Configuration						
Port	Trunk	V1	V2	V3	V4	V5
1		[ X ]	[ ]	[ ]	[ ]	[ ]
2		[ X ]	[ ]	[ ]	[ ]	[ ]
3		[ X ]	[ ]	[ ]	[ ]	[ ]
4		[ X ]	[ ]	[ ]	[ ]	[ ]
5		[ X ]	[ ]	[ ]	[ ]	[ ]
6	S1	[ X ]	[ ]	[ ]	[ ]	[ ]
7	S1	[ X ]	[ ]	[ ]	[ ]	[ ]
8		[ X ]	[ ]	[ ]	[ ]	[ ]
9	S1	[ X ]	[ ]	[ ]	[ ]	[ ]
10		[ X ]	[ ]	[ ]	[ ]	[ ]
11		[ X ]	[ ]	[ ]	[ ]	[ ]
12		[ X ]	[ ]	[ ]	[ ]	[ ]

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.

**Figure 1-22. VLAN Configuration screen example for switch SW1 (1 of 2)**



VLAN Configuration						
Port	Trunk	V1	V2	V3	V4	V5
13	I2	[ X ]	[ ]	[ ]	[ ]	[ ]
14	I2	[ X ]	[ ]	[ ]	[ ]	[ ]
15		[ X ]	[ ]	[ ]	[ ]	[ ]
16		[ X ]	[ ]	[ ]	[ ]	[ ]
17	S1	[ X ]	[ ]	[ ]	[ ]	[ ]
18		[ X ]	[ ]	[ ]	[ ]	[ ]
19	I3	[ X ]	[ ]	[ ]	[ ]	[ ]
20	I3	[ X ]	[ ]	[ ]	[ ]	[ ]
21		[ X ]	[ ]	[ ]	[ ]	[ ]
22	I4	[ X ]	[ ]	[ ]	[ ]	[ ]
23	I4	[ X ]	[ ]	[ ]	[ ]	[ ]
24		[ X ]	[ ]	[ ]	[ ]	[ ]
25	I1	[ X ]	[ ]	[ ]	[ ]	[ ]
26	I1	[ X ]	[ ]	[ ]	[ ]	[ ]

Press Ctrl-P to display choices for ports 1-12.  
 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 1-23. VLAN Configuration screen example for switch SW1 (2 of 2)**

To move a port or trunk to another VLAN, you simply use the arrow keys to navigate the screen and press the space bar to display choices. Press [Enter] to select your choice.

For more information about navigating the screens, see “Navigating the CI Menus and Screens” on page 3-5. For more information about configuring VLANs, see “[VLAN Workgroups](#)” on [page 1-16](#).

### ***Trunk Configuration Screen for Switch SW2***

As shown in [Figure 1-17](#), switch SW2 is set up with two inter-switch trunk configurations (I1 and I2). Both trunks connect directly to switch SW1.

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

[Figure 1-24](#) shows the Inter-Switch Trunk Configuration screen for switch SW2.

```

Inter-Switch Trunk Configuration

Trunk      Trunk Members      STP      Trunk Mode      Trunk Status
-----
I1 [ 25 ][ 26 ][      ][      ] [ Enabled ] [ Enhanced ] [ Enabled ]
I2 [  1 ][  2 ][      ][      ] [ Enabled ] [ Enhanced ] [ Enabled ]
I3 [      ][      ] [ Enabled ] [ Enhanced ] [ Disabled ]
I4 [      ][      ] [ Enabled ] [ Enhanced ] [ Disabled ]

Valid inter-switch trunk configurations are:
    1 or 2 trunks of up to 4 links each
    Up to 4 trunks of 2 links each

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 1-24. Trunk Configuration screen for switch SW2**

The Inter-Switch Trunk Configuration screen for switch SW2 is configured as follows:

- **Trunk** (read only) indicates the trunks (I1 and I2 for this switch) 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 I1.
  - Ports 1 and 2 are assigned as trunk members of trunk I2.
- **STP** indicates the spanning tree participation setting for each of the trunks:
  - In this example, trunks I1 and I2 are enabled for spanning tree participation.

- **Trunk Mode** indicates the Trunk Mode for each of the trunks:  
In this example, the Trunk Mode fields for trunks I1 and I2 are set to Enhanced. When in this mode, the switch evenly distributes source MAC addresses to the trunk members, balancing traffic throughout each trunk (see Note on [page 1-33](#)).
- **Trunk Status** indicates the Trunk Status for each of the trunks. When set to Enabled, the configuration settings for that trunk are activated.

### **Trunk Configuration Screen for Switch SW3**

As shown in [Figure 1-17](#), switch SW3 is set up with one inter-switch trunk configuration (I3). This trunk connects directly to switch SW1.

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

[Figure 1-25](#) shows the Inter-Switch Trunk Configuration screen for switch SW3.

```

Inter-Switch Trunk Configuration

Trunk      Trunk Members      STP      Trunk Mode      Trunk Status
-----
I1 [ 1 ] [ 2 ] [      ] [      ] [ Enabled ] [ Enhanced ] [ Enabled ]
I2 [      ] [      ] [      ] [      ] [ Enabled ] [ Enhanced ] [ Disabled ]
I3 [      ] [      ] [      ] [      ] [ Enabled ] [ Enhanced ] [ Disabled ]
I4 [      ] [      ] [      ] [      ] [ Enabled ] [ Enhanced ] [ Disabled ]

Valid inter-switch trunk configurations are:
    1 or 2 trunks of up to 4 links each
    Up to 4 trunks of 2 links each

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 1-25. Trunk Configuration screen for switch SW3**

The Inter-Switch Trunk Configuration screen for switch SW3 is configured as follows:

- **Trunk field** (read only) indicates the trunk (I1 for this switch) 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 I1.
- **STP** indicates the spanning tree participation setting for each of the trunks:  
  
In this example, trunk I1 is enabled for spanning tree participation.
- **Trunk Mode** indicates the Trunk Mode for each of the trunks:  
  
In this example, the Trunk Mode field for trunk I1 is set to Enhanced. When in this mode, the switch evenly distributes source MAC addresses to the trunk members, balancing traffic throughout each trunk (see Note on [page 1-33](#)).
- **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 Configuration Screen for Switch SW4***

As shown in [Figure 1-17](#), switch SW4 is set up with one inter-switch trunk configuration (I4). This trunk connects directly to switch SW1.

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

[Figure 1-26](#) shows the Inter-Switch Trunk Configuration screen for switch SW4.

```

Inter-Switch Trunk Configuration

Trunk      Trunk Members      STP      Trunk Mode      Trunk Status
-----
I1 [ 3 ][ 6 ][      ][      ] [ Enabled ] [ Enhanced ] [ Enabled ]
I2 [      ][      ][      ][      ] [ Enabled ] [ Enhanced ] [ Disabled ]
I3 [      ][      ]      [ Enabled ] [ Enhanced ] [ Disabled ]
I4 [      ][      ]      [ Enabled ] [ Enhanced ] [ Disabled ]

Valid inter-switch trunk configurations are:
    1 or 2 trunks of up to 4 links each
    Up to 4 trunks of 2 links each

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 1-26. Trunk Configuration screen for switch SW4**

The Inter-Switch Trunk Configuration screen for switch SW4 is configured as follows:

- **Trunk field** (read only) indicates the trunk (I1 for this switch) 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:

In this example, ports 3 and 6 are assigned as trunk members of trunk I1.

- **STP** indicates the spanning tree participation setting for each of the trunks:  
In this example, trunk I1 is enabled for spanning tree participation.

- **Trunk Mode** indicates the Trunk Mode for each of the trunks:

In this example, the Trunk Mode field for trunk I1 is set to Enhanced. When in this mode, the switch evenly distributes source MAC addresses to the trunk members, balancing traffic throughout each trunk (see Note on [page 1-33](#)).

- **Trunk Status** indicates the Trunk Status for each of the trunks. When set to Enabled, the configuration settings for that specific trunk are activated.

## 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 4) are to become *trunk members* (the specific ports making up the trunk). Be sure that:**
  - a. **At least two ports (minimum) are configured for each trunk.**
  - b. **The chosen switch ports are set to Enabled, using the Port Configuration screen (see “Port Configuration” on page 3-36) or through network management.**
  - c. **The trunk member ports are in the same VLAN.**
3. **Ensure that all network cabling is complete and stable before configuring any trunks, to avoid misconfiguration errors.**
4. **Consider how the existing spanning tree will react to the new trunk configuration (see “[Spanning Tree Considerations](#)” on [page 1-42](#)).**
5. **Consider how existing VLANs will be affected by the addition of a trunk; when MultiLink Trunking is active, only five VLANs are allowed.**

After completing the above steps, see “MultiLink Trunk Configuration” on page 3-39 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:

1. Any port that participates in MultiLink Trunking must be an active port (set to Enabled via the Port Configuration screen or through network management).
2. 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 3-34).
3. 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.
4. 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 1-42](#)).
5. 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 Inter-Switch Trunk Configuration screen or the Spanning Tree Configuration screen.
6. Only five VLANs are allowed when MultiLink Trunking is active.
7. If the VLAN settings of any trunk member are changed, the VLAN settings of all members of that trunk are changed similarly.
8. 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. A screen prompt precedes this action.



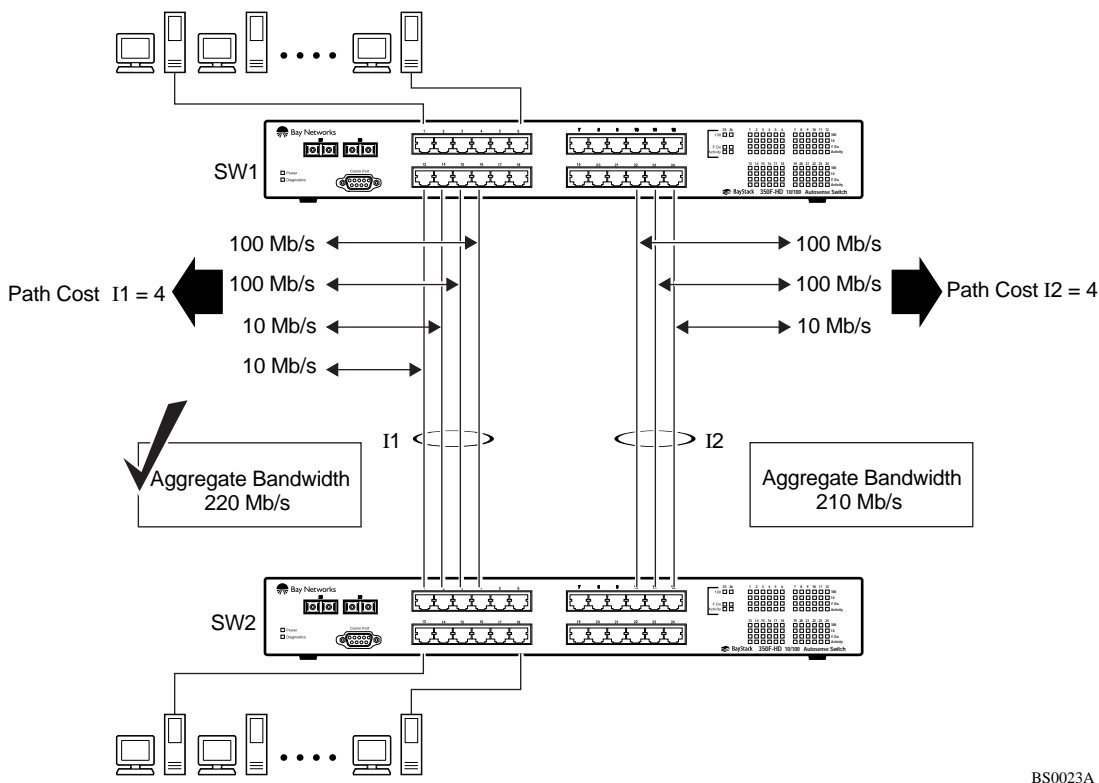
**Note:** A removed trunk member does not rejoin the trunk if it is then reset to Enabled. The removed trunk member has to be reconfigured through the Trunk Configuration screen to rejoin the trunk.

---

9. A trunk member cannot be configured as a monitor port (see "Port Mirroring Configuration" on page 3-48).
10. Trunks cannot be monitored by a monitor port; however, trunk members can be monitored (see "[Port-Based Mirroring Configuration](#)" on [page 1-46](#)).

## Spanning Tree Considerations

The spanning tree Path Cost parameter is recalculated based on the aggregate bandwidth of the trunk. For example, [Figure 1-27](#) shows a four port inter-switch trunk (I1) with two port members operating at 100 Mb/s and the other two port members operating at 10 Mb/s. Trunk I1 provides an aggregate bandwidth of 220 Mb/s. The Path Cost for I1 is 4 (Path Cost = 1000/LAN speed, in Mb/s). If a second three port trunk (I2) 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 (I1) to determine the most efficient path.



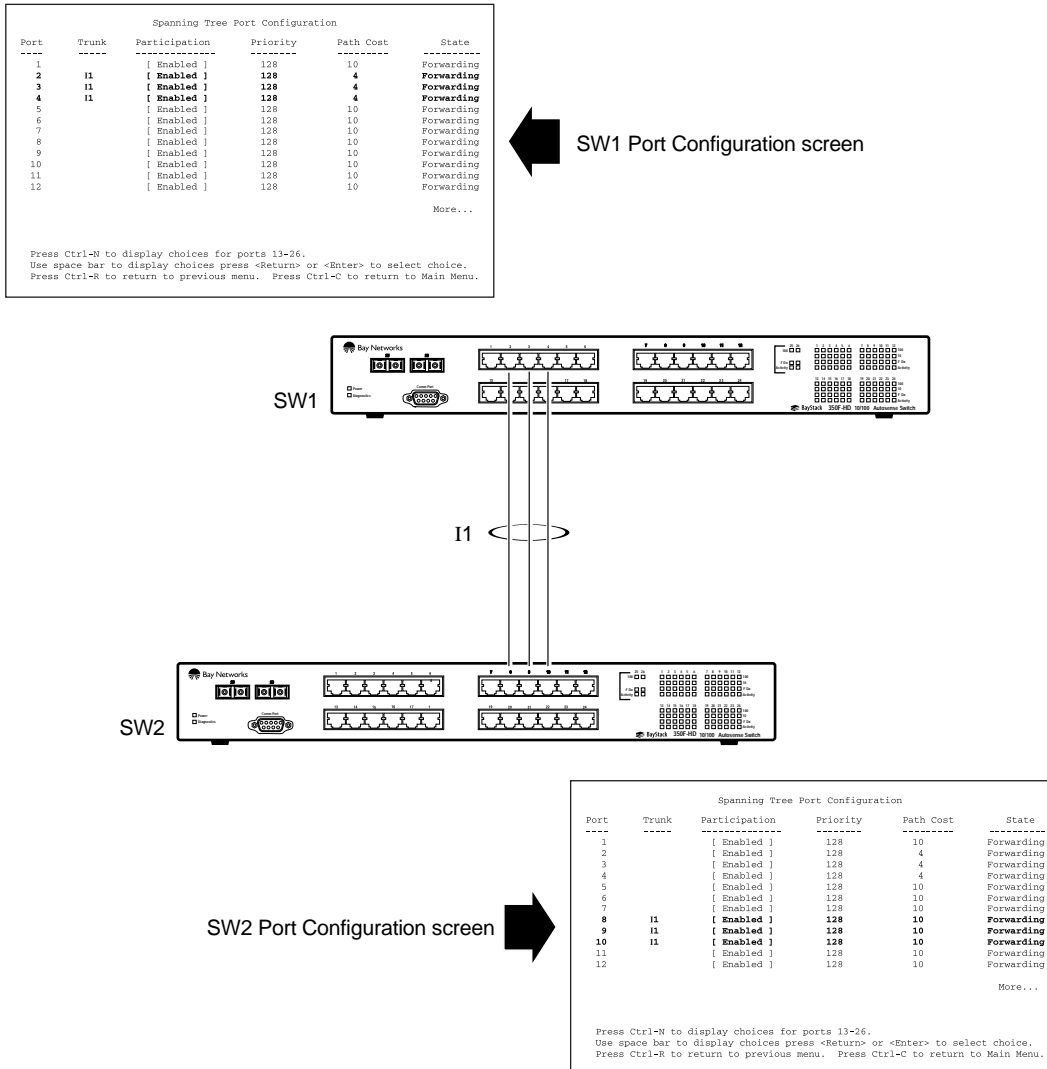
BS0023A

**Figure 1-27. Path cost arbitration example**

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 I1, the management station views Trunk I1 as spanning tree port 13.



The switch can also detect trunk member ports that are physically misconfigured. For example, in [Figure 1-28](#), trunk member ports 2, 3, and 4 of switch SW1 are configured *correctly* to trunk member ports 8, 9, and 10 of switch SW2. The Spanning Tree Port Configuration screen for each switch shows the port State field for each port in the Forwarding state.



BS0024B

**Figure 1-28. Example 1: Correctly configured trunk**

If switch SW2's trunk member port 10 is physically disconnected and then reconnected to port 12, the Spanning Tree Port Configuration screen for switch SW1 changes to show port 4 in the Blocking state (Figure 1-29).

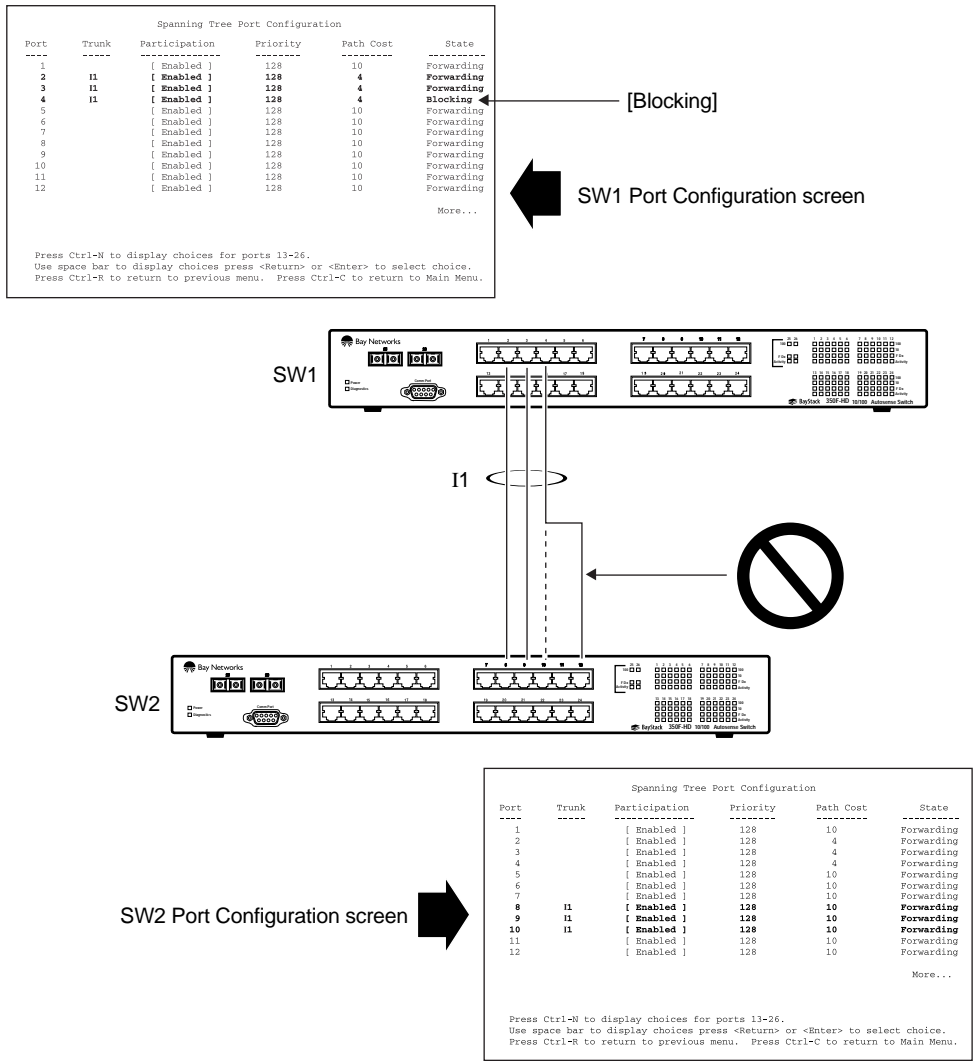


Figure 1-29. Example 2: Detecting a misconfigured port

## Additional Tips About the MultiLink Trunking Feature

When you create a MultiLink Trunk, the individual trunk members (the specific ports comprising 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.

When MultiLink Trunking is active, all VLAN screens change to show only five VLANs available for configuration. VLAN columns V6 to V8 are not displayed. Also, if more than five VLANs are configured and you try to enable a MultiLink trunk, the trunk configuration screen prompts you to reconfigure VLANs V6 through V8.

## 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 Nortel Networks StackProbe or equivalent, must be connected to the designated monitor port to use this feature (contact your Nortel Networks sales agent for details about the StackProbe).

---

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

- Port-based Mirroring
- Address-based Mirroring

A sample 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 ]
```

For more information about the Port Mirroring feature, see “Port Mirroring Configuration” on page 3-48.

### Port-Based Mirroring Configuration

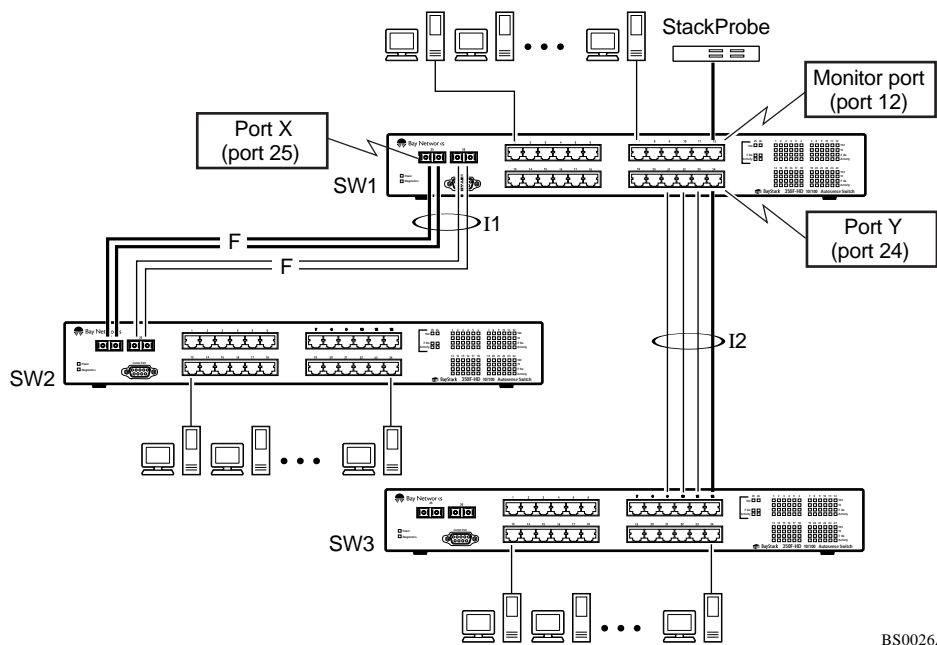
[Figure 1-30](#) shows an example of a port-based mirroring configuration where port 12 is designated as the monitor port for ports 24 and 25 of switch SW1. Although this example shows ports 24 and 25 monitored by the monitor port (port 12), any of the trunk members of I1 and I2 can also be monitored.



**Note:** Trunks cannot be monitored and trunk members cannot be configured as monitor ports (see “[MultiLink Trunking Configuration Rules](#)” on [page 1-41](#)).

---

[Figure 1-31](#) shows the Port Mirroring Configuration screen setup for this example.



BS0026A

**Figure 1-30. Port-based mirroring configuration example**

In this configuration example, 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 or received/transmitted by port Y (or all conversations between port X and port Y)

As shown in the Port Mirroring Configuration screen example ([Figure 1-31](#)), a user has designated port 12 as the Monitor Port for ports 24 and 25 in switch SW1.

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

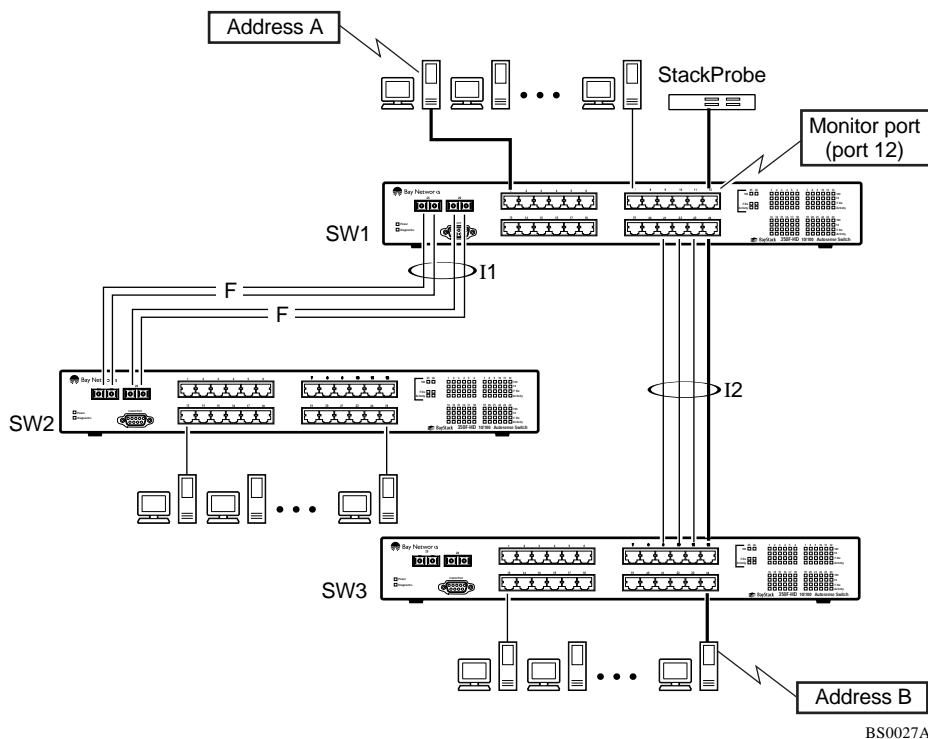
Use space bar to display choices, press <Return> or <Enter> to select choice.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.
```

**Figure 1-31. Port Mirroring port-based screen example**

See “Port Mirroring Configuration” on page 3-48 for a full description of the Port Mirroring Configuration screen fields.

## Address-Based Mirroring Configuration

[Figure 1-32](#) shows an example of an address-based mirroring configuration where port 12, the designated monitor port for switch SW1, is monitoring traffic occurring between address A and address B.



**Figure 1-32. 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 1-33](#) shows the Port Mirroring Configuration screen setup for this example.

In this example, port 12 becomes the designated Monitor Port for switch SW1 when you press [Enter] in response to the [Yes] screen prompt. The screen data displayed at the bottom of the screen changes to show the *new* currently active port mirroring configuration.

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 3-24).

```

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 1-33. Port Mirroring address-based screen example**

See “Port Mirroring Configuration” on page 3-48 for a full description of the Port Mirroring Configuration screen fields.



## Port Mirroring Configuration Rules

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

1. A monitor port cannot be configured as a trunk member.
2. 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.
3. 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, are configured on the same VLAN. Use the VLAN Configuration screen to configure the VLAN (see “VLAN Configuration” on page 3-34).
4. 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 Step 3.

## Quick-Start Procedures

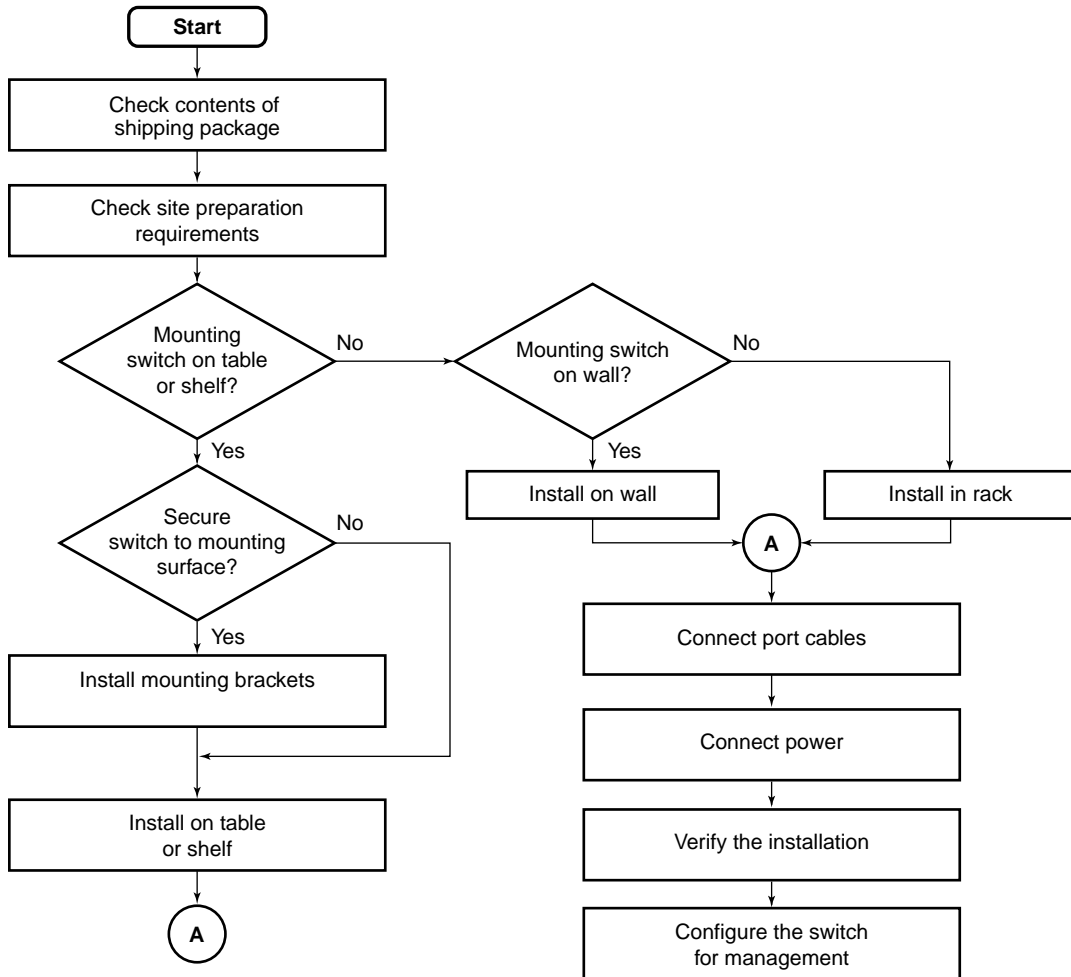
This section provides Quick-Start procedures for installing and setting up the BayStack 350 switch. It is intended for experienced network installers or system administrators who are familiar with the BayStack 350 switch installation and setup procedures in this manual.

If you have experience installing network devices, or if you are installing multiple BayStack 350 switches, you can use the installation flowchart provided in this section to guide you through the installation. If you need more information about any of the steps in the flowchart, see Chapter 2, “Installing the BayStack 350 Switch” for a complete explanation of the installation process.

After you have verified the installation, you can use other Quick-Start procedures in this section to set up and begin managing the switch. For detailed information about setting up the switch and using the console interface (CI) menus and screens, see Chapter 3, “Using the Console Interface.”

## Quick-Start to Installing the BayStack 350 Switch

You can use the installation flowchart ([Figure 1-34](#)) to install the BayStack 350 switch. If you need more information about any of the steps in the flowchart, see the appropriate section in Chapter 2, “Installing the BayStack 350 Switch.”



721EB

**Figure 1-34. Installation flowchart**

---

## Quick-Start to Managing the BayStack 350 Switch

If you are already familiar with managing network devices, you can use the Quick-Start procedures in this section to set up and begin managing the BayStack 350 switch. Before you begin these procedures, make sure that the BayStack 350 switch has been installed and verified (as described in Chapter 2, “Installing the BayStack 350 Switch”), and that the network cables are attached to the switch.

This section describes how to manage the BayStack 350 switch using one of two methods:

- The console/service port interface, using the CI menus and screens
- An SNMP management application

### Console/Service Port Interface

If you are managing the BayStack 350 switch using the console/service port interface, follow these steps:

1. **Connect a console terminal directly to the BayStack 350 switch console/service port or through a modem connection.**



**Note:** The console/service 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/Service Port Connector” on page C-5).

---

The console terminal can be a VT100-compatible terminal or a PC running VT100 terminal-emulation software (see “Console/Service Port Cabling” on page 3-2).

2. **Configure the console terminal for 9600 baud, 8 data bits, no parity, and 1 stop bit.**

Be sure to set the console terminal to online mode; do not leave it in setup mode.

3. **Press [Ctrl]+C on the console terminal keyboard.**
4. **The CI main menu opens.**

For more information about the CI main menu, see “Using the CI Menus and Screens” on page 3-4.

## SNMP Management Applications

To use an SNMP application to manage the BayStack 350 switch, you must assign an IP address to the switch so that the SNMP application can communicate with it.

To assign the BayStack 350 switch IP address, follow these steps:

1. **Connect a console terminal directly to the BayStack 350 switch console/service port or through a modem connection.**



**Note:** The console/service 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/Service Port Connector” on page C-5).

---

The console terminal can be a VT100-compatible terminal or a PC running VT100 terminal-emulation software (see “Console/Service Port Cabling” on page 3-2).

2. **Configure the console terminal for 9600 baud, 8 data bits, no parity, and 1 stop bit.**

Be sure to set the console terminal to online mode; do not leave it in setup mode.

3. **Press [Ctrl]+C on the console terminal keyboard.**

4. **The CI main menu opens.**

For more information about the CI main menu, see “Using the CI Menus and Screens” on page 3-4.

5. **Choose the IP Configuration option from the main menu.**

The IP Configuration screen opens.

6. **In the IP Configuration screen, complete the following fields:**

- In-Band IP Address
- In-Band Subnet Mask (if required)
- Default Gateway (if required)

7. **Set SNMP traps (if required).**

To set SNMP traps, see “SNMP Configuration” on page 3-14.

8. **Press [Ctrl]+C to return to the main menu.**

---

## Chapter 2

# Installing the BayStack 350 Switch

This chapter explains how to install the BayStack 350 switch. The switch can be placed on a table or shelf, mounted on a wall, or installed in a standard 19-inch equipment rack.

To install the BayStack 350 switch, you unpack the equipment, physically install the switch, connect the network cables, connect the power, and then verify the installation.

### Required Tools and Materials

You will need the following tools to install the BayStack 350 switch:

- For installation in an equipment rack, use a Phillips or crosshead screwdriver.
- For wall mounting, you need four screws (not supplied). The screw size and type depends on the composition of the wall on which you intend to mount the switch. Have an experienced maintenance person choose the appropriate hardware for your wall composition.

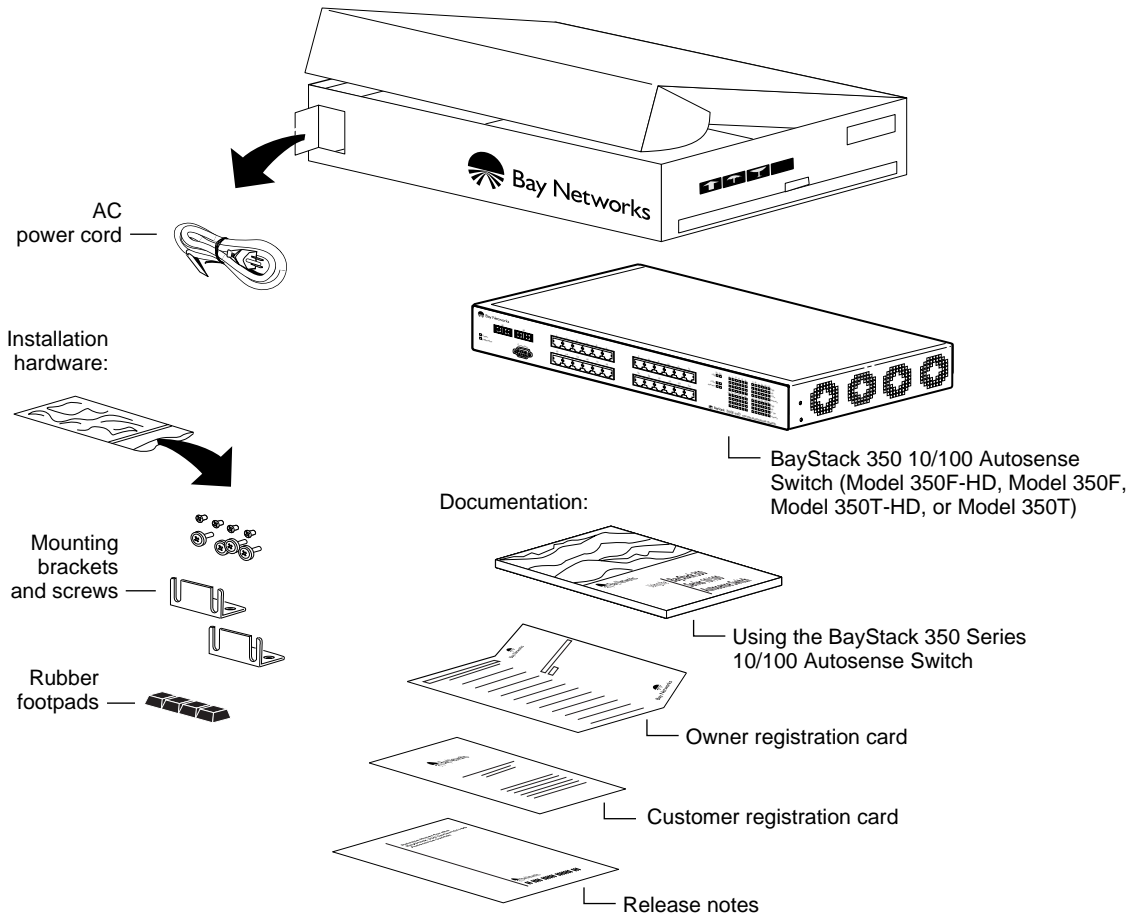


**Caution:** The screws and wall composition must be able to withstand the weight of the device, plus the additional weight of the attached network cables and power cords.

---

## Package Contents

Verify that your BayStack 350 switch shipment includes all of the items shown in [Figure 2-1](#).



7829FB

**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 350 switch.

## Site Preparation

This section describes what you need to do to prepare your site before installing the BayStack 350 switch.

## Hardware

Verify that you have the hardware components appropriate for your method of installation:

- **Console terminal:** You must have a console terminal available. The console terminal must be a VT100-compatible terminal or a PC running VT100 terminal-emulation software. (Although the BayStack 350 switch is operational as soon as you install it, you can customize the parameters to suit your needs.)
- **Rack mounting:** You need a single-unit (1u) rack space for installing the Model 350T and the Model 350F switches in an equipment rack. The Model 350T-HD and the Model 350F-HD switches require a 1.5-unit (1.5u) rack space.
- **Surface mounting:**
  - Table: The table or shelf must be level and able to support at least 12 pounds, plus the weight of the suspended port cables. If you intend to stack additional BayStack 350 switches, remember to include this weight in your calculations when selecting a suitable table or shelf.



**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.

---

-- Wall-mounting hardware: Mounting brackets are provided for securing the BayStack 350 switch (Model 350F and Model 350T only) on a table, shelf, or wall. However, because wall compositions vary at different sites, Nortel Networks recommends that an experienced maintenance person choose the appropriate wall-mounting hardware to install your BayStack 350 switch properly.

- **Network cabling:** Ensure that all network cables are in place and that they have been tested and tagged before you begin the installation.

## Software

Verify that you have the software components appropriate for your method of installation:

- **BootP server:** The BayStack 350 switch can learn its IP address through BootP. To use this feature, ensure that you have a properly configured BootP server in your network.
- **TFTP server:** You can keep your BayStack 350 switch firmware up-to-date by upgrading the firmware as new versions become available. To upgrade the firmware, you need a properly configured TFTP server in your network.

The Nortel Networks network management applications EZ LAN™, Optivity Campus™, and Optivity Enterprise™ can help you with these BootP and firmware functions.

## Environment

The following items must conform to the specifications described in Appendix A, “Technical Specifications”:

- **Temperature:** Ensure that the temperature in the operating environment remains between 0° and 40° C (32° and 104°F). Do not place the BayStack 350 switch in direct sunlight or near warm air exhausts or heaters.
- **Humidity:** Ensure that the humidity level in the operating environment does not exceed 85 percent and that no water condenses on or around the BayStack 350 switch.
- **Ventilation:** Ensure that there is adequate airflow and clearance for air circulation around the BayStack 350 switch. Air enters the switch on one side and flows out the opposite side. Allow at least two inches of ventilation space on both sides of the BayStack 350 switch.
- **Electrical power:** Ensure that the site’s power outlet meets the power requirement of the BayStack 350 switch and is within 1.8 meters (6 feet) of the installation location.



## Installation

This section explains how to install, power up, and verify the operation of the BayStack 350 switch. Before you begin these procedures, read and follow the instructions in [“Site Preparation”](#) on [page 2-3](#).



**Warning:** To avoid bodily injury from hazardous electrical current, do not connect the power cord until instructed to do so.

---

You can install the BayStack 350 switch in any of the following locations:

- Surface mounting:
  - Table or shelf (secured or unsecured)
  - Wall (Model 350F and Model 350T only)
- Rack mounting:
  - Standard equipment rack

### Surface Mounting

You can mount the BayStack 350 switch on any surface that can safely support the weight of the switch and attached cables, as long as there is adequate space around the unit for ventilation and access to cable connectors. You can use the mounting brackets supplied with the switch (Model 350F and Model 350T only) to secure it to the installation location.



**Note:** In most cases, it is not necessary to secure the BayStack 350 switch to a table or shelf. However, if conditions warrant securing the switch (for example, in locations where the switch might accidentally fall from a shelf or overhead location), you can secure the switch using two mounting brackets (Model 350F and Model 350T only).

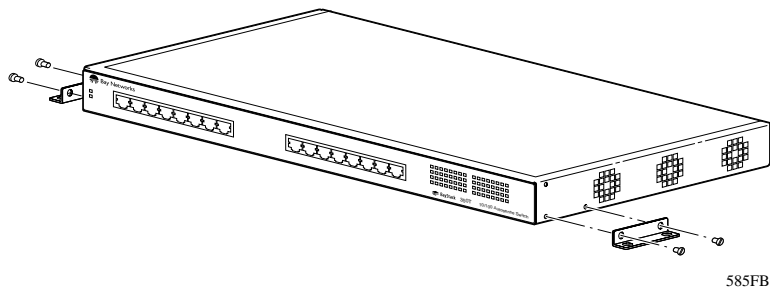
---

## Attaching the Mounting Brackets

[Figure 2-2](#) shows the mounting-bracket positions for mounting the Model 350F or Model 350T switch on a flat surface such as a table, shelf, or wall. When rack mounting the switch, you use the same brackets, but position them to attach to the holes in the chassis ([Figure 2-5](#)).

To attach the mounting brackets for a surface mount, follow these steps:

1. **Locate the rack-mounting holes on each side of the switch ([Figure 2-2](#)).**
2. **Using a Phillips or crosshead screwdriver, attach a mounting bracket to each side of the switch using the supplied screws.**
3. **Secure the switch to the table, shelf, or wall as described in the appropriate section.**

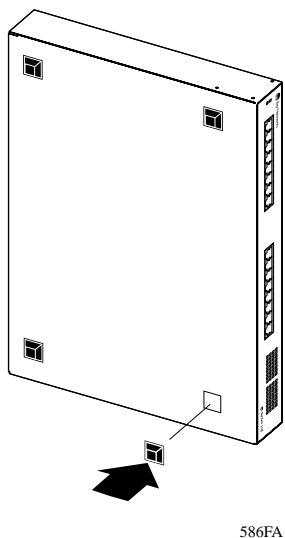


**Figure 2-2. Attaching mounting brackets for a surface mount**

## Installing on a Table or Shelf

To install the BayStack 350 switch on a table or shelf, follow these steps:

1. Attach a rubber footpad to each corner on the bottom of the switch ([Figure 2-3](#)).
2. Position the switch on the table or shelf, with the front panel facing you. Be sure to leave adequate space around the unit for ventilation and access to the cables.
3. If you are securing the switch to a table or shelf, insert two screws (not supplied) through each of the mounting brackets, then tighten the screws.
4. Proceed to [“Connecting Port Cables”](#) on [page 2-13](#) to connect the network cables.



**Figure 2-3. Attaching rubber footpads**

## Wall Mounting

You can mount the Model 350F and Model 350T on any wall that can safely support the weight of the device and attached cables (see [“Site Preparation”](#) on [page 2-3](#) for safety considerations). For a wall mount, use of the rubber footpads is optional.



**Note:** You cannot mount the Model 350F-HD on a wall.

---

### Before You Begin

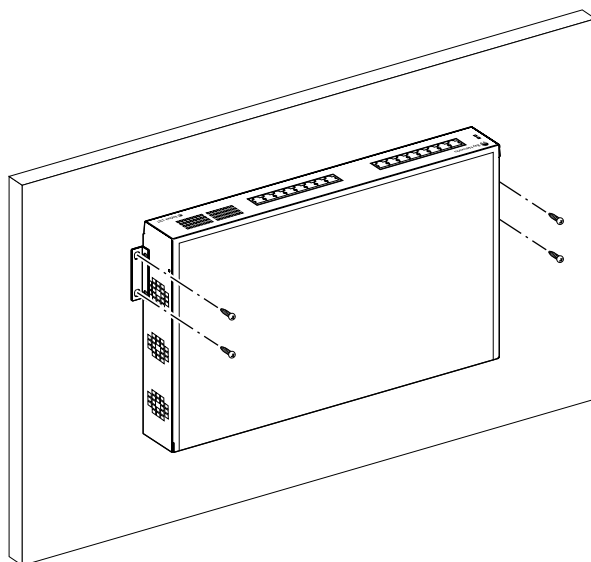
Before mounting the switch on a wall, note the following considerations:

- Mount the switch on the wall, with the front panel facing up, as shown in [Figure 2-4](#).
- Position the switch at a height that allows the LEDs to be visible at all times.
- Do not let the attached port cables hang freely from the port connectors. Install plastic cable clamps to support and arrange the cables.
- Choose the appropriate mounting hardware for your wall composition. (Wall-mounting screws are not supplied.)
- Optionally, attach the switch to a piece of plywood (at least 0.5 in. thick) that is firmly secured to the wall, preferably to the wall studs.

## Wall Mounting the Model 350F and Model 350T

To mount the Model 350F or Model 350T on a wall, follow these steps:

1. Using a Phillips or crosshead screwdriver, attach a mounting bracket to each side of the switch using the supplied screws ([Figure 2-2](#)).
2. Insert two screws (not supplied) through each of the mounting brackets, then tighten the screws ([Figure 2-4](#)).
3. Proceed to [“Connecting Port Cables”](#) on [page 2-13](#) to connect the network cables.



587FA

**Figure 2-4.** Wall mounting the Model 350F and Model 350T

## Rack Mounting

You can install the BayStack 350 switch in most standard equipment racks. The Model 350F and Model 350T require a single-unit (1u) rack space for installation. The Model 350F-HD requires a 1.5-unit (1.5u) rack space for installation.

In most cases, you can install the switch in the rack with the mounting brackets attached, as shown in [Figure 2-5](#). However, because of variances in rack hardware (cagenuts), the switch may not fit between the rails. In this case, you can install the switch by attaching the mounting brackets as shown in [Figure 2-6](#).



**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 350 switch in an equipment rack, follow these steps:

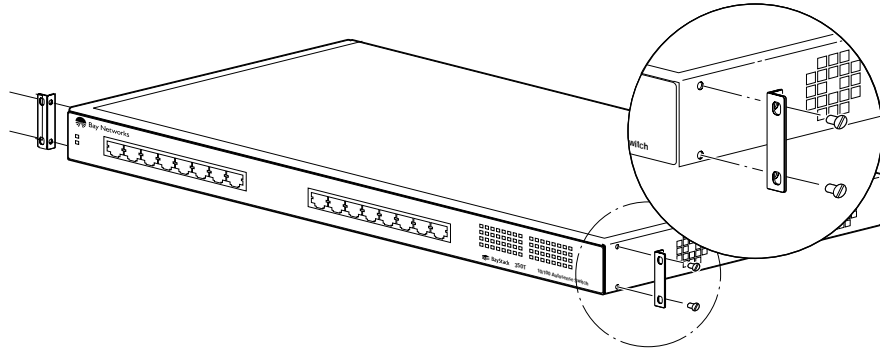
1. **If rubber footpads are attached to the bottom of the switch, remove them.**
2. **Depending on the width of your rack, use the standard or alternative method of attaching the mounting brackets ([Figure 2-5](#) or [Figure 2-6](#)).**



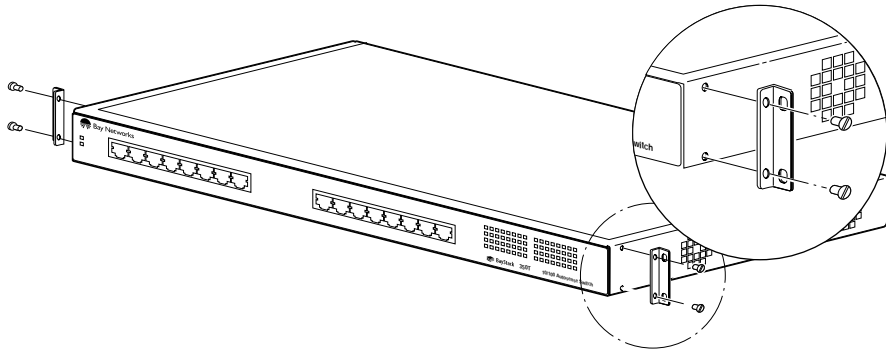
**Note:** If you use the alternative method of attaching the mounting brackets to the switch, the switch front panel will extend 2.54 centimeters (1 inch) from the rack.

---

3. **Using a Phillips or crosshead screwdriver, attach a mounting bracket to each side of the switch using the supplied screws ([Figure 2-5](#) or [Figure 2-6](#)).**

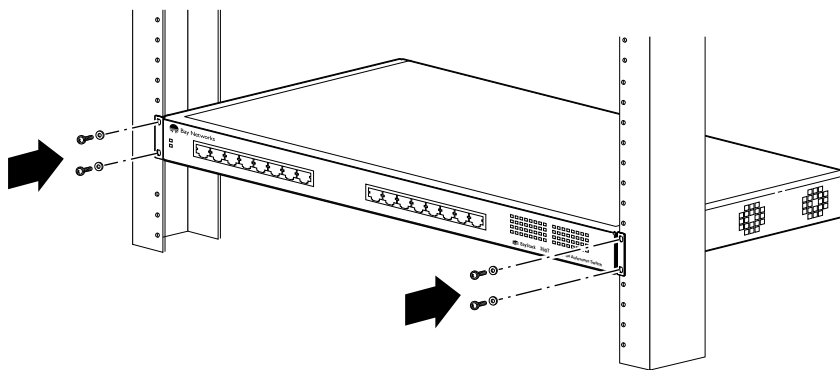


**Figure 2-5. Attaching mounting brackets for a rack mount (standard method)**



**Figure 2-6. Attaching mounting brackets for a rack mount (alternative method)**

4. Position the switch in the rack and align the holes in the mounting brackets with the holes in the rails ([Figure 2-7](#)).
5. Insert two screws (not supplied) through each of the mounting brackets, then tighten the screws.
6. Proceed to [“Connecting Port Cables”](#) on [page 2-13](#) to connect the network cables.



611FA

**Figure 2-7.** Installing the BayStack 350 switch in an equipment rack



## Connecting Port Cables

This section describes how to connect the BayStack 350 switch ports to the network. Depending on your network configuration requirements, you connect the RJ-45 port cables, 100BASE-FX port cables, or both. After connecting the port cables, proceed to [“Connecting Power”](#) on [page 2-15](#) to connect the AC power cord and power up the BayStack 350 switch.

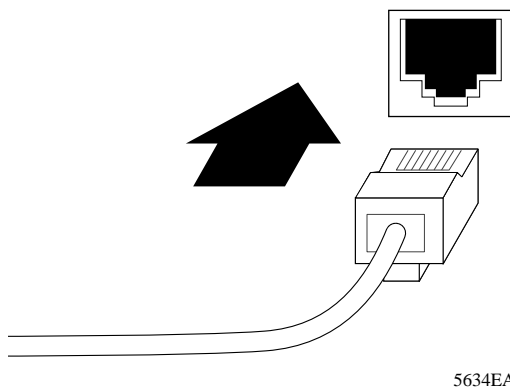
The BayStack 350 10BASE-T/100BASE-TX switch ports are configured with RJ-45 connectors that are wired as MDI-X ports. As in conventional Ethernet repeater hubs, the BayStack 350 switch ports connect via straight-through cables to the network interface card (NIC) in a node or server. When connecting to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



**Note:** By default, all BayStack 350 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.

## RJ-45 Port Cables

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 2-8](#)).



**Figure 2-8.** Connecting RJ-45 port cables

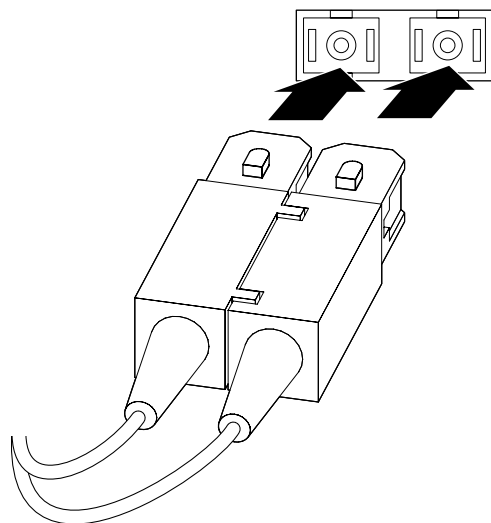
## 100BASE-FX Port Cables



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

---

To connect the 100BASE-FX port cables, align the keyway on the cable plug with the key slot on the appropriate connector, then insert the cable plug into the fiber optic port connector ([Figure 2-9](#)).



156FA

**Figure 2-9. Connecting 100BASE-FX port cables**

After connecting the port cables, proceed to the next section, [“Connecting Power,”](#) to connect the AC power cord and power up the BayStack 350 switch.

## Connecting Power

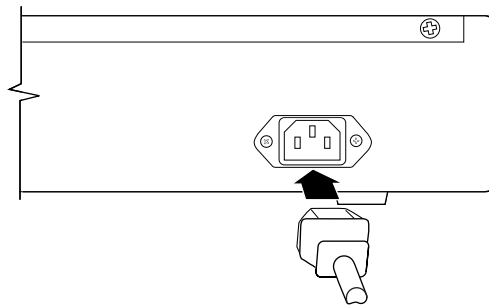
The BayStack 350 switch does not have a power on/off switch. When you connect the AC power cord to a suitable AC power outlet, the switch powers up immediately.



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

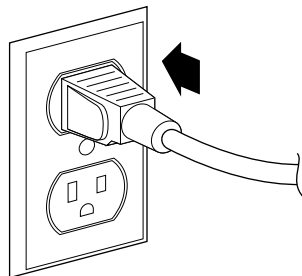
To connect the AC power cord, follow these steps:

1. **Plug one end of the AC power cord into the AC power receptacle on the switch back panel.**



7834FA

2. **Plug the other end of the AC power cord into a grounded AC power outlet.**



612FA

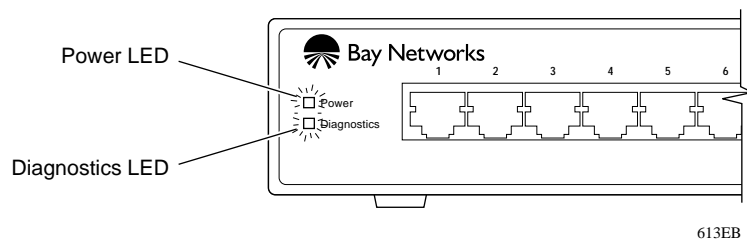
3. **Proceed to the next section, [“Verifying the Installation,”](#) to verify proper operation.**

## Verifying the Installation

To verify proper operation of the BayStack 350 switch, observe the front-panel LEDs 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 (<a href="#">Figure 2-10</a>).</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 Diagnostics LED turns on (<a href="#">Figure 2-10</a>).</p> <p>If a nonfatal error occurs during the self-test, the Diagnostics LED blinks.</p> <p>If the switch fails the self-test, the Diagnostics LED remains off. Contact the sales agent or the customer service representative from whom you purchased the switch.</p>



**Figure 2-10. Observing LEDs to verify proper operation**

After verifying proper operation of the BayStack 350 switch, proceed to Chapter 3, “Using the Console Interface,” to configure and manage the switch.

---

# Chapter 3

## Using the Console Interface

This chapter describes how to configure and manage the BayStack 350 switch using the menu-driven console interface (CI). You can access the CI menus and screens through the console/service port located on the switch back panel. You can also manage the BayStack 350 switch using Nortel Networks Optivity network management software or any generic SNMP-based management software; however, you must first assign an IP address to the switch, as described in this chapter.



**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.

---

See your network management documentation for information about SNMP.

### Console Interface

The CI consists of menus and screens that enable you to manage the BayStack 350 switch and monitor its performance. You can manage the switch by using configuration menus to change its operational parameters. You can monitor the performance of the switch by using the statistics screen, which displays the counters of the switch ports.

You can access the CI menus and screens in the following ways:

- Locally through a console terminal (must be a VT100-compatible terminal or a PC running VT100 terminal-emulation software)
- Remotely through a dial-up modem connection
- In-band through a TELNET session

## Console/Service Port Cabling

You can connect a console terminal directly to the BayStack 350 switch console/service port, or you can connect a modem to the console/service port for remote access to the CI menus and screens.



**Note:** To ensure correct connections between the console/service port and the console terminal or modem port, refer to the service-port pin assignments in Appendix C, “Connectors and Pin Assignments.”

---

## Console Terminal Requirements

To connect a console terminal to the BayStack 350 switch console/service port, you need the following equipment:

- An ASCII character terminal that has an RS-232 serial port, or a computer that has an RS-232 serial port and terminal emulation (typically a PC running common communications software)
- A standard RS-232 serial communications cable with a DB-9 connector at one end for connection to the console/service port, and an appropriate connector (typically a DB-9 or DB-25 connector) at the other end for connection to the serial port on the console terminal

## Modem Requirements

To connect a modem to the BayStack 350 switch console/service port, you need the following equipment:

- A 9600 baud (or higher speed) modem is recommended. The console/service port speed is set to 9600 baud (the factory default setting), but supports 2400 to 38400 baud, as long as the speed at both ends of the communications link is identical.
- A standard RS-232 serial communications null-modem cable with a DB-9 connector at one end for connection to the console/service port, and an appropriate connector (typically a DB-9 or DB-25 connector) at the other end for connection to the modem’s serial port.

Set the modem’s serial port speed to match the speed of the BayStack 350 switch console/service port (9600 baud is the default). See [“Console/Service Port Configuration”](#) on [page 3-58](#) to modify the console/service port parameters.

---

## Connecting to the BayStack 350 Switch Console/Service Port

To connect a console terminal or modem to the console/service port, follow these steps:



**Note:** The console/service port is configured as a data communications equipment (DCE) connector. Ensure that your RS-232 cable pinouts are configured for DCE connections (see “Appendix C, “Connectors and Pin Assignments”).

---

1. **Plug the RS-232 cable DB-9 receptacle into the console/service port plug. Secure the connection by tightening the two screws on the DB-9 receptacle.**
2. **Plug the other end of the RS-232 cable (DB-9 or DB-25, as appropriate) into the RS-232 serial port on the console terminal or modem.**

## Accessing the CI Menus and Screens

You can access the CI menus and screens locally through a console terminal, remotely through a dial-up modem connection, or in-band through a TELNET session.

To access the CI menus and screens through a TELNET session, your workstation must have an IP address, and you must know the IP address of the BayStack 350 switch. You can configure an IP address for the switch by using a console terminal, as described in this section.



**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.

---

See your TELNET documentation for information about establishing TELNET connections.

To access the CI menus and screens, follow these steps:

1. **Turn on the console terminal, or make sure that your PC is running in terminal-emulation mode.**
2. **Set the console terminal configuration parameters as follows:**
  - 9600 baud
  - 8 data bits
  - No parity
  - 1 stop bit
3. **Set the console terminal to online mode; do not leave it in setup mode.**
4. **Press [Ctrl]+C on the console terminal keyboard.**

The CI main menu opens (see [Figure 3-2](#)). For more information about using the main menu, proceed to the next section, [“Using the CI Menus and Screens.”](#)

## Using the CI Menus and Screens

The CI menus and screens provide commands that allow you to configure and manage the BayStack 350 switch. Help prompts at the bottom of each menu and screen explain how to enter data in the highlighted field and how to navigate the menus and screens.

Although some commands take effect immediately, other commands are followed by an ellipsis (for example, IP Configuration...), indicating that there is a submenu with other options.

Some commands allow you to toggle between several possible settings; other commands 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 command:
  - a. Use the arrow keys to highlight the command name.
  - b. Press [Enter].

The command takes effect immediately after you press [Enter].

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

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

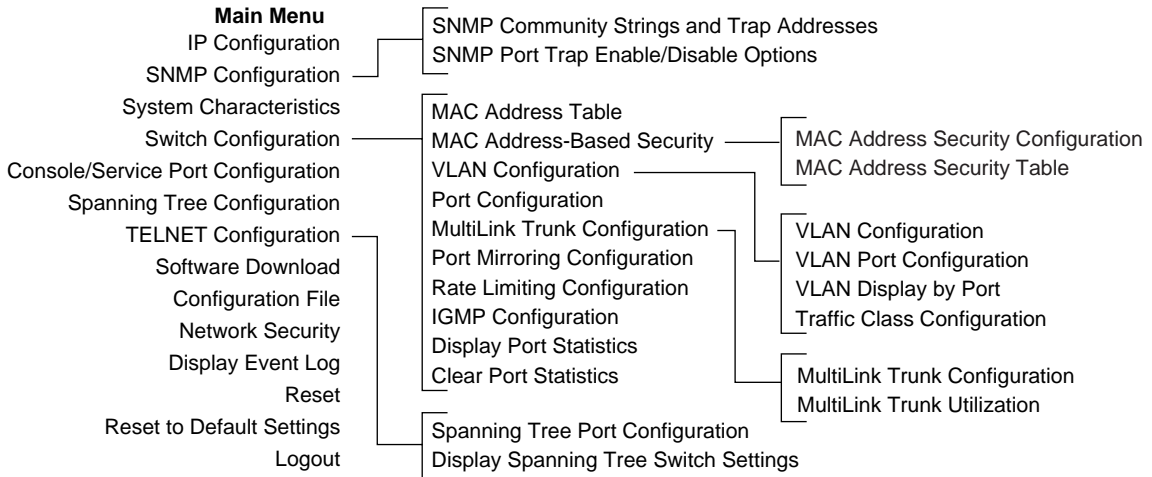
You can use accelerator keys to enter repetitive data into the fields of certain screens.

The accelerator keys can be used only on fields that require entering a list, which includes the MAC Address Security Configuration screen and the MAC Address Security Table screen.

For more information about using the accelerator keys, see [“Accelerator Keys for Repetitive Tasks”](#) on [page 3-32](#).

## 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.



BS35075A

**Figure 3-1. Map of console interface screens**

The CI screen examples provided in this chapter are for the BayStack Model 350T switch. Most of the screens and fields apply to all three models. If there are differences, it is clearly noted in the text.

The CI screens for your switch will show the correct model name in the screen title and the correct number of ports and port type.

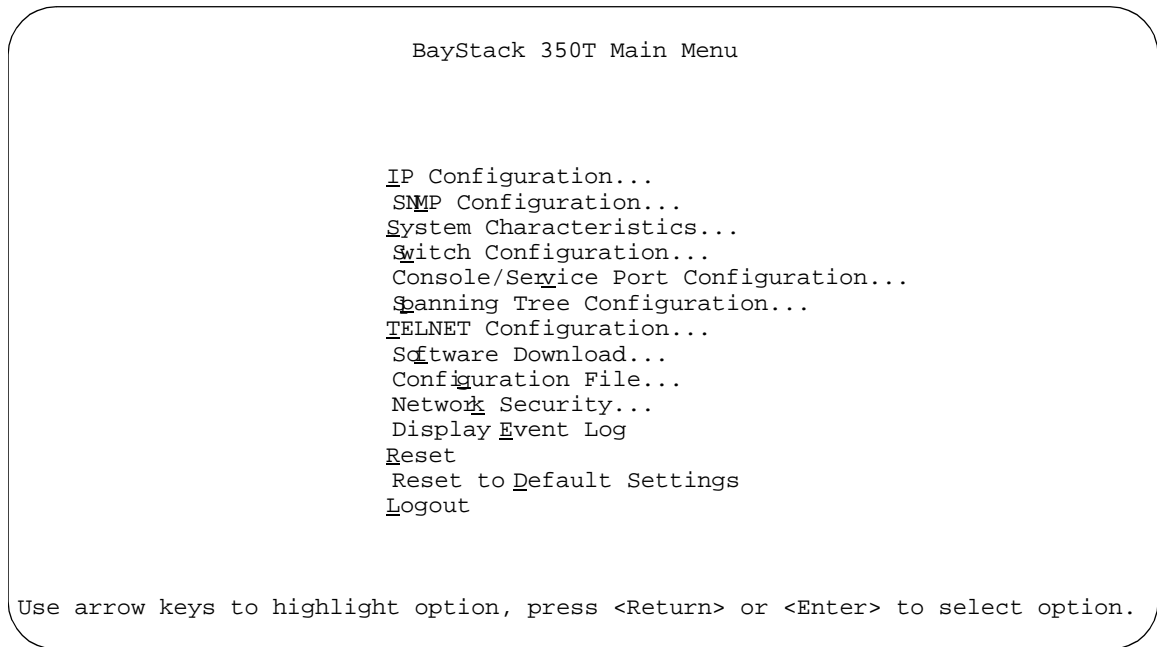


**Note:** The field values shown in the CI screens in this section are provided as examples only.

---

## Main Menu

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



**Figure 3-2. Console interface main menu**

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

**Table 3-1. Console interface main menu commands**

Command	Description
IP Configuration...	Displays the IP Configuration screen (see <a href="#">"IP Configuration"</a> on <a href="#">page 3-10</a> ). This screen allows you to set or modify IP configuration parameters.


*(continued)*

**Table 3-1. Console interface main menu commands** *(continued)*

Command	Description
<b>SNMP Configuration...</b>	Displays the SNMP Configuration Menu screen (see <a href="#">“SNMP Configuration”</a> on <a href="#">page 3-14</a> ). This screen allows you to set or modify the SNMP read-only community and read-write community strings, enable or disable the authentication trap for each port, set the IP address of trap receivers, and set the trap community strings.
<b>System Characteristics...</b>	Displays the System Characteristics screen (see <a href="#">“System Characteristics”</a> on <a href="#">page 3-20</a> ). This screen allows you to view switch characteristics such as the number of resets and the hardware and firmware version. This screen also contains three user-configurable fields: sysContact, sysName, and sysLocation.
<b>Switch Configuration...</b>	Displays the Switch Configuration Menu screen (see <a href="#">“Switch Configuration”</a> on <a href="#">page 3-22</a> ). This menu provides the following configuration options: MAC Address Table, MAC Address-Based Security, VLAN Configuration, Port Configuration, MultiLink Trunk Configuration, Port Mirroring Configuration, Rate Limiting Configuration, Display Port Statistics, and Clear All Port Statistics.
<b>Console/Service Port Configuration...</b>	Displays the Console/Service Port Configuration screen (see <a href="#">“Console/Service Port Configuration”</a> on <a href="#">page 3-58</a> ).
<b>Spanning Tree Configuration...</b>	Displays the Spanning Tree Configuration Menu (see <a href="#">“Spanning Tree Configuration”</a> on <a href="#">page 3-61</a> ). This menu provides the following configuration options: Spanning Tree Port Configuration, Display Spanning Tree Switch Settings.
<b>TELNET Configuration...</b>	Displays the TELNET Configuration screen (see <a href="#">“TELNET Configuration”</a> on <a href="#">page 3-68</a> ).
<b>Software Download...</b>	Displays the Software Download screen (see <a href="#">“Software Download”</a> on <a href="#">page 3-71</a> ).
<b>Configuration File...</b>	Displays the Configuration File Download/Upload screen (see <a href="#">“Configuration File”</a> on <a href="#">page 3-74</a> ). This screen allows you to store your switch configuration parameters on a TFTP server. You can retrieve the configuration parameters for automatically configuring a replacement switch or other switches with the same parameters.
<b>Network Security...</b>	Displays the Radius Network Security screen (see <a href="#">“Network Security”</a> on <a href="#">3-77</a> ). This screen allows you to set up or modify parameters for using the Radius (Remote Authentication Dial-In User Services) protocol.
<b>Display Event Log</b>	Displays the Event Log screen (see <a href="#">“Display Event Log”</a> on <a href="#">page 3-79</a> ).

*(continued)*

**Table 3-1. Console interface main menu commands** *(continued)*

Command	Description
<b>Reset</b>	Resets the switch with the current configuration settings. When you select this command, the switch resets, runs a self-test, then displays the main menu. This command is followed by a screen prompt which precedes the action. Enter Yes to reset the switch; enter No to abort the command.
<b>Reset to Default Settings</b>	Resets the switch to the factory default configuration settings. When you select this command, the switch resets, runs a self-test, then displays the main menu. This command is followed by a screen prompt which precedes the action. Enter Yes to reset the switch to the factory default configuration settings; enter No to abort the command.
	<b>Caution:</b> 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].
<b>Logout</b>	The Logout command allows a user in a TELNET session or a user working at a password-protected console terminal to terminate the session (see <a href="#">“Logout”</a> on <a href="#">page 3-83</a> ).

## IP Configuration

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

Choose IP Configuration (or press i) from the main menu to open the IP Configuration 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 3-12](#) for more information.)

```

IP Configuration

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 screen**

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

**Table 3-2. IP Configuration screen fields**

Field	Description
<b>BootP Request Mode</b>	One of four modes of operation for BootP. (See <a href="#">“Choosing a BootP Request Mode”</a> on <a href="#">page 3-12</a> for details about the four modes.)
	Default            BootP When Needed
	Range             BootP When Needed, BootP Always, BootP Disabled, BootP or Last Address
<b>Configurable</b>	Column header for the user-configurable fields in this screen.
<b>In Use</b>	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.
<b>Last BootP</b>	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.
<b>In-Band IP Address</b>	The in-band IP address of the BayStack 350 switch.
	Default            0.0.0.0 (no IP address assigned)
	Range             Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
<b>In-Band Subnet Mask</b>	The subnet address mask associated with the in-band IP address shown on the screen.
	Network routers use the subnet mask to determine the network or subnet address portion of a host’s IP address. The bits in the IP address that contain the network address (including the subnet) are set to 1 in the address mask, and the bits that contain the host identifier are set to 0.
	Default            0.0.0.0 (no subnet mask assigned)
	Range             Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
<b>Default Gateway</b>	The IP address of the default gateway.
	Default            0.0.0.0 (no IP address assigned)
	Range             Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point

## 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

### 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.

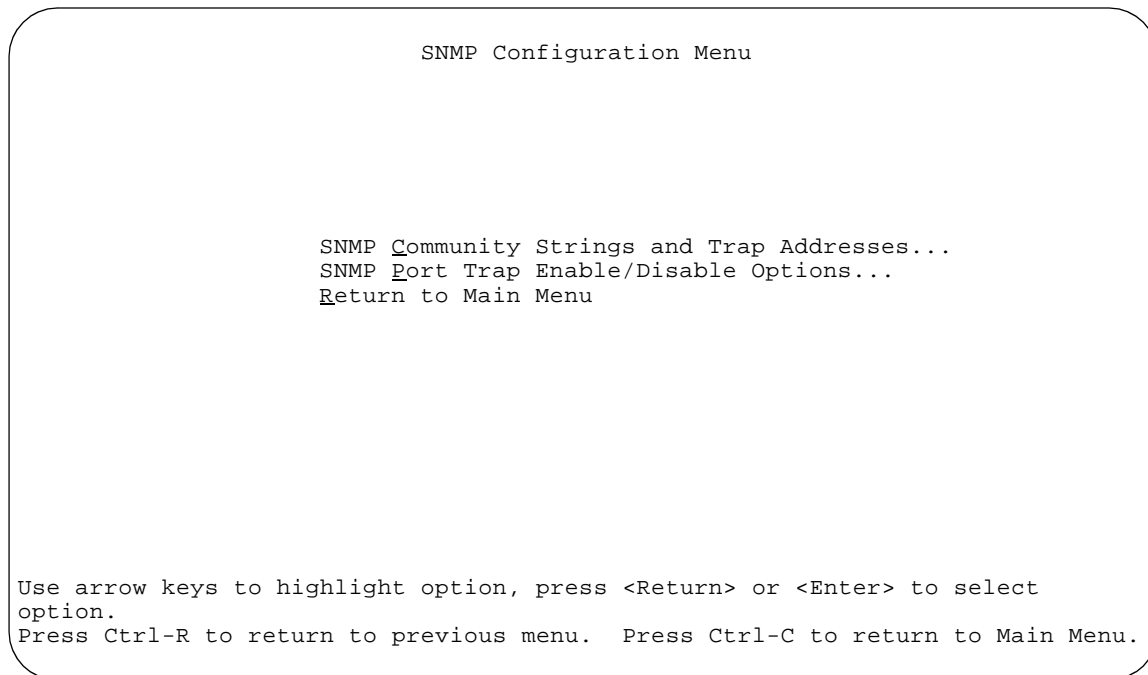
If an IP address is *not* currently in use, these actions take effect immediately.

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

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



**Figure 3-4. SNMP Configuration Screen**

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

**Table 3-3. SNMP Configuration Menu Screen Options**

Option	Description
<b>SNMP Community Strings and Trap Addresses...</b>	Displays the SNMP Community Strings and Trap Addresses screen (see <a href="#">“SNMP Community Strings and Trap Addresses”</a> on 3-16). This screen allows you to set or modify your SNMP configuration parameters.
<b>SNMP Port Trap Enable/Disable Options...</b>	Displays the SNMP Port Link Up/Down Trap Options screen (see <a href="#">“SNMP Port Trap Enable/Disable Options”</a> on 3-18). This screen allows you to Enable or Disable SNMP port link traps for any of the switch ports.
<b>Return to Main Menu</b>	Exits the SNMP Configuration Menu screen and displays the main menu.

## SNMP Community Strings and Trap Addresses

The SNMP Community Strings and Trap Addresses screen ([Figure 3-5](#)) allows you to set or modify your SNMP configuration parameters.

Choose SNMP Community Strings and Trap Address (or press c) from the SNMP Configuration Menu screen to open the SNMP Community Strings and Trap Addresses screen.

```
SNMP Community Strings and Trap Addresses

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

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

Authentication Trap:        [ Enabled ]
AutoTopology MIB:           [ 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 3-5.** SNMP Community Strings and Trap Addresses screen

[Table 3-4](#) describes the SNMP Configuration screen fields.

**Table 3-4. SNMP Configuration screen fields**

Field	Description
<b>Read-Only Community String</b>	The community string used for in-band read-only SNMP operations. Default            public Range             Any ASCII string of up to 32 printable characters
<b>Read-Write Community String</b>	The community string used for in-band read-write SNMP operations. Default            private Range             Any ASCII string of up to 32 printable characters
<b>Trap #1 IP Address<sup>1</sup></b>	Number one of four trap IP addresses. Successive trap IP address fields are numbered 2, 3, and 4. Each trap address has an associated community string (see Community String). Default            0.0.0.0 (no IP address assigned) Range             Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
<b>Community String</b>	The community string associated with one of the four trap IP addresses (see Trap #1 IP Address). Default            Zero-length string Range             Any ASCII string of up to 32 printable characters
<b>Authentication Trap</b>	Determines whether a trap will be sent when there is an SNMP authentication failure. Default            Enabled Range             Enabled, Disabled
<b>AutoTopology MIB</b>	Allows you to enable or disable the switch participation in autotopology, which allows network topology mapping of other switches in your network. Default            Enabled Range             Enabled, Disabled

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

## SNMP Port Trap Enable/Disable Options

The SNMP Port Link Up/Down Trap Options screen ([Figure 3-6](#)) allows you to set or modify SNMP port link up/down traps for any (or all) switch ports.

Choose SNMP Port Trap Enable/Disable Options (or press p) from the SNMP Configuration Menu screen to open the SNMP Port Link Up/Down Trap Options screen.

Port	Link Up/Down Trap Status
1	[ Disabled ]
2	[ Disabled ]
3	[ Disabled ]
4	[ Disabled ]
5	[ Disabled ]
6	[ Disabled ]
7	[ Disabled ]
8	[ Disabled ]
9	[ Disabled ]
10	[ Disabled ]
11	[ Disabled ]
12	[ Disabled ]
13	[ Disabled ]
14	[ Disabled ]
15	[ Disabled ]
16	[ Disabled ]
All	[ Disabled ]

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

**Figure 3-6. SNMP Port Link Up/Down Trap Option Screen**

[Table 3-5](#) describes the SNMP Port Link Up/Down Trap Option screen fields.

**Table 3-5. SNMP Port Link Up/Down Trap Option Screen Fields**

<b>Field</b>	<b>Description</b>
<b>Port</b>	Indicates the switch port numbers that correspond to the values in that row of the screen (for example, the values in row 2 apply to switch port 2). Note that the settings in the All row (bottom row) apply to all switch ports.
<b>Link Up/Down Trap Status</b>	Allows you to set (Enable or Disable) whether an SNMP Link Up/Down trap is sent, for any or all switch ports. You can also view the Link Up/Down trap setting for any (or all) switch ports.
	Default            Enabled
	Range            Enabled, Disabled

## System Characteristics

The System Characteristics screen ([Figure 3-7](#)) 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:      00-00-A2-EF-D3-80

Reset Count:     2
Last Reset Type: Power Cycle

sysDescr:        BayStack 350T   HW:RevC  FW:V1.01  SW:V3.0.0.5
sysObjectID:     1.3.6.1.4.1.45.3.30.1
sysUpTime:       02:36:14
sysServices:     3
sysContact:      [ Mario Lento ]
sysName:         [ Publications ]
sysLocation:     [ Building 12, Floor 20 ]

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

**Figure 3-7. System Characteristics screen**



[Table 3-6](#) describes the System Characteristics screen fields.

**Table 3-6. System Characteristics screen fields**

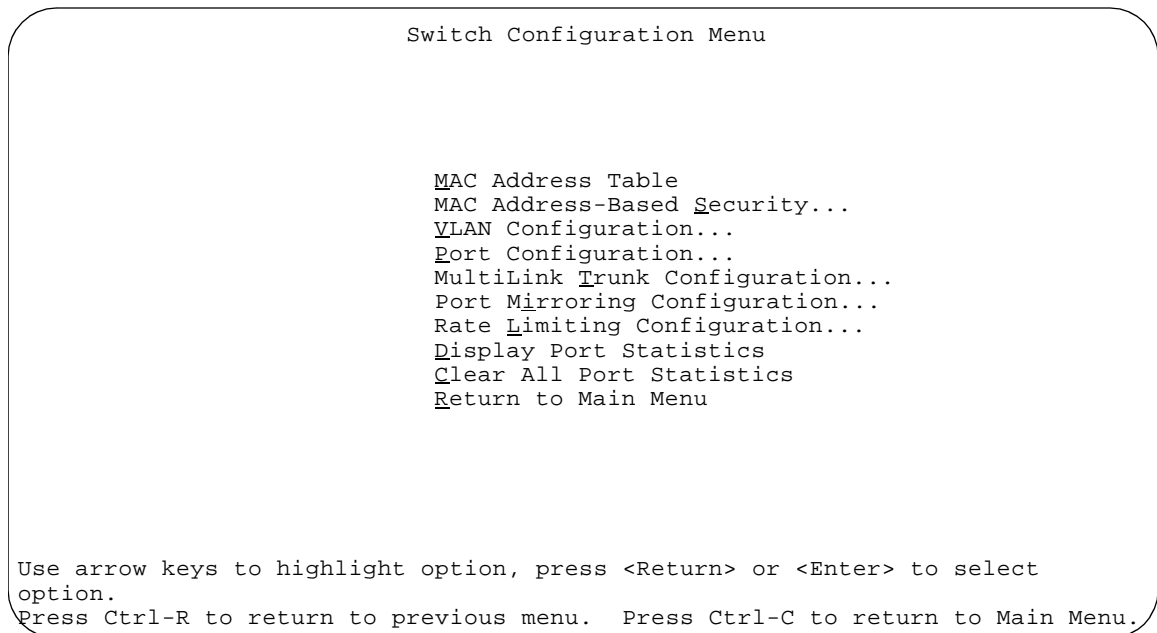
Field	Description
<b>MAC Address</b>	The MAC address of the BayStack 350 switch.
<b>Reset Count</b>	A read-only field that indicates the number of resets since the operational firmware was first loaded on the switch. Default            1 Range             0 to 2 <sup>32</sup> -1
<b>Last Reset Type</b>	A read-only field that indicates the last type of reset. Default            Power Cycle Range             Power Cycle, Software Download, Management Reset, Management Factory Reset
<b>sysDescr</b>	A read-only field that specifies the hardware and software version.
<b>sysObjectID</b>	A read-only field that provides a unique identification of the switch, which contains the vendor's private enterprise number.
<b>sysUpTime</b>	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.
<b>sysServices</b>	A read-only field that indicates the switch's physical and data link layer functionality.
<b>sysContact</b>	The name and phone number of the person responsible for the switch. Default            Zero-length string Range             Any ASCII string of up to 56 printable characters <sup>1</sup>
<b>sysName</b>	A name that uniquely identifies the switch. Default            Zero-length string Range             Any ASCII string of up to 56 printable characters <sup>1</sup>
<b>sysLocation</b>	The physical location of the switch. Default            Zero-length string Range             Any ASCII string of up to 56 printable characters

<sup>1</sup> 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 3-8](#)) allows you to set or modify your switch configuration.

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



**Figure 3-8. Switch Configuration Menu screen**

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

**Table 3-7. Switch Configuration Menu Options**

Option	Description
<b>MAC Address Table</b>	Displays the MAC Address Table screen (see <a href="#">“MAC Address Table”</a> on <a href="#">page 3-24</a> ). This screen allows you to view the MAC addresses that the switch has learned.
<b>MAC Address-Based Security...</b>	Displays the MAC Address Security Configuration Menu (see <a href="#">“MAC Address-Based Security”</a> on <a href="#">page 3-26</a> ). This menu allows you to set up the MAC Address Security feature. The following options are available: MAC Address Security Configuration and MAC Address Security Table.
<b>VLAN Configuration...</b>	Displays the VLAN Configuration screen (see <a href="#">“VLAN Configuration”</a> on <a href="#">page 3-34</a> ). This screen allows you to set up VLAN workgroups.
<b>Port Configuration...</b>	Displays the Port Configuration screen (see <a href="#">“Port Configuration”</a> on <a href="#">page 3-36</a> ). This screen allows you to configure a specific switch port or all switch ports.
<b>MultiLink Trunk Configuration...</b>	Displays the MultiLink Trunk Configuration Menu (see <a href="#">“MultiLink Trunk Configuration”</a> on <a href="#">page 3-39</a> ). This menu allows you to create trunks, to modify configured trunks, and to monitor the bandwidth utilization of configured trunks. The following options are available: Inter-Switch Trunk Configuration, Server Trunk Configuration, Trunk Utilization, and Return to Switch Configuration Menu screen.
<b>Port Mirroring Configuration...</b>	Displays the Port Mirroring Configuration screen (see <a href="#">“Port Mirroring Configuration”</a> on <a href="#">page 3-48</a> ). This screen allows you to designate a single switch port as a traffic monitor for up to two specified ports.
<b>Rate Limiting Configuration...</b>	Displays the Rate Limiting Configuration screen (see <a href="#">“Inter-Switch Trunk Configuration”</a> on <a href="#">page 3-41</a> ). This screen allows you to limit the forwarding rate of broadcast and multicast packets.
<b>Display Port Statistics</b>	Displays the Port Statistics screen (see <a href="#">“Port Statistics”</a> on <a href="#">page 3-54</a> ). This screen allows you to view detailed information about any switch port.
<b>Clear All Port Statistics</b>	The Clear All Port Statistics command allows you to clear all port statistics for all switch ports. This command is followed by a screen prompt which precedes the action. Enter Yes to clear all port statistics; enter No to abort the command.
<b>Return to Main Menu</b>	Exits the Switch Configuration Menu screen and displays the main menu.

## MAC Address Table

The MAC Address Table screen ([Figure 3-9](#)) allows you to view the 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 3-48](#)).

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

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 3-9.** MAC Address Table screen

[Table 3-8](#) describes the MAC Address Table screen fields.

**Table 3-8. MAC Address Table screen fields**

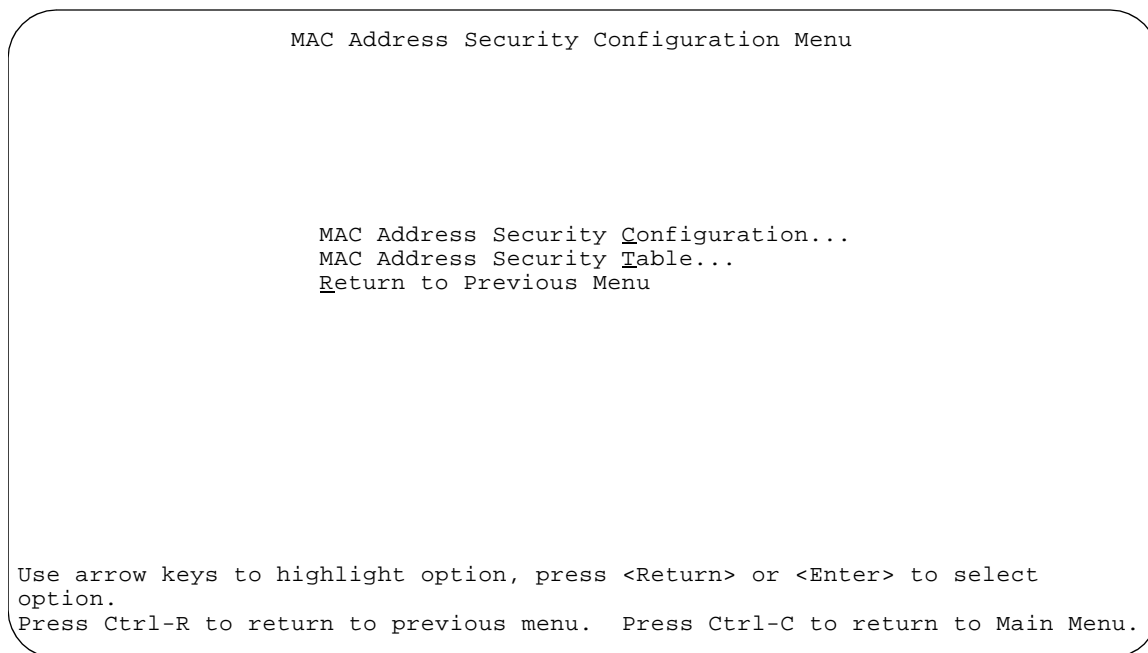
Field	Description
<b>Aging Time</b>	<p>Specifies how long a learned MAC address remains in the switch's forwarding database. If an entry is inactive for a period of time that exceeds the specified aging time, the address is removed.</p> <p>Default            300 seconds</p> <p>Range              10 to 1,000,000 seconds</p>
<b>Find an Address</b>	<p>Allows the user to search for a specific MAC address.</p> <p>Default            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>
<b>Port Mirroring Address A</b>	<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 "<a href="#">Port Mirroring Configuration</a>" on <a href="#">page 3-48</a> for more information.</p> <p>Default            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>
<b>Port Mirroring Address B</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 "<a href="#">Port Mirroring Configuration</a>" on <a href="#">page 3-48</a> for more information.</p> <p>Default            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>

## MAC Address-Based Security

The MAC Address Security Configuration Menu screen ([Figure 3-10](#)) allows you to specify a range of system responses to unauthorized network access to your switch. The system response can range from sending a trap to disabling the port. The network access control is based on the MAC addresses of the authorized stations. You can specify a list of up to 98 MAC addresses that are authorized to access the switch. You can also specify the ports that each MAC address is allowed to access. The options for allowed port access include: NONE, ALL, and single or multiple ports that are specified in a list, for example, 1-4, 6, 9, etc., (see [“Accelerator Keys for Repetitive Tasks”](#) on [page 3-32](#)). You must also include the MAC address of any router connected to any secure ports.

When the switch software detects a security violation, the response can be to send a trap, turn on destination address (DA) filtering, disable the specific port, or any combination of these three options.

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



**Figure 3-10. MAC Address Security Configuration Menu**

---

[Table 3-9](#) describes the MAC Address Security Configuration Menu options.

**Table 3-9. MAC Address Security Configuration Menu Options**

Option	Description
<b>MAC Address Security Configuration...</b>	Displays the MAC Address Security Configuration screen (see <a href="#">“MAC Address Security Configuration”</a> on <a href="#">page 3-28</a> ). This screen allows you to Enable or Disable the MAC Address Security feature.
<b>MAC Address Security Table...</b>	Displays the MAC Address Security Table screen (see <a href="#">“MAC Address Security Table”</a> on <a href="#">page 3-31</a> ). This screen allows you to specify the MAC addresses that are allowed to access the switch.
<b>Return to Previous Menu...</b>	Exits the MAC Address Security Configuration Menu screen and displays the Switch Configuration Menu screen.

## MAC Address Security Configuration

The MAC Address Security Configuration screen ([Figure 3-11](#)) allows you to Enable (or Disable) the MAC Address Security feature and to specify the appropriate system response to any unauthorized network access to your switch.

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

```
MAC Address Security Configuration

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

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

MAC Security Table:

Secure Ports:      [ NONE ]

Clear by Ports:   [ NONE ]

Learn by Ports:   [ NONE ]

Current Learning Mode:      [ Not Learning ]

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

**Figure 3-11. MAC Address Security Configuration Screen**

[Table 3-10](#) describes the MAC Address Security Configuration screen fields.



**Table 3-10. MAC Address Security Configuration Screen Fields**

Field	Description
<b>MAC Address Security SNMP-Locked</b>	<p>When this field is set to Enabled, the MAC Address Security screens cannot be modified using SNMP.</p> <p>Default            Disabled</p> <p>Range             Disabled, Enabled</p>
<b>MAC Address Security</b>	<p>When this field is set to Enabled, the software checks source MAC addresses of packets that arrive on secure ports against MAC Addresses listed in the MAC Address Security Table for allowed membership (see <a href="#">“MAC Address Security Table”</a> on <a href="#">page 3-31</a>). If the software detects any source MAC address that is not an allowed member, the software registers a MAC intrusion event.</p> <p>Default            Disabled</p> <p>Range             Disabled, Enabled</p>
<b>Partition Port on Intrusion Detected</b>	<p>This field value determines how the switch reacts to an intrusion event. When an intrusion event is detected (see MAC Address Security field description) the specified switch port is set to Disabled (partitioned from other switch ports).</p> <p>When this field is set to:</p> <ul style="list-style-type: none"> <li>• Disabled -- the port remains Enabled even if an intrusion event is detected.</li> <li>• Enabled -- the port becomes Disabled, then automatically resets to Enabled depending on the value set in the Partition Time field (see Partition Time Field description).</li> <li>• Forever -- the port becomes Disabled, and remains Disabled (partitioned). The Partition Time field cannot be used to automatically reset the port to Enabled if you set this field to Forever.</li> </ul> <p>You can always manually set the port's status field to Enabled using the Port Configuration screen (see <a href="#">“Port Configuration”</a> on <a href="#">3-36</a>).</p> <p>Default            Disabled</p> <p>Range             Disabled, Forever, Enabled</p>
<b>Partition Time</b>	<p>Determines the length of time a partitioned port remains Disabled (see Partition Port on Intrusion Detected field, above). This field is not operational when the Partition Port on Intrusion Detected field is set to Forever.</p> <p>Default            0 seconds (the value 0 indicates forever)</p> <p>Range             0-65536 seconds</p>

*(continued)*

**Table 3-10. MAC Address Security Configuration Screen Fields** *(continued)*

Field	Description
<b>DA Filtering on Intrusion Detected</b>	<p>When set to Enabled, this field isolates the intruding node by filtering (discarding) packets sent to that MAC address.</p> <p>Default            Disabled</p> <p>Range              Disabled, Enabled</p>
<b>Generate SNMP Trap on Intrusion</b>	<p>When set to Enabled and a MAC intrusion event is detected, the software issues an SNMP trap message to all registered SNMP trap addresses (see <a href="#">“SNMP Community Strings and Trap Addresses”</a> on <a href="#">page 3-16</a>).</p> <p>Default            Disabled</p> <p>Range              Disabled, Enabled</p>
<b>Secure Ports</b>	<p>The ports that are chosen to participate in the MAC Address Security feature. You cannot include any of the port values you have chosen for the Learn by ports field.</p> <p>Default            NONE</p> <p>Range              NONE, ALL, A port number list (for example, 1-4, 6, 9, etc.)</p>
<b>Clear by Ports</b>	<p>This field clears the specified port (or ports) that are listed in the Allowed Source Port (s) field of the MAC Address Security Table screen (see <a href="#">“MAC Address Security Table”</a> on <a href="#">page 3-31</a>). When you specify a port (or ports) to be cleared using this field, the specific port (or ports) will be cleared for each of the entries listed in the MAC Address Security Table. If you totally clear the allowed Source Port (s) field (leaving a blank field) for any entry, the associated MAC Address for that entry is also cleared.</p> <p>Default            NONE</p> <p>Range              NONE, ALL, A port number list (for example, 1-4, 6, 9, etc.)</p>
<b>Learn by Ports</b>	<p>All source MAC addresses of any packets received on the specified port (or ports) are added to the MAC Security Table when the Current Learning Mode field (see next field description) is set to Learning in Progress. You cannot include any of the port values you have chosen for the secure ports field.</p> <p>Default            NONE</p> <p>Range              NONE, ALL, A port number list (for example, 1-4, 6, 9, etc.)</p>
<b>Current Learning Mode</b>	<p>Indicates the current learning mode for the switch ports. When this field is set to Learning in Progress, all source MAC addresses of any packets received on the specified port (or ports) are added to the MAC Security Table (maximum of 98 MAC address entries allowed). If you exceed the limit of 98 entries, the system prompts you with an alert message.</p> <p>Default            Not Learning</p> <p>Range              Not Learning, Learning in Progress</p>

## MAC Address Security Table

The MAC Address Security Table screen ([Figure 3-12](#)) allows you to specify the ports that each MAC Address is allowed to access. As shown in [Figure 3-12](#), the options for allowed port access include: NONE, ALL, and ports that are specified in a list (for example, 1-4, 6, 9, etc.). You must also include the MAC addresses of any routers that are connected to any secure ports.

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

MAC Address Security Table		
Entry	MAC Address	Allowed Source Port(s)
1	[ 02-12-34-22-33-12 ]	[ 1-4,6,9,11,14 ]
2	[ 02-33-55-22-33-44 ]	[ 1-10,14 ]
3	[ 08-36-24-55-42-18 ]	[ ALL ]
4	[ 02-33-55-22-54-65 ]	[ 2,4,6-12 ]
5	[ 16-23-65-44-77-47 ]	[ NONE ]
6	[ 22-33-54-66-33-99 ]	[ 1,3,5,9,12,16 ]
7	[ - - - - - ]	[ - ]
8	[ - - - - - ]	[ - ]
9	[ - - - - - ]	[ - ]
10	[ - - - - - ]	[ - ]
11	[ - - - - - ]	[ - ]
12	[ - - - - - ]	[ - ]
13	[ - - - - - ]	[ - ]
14	[ - - - - - ]	[ - ]

More...

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

**Figure 3-12. MAC Address Security Table Screen**

[Table 3-11](#) describes the MAC Address Security Configuration screen fields.

**Table 3-11. MAC Address Security Table Screen Fields**

Field	Description
<b>MAC Address</b>	<p>Allows you to specify up to 98 MAC addresses that are authorized to access the switch. You can specify the ports that each MAC address is allowed to access using the Allowed Source Ports field (see next field description). The specified MAC address does not take effect until the Allowed Source Port field is set to some value. You can clear an existing MAC address field by entering zero (0) in the field and pressing [Enter].</p> <p>Default            - - - - - (no address assigned)</p> <p>Range             A range of 6 Hex Octets, separated by dashes (multicast<sup>1</sup> and broadcast addresses are not allowed).</p>
<b>Allowed Source Ports</b>	<p>Allows you to specify the ports that each MAC address is allowed to access. The options for port access include none, all, and ports that are specified in a list (for example, 1-4, 6, 9, etc.).</p> <p>Default            - (Blank field)</p> <p>Range             A port number list (for example, 1-4, 6, 9, etc.), NONE, ALL</p>

<sup>1</sup> Multicast address -- Note that the first octet of any Multicast address will always be an odd number.

### Accelerator Keys for Repetitive Tasks

You can use accelerator keys to help speed up repetitive tasks. For example, suppose you want to modify one of the port number lists shown in [Figure 3-12](#) on [page 3-31](#).

#### Adding A New Port to an Existing Port Number List:

In the example shown in [Figure 3-12](#), entry 6 shows the Allowed Source Ports (s) field values as:

1, 3, 5, 9, 12, 16

If you want to add another port (port **14**) to the existing port number list, you would normally have to highlight the field and then type another port list, including the new port number: 1, 3, 5, 9, 12, **14**, 16 [Return].

This works but is quite time-consuming.

Instead, you can highlight the field, and then enter **+14** [Return]. The existing field keeps the previous list, and adds the new port number (14) between ports 12 and 16.

(If you had chosen to add port **15** to the existing port number list, the field accepts the new port 15 but shows the new port number list field as: 1, 3, 5, 9, 12, **15-16**.)

#### **Removing a Port from an Existing Port Number List:**

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

#### **Copying an Existing Field into an Adjacent Field:**

Another accelerator key you can use is the period (.) character. This character is used to copy a previously entered field into the field directly next to it.

For example, to copy the entire port number list 1, 3, 5, 9, 12, 16 (shown in [Figure 3-12](#) on [page 3-31](#)) into the next field (entry 7):

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

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

These accelerator keys work only on fields that require entering a list, which includes the MAC Address Security Configuration screen and the MAC Address Security Table screen.

## VLAN Configuration

The VLAN Configuration screen allows you to configure the BayStack 350 switch with up to eight virtual LANs (VLANs).



**Note:** When MultiLink trunking is active, only five VLANs can be configured and the VLAN Configuration screen shows only five VLAN columns.

The VLAN Configuration screen provides a matrix that you use to group the switch ports into logical (virtual) workgroups. Users in each logical workgroup can share resources but cannot communicate with users in other logical workgroups. See “MultiLink Trunks” on page 1-24 for more information about MultiLink Trunks. For more information about Configuring VLANs, see “VLAN Workgroups” on page 1-16.

[Figure 3-13](#) and [Figure 3-14](#) show the default settings for the two Model 350F-HD VLAN Configuration screens, with all ports configured for VLAN V1.

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

VLAN Configuration						
Port	Trunk	V1	V2	V3	V4	V5
1		[ X ]	[ ]	[ ]	[ ]	[ ]
2		[ X ]	[ ]	[ ]	[ ]	[ ]
3		[ X ]	[ ]	[ ]	[ ]	[ ]
4		[ X ]	[ ]	[ ]	[ ]	[ ]
5		[ X ]	[ ]	[ ]	[ ]	[ ]
6	S1	[ X ]	[ ]	[ ]	[ ]	[ ]
7	S1	[ X ]	[ ]	[ ]	[ ]	[ ]
8		[ X ]	[ ]	[ ]	[ ]	[ ]
9	S1	[ X ]	[ ]	[ ]	[ ]	[ ]
10		[ X ]	[ ]	[ ]	[ ]	[ ]
11		[ X ]	[ ]	[ ]	[ ]	[ ]
12		[ X ]	[ ]	[ ]	[ ]	[ ]

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.

**Figure 3-13. Model 350F-HD VLAN Configuration screen (1 of 2)**

VLAN Configuration						
Port	Trunk	V1	V2	V3	V4	V5
13	I2	[ X ]	[ ]	[ ]	[ ]	[ ]
14	I2	[ X ]	[ ]	[ ]	[ ]	[ ]
15		[ X ]	[ ]	[ ]	[ ]	[ ]
16		[ X ]	[ ]	[ ]	[ ]	[ ]
17	S1	[ X ]	[ ]	[ ]	[ ]	[ ]
18		[ X ]	[ ]	[ ]	[ ]	[ ]
19	I3	[ X ]	[ ]	[ ]	[ ]	[ ]
20	I3	[ X ]	[ ]	[ ]	[ ]	[ ]
21		[ X ]	[ ]	[ ]	[ ]	[ ]
22	I4	[ X ]	[ ]	[ ]	[ ]	[ ]
23	I4	[ X ]	[ ]	[ ]	[ ]	[ ]
24		[ X ]	[ ]	[ ]	[ ]	[ ]
25	I1	[ X ]	[ ]	[ ]	[ ]	[ ]
26	I1	[ X ]	[ ]	[ ]	[ ]	[ ]

Press Ctrl-P to display choices for ports 1-12.  
 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. Model 350F-HD VLAN Configuration screen (2 of 2)**

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

**Table 3-12. VLAN Configuration screen fields**

Field	Description
<b>Port</b>	Indicates the switch port numbers, from 1 to 26, 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).
<b>Trunk<sup>1</sup></b>	The read-only data displayed in this column indicates the trunks (I1 to I4 and S1 to S4) that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen.  For example, if switch ports 22 and 23 are configured as trunk members to inter-switch trunk I4 in the Trunk Configuration screen, the designation I4 is displayed in the Trunk column, adjacent to ports 22 and 23. For more information about the MultiLink trunking feature, see " <a href="#">MultiLink Trunk Configuration</a> " on <a href="#">page 3-39</a> .

(continued)

**Table 3-12. VLAN Configuration screen fields** *(continued)*

Field	Description
<b>V1 to V8</b>	Indicates the VLAN names for VLAN V1 to VLAN V8.
Default	All ports configured in VLAN V1
Range	Enabled [ x ], Disabled [ ]

<sup>1</sup> MultiLink trunking is available for BayStack 350 Series switches using software release version V2.0 (or later). Earlier version BayStack 350 Series switches do not display this field in the VLAN Configuration screens.

## Port Configuration

The Port Configuration screen (see [Figure 3-15](#) and [Figure 3-16](#)) 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.

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	S1	[ Enabled ]	Up	[ Enabled ]	[ 100Mbs / Full ]	
7	S1	[ Enabled ]	Up	[ Enabled ]	[ 100Mbs / Full ]	
8		[ Enabled ]	Up	[ Enabled ]	[ 10Mbs / Full ]	
9	S1	[ Enabled ]	Up	[ Disabled ]	[ 100Mbs / Full ]	
10		[ Enabled ]	Down	[ Enabled ]	[ 100Mbs / Full ]	
11		[ Enabled ]	Down	[ Enabled ]	[ 100Mbs / Full ]	
12		[ Enabled ]	Down	[ Disabled ]	[ 100Mbs / Half ]	

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.

**Figure 3-15. Model 350F-HD Port Configuration screen (1 of 2)**



Port Configuration						
Port	Trunk	Status	Link	Auto Negotiation	Speed	Duplex
13	I2	[ Enabled ]	Up	[ Enabled ]	[ 100Mbs / Full ]	
14	I2	[ Enabled ]	Up	[ Enabled ]	[ 100Mbs / Full ]	
15		[ Enabled ]	Up	[ Enabled ]	[ 100Mbs / Full ]	
16		[ Enabled ]	Down	[ Disabled ]	[ 100Mbs / Half ]	
17	S1	[ Enabled ]	Up	[ Disabled ]	[ 100Mbs / Half ]	
18		[ Enabled ]	Down	[ Disabled ]	[ 100Mbs / Half ]	
19	I3	[ Enabled ]	Up	[ Disabled ]	[ 100Mbs / Half ]	
20	I3	[ Enabled ]	UP	[ Disabled ]	[ 100Mbs / Half ]	
21		[ Enabled ]	Down	[ Disabled ]	[ 100Mbs / Half ]	
22	I4	[ Enabled ]	Up	[ Enabled ]	[ 100Mbs / Full ]	
23	I4	[ Enabled ]	Up	[ Enabled ]	[ 100Mbs / Full ]	
24		[ Enabled ]	Down	[ Enabled ]	[ 100Mbs / Full ]	
25	I1	[ Enabled ]	Up	[ Disabled ]	[ 100Mbs / Full ]	
26	I1	[ Enabled ]	Up	[ Disabled ]	[ 100Mbs / Full ]	
All		[ Enabled ]		[ Disabled ]	[ 100Mbs / Full ]	

Press Ctrl-P to display choices for ports 1-12.  
 Use space bar to display choices, press <Return> or <Enter> to select choice.  
 Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

**Figure 3-16. Model 350F-HD Port Configuration screen (2 of 2)**

[Table 3-13](#) describes the Port Configuration screen fields.

**Table 3-13. Port Configuration screen fields**

Field	Description
<b>Port</b>	Indicates the switch port numbers, from 1 to 26, 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 settings in the All row (bottom row) apply to all 26 switch ports.
<b>Trunk</b>	The read-only data displayed in this column indicates the trunks (I1 to I4 and S1 to S4) that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen (see " <a href="#">MultiLink Trunk Configuration</a> " on <a href="#">page 3-39</a> ).

*(continued)*

**Table 3-13. Port Configuration screen fields** *(continued)*

Field	Description
<b>Status</b>	Allows you to disable any of the switch ports. You can also use this field to control access to any switch port. Default            Enabled Range             Enabled, Disabled
<b>Link</b>	A read-only field that indicates the current link state of the corresponding port, as follows: <ul style="list-style-type: none"> <li>• Up: The port is connected and operational.</li> <li>• Down: The port is not connected or is not operational.</li> </ul>
<b>Autonegotiation<sup>1</sup></b>	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. Default            Enabled Range             Enabled, Disabled
<b>Speed/Duplex<sup>2</sup></b>	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. Default            100Mbs/Half (when Autonegotiation is Disabled) Range             10Mbs/Half, 10Mbs/Full, 100Mbs/Half, 100Mbs/Full

<sup>1</sup> You cannot modify this field for the Model 350F-HD and Model 350F 100BASE-FX fiber optic ports.

<sup>2</sup> The Model 350F-HD and Model 350F 100BASE-FX fiber optic ports can be set to 100 Mbs/Half or 100 Mbs/Full.

## MultiLink Trunk Configuration

The MultiLink Trunk Configuration Menu screen (see [Figure 3-17](#)) allows you to select the appropriate screen to configure up to four inter-switch trunks and four server trunks. Any combination of each configuration type (inter-switch and server trunk) can be used to configure up to 16 trunk members on each switch).

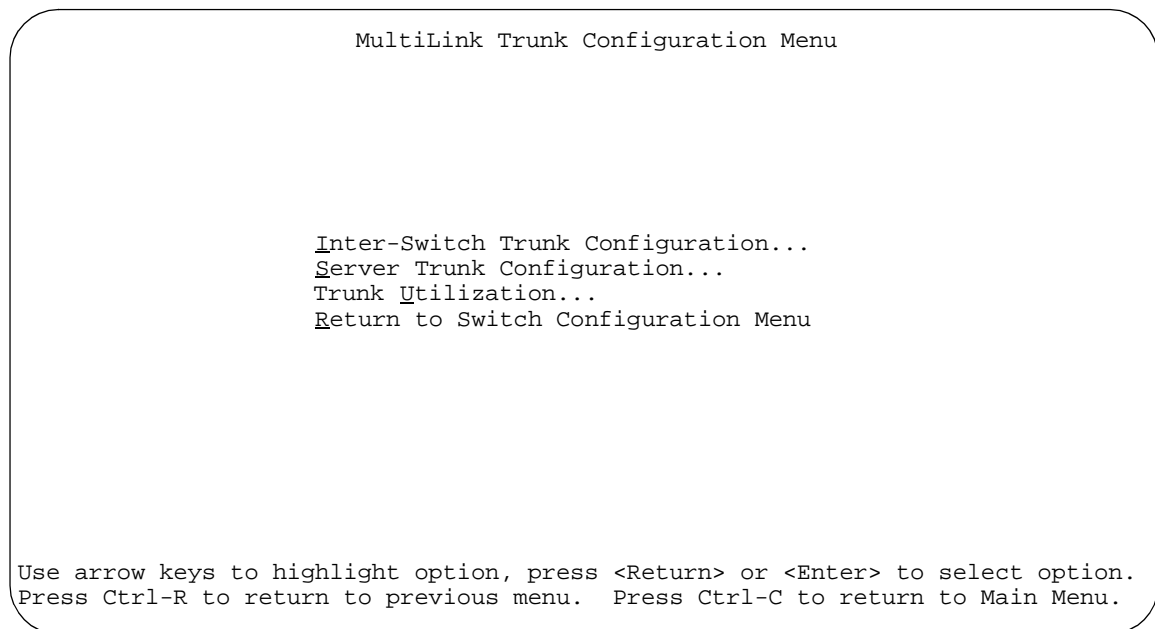
Bandwidth utilization can be monitored for the trunk member ports within each trunk and trunk-type.

For more information about configuring MultiLink Trunks, see “MultiLink Trunks” on page 1-24.



**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.



**Figure 3-17. MultiLink Trunk Configuration Menu screen**

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

**Table 3-14. MultiLink Trunk Configuration Menu Options**

Option	Description
<b>Inter-Switch Trunk Configuration...</b>	Displays the Inter-Switch Trunk Configuration screen ( <a href="#">Figure 3-18</a> ). This screen allows you to logically connect up to eight switch ports together to form up to four <i>inter-switch trunks</i> to another switch.
<b>Server Trunk Configuration...</b>	Displays the Server Trunk Configuration screen ( <a href="#">Figure 3-19</a> ). This screen allows you to logically connect up to eight switch ports together to form up to four <i>server trunks</i> to a server.
<b>Trunk Utilization...</b>	Displays the Trunk Utilization screen ( <a href="#">Figure 3-20</a> and <a href="#">Figure 3-21</a> ). This screen allows you to monitor the bandwidth utilization of the configured trunks. You can monitor bandwidth utilization for either type of trunk: inter-switch trunk or server trunk.
<b>Return to Switch Configuration Menu</b>	Exits the MultiLink Trunk Configuration Menu screen and displays the Switch Configuration Menu screen.

## Inter-Switch Trunk Configuration

The Inter-Switch Trunk Configuration screen allows you to configure two to eight switch ports together as members of an inter-switch trunk. Up to four inter-switch trunks can be created for each BayStack 350 switch. [Figure 3-18](#) shows an example of the Inter-Switch Trunk Configuration screen. In this screen example, four trunks are shown, with each trunk 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 1-24 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 Inter-Switch Trunk Configuration (or press i) from the MultiLink Trunk Configuration Menu screen to open the Inter-Switch Trunk Configuration screen.

```

Inter-Switch Trunk Configuration

Trunk      Trunk Members      STP      Trunk Mode      Trunk Status
-----
I1 [ 25 ][ 26 ][      ][      ] [ Enabled ] [ Enhanced ] [ Enabled ]
I2 [ 13 ][ 14 ][      ][      ] [ Enabled ] [ Enhanced ] [ Enabled ]
I3 [ 19 ][ 20 ]          [ Enabled ] [ Enhanced ] [ Enabled ]
I4 [ 22 ][ 23 ]          [ Enabled ] [ Enhanced ] [ Enabled ]

Valid inter-switch trunk configurations are:
    1 or 2 trunks of up to 4 links each
    Up to 4 trunks of 2 links each


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.** Inter-Switch Trunk Configuration screen

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

**Table 3-15. Inter-Switch Trunk Configuration screen fields**

Field	Description
<b>Trunk</b>	Column header for the read-only fields in this screen. The read-only data displayed in the Trunk column indicates the trunks (I1 to I4) that correspond to the switch ports specified in the user-configurable Trunk Members fields.
<b>Trunk Members</b>	<p>The Trunk Members column contains fields in each row that can be configured to create the corresponding trunk. The combined trunks cannot exceed eight trunk members. 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, Spanning Tree Configuration screen, and VLAN Configuration screen.</p> <p>Default            blank field</p> <p>Range             1 to 26 (depending on model type)</p>
<b>STP</b>	<p>The STP 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>Default            Enabled</p> <p>Range             Enabled, Disabled</p>
<b>Trunk Mode</b>	<p>The Trunk Mode column contains a single field for each row that allows a user to set the trunk to operate in one of two modes: Basic or Enhanced.</p> <p><b>Basic:</b> Basic mode is the default mode for the switch. When in this mode, the switch locks a source MAC address to a specific trunk member for a certain time interval. This allows the switch to stabilize data streams of source addresses within the trunk members.</p> <p><b>Enhanced:</b> When in this mode, the switch evenly distributes source MAC addresses to the trunk members, thereby balancing traffic throughout the trunk.</p>
	<p> <b>Note:</b> Certain protocols, such as Local Area Transport (LAT), require proper sequencing of received packets for correct operation. Using Enhanced mode may cause some packets to be received out of sequence. If your application is using a protocol requiring proper sequencing of packets, use the Basic mode.</p>
	<p>Default            Basic</p> <p>Range             Basic, Enhanced</p>
<b>Trunk Status</b>	<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            Disabled</p> <p>Range             Enabled, Disabled</p>

## Server Trunk Configuration

The Server Trunk Configuration screen allows you to configure two to eight switch ports together as members of a server trunk. Up to four server trunks can be created for each BayStack 350 switch. [Figure 3-19](#) shows an example of the Server Trunk Configuration screen. In this screen example, one server trunk is shown configured with four 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. For more information, see “MultiLink Trunks” on page 1-24.



**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 Server Trunk Configuration (or press s) from the MultiLink Trunk Configuration Menu screen to open the Server Trunk Configuration screen.

```

Server Trunk Configuration

Trunk          Trunk Members          Trunk Status
-----
S1             [ 6 ][ 7 ][ 9 ][ 17 ]             [ Enabled ]
S2             [   ][   ][   ][   ]             [ Disabled ]
S3             [   ][   ]                       [ Disabled ]
S4             [   ][   ]                       [ Disabled ]

Valid server trunk configurations are:
    1 or 2 trunks of up to 4 links each
    Up to 4 trunks of 2 links each

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. Server Trunk Configuration screen**

[Table 3-16](#) describes the Server Trunk Configuration screen fields.

**Table 3-16. Server Trunk Configuration screen fields**

---

<b>Field</b>	<b>Description</b>
<b>Trunk</b>	Column header for the read-only fields in this screen. The read-only data displayed in the Trunk column indicates the trunks (S1 to S4) that correspond to the switch ports specified in the user-configurable Trunk Members fields.
<b>Trunk Members</b>	<p>The Trunk Members column contains fields in each row that can be configured to create the corresponding trunk. The combined trunks cannot exceed eight trunk members. 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, Spanning Tree Configuration screen, and VLAN Configuration screen.</p> <p>Default            blank field</p> <p>Range             1 to 26 (depending on model type)</p>
<b>Trunk Status</b>	<p>The Trunk Status column contains a single field for each row that allows users to enable or disable any of the server trunks.</p> <p>Default            Disabled</p> <p>Range             Enabled, Disabled</p>

---



## Trunk Utilization

The Trunk Utilization screen ([Figure 3-20](#) and [Figure 3-21](#)) allows you to monitor the percentage of bandwidth used by configured trunk members. You can choose the type of traffic to monitor.

[Figure 3-20](#) shows an example of bandwidth utilization rates for the trunk member ports configured in inter-switch trunks I1, I2, I3, and I4. To display utilization for server trunks S1 to S4, press [Ctrl]+N.

[Figure 3-21](#) shows an example of bandwidth utilization rates for the trunk member ports configured in server trunk S1.

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

Trunk Utilization					
Trunk	Traffic Type	Port	Last 5 Minutes	Last 30 Minutes	Last Hour
I1	[ Rx and Tx ]	25	90.0%	70.0%	80.0%
		26	20.0%	50.0%	100.0%
I2	[ Rx and Tx ]	13	15.0%	45.0%	30.0%
		14	60.0%	10.0%	20.0%
I3	[ Rx and Tx ]	19	30.0%	90.0%	80.0%
		20	20.0%	10.0%	50.0%
I4	[ Rx and Tx ]	22	85.0%	35.0%	50.0%
		23	90.0%	80.0%	70.0%

More...

Press Ctrl-N to display utilization for trunks S1-S4.  
 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. Trunk Utilization screen (1 of 2)**

Trunk Utilization					
Trunk	Traffic Type	Port	Last 5 Minutes	Last 30 Minutes	Last Hour
S1	[ Rx and Tx ]	6	40.0%	20.0%	55.0%
		7	20.0%	70.0%	10.0%
		9	25.0%	15.0%	50.0%
		17	65.0%	50.0%	80.0%
S2	[ Rx and Tx ]				
S3	[ Rx and Tx ]				
S4	[ Rx and Tx ]				

Press Ctrl-P to display utilization for trunks I1-I4.  
 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. Trunk Utilization screen (2 of 2)**

[Table 3-17](#) describes the Trunk Utilization screen fields.

**Table 3-17. Trunk Utilization screen fields**

Field	Description
<b>Trunk</b>	Column header for the read-only fields in this screen. The read-only data displayed in this column indicates the trunks (I1 to I4 or S1 to S4) that correspond to the switch ports specified in the Port field.
<b>Traffic Type</b>	Allows you to choose the traffic type to be monitored for percent of bandwidth utilization (see Range). Default            Rx and Tx Range              Rx and Tx, Rx, Tx
<b>Port</b>	This field lists the trunk member ports that correspond to the trunk specified in the Trunk column.

*(continued)*

**Table 3-17. Trunk Utilization screen fields** *(continued)*

<b>Field</b>	<b>Description</b>
<b>Last 5 Minutes</b>	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.
<b>Last 30 Minutes</b>	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.
<b>Last Hour</b>	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 1-45.

[Figure 3-22](#) 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 3-22. Port Mirroring Configuration screen**

[Table 3-18](#) describes the Port Mirroring Configuration screen fields.

**Table 3-18. Port Mirroring Configuration screen fields**

Field	Description
<b>Monitoring Mode</b>	<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 <a href="#">Table 3-19</a>). 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            Disabled</p> <p>Range             See <a href="#">Table 3-19</a></p>
<b>Monitor Port</b>	<p>Indicates the switch port designated as the monitor port.</p> <p>Default            Zero-length string</p> <p>Range             1 to 26 (Model dependent)</p>
<b>Port X</b>	<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 <a href="#">Table 3-19</a>).</p> <p>Default            Zero-length string</p> <p>Range             1 to 26 (Model dependent)</p>
<b>Port Y</b>	<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 <a href="#">Table 3-19</a>).</p> <p>Default            Zero-length string</p> <p>Range             1 to 26 (Model dependent)</p>
<b>Address A</b>	<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 <a href="#">Table 3-19</a>). 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 "<a href="#">MAC Address Table</a>" on <a href="#">page 3-24</a>).</p> <p>Default            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 3-18. Port Mirroring Configuration screen fields** *(continued)*

Field	Description
<b>Address B</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 <a href="#">Table 3-19</a> ). 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 " <a href="#">MAC Address Table</a> " on <a href="#">page 3-24</a> ).
Default	00-00-00-00-00-00 (no MAC address assigned)
Range	00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF

[Table 3-19](#) describes the various monitoring modes available from the Port Mirroring Configuration screen.

**Table 3-19. Monitoring Modes**

Port-based Fields	Description
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 or Port Y <->	Monitor all traffic received/transmitted by Port X and received/transmitted by Port Y

Address-based Fields	Description
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.

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

[Figure 3-23](#) and [Figure 3-24](#) show sample rate limiting settings for the two Model 350F-HD Rate Limiting Configuration screens.



**Note:** The Model 350F and Model 350T display all ports on one screen.

Rate Limiting Configuration					
Port	Packet Type	Limit	Last 5 Minutes	Last Hour	Last 24 Hours
1	[ Both ]	[ None ]	56.0%	22.0%	13.0%
2	[ Multicast ]	[ 9% ]	30.0%	27.0%	12.0%
3	[ Both ]	[ None ]	25.0%	24.0%	18.0%
4	[ Both ]	[ 10% ]	72.0%	53.0%	14.0%
5	[ Broadcast ]	[ 10% ]	35.0%	57.0%	12.0%
6	[ multicast ]	[ 10% ]	96.0%	98.0%	99.0%
7	[ Both ]	[ 10% ]	86.0%	85.0%	95.0%
8	[ Both ]	[ 5% ]	58.0%	65.0%	72.0%
9	[ Broadcast ]	[ None ]	11.0%	13.0%	52.0%
10	[ Both ]	[ None ]	27.0%	21.0%	43.0%
11	[ Both ]	[ None ]	15.0%	25.0%	23.0%
12	[ Both ]	[ None ]	12.0%	15.0%	22.0%

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.

**Figure 3-23. Model 350F-HD Rate Limiting Configuration screen (1 of 2)**

Rate Limiting Configuration					
Port	Packet Type	Limit	Last 5 Minutes	Last Hour	Last 24 Hours
13	[ Both ]	[ None ]	44.0%	0.0%	0.0%
14	[ Multicast ]	[ None ]	34.0%	0.0%	0.0%
15	[ Both ]	[ None ]	45.0%	0.0%	0.0%
16	[ Broadcast ]	[ 10% ]	35.0%	66.0%	13.0%
17	[ Broadcast ]	[ None ]	27.0%	59.0%	22.0%
18	[ Both ]	[ 10% ]	12.0%	33.0%	0.0%
19	[ Both ]	[ None ]	23.0%	77.0%	44.0%
20	[ Both ]	[ None ]	45.0%	0.0%	0.0%
21	[ Both ]	[ None ]	67.0%	0.0%	0.0%
22	[ Both ]	[ None ]	29.0%	0.0%	0.0%
23	[ Both ]	[ None ]	32.0%	47.0%	44.0%
24	[ Both ]	[ None ]	38.0%	22.0%	0.0%
25	[ Both ]	[ None ]	12.0%	66.0%	0.0%
26	[ Both ]	[ 5% ]	73.0%	88.0%	97.0%
All	[ Both ]	[ None ]			

Press Ctrl-P to display choices for ports 1-12.  
 Use space bar to display choices, press <Return> or <Enter> to select choice.  
 Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

**Figure 3-24. Model 350F-HD 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 3-20](#) describes the Rate Limiting Configuration screen fields.

**Table 3-20. Rate Limiting Configuration screen fields**

Field	Description
<b>Port</b>	Indicates the switch port numbers, from 1 to 26, 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) apply to all 26 switch ports.
<b>Packet Type</b>	Allows you to select the packet types for rate limiting or viewing. Default Both Range Both, Multicast, Broadcast
<b>Limit</b>	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 <sup>1</sup> . Default None Range None, 10%, 9%, 8%, 7%, 6%, 5%, 4%, 3%, 2%, 1%
<b>Last 5 Minutes</b>	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.
<b>Last Hour</b>	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.
<b>Last 24 Hours</b>	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.

<sup>1</sup> 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.

## Port Statistics

The Port Statistics screen ([Figure 3-25](#)) 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 command to clear port counters for all ports (see “[Switch Configuration](#)” on [page 3-22](#)).

Choose 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 3-25. Port Statistics screen**

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



**Note:** With the exception of the Port field, all fields in this screen are read-only.

**Table 3-21. Port Statistics screen fields**

Field	Description
<b>Port</b>	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.
<b>Packets</b>	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.
<b>Multicasts</b>	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.
<b>Broadcasts</b>	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.
<b>Total Octets</b>	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.
<b>Lost Packets</b>	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.
<b>FCS Errors</b>	Indicates the total number of valid-size packets that were received with proper framing but discarded because of cyclic redundancy check (CRC) errors.
<b>Frame Errors</b>	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)*

<b>Field</b>	<b>Description</b>
<b>Undersized Packets</b>	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).
<b>Oversized Packets</b>	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).
<b>Collisions</b>	Indicates the total number of collisions detected on this port.
<b>Single Collisions</b>	Indicates the total number of packets that were transmitted successfully on this port after a single collision.
<b>Multiple Collisions</b>	Indicates the total number of packets that were transmitted successfully on this port after more than one collision.
<b>Excessive Collisions</b>	Indicates the total number of packets lost on this port due to excessive collisions.
<b>Packets 64 bytes</b>	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.
<b>65-127 bytes</b>	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.
<b>128-255 bytes</b>	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.
<b>256-511 bytes</b>	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.
<b>512-1023 bytes</b>	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.
<b>1024-1518 bytes</b>	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)*

---

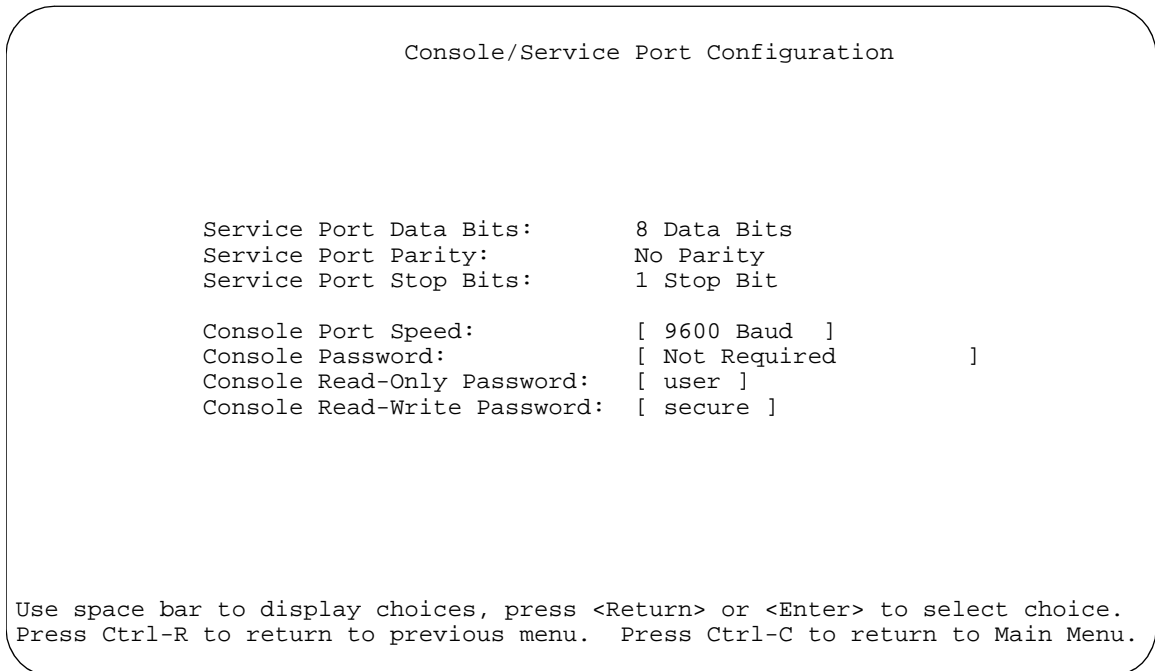
<b>Field</b>	<b>Description</b>
<b>Filtered Packets</b>	Indicates the number of packets filtered (not forwarded) by this port.
<b>Flooded Packets</b>	Indicates the total number of packets flooded (forwarded) through this port because the destination address was not in the address database.
<b>Deferred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

---

## Console/Service Port Configuration

The Console/Service Port Configuration screen ([Figure 3-26](#)) allows you to configure and modify the console/service port parameters.

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



**Figure 3-26. Console/Service Port Configuration screen**


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

**Table 3-22. Console/Service Port Configuration screen fields**

Field	Description
<b>Service Port Data Bits</b>	A read-only field that indicates the current service port data bit setting.
<b>Service Port Parity</b>	A read-only field that indicates the current service port parity setting.


*(continued)*

**Table 3-22. Console/Service Port Configuration screen fields** *(continued)*

Field	Description
<b>Service Port Stop Bits</b>	A read-only field that indicates the current service port stop bit setting.
<b>Console Port Speed</b>	Allows you to set the console/service port baud rate to match the baud rate of the console terminal.
	 <b>Caution:</b> 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/service port setting.
	Default            9600 Baud Range             2400 Baud, 4800 Baud, 9600 Baud, 19200 Baud, 38400 Baud
<b>Console Password</b>	Enables password protection for accessing the CI through a TELNET session, a console terminal, or both. The value you choose for this field also impacts your network security password/user access settings (see <a href="#">“Setting Security Passwords</a> on <a href="#">page 3-60</a> ).  If you set this field to Required, you can use the Logout command 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            Not Required Range             Not Required, Required for TELNET, Required for Console, Required for Both
<b>Console Read-Only Password</b>	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), but cannot change any parameters or use the Reset command or Reset to Default command.
	Default            user Range             An ASCII string of up to 15 printable characters
<b>Console Read-Write Password</b>	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), 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/Service Port Configuration screen fields** *(continued)*

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

## Setting Security Passwords

Setting security passwords for your switch requires setting the appropriate parameter values in two screens:

- Console Service Port Configuration screen ([page 3-58](#))
- Radius Network Security screen ([page 3-77](#))

This section provides a matrix you can use to determine the proper values to enter according to your security requirements. To use the matrix, do the following:

1. Determine your console security requirements ([Table 3-23](#)).

**Table 3-23. Determining Console Security Requirements**

Security requirement:	Choose one of the following values <sup>1</sup> :		
Console	None (CN)	Local (CL)	RADIUS (CR)

<sup>1</sup> C = Console, L = Local, N = None, R = RADIUS.

2. Determine your TELNET sessions security requirements ([Table 3-24](#)).

**Table 3-24. Determining TELNET Sessions Security Requirements**

Security requirement:	Choose one of the following values <sup>1</sup> :		
TELNET	None (TN)	Local (TL)	RADIUS (TR)

<sup>1</sup> L = Local, N = None, R = RADIUS, T = TELNET.



3. Apply the values to [Table 3-25](#).
  - a. Consider the values you choose from [Tables 3-23](#) and [3-24](#) as a set (for example, CL and TL).
  - b. Find your value set in the matrix ([Table 3-25](#)).
  - c. Set the field value (shown shaded to the left of the set) in the Console/Service Port Configuration screen.
  - d. Set the field value (shown shaded above the set) in the RADIUS Network Security screen.

**Table 3-25. Determining the Screen Values<sup>1</sup>**

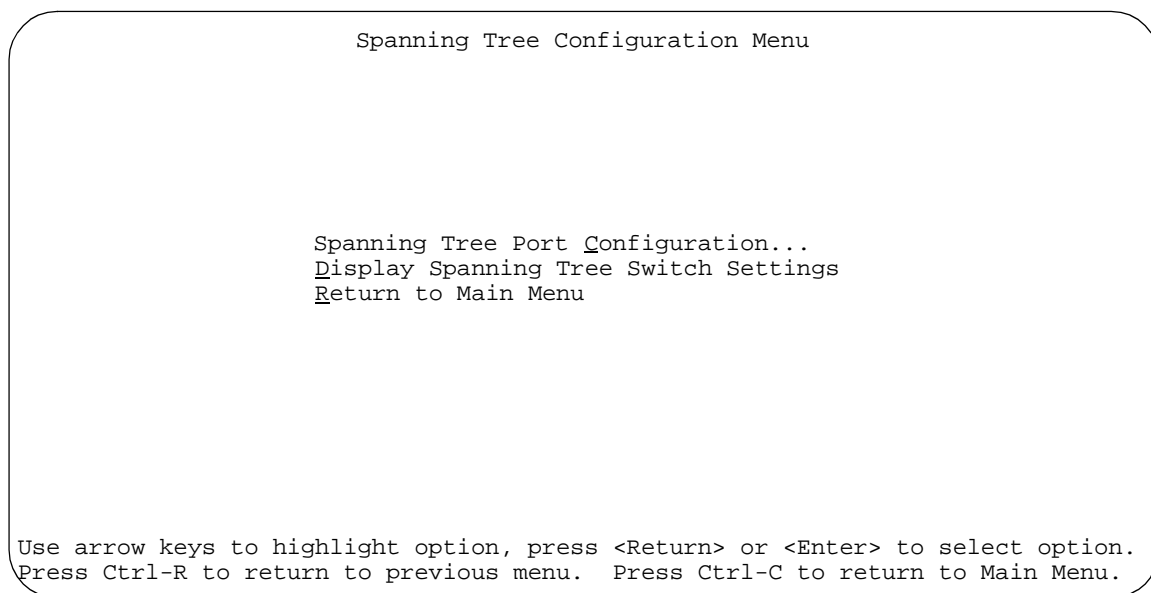
		Radius Network Security screen (Password/User Access) values			
Console/Service Port Configuration screen (Console Password) values	Local Password	RADIUS TELNET	RADIUS Console	RADIUS Both	
Not Required	CN and TN	-	-	-	
Required for TELNET	TL and CN	TR and CN			
Required for Console	CL and TN	-	CR and TN	-	
Required for Both	CL and TL	CL and TR	CR and TL	CR and TR	

<sup>1</sup> C = Console, L = Local, N = None, R = RADIUS, T = TELNET.

## Spanning Tree Configuration

The Spanning Tree Configuration Menu screen ([Figure 3-27](#)) 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 3-27. Spanning Tree Configuration Menu screen**

[Table 3-26](#) describes the Spanning Tree Configuration Menu options.

**Table 3-26. Spanning Tree Configuration Menu Options**

Option	Description
<b>Spanning Tree Port Configuration...</b>	Displays the Spanning Tree Port Configuration screen (see <a href="#">“Spanning Tree Port Configuration”</a> on <a href="#">page 3-63</a> ).
<b>Display Spanning Tree Switch Settings</b>	Displays the Spanning Tree Switch Settings screen (see <a href="#">“Display Spanning Tree Switch Settings”</a> on <a href="#">page 3-65</a> ).
<b>Return to Main Menu</b>	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 STA.

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

[Figure 3-28](#) shows sample port configurations for the 350T 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		[ Normal Learning ]	128	10	Forwarding
7		[ Normal Learning ]	128	10	Forwarding
8		[ Normal Learning ]	128	10	Forwarding
9		[ Normal Learning ]	128	10	Forwarding
10		[ Normal Learning ]	128	10	Forwarding
11		[ Normal Learning ]	128	10	Forwarding
12		[ Normal Learning ]	128	10	Forwarding
13		[ Normal Learning ]	128	10	Forwarding
14		[ Normal Learning ]	128	10	Forwarding
15		[ Normal Learning ]	128	10	Forwarding
16		[ Normal Learning ]	128	10	Forwarding
All		[ Normal Learning ]			

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. Model 350T Spanning Tree Port Configuration screen**

[Table 3-27](#) describes the Spanning Tree Port Configuration screen fields.

**Table 3-27. Spanning Tree Port Configuration screen fields**

Field	Description
<b>Port</b>	Indicates the switch port numbers, from 1 to 16, 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 16 switch ports.
<b>Trunk</b>	The read-only data displayed in this column indicates the trunks (if configured) that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen (see " <a href="#">MultiLink Trunk Configuration</a> " on <a href="#">page 3-39</a> ).
<b>Participation</b>	<p>Allows you to enable or disable any (or all) of the switch ports for Spanning tree participation. When an individual port is a trunk member (see Trunk field), changing this setting for one of the trunk members changes the setting for all members of that trunk. You should consider how this can change your network topology before you change this setting (see "MultiLink Trunking Configuration Rules" on page 1-41). The Fast Learning value is the same as Normal Learning except that the port state transition timer is shortened to two seconds.</p> <p>Default                      Normal Learning</p> <p>Range                         Normal Learning, Fast Learning, Disabled</p>
<b>Priority</b>	<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                      128</p> <p>Range                         0 to 255</p>
<b>Path Cost</b>	<p>This read-only field is a bridge spanning tree parameter that determines the lowest path cost to the root.</p> <p>Default                      10 or 100</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>
<b>State</b>	<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                      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 350 switch.

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

```
Spanning Tree Switch Settings

Bridge Priority:           8000
Designated Root:         80000000A2EFD380
Root Port:                0
Root Path Cost:          0
Hello Time:               2 seconds
Maximum Age Time:        20 seconds
Forward Delay:           15 seconds
Bridge Hello Time:       2 seconds
Bridge Maximum Age Time: 20 seconds
Bridge Forward Delay:    15 seconds

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

**Figure 3-29.** Spanning Tree Switch Settings screen

[Table 3-28](#) describes the Spanning Tree Switch Settings parameters.

**Table 3-28. Spanning Tree Switch Settings parameters**

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

*(continued)*

**Table 3-28. Spanning Tree Switch Settings parameters** *(continued)*

Parameter	Description
<b>Forward Delay</b>	<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            15 seconds</p> <p>Range              4 to 30 seconds</p>
<b>Bridge Hello Time</b>	<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            2 seconds</p> <p>Range              1 to 10 seconds</p>
<b>Bridge Maximum Age Time</b>	<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            20 seconds</p> <p>Range              6 to 40 seconds</p>
<b>Bridge Forward Delay</b>	<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            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 350 switch as if the console terminal were directly connected to it. You can have up to four active TELNET sessions at one time.

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

```

                                TELNET Configuration

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

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

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

**Figure 3-30.** TELNET Configuration screen

[Table 3-29](#) describes the TELNET Configuration screen fields.



**Table 3-29. TELNET Configuration screen fields**

Field	Description
<b>TELNET Access</b>	Allows a user remote access to the CI through a TELNET session. Default            Enabled Range             Enabled, Disabled
<b>Login Timeout</b>	Specifies the amount of time a user has to enter the correct password at the console-terminal prompt. Default            1 minute Range             0 to 10 minutes (0 indicates "no timeout")
<b>Login Retries</b>	Specifies the number of times a user can enter an incorrect password at the console-terminal prompt before terminating the session. Default            3 Range             1 to 100
<b>Inactivity Timeout</b>	Specifies the amount of time the session can be inactive before it is terminated. Default            15 minutes Range             0 to 60 minutes (0 indicates "no timeout")
<b>Event Logging</b>	Specifies the types of events that will be displayed in the Event Log screen (see " <a href="#">Display Event Log</a> " on <a href="#">page 3-79</a> ). Default            All Range             All, None, Accesses, Failures Description:     All: Logs the following TELNET events to the Event Log screen: <ul style="list-style-type: none"> <li>• TELNET connect: Indicates the IP address and access mode of a TELNET session.</li> <li>• TELNET disconnect: Indicates the IP address of the remote host and the access mode, due to either a logout or inactivity.</li> <li>• 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.</li> </ul> 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 3-29. TELNET Configuration screen fields** *(continued)*

---

<b>Field</b>	<b>Description</b>
<b>Allowed Source IP Address</b>	Specifies up to 10 user-assigned host IP addresses that are allowed TELNET and SNMP access to the switch.
	Default            0.0.0.0 (no IP address assigned)
	Range              Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
<b>Allowed Source Mask</b>	Specifies up to 10 user-assigned allowed source address masks. The remote IP address is masked with the source mask and, if the resulting value equals the source IP address, the connection is allowed.
	Default            0.0.0.0 (no IP mask assigned)
	Range              Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point

---

## Software Download

The Software Download screen ([Figure 3-31](#)) allows you to revise the BayStack 350 switch software image that is located in nonvolatile flash memory. To download the BayStack 350 switch software image, a properly configured Trivial File Transfer Protocol (TFTP) server must be present in your network, and the switch must have an IP address. (See “IP Configuration” on [page 3-10](#) to learn how to configure the switch’s IP address.)

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

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



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

```
Software Download

Image Filename:          [ b350_300.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 3-30](#) describes the Software Download screen fields.

**Table 3-30. Software Download screen fields**

Field	Description				
<b>Image Filename</b>	The software image load file name.				
	<table> <tr> <td>Default</td> <td>Zero-length string</td> </tr> <tr> <td>Range</td> <td>An ASCII string of up to 30 printable characters</td> </tr> </table>	Default	Zero-length string	Range	An ASCII string of up to 30 printable characters
Default	Zero-length string				
Range	An ASCII string of up to 30 printable characters				
<b>TFTP Server IP Address</b>	The IP address of your TFTP load host.				
	<table> <tr> <td>Default</td> <td>0.0.0.0 (no IP address assigned)</td> </tr> <tr> <td>Range</td> <td>Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point</td> </tr> </table>	Default	0.0.0.0 (no IP address assigned)	Range	Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
Default	0.0.0.0 (no IP address assigned)				
Range	Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point				
<b>Start TFTP Load of New Image</b>	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.				
	<b>Note:</b> 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.				
	<table> <tr> <td>Default</td> <td>No</td> </tr> <tr> <td>Range</td> <td>Yes, No</td> </tr> </table>	Default	No	Range	Yes, No
Default	No				
Range	Yes, No				

### LED Indications During the Download Process

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

During the download process, the BayStack 350 switch is not operational. You can monitor the progress of the download process by observing the LED indications.

[Table 3-31](#) describes the LED indications displayed by the Model 350T during the software download process. Other BayStack 350 Series models show similar indications, but the indications correspond to the port numbers for the specific model.

**Table 3-31. 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 11 to 16 only): The LEDs (green) begin to turn on from right to left, beginning with port 16. The LED pattern indicates the progress of the download process. When LEDs 11 to 16 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 9 only): The LEDs (yellow) 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 9 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 (green) 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. After LEDs 1 to 8 are all on, LEDs 9 to 16 turn on, indicating that the new software image has been programmed successfully into the switch's flash memory.
4	The switch is reset automatically.	The reset can take up to 20 seconds to complete. 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.

## Configuration File

The Configuration File Download/Upload screen ([Figure 3-32](#)) allows you to store your switch configuration parameters on a TFTP server. You can retrieve the configuration parameters and use the retrieved parameters to automatically configure a replacement switch or a group of switches if required.

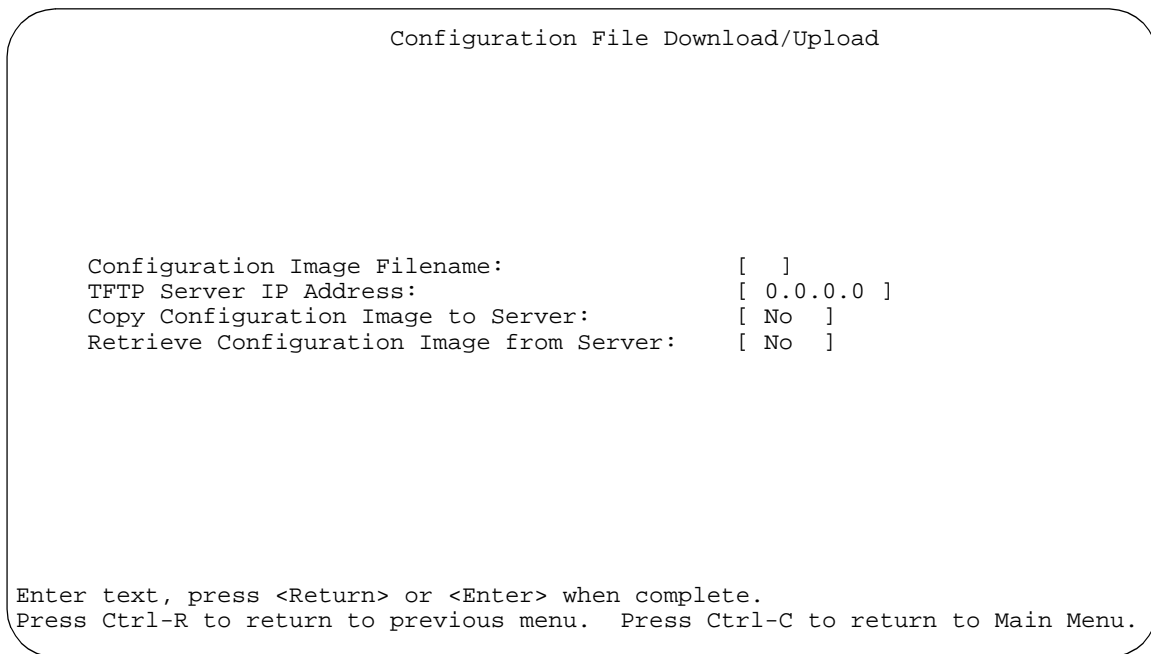


**Note:** A configuration file obtained from a donor BayStack 350 switch can only be used to properly configure other BayStack 350 switches that have the same firmware revision and model type as the donor switch.

---

You must set up the file on your TFTP server and set the filename read/write permission to enabled before you can save the configuration parameters. Although most configuration parameters are saved to the configuration file, certain parameters are not saved (see [Table 3-33](#) on [page 3-76](#)).

Choose Configuration File (or press g) from the main menu to open the Configuration File Download/Upload screen.



**Figure 3-32. Configuration File Download/Upload Screen**

[Table 3-32](#) describes the Configuration File Download/Upload screen fields.

**Table 3-32. Configuration File Download/Upload Screen Fields**

Field	Description
<b>Configuration Image Filename</b>	<p>The file name you have chosen for the configuration file. Choose a meaningful file name that will allow you to identify the file for retrieval when required. The file must already exist on your TFTP server and must be read/write enabled.</p> <p>Default            Zero-length string</p> <p>Range             An ASCII string of up to 30 printable characters</p>
<b>TFTP Server IP Address</b>	<p>The IP address of your TFTP load host.</p> <p>Default            0.0.0.0 (no IP address assigned)</p> <p>Range             Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point</p>
<b>Copy Configuration Image to Server</b>	<p>Specifies whether to copy the presently configured switch parameters to the specified TFTP server (default is No). Use the spacebar to toggle the selection to Yes.</p> <p>Press [Enter] to initiate the process.</p> <p>Default            No</p> <p>Range             Yes, No</p>
<b>Retrieve Configuration Image from Server</b>	<p>Specifies whether to retrieve the stored switch configuration parameters from the specified TFTP server (default is No). If you choose Yes, the download process begins immediately and, when completed, causes the switch to reset with the new configuration parameters.</p> <p>Use the spacebar to toggle the selection to Yes. Press [Enter] to initiate the process.</p> <p>Default            No</p> <p>Range             Yes, No</p>

[Table 3-33](#) lists the parameters that are Not saved to the Configuration File.

**Table 3-33. Parameters Not Saved to the Configuration File**

<b>These parameters are not saved:</b>	<b>Used in this screen:</b>	<b>See page:</b>
In-Band Switch IP Address	IP Configuration/Setup	<a href="#">3-10</a>
In-Band Subnet Mask		
Default Gateway		
MAC Address	System Characteristics	<a href="#">3-20</a>
Reset Count		
Last Reset Type		
Console Read-Only Switch Password	Console/Comm Port Configuration	<a href="#">3-58</a>
Console Read-Write Switch Password		
Last Event Log Entry Number	Event Log	<a href="#">3-79</a>
TFTP Server IP Address	Configuration File Download/Upload	<a href="#">3-74</a>



## Network Security

The RADIUS Network Security screen ([Figure 3-33](#)) allows you to set up or modify the Radius server. You can configure a primary RADIUS server and also add a secondary RADIUS server to provide redundant security in case the Primary server is out of commission.

You can Enable or Disable RADIUS authentication to your Console or any TELNET session using this screen.

Choose Network Security (or press k) from the main menu to open the RADIUS Network Security screen.

```

                                RADIUS Network Security

Primary RADIUS Server:  [ 0.0.0.0 ]
Secondary RADIUS Server: [ 0.0.0.0 ]
RADIUS UDP Port:       [ 0 ]
Shared Secret:         [ ]
Password/User Access:  [ Local password ]

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

**Figure 3-33. Radius Network Security Screen**

[Table 3-34](#) describes the RADIUS Network Security screen fields.

**Table 3-34. RADIUS Network Security Screen Fields**

---

<b>Field</b>	<b>Description</b>
<b>Primary RADIUS Server</b>	The IP address of the Primary RADIUS server. Default            0.0.0.0 (no IP address assigned) Range             Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
<b>Secondary RADIUS Server</b>	The IP address of the Secondary RADIUS server. Default            0.0.0.0 (no IP address assigned) Range             Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
<b>RADIUS Server UDP Port</b>	The user datagram protocol (UDP) port for the RADIUS server. Default            1645 Range             0 to 65536
<b>Shared Secret</b>	Your special switch security code that provides authentication to the RADIUS server. Default            Null string (which will not authenticate) Range             Any contiguous ASCII string that contains at least 1 printable character, up to a maximum of 35.
<b>Password/User Access</b>	The RADIUS authentication password which can be Enabled or Disabled for Console and TELNET. The value you choose for this field must be set in conjunction with the console password field value (see <a href="#">“Setting Security Passwords”</a> on <a href="#">page 3-60</a> ) Default            Local password Range             Local password, Radius TELNET, RADIUS Console, RADIUS both.

---

## Display Event Log

The Event Log screen ([Figure 3-34](#)) 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 3-68](#).)
- **Operational exception:** Indicates that the microprocessor has received an exception at the specified vector number.

Choose Display Event Log from the main menu to open the Event Log screen.



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

```
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 350T HW:RevC FW:V1.00 SW:V1.00.

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 3-34.** Event Log screen

## 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 3-35](#) 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 3-35. 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 3-36](#) shows an example of the event log entry for this type of event.

```
Entry Number: 3          sysUpTime: 00:38:53          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 3-36. Sample event log event exceeding the write threshold**

The write threshold is reset when either of the following occurs:

- The BayStack 350 switch is reset.
- The firmware determines that compression is required for maintenance of the event log's flash memory.

## Reset

The Reset command (accessed from the main menu) allows you to reset the BayStack 350 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 in the Self-Test screen ([Figure 3-37](#)), which is followed by the CI screens.

```
BayStack Model 350T Self-Test

          ASIC addressing test           ... Pass
          ASIC buffer RAM test          ... Pass
          Physical layer test            ... Pass
          Port internal loopback test    ... Pass

Self-test complete.
```

**Figure 3-37. Self-Test screen after resetting the switch**



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

## Reset to Default Settings

The Reset to Default Settings command (accessed from the main menu) allows you to reset the BayStack 350 switch and replace all configured switch parameters with the factory default settings. For a list of the factory default settings, see Appendix D, “Default Settings.”



**Caution:** If you choose this command, all of your configured settings will be replaced with factory default settings when you press [Enter].

---

The Reset to Default Settings command 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 in the Self-Test screen ([Figure 3-38](#)), which is followed by the CI screens.

```
BayStack Model 350T Self-Test
      ASIC addressing test      ... Pass
      ASIC buffer RAM test     ... Pass
      Physical layer test      ... Pass
      Port internal loopback test ... Pass
Self-test complete.
```

**Figure 3-38.** Self-Test screen after resetting the switch to factory default settings



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

---

## Logout

The Logout command (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 command works as follows:

- If you are accessing the BayStack 350 switch through a TELNET session, the Logout command terminates the TELNET session.
- If you are accessing the BayStack 350 switch through a password-protected console terminal (connected to the console/service port on the switch), the Logout command displays the console-terminal password prompt ([Figure 3-39](#)). You must enter the correct password to access the CI.

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

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

```
Enter Password:
```

**Figure 3-39. Password prompt screen**

You can specify whether a password is required for the TELNET session or the console terminal using the Console/Service Port Configuration screen (see [“Console/Service Port Configuration”](#) on [page 3-58](#)).

If the console terminal is not password protected, the system ignores the Logout command.





---

# Chapter 4

## Troubleshooting

This chapter explains how to isolate and diagnose problems with the BayStack 350 switch.



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

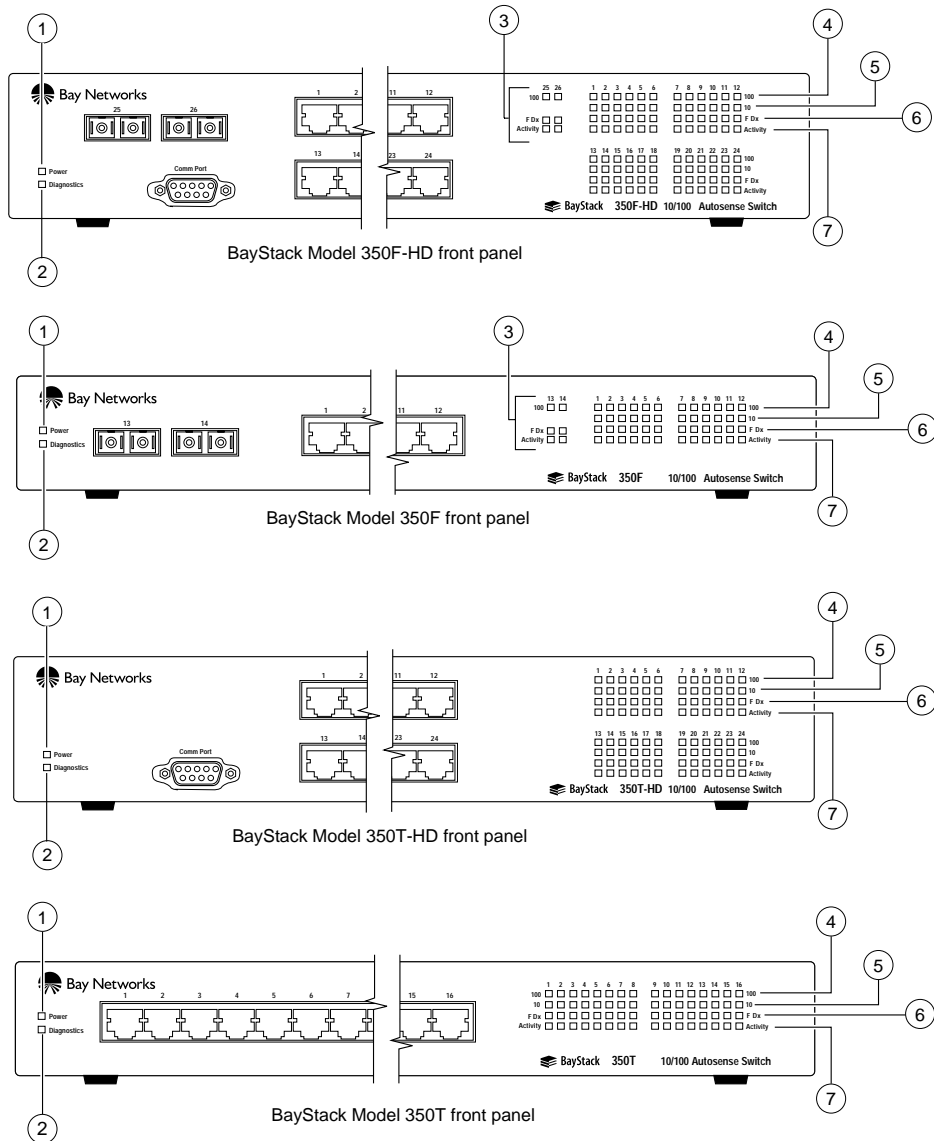
---

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

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

The BayStack 350 switch LEDs are located on the front panel ([Figure 4-1](#)).



7832FA

**Figure 4-1. LED locations**

[Table 4-1](#) describes the BayStack 350 switch LEDs, as numbered in [Figure 4-1](#).

**Table 4-1. LED indications**

Item	Icon/Label	Description
1	Power	Power LED (green): On: DC power is available to the switch's internal circuitry.
2	Diagnostics	Diagnostics LED (green): On: The switch passed the self-test. Blinking: A nonfatal error occurred during the self-test. Off: The switch failed the self-test.
3	(port numbers)	100BASE-FX LED matrix.
4	100	100BASE-FX/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.
5	10 <sup>1</sup>	10BASE-T port status LEDs (yellow): 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.
6	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.
7	Activity	Port activity LEDs (green): Blinking: Indicates the network activity level for the corresponding port. A high level of network activity can cause the LEDs to appear to be on continuously.

<sup>1</sup> Not available on the fiber optic 100BASE-FX LED matrix.

## Diagnosing and Correcting the Problem

Before you perform the problem-solving steps in this section, cycle the power to the BayStack 350 switch (disconnect and then reconnect the AC power cord); then, verify that the switch follows the normal power-up sequence.

### Normal Power-Up Sequence

In a normal power-up sequence, the LEDs display as follows:

1. After power is applied to the switch, the 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 Diagnostics 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.	See <a href="#">"Port Connection Problems"</a> on <a href="#">page 4-5</a> .
	The switch's link partner is not autonegotiating properly.	



**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.

*(continued)*

**Table 4-2. Corrective actions (continued)**

Symptom	Probable cause	Corrective action
The Diagnostics 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 Diagnostics LED is blinking.	A nonfatal error occurred during the self-test.	Cycle the power to the switch (disconnect and then reconnect the AC power cord).  If the problem persists, contact the Nortel Networks Technical Solutions Center.

## Port Connection Problems

Port connection problems can usually be traced to a poor cable connection or an improper connection of the port cables at either end of the link. These types of problems can be remedied by making sure that the cable connections are secure and that the cables are connected to the correct ports at both ends of the link.

Port connection problems can also be traced to the autonegotiation mode or the port interface.

## Autonegotiation Modes

Port connection problems can occur when a port (or station) is connected to another port (or station) that is not operating in a compatible mode (for example, connecting a full-duplex port on one station to a half-duplex port on another station).

The BayStack 350 switch negotiates port speeds according to the IEEE 802.3u autonegotiating standard. The switch adjusts (autonegotiates) its port speed and duplex mode to match the best service provided by the connected station, up to 100 Mb/s in full-duplex mode.

- If the connected station uses a form of autonegotiation that is not compatible with the IEEE 802.3u autonegotiating standard, the BayStack 350 switch cannot negotiate a compatible mode for correct operation.
- If the autonegotiation feature is not present or is not enabled at the connected station, the BayStack 350 switch may not be able to determine the correct duplex mode.

In both situations, the BayStack 350 switch “autosenses” the speed of the connected station and, by default, reverts to half-duplex mode. If the connected station is operating in full-duplex mode, it cannot communicate with the switch.

To correct this mode mismatch problem, follow these steps:

1. **Use the Port Configuration screen to disable autonegotiation for the suspect port (see “Port Configuration” on page 3-36).**
2. **Manually set the Speed/Duplex field to match the speed/duplex mode of the connected station (see Table 3-13 on page 3-37).**

You may have to try several settings before you find the correct speed/duplex mode of the connected station.

If the problem persists, follow these additional steps:

1. **Disable the autonegotiation feature at the connected station.**
2. **Manually set the speed/duplex mode of the connected station to the same speed/duplex mode you have manually set for the BayStack 350 switch port.**



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

- Nortel Networks 28000 product family
  - Nortel Networks 58000 product family
  - BayStack Model 302T switch (100 Mb/s port)
- 

## Port Interface

Ensure that the devices are connected using the appropriate crossover or straight-through cable (see Appendix C, “Connectors and Pin Assignments”).

---

# Appendix A

## Technical Specifications

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

### Environmental

Temperature:	Operating:	0° to 40°C (32° to 104°F)
	Storage:	-25° to 70°C (-13° to 158°F)
Humidity:	Operating:	85% maximum relative humidity, noncondensing
	Storage:	95% maximum relative humidity, noncondensing
Altitude:	Operating:	3024 m (10,000 ft)
	Storage:	3024 m (10,000 ft)

### Electrical

Input Voltage:	90 to 250 VAC @ 47 to 63 Hz
Power Consumption:	100 W maximum

## Physical Dimensions

Dimension	Model 350T/350F	Model 350T-HD/350F-HD
Height	4.37 cm (1.72 in.)	6.35 cm (2.50 in.)
Width	44.58 cm (17.55 in.)	44.07 cm (17.35 in.)
Depth	30.48 cm (12.0 in.)	32.39 cm (12.75 in.)
Weight	4.31 kg (9.50 lb)	5.26 kg (11.60 lb)

## Performance Specifications

Frame Forward Rate (64-byte packets):	1.6 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:	8,000 entries
Addressing:	48-bit MAC address
Frame Length:	64 to 1518 bytes

## 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)

## 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
- Models 350F-HD and 350F have 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

- FCC Part 15, Subpart B, Class A
- EN55022 (CISPR 22: 1985), Class A
- VCCI Class 1 ITE
- Australian AS 3548

## Electromagnetic Susceptibility

EN50082-1

## **Declaration of Conformity**

The Declaration of Conformity for the BayStack 350 switches complies with ISO/IEC Guide 22 and EN45014. The declaration identifies the product models, the Nortel Networks name and address, and the specifications recognized by the European community.

As stated in the Declaration of Conformity, the BayStack 350 switches comply with the provisions of Council Directives 89/336/EEC and 73/23/EEC.

---

# Appendix B

## Server/Trunk Connections

### Optimal Server/Trunk Connections

When you connect MultiLink Trunks to servers that use a single MAC address, configure the trunk members using the port groups shown in [Table B-1](#) for optimal throughput:

**Table B-1. Optimal server/trunk connections**

To connect this Model...	to a 2-port server, group these ports:	to a 3-port server, group these ports:	to a 4-port server, group these ports:
BayStack 350T	(3 and 6) or (4 and 5) or (7 and 9) or (10 and 16)	(3, 6, and 11) or (4, 5, and 12) or (7, 9, and 15) or (8, 10, and 16)	(3, 6, 1, and 14) or (4, 5, 12, and 13) or (1, 7, 9, and 15) or (2, 8, 10, and 16)
BayStack 350F	(4 and 5) or (6 and 7) or (8 and 9) or (12 and 14)	(4, 5, and 12) or (6, 7, and 13) or (8, 9, and 13) or (10, 12, and 14)	Not supported for this model.
BayStack 350F-HD	(4 and 5) or (6 and 7) or (8 and 9) or (20 and 21)	(4, 5, and 12) or (6, 7, and 9) or (8, 9, and 13) or (13, 20, and 21)	(4, 5, 12, and 16) or (6, 7, 9, and 17) or (8, 9, 13, and 19) or (12, 13, 20, and 21)
BayStack 350T-HD	(4 and 5) or (6 and 7) or (8 and 9) or (20 and 21)	(4, 5, and 12) or (6, 7, and 9) or (8, 9, and 13) or (13, 20, and 21)	(4, 5, 12, and 17) or (6, 7, 9, and 17) or (8, 9, 13, and 19) or (12, 13, 20, and 21)

For more information about server/trunk connections, see “Server Trunk Configuration” on page 1-26.



---

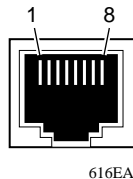
# Appendix C

## Connectors and Pin Assignments

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

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

The RJ-45 port connectors ([Figure C-1](#)) are wired as MDI-X ports to connect end stations without using crossover cables. (See [“MDI and MDI-X Devices”](#) on [page C-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 C-1.** RJ-45 (8-pin modular) port connector

[Table C-1](#) lists the RJ-45 (8-pin modular) port connector pin assignments.

**Table C-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.

In order for two devices to communicate, the transmitter of one device must connect to the receiver of the other device. The connection is established through a crossover function, which can be a crossover cable or a port that implements the crossover function internally.

Ports that implement the crossover function internally are known as MDI-X ports, where X refers to the crossover function.



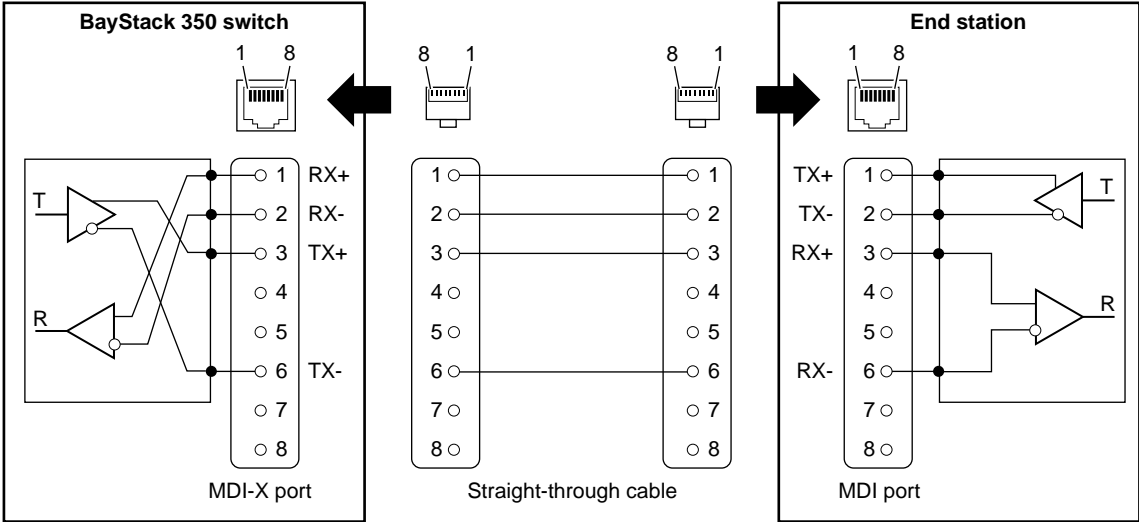
**Note:** For the transmitter of one device to connect to the receiver of another device, the total number of crossovers must always be an odd number.

---

The following sections describe the use of straight-through and crossover cables for connecting MDI and MDI-X devices.

# MDI-X to MDI Cable Connections

BayStack 350 switches use MDI-X ports that allow you to connect directly to end stations without using crossover cables ([Figure C-2](#)).

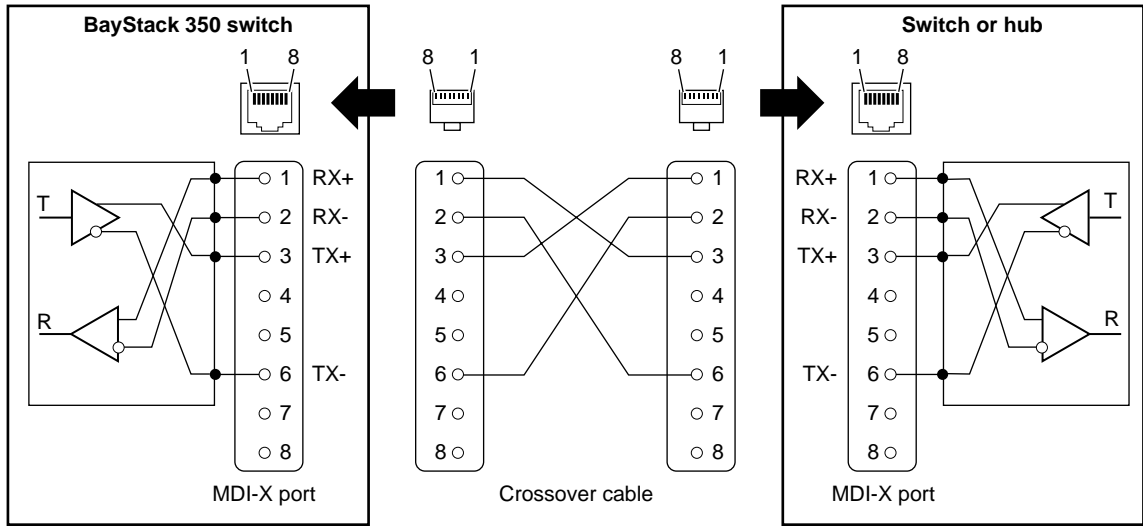


617EA

Figure C-2. MDI-X to MDI cable connections

## MDI-X to MDI-X Cable Connections

If you are connecting the BayStack 350 switch to a device that also implements MDI-X ports, use a crossover cable ([Figure C-3](#)).



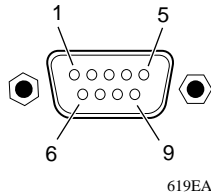
618EA

**Figure C-3. MDI-X to MDI-X cable connections**



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

The DB-9 console/service port connector ([Figure C-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 C-4.** DB-9 console/service port connector

[Table C-2](#) lists the DB-9 console/service port connector pin assignments.

**Table C-2.** DB-9 console/service 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

## 100BASE-FX Fiber Optic Port Connectors

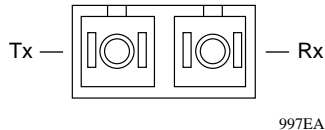
The Models 350F-HD and 350F have 100BASE-FX SC connectors for supporting switched 100 Mb/s (100BASE-FX) connections over 50/125 and 62.5/125 micron multimode fiber optic cable.



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

---

[Figure C-5](#) shows a 100BASE-FX multimode fiber optic port connector and its pin assignments.



**Figure C-5. 100BASE-FX multimode fiber optic port connector**

---

# Appendix D

## Default Settings

[Table D-1](#) lists the factory default settings for the BayStack 350 switch.

**Table D-1. Factory default settings for the BayStack 350 switch**

Field	Default setting	Appears in this CLI screen
BootP Request Mode	BootP When Needed	IP Configuration
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 Community Strings and Trap Addresses
Read-Write Community String	private	
Trap IP Address	0.0.0.0 (no IP address assigned)	
Community String	Zero-length string	
Authentication Trap	Enabled	
AutoTopology MIB	Enabled	
Link Up/Down Trap Status	Enabled	SNMP Port Link Up/Down Trap Options
sysContact	Zero-length string	System Characteristics
sysName	Zero-length string	
sysLocation	Zero-length string	

*(continued)*

**Table D-1. Factory default settings for the BayStack 350 switch (continued)**

<b>Field</b>	<b>Default setting</b>	<b>Appears in this CI screen</b>
Aging Time	300 seconds	MAC Address Table
Find an Address	00-00-00-00-00-00 (no MAC address assigned)	
V1 to V8	All ports configured in VLAN V1	VLAN Configuration
Status	Enabled for all ports	Port Configuration
Autonegotiation	Enabled for all ports	
Speed/Duplex	100Mbps/Half (when Autonegotiation is Disabled)	
Trunk Members	blank field	Trunk Configuration
STP	Enabled	
Trunk Mode	Basic	
Trunk Status	Disabled	
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	
Port	1	Port Statistics
Console Port Speed	9600 Baud	Console/Service Port Configuration
Console Password	Not Required	
Console Read-Only Password	user	
Console Read-Write Password	secure	

*(continued)*

**Table D-1. Factory default settings for the BayStack 350 switch (continued)**

Field	Default setting	Appears in this CI screen
Participation	Enabled	Spanning Tree Port Configuration
Priority	128	
Path Cost	10 or 100	
Bridge Priority	8000	Spanning Tree Switch Settings
Designated Root	8000 (bridge_id)	
Root Port	0	
Root Path Cost	0	
Hello Time	2 seconds	
Maximum Age Time	20 seconds	
Forward Delay	15 seconds	
Bridge Hello Time	2 seconds	
Bridge Maximum Age Time	20 seconds	
Bridge Forward Delay	15 seconds	
TELNET Access	Enabled	TELNET Configuration
Login Timeout	1 minute	
Login Retries	3	
Inactivity Timeout	15 minutes	
Event Logging	All	
Allowed Source IP Address (10 user-configurable fields)	First field: 0.0.0.0 (no IP address assigned)  Remaining nine fields: 255.255.255.255 (any address is allowed)	
Allowed Source Mask (10 user-configurable fields)	First field: 0.0.0.0 (no IP address assigned)  Remaining nine fields: 255.255.255.255 (any address is allowed)	
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	

\* You cannot modify this field for the Model 350F-HD and Model 350F 100BASE-FX fiber optic ports.



---

# Appendix E

## Sample BootP Configuration File

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

A sample BootP configuration file follows:

```
# The following is a sample of a BootP configuration file that was extracted
# from a Bay Networks EZ LAN network management application. Note that other
# BootP daemons can use a configuration file with a different format.
#
# Before using your switch BootP facility, you must customize your BootP
# configuration file with the appropriate data.
#
# Blank lines and lines beginning with '#' are ignored.
#
# Legend:
#
#     first field -- hostname
#             ht -- hardware type
#             ha -- host hardware address
#             tc -- template host (points to similar host entry)
#             ip -- host IP address
#             hd -- bootfile home directory
#             bf -- bootfile
# EZ         dt -- device type
# EZ         fv -- firmware version
# EZ         av -- agent version
#
# Fields are separated with a pipe (|) symbol. Forward slashes (/) are
# required to indicate that an entry is continued to the next line.
#
```

```
# Caution
#
#   Omitting a Forward slash (/) when the entry is continued to the next
#   line, can cause the interruption of the booting process or the
#   incorrect image file to download. Always include forward slashes
#   where needed.
#
# Important Note:
#
#   If a leading zero (0) is used in the IP address it is calculated as an
#   octal number. If the leading character is "x" (upper or lower case),
#   it is calculated as a hexadecimal number. For example, if an IP address
#   with a base 10 number of 45 is written as .045 in the BOOTPTAB.TXT file,
#   the Bootp protocol assigns .037 to the client.
#
# Global entries are defined that specify the parameters used by every device.
# Note that hardware type (ht) is specified first in the global entry.
#
# The following global entry is defined for an Ethernet device. Note that this
# is where a client's subnet mask (sm) and default gateway (gw) are defined.
#
global1|/
    |ht=ethernet|/
    |hd=c:\opt\images|/
    |sm=255.255.255.0|/
    |gw=192.0.1.0|
#
# The following sample entry describes a BootP client:

bay1|ht=ethernet|ha=0060fd000000|ip=192.0.0.1|hd=c:\ezlan\images|bf=b350_100.img

# Where:
#   host name:                bay1
#   hardware type:           Ethernet
#   MAC address:             00-60-FD-00-00-00
#   IP address:              192.0.0.1
#   home directory of boot file: c:\ezlan\images
#   boot file:               b350_100.img
```



## A

- acronyms, xxii
- Activity LEDs, 1-3
- Actual Hello Interval, 3-66
- Aging Time field, 3-25
- Allowed Source IP Address field, 3-70
- Allowed Source Mask field, 3-70
- Authentication Trap field, 3-17
- Autonegotiation
  - field, 3-38
- autonegotiation
  - description, 1-10
- autonegotiation modes
  - description, 1-6
  - troubleshooting, 4-5
- Autosensing, 1-9

## B

- bandwidth, mixing, 1-14
- BayStack 350 switch
  - components, 1-2, 1-4
  - connectors, C-1
  - features, 1-5 to 1-7
- BootP Request Mode field, 3-11
- BootP. *See* Bootstrap Protocol
- Bootstrap Protocol (BootP)
  - Always setting, 3-12
  - automatic IP configuration, 1-12
  - BOOTPTAB.TXT file, E-1
  - choosing a request mode, 3-12
  - Disabled setting, 3-13
  - Last Address setting, 3-13
  - sample configuration file, E-1
  - server, 2-4

- setting IP address with, 1-13
- When Needed setting, 3-12

- Bridge Forward Delay field, 3-67
- Bridge Hello Time field, 3-67
- Bridge Maximum Age Time field, 3-67
- Bridge Priority field, 3-66
- Broadcasts field, 3-55

## C

- CI. *See* console interface
- Clear All Port Statistics command, 3-23
- Collisions field, 3-56
- commands
  - Clear All Port Statistics, 3-23
  - Console/Service Port Configuration, 3-8
  - Display Event Log, 3-8
  - Display Port Statistics, 3-23
  - Display Spanning Tree Switch Settings, 3-62
  - IP Configuration, 3-7
  - Logout, 3-9
  - MAC Address Table, 3-23
  - MultiLink Trunk Configuration, 3-23
  - Port Configuration, 3-23
  - Port Mirroring Configuration, 3-23
  - Rate Limiting Configuration, 3-23
  - Reset, 3-7
  - Reset to Default Settings, 3-9
  - SNMP Configuration, 3-8
  - Software Download, 3-8
  - Spanning Tree Configuration, 3-8
  - Spanning Tree Port Configuration, 3-62
  - Switch Configuration, 3-8
  - System Characteristics, 3-8
  - TELNET Configuration, 3-8
  - VLAN Configuration, 3-23

- Community String field, 3-17
- Configurable field, 3-11
- connectors, C-1
  - 100BASE-FX fiber optic port connectors, C-6
  - AC power receptacle, 1-4
  - DB-9 console/service port connector, C-5
  - RJ-45 port connector, C-1
- console interface (CI)
  - access options, 3-1
  - description, 3-1
  - main menu, 3-7
  - menus, accessing, 3-3
  - menus, using, 3-4
- Console Password field, 3-59
- Console Port Speed field, 3-59
- Console Read-Only Password field, 3-59
- Console Read-Write Password field, 3-59
- console terminal
  - allowed types, 1-53, 1-54, 2-3, 3-2
  - configuration parameters, 3-4
- console/service port
  - connecting to, 3-3
  - connector, 1-4
  - illustration, C-5
  - pin assignments, C-5
  - requirements for, 3-2
  - using to manage the switch, 1-53
- Console/Service Port Configuration command, 3-8
- Console/Service Port Configuration screen, 3-58
- conversation steering, 1-11
- cooling fans, 1-5
- crossover cable, C-4
- customer support, xxiv

## D

- DB-9 console/service port connector, C-5
- Declaration of Conformity, A-4
- Default Gateway field, 3-11
- default settings, D-1
- Deferred Packets field, 3-57
- Designated Root field, 3-66

- Diagnostics LED, 1-3, 2-16, 4-3
- Display Event Log command, 3-8
- Display Port Statistics command, 3-23
- Display Spanning Tree Switch Settings command, 3-62

## E

- Event Log screen, 3-79
  - authentication failure, 3-79
  - event log flash memory, 3-80
  - excessive bad entries, 3-80
  - operational exception, 3-79
  - software download, 3-79
  - TELNET session status, 3-79
  - write threshold, 3-80
- Event Logging field, 3-69
- Excessive Collisions field, 3-56
- EZ LAN, 2-4

## F

- F Dx LEDs, 1-3
- FCS Errors field, 3-55
- Filtered Packets field, 3-57
- Find an Address field, 3-25
- flash memory for software image upgrades, 1-11
- Flooded Packets field, 3-57
- Forward Delay field, 3-67
- forwarding rate (packets per second), 1-5
- Frame Errors field, 3-55

## H

- Hello Interval, 3-66, 3-67
- Hello Time field, 3-66

## I

- IEEE 802.3u standard, 1-10
- IEEE 802.3u-compliant autonegotiation, 1-6
- Image Filename field, 3-72

- In Use field, 3-11
- Inactivity Timeout field, 3-69
- In-Band IP Address field, 3-11
- In-Band Subnet Mask field, 3-11
- installation
  - console terminal, 2-3
  - environmental specifications, 2-4
  - flowchart, 1-52
  - LED verification, 2-16
  - mounting brackets, 2-3
  - network cable preparation, 2-3
  - package contents, 2-2
  - Quick-Start procedures, 1-52
  - rack mounting, 2-10
  - required servers, 2-4
  - required tools, 2-1
  - software requirements, 2-4
  - surface mounting, 2-5
  - table or shelf mounting, 2-7
  - verifying, 2-16
  - wall mounting, 2-8
- IP address, automatic configuration, 1-12
- IP Configuration command, 3-7
- IP Configuration screen, 1-54, 3-10

## L

- Last BootP field, 3-11
- Last Reset Type field, 3-21
- Late Collisions field, 3-57
- learning rate, addresses per second, 1-5
- LEDs
  - descriptions, 1-3
  - indications during software download process, 3-73
  - locations, 1-3
  - status monitors, 1-7
  - verifying installation with, 2-16
- Link field, 3-38
- Login Retries field, 3-69
- Login Timeout field, 3-69
- Logout command, 3-9, 3-83
- logout, password-protected, 3-83
- Lost Packets field, 3-55

## M

- MAC address
  - location, 1-12
  - when configuring the BootP server, 1-12
- MAC Address field, 3-21
- MAC Address Table command, 3-23
- MAC Address Table screen, 3-24
- main menu, console interface, 3-7
- Management Information Base (MIB), 1-5
- manufacturing label, 1-4
- Maximum Age Time field, 3-66
- MDI-X to MDI cable connections, C-3
- MDI-X to MDI-X cable connections, C-4
- MIB. *See* Management Information Base
- modem requirements, 3-2
- mounting brackets, installing, 2-6
- Multicasts field, 3-55
- MultiLink Trunk Configuration command, 3-23
- MultiLink Trunk Configuration screen, 3-39
- MultiLink Trunking
  - configuration example, 1-24
  - configuration rules, 1-41
  - description, 1-10
- Multiple Collisions field, 3-56

## N

- network configuration
  - configuring power workgroups, 1-14
  - configuring power workgroups and a shared media hub, 1-15
- network interface card (NIC)
  - connecting to, 2-13
- network management, 1-12
  - Bay Networks applications, 2-4
  - SNMP, 1-54
  - through the console/service port, 1-53
- network protocol/standards compatibility, A-2
- NIC. *See* network interface card

## O

Optivity, 2-4  
Oversized Packets field, 3-56

## P

Packets field, 3-55  
Participation field, 3-64  
password prompt screen, 3-83  
Path Cost field, 3-64  
port cables, connecting, 2-13  
Port Configuration command, 3-23  
Port Configuration screen, 3-36  
port connections, troubleshooting, 4-5  
Port field, 3-35, 3-37, 3-55, 3-64  
Port Mirroring  
    address-based, 1-49  
    Bay Networks StackProbe, 1-11  
    configuration rules, 1-51  
    conversation steering, 1-11  
    description, 1-11  
    monitoring modes, 3-50  
    port-based, 1-46  
Port Mirroring Configuration command, 3-23  
Port Mirroring Configuration screen, 3-48  
Port Statistics screen, 3-54  
port status LEDs, 1-3, 2-16  
ports  
    IEEE 802.3u-compliant autonegotiation, 1-6  
    modes, 1-6  
Power LED, 2-16  
power, connecting, 2-15  
power-up sequence, 4-4  
Priority field, 3-64  
product support, xxiv  
publications  
    hard copy, xxiii  
    related, xxiii

## Q

Quick-Start procedures, 1-51

## R

Rate limiting, 1-6  
    broadcast and multicast storms, 3-52  
    configuration, 3-51  
Rate Limiting Configuration command, 3-23  
Rate Limiting Configuration screen, 3-51  
Read-Only Community String field, 3-17  
Read-Write Community String field, 3-17  
remote access, connecting a modem, 3-2  
remote monitoring (RMON), 1-7  
request mode, choosing, 3-12  
Reset command, 3-9, 3-81  
Reset Count field, 3-21  
Reset to Default Settings command, 3-9, 3-82  
RJ-45 port connector  
    illustration, C-1  
    pin assignments, C-2  
RMON. *See* remote monitoring  
Root Path Cost field, 3-66  
Root Port field, 3-66

## S

safety alert messages, xxv  
Self-Test screen  
    after Reset command, 3-81  
    after Reset to Default Settings command, 3-82  
    during software download process, 3-72  
servers  
    BootP, 2-4  
    TFTP, 2-4  
Service Port Data Bits field, 3-58  
Service Port Parity field, 3-58  
Service Port Stop Bits, 3-59  
settings, default, D-1  
Simple Network Management Protocol (SNMP)  
    MIB support, 1-5, 1-12

- traps, 1-54
  - using to manage the switch, 1-12
- Single Collisions field, 3-56
- SNMP Configuration command, 3-8
- SNMP Configuration screen, 3-14
- SNMP. *See* Simple Network Management Protocol
- software
  - download process, 3-72
  - image upgrades, 1-11
  - requirements, 2-4
- Software Download command, 3-8
- Software Download screen, 3-71
- Spanning Tree Configuration command, 3-8
- Spanning Tree Configuration Menu, 3-61
- Spanning Tree Port Configuration command, 3-62
- Spanning Tree Port Configuration screen, 3-63
- Spanning Tree Switch Settings screen, 3-65
- Speed/Duplex field, 3-38
- Start TFTP Load of New Image field, 3-72
- State field, 3-64
- Status field, 3-38
- support, Nortel Networks, xxiv
- Switch Configuration command, 3-8
- Switch Configuration Menu, 3-22
  - commands, 3-15, 3-23
- sysContact field, 3-21
- sysDescr field, 3-21
- sysLocation field, 3-21
- sysName field, 3-21
- sysObjectID field, 3-21
- sysServices field, 3-21
- System Characteristics command, 3-8
- System Characteristics screen, 3-20
- sysUpTime field, 3-21

## T

- technical publications, xxiii
- technical specifications, A-1
- technical support, xxiv

## TELNET

- accessing CI menus and screens, 3-3
- event log operational exception, 3-79
- event log session status, 3-79
- in-band access, 3-1
- Logout command, 3-83
- supported features, 1-6
  - See also* Console/Service Port Configuration screen
  - See also* TELNET Configuration screen
- TELNET Access field, 3-69
- TELNET Configuration command, 3-8
- TELNET Configuration screen, 3-68
- TFTP Server IP Address field, 3-72, 3-75
- TFTP. *See* Trivial File Transfer Protocol
- Total Octets field, 3-55
- Trap IP Address fields, 3-17
- traps, 1-12
- Trivial File Transfer Protocol (TFTP)
  - server, 2-4
  - software download, 3-71
  - using to upgrade firmware, 1-7

- troubleshooting
  - port interface, 4-5
  - power-up sequence, 4-4

## U

- Undersized Packets field, 3-56

## V

- virtual LAN (VLAN), 1-13, 3-34
  - creating and configuring, 1-16, 3-34
  - network example, 1-13, 3-34
  - VLAN Configuration screen, 3-34
- VLAN Configuration command, 3-23
- VLAN Configuration screen, 3-34, 3-35

