

Part No. 215661-B  
July 2004

4401 Great America Parkway  
Santa Clara, CA 95054

# Using the BayStack 420/425 Switch, Software Release 3.1



**NORTEL**  
NETWORKS™

## Copyright © 2004 Nortel Networks

All rights reserved. July 2004.

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.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

## Trademarks

Autotopology, BayStack, BaySecure, Business Policy Switch 2000, Nortel Networks, the Nortel Networks logo, Optivity, Optivity Policy Services, Preside, and Quick2Config are trademarks of Nortel Networks.

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

Java is a trademark of Sun Microsystems, Inc.

Acrobat and Adobe are trademarks of Adobe Systems, Inc.

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

## Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

## Statement of conditions

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

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

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

**SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.**

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

---

## International regulatory statements of conformity

This is to certify that the Nortel Networks BayStack 425 switch was evaluated to the international regulatory standards for electromagnetic compliance (EMC) and safety and were found to have met the requirements for the following international standards:

- EMC - Electromagnetic Emissions – CISPR 22, Class A
- EMC - Electromagnetic Immunity – CISPR 24
- Electrical Safety – IEC 60950, with CB member national deviations

Further, the equipment has been certified as compliant with the national standards as detailed below.

## National electromagnetic compliance (EMC) statements of compliance

### FCC statement (USA only)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission (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.

### ICES statement (Canada only)

#### Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Nortel Networks BayStack 425 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 (Nortel Networks BayStack 425 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.

### CE marking statement (Europe only)

#### EN 55 022 statements

This is to certify that the Nortel Networks BayStack 425 switch is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC. Conformity is declared by the application of EN 55 022 Class A (CISPR 22).



**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.

---

**EN 55 024 statement**

This is to certify that the Nortel Networks BayStack 425 switch is shielded against the susceptibility to radio interference in accordance with the application of Council Directive 89/336/EEC. Conformity is declared by the application of EN 55 024 (CISPR 24).

**EC Declaration of Conformity**

This product conforms to the provisions of the R&TTE Directive 1999/5/EC.

**VCCI statement (Japan/Nippon only)**

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI) for information technology equipment. 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.

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。

**BSMI statement for BayStack 425 (Taiwan only)**

This is a Class A product based on the standard of the Bureau of Standards, Metrology and Inspection (BSMI) CNS 13438, Class A.

**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。

**MIC notice for BayStack 425 (Republic of Korea only)**

This device has been approved for use in Business applications only per the Class A requirements of the Republic of Korea Ministry of Information and Communications (MIC). This device may not be sold for use in a non-business application.

Observe the Regulatory Marking label on the bottom surface of the chassis for specific certification information pertaining to this model. Each model in the BayStack Series which is approved for shipment to/usage in Korea is labeled as such, with all appropriate text and the appropriate MIC reference number.

---

## National safety statements of compliance

### CE marking statement (Europe only)

#### EN 60 950 statement

This is to certify that the Nortel Networks BayStack 425 switch is in compliance with the requirements of EN 60 950 in accordance with the Low Voltage Directive. Additional national differences for all European Union countries have been evaluated for compliance.

### NOM statement BayStack 425 (Mexico only)

The following information is provided on the devices described in this document in compliance with the safety requirements of the Norma Oficial Mexicana (NOM):

Exporter: Nortel Networks, Inc.  
4655 Great America Parkway  
Santa Clara CA 95054 USA

Importer: Nortel Networks de México, S.A. de C.V.  
Avenida Insurgentes Sur #1605  
Piso 30, Oficina  
Col. San Jose Insurgentes  
Deleg-Benito Juarez  
México D.F. 03900

Tel: 52 5 480 2100

Fax: 52 5 480 2199

Input: BayStack 425  
100 - 120 VAC 16A 50 to 60 Hz  
200 - 240 VAC 12 A 50 to 60 Hz

### Información NOM (unicamente para México)

La información siguiente se proporciona en el dispositivo o en los dispositivos descritos en este documento, en cumplimiento con los requisitos de la Norma Oficial Mexicana (NOM):

Exportador: Nortel Networks, Inc.  
4655 Great America Parkway  
Santa Clara, CA 95054 USA

Importador: Nortel Networks de México, S.A. de C.V.  
Avenida Insurgentes Sur #1605  
Piso 30, Oficina  
Col. San Jose Insurgentes  
Deleg-Benito Juarez  
México D.F. 03900

Tel: 52 5 480 2100

Fax: 52 5 480 2199

Embarcar a: BayStack 425  
100 - 120 VAC 16A 50 to 60 Hz  
200 - 240 VAC 12 A 50 to 60 Hz

---

## Nortel Networks Inc. software license agreement

This Software License Agreement (“License Agreement”) is between you, the end-user (“Customer”) and Nortel Networks Corporation and its subsidiaries and affiliates (“Nortel Networks”). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

“Software” is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. **Licensed Use of Software.** Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment (“CFE”), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer’s Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.
2. **Warranty.** Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided “AS IS” without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.
3. **Limitation of Remedies.** IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER’S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.
4. **General**
  - a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government,

---

the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-Odd entities) and 48 C.F.R. 227.7202 (for Odd entities).

- b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.
- c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.
- d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.
- e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.
- f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

**Revision History**

<b>Date Revised</b>	<b>Version</b>	<b>Reason for revision</b>
July 2004	1.0	Documenting new features for 3.1 release.



---

# Contents

---

<b>Preface</b> .....	<b>21</b>
Before you begin .....	21
Text conventions .....	22
How to get help .....	25
<b>Chapter 1</b>	
<b>BayStack 425 Switch</b> .....	<b>27</b>
Physical description .....	27
Front panel .....	28
User Interface reset button .....	28
Console port .....	29
Gigabit Interface Converter .....	29
Port connectors .....	29
LED display panel .....	31
Back panel .....	33
Cascade Up and Down connectors .....	33
Cooling fans .....	33
AC power receptacle .....	34
Features .....	37
Virtual Local Area Networks .....	37
VLAN Support .....	38
802.1Q Tagging .....	39
Security .....	39
RADIUS-based network security .....	42
MAC address-based security .....	42
Flash memory storage .....	43
Switch software image storage .....	43
Configuration parameters storage .....	43

Multi-Link Trunking .....	43
MLT Operation .....	44
Forwarding Model .....	44
Port mirroring .....	45
Autosensing, autonegotiation, and autopolarity .....	46
RFCs .....	46
Standards .....	47
SNMP MIB support .....	47
Management Agent .....	48
SNMP trap support .....	49
BootP automatic IP configuration/MAC address .....	50
Configuration and switch management .....	50
802.1p Class of Service support .....	51
802.1p COS Remarking .....	52
Spanning Tree .....	52
Port States .....	52
Aging of Dynamic Entries in FDB .....	53
Port Path Cost .....	54
IGMP Snooping .....	54
Banner Display Control .....	55

## **Chapter 2**

### **Network configuration .....** 57

Network configuration examples .....	57
Desktop switch application .....	57
Segment switch application .....	58
High-density switched workgroup application .....	60
BayStack 425 Switch stack operation .....	61
Unit Select switch .....	62
Base unit .....	62
Initial installation .....	62
Stack MAC address .....	63
Removing a unit from the stack .....	63
Stack configurations .....	63
Stack up configurations .....	64

---

Stack down configurations	65
IEEE 802.1Q VLAN workgroups	66
IEEE 802.1Q tagging	67
VLANs spanning multiple switches	72
VLANs spanning multiple 802.1Q tagged switches	72
VLANs spanning multiple untagged switches	73
Shared servers	75
VLAN workgroup summary	80
VLAN configuration rules	82
MultiLink Trunks	82
Client/server configuration using MultiLink Trunks	84
Trunk configuration screen examples	85
Trunk configuration screen for Switch S1	86
Trunk configuration screen for Switch S2	88
Trunk Configuration screen for Switch S3	90
Trunk Configuration screen for Switch S4	92
Before you configure trunks	94
Spanning tree considerations for MultiLink Trunks	95
Additional tips about the MultiLink Trunking feature	98
Port mirroring	99
<b>Chapter 3</b>	
<b>Using the console interface</b>	<b>101</b>
Accessing the CI menus and screens	101
Using the CI menus and screens	102
Navigating the CI menus and screens	102
Screen fields and descriptions	103
Main menu	104
IP Configuration/Setup screen	108
Choosing a BootP request mode	110
BootP When Needed	111
BootP Always	111
BootP Disabled	112
BootP or Last Address	112
SNMP Configuration screen	113

System Characteristics screen	115
Switch Configuration Menu screen	118
MAC Address Table screen	120
MAC Address Security Configuration Menu screen	122
MAC Address Security Port Configuration screen	127
MAC Address Security Port Lists screens	130
Port list syntax	132
Accelerator keys for repetitive tasks	132
Adding a new port to an existing port number list	132
Removing a port from an existing port number list	133
MAC Address Security Table screens	134
VLAN Configuration Menu screen	136
VLAN Configuration screen	138
VLAN Port Configuration screen	141
VLAN Display by Port screen	143
Port Configuration screen	145
High Speed Flow Control Configuration screen	148
Choosing a high speed flow control mode	150
Symmetric mode	150
Asymmetric mode	150
MultiLink Trunk Configuration Menu screen	151
MultiLink Trunk Configuration screen	153
MultiLink Trunk Utilization screen	155
Port Mirroring Configuration screen	157
Port Statistics screen	159
System Log screen	163
Console/Comm Port Configuration screen	165
Rename Stack Units screen	172
Hardware Unit Information screen	173
Spanning Tree Configuration Menu screen	174
Spanning Tree Port Configuration screen	175
Spanning Tree Switch Settings screen	179
TELNET Configuration screen	182
Software Download screen	184
LED Indications during the download process	187

---

Configuration File Download/Upload screen .....	187
Requirements .....	190
<b>Chapter 4</b>	
<b>Troubleshooting .....</b>	<b>191</b>
Interpreting the LEDs .....	191
Diagnosing and correcting problems .....	193
Normal power-up sequence .....	194
Port connection problems .....	194
Autonegotiation modes .....	195
Port interface .....	196
<b>Appendix A</b>	
<b>Technical specifications .....</b>	<b>197</b>
Environmental .....	197
Electrical .....	197
Physical dimensions .....	198
Performance specifications .....	198
Network protocol and standards compatibility .....	199
Safety agency certification .....	199
Electromagnetic emissions .....	199
Electromagnetic immunity .....	200
<b>Appendix B</b>	
<b>Installing a Gigabit Interface Converter (GBIC) .....</b>	<b>201</b>
Product description .....	201
GBIC labeling .....	202
GBIC Models .....	203
GBIC specifications .....	203
Standards, connectors, cabling, and distance .....	203
1000BASE-SX .....	203
1000BASE-LX .....	204
1000BASE-XD .....	206
1000BASE-ZX .....	207
Handling, safety, and environmental guidelines .....	208

<b>Appendix C</b>	
<b>Quick configuration for MultiLink Trunking</b> .....	<b>211</b>
<b>Appendix D</b>	
<b>Connectors and pin assignments</b> .....	<b>213</b>
RJ-45 (10BASE-T/100BASE-TX) port connectors .....	213
MDI and MDI-X devices .....	214
MDI-X to MDI cable connections .....	215
MDI-X to MDI-X cable connections .....	215
DB-9 (RS-232-D) Console/Comm Port connector .....	216
<b>Appendix E</b>	
<b>Default settings</b> .....	<b>219</b>
<b>Appendix F</b>	
<b>Sample BootP configuration file</b> .....	<b>225</b>
<b>Index</b> .....	<b>227</b>

---

# Figures

---

Figure 1	BayStack 425 Switch	27
Figure 2	BayStack 425 Switch front panel	28
Figure 3	BayStack 425 Switch LED display panel	31
Figure 4	BayStack 425 Switch back panel	33
Figure 5	BayStack 425 Switch security feature	40
Figure 6	BayStack 425 Switch used as a desktop switch	58
Figure 7	BayStack 425 Switch used as a segment switch	59
Figure 8	Configuring power workgroups and a shared media hub	61
Figure 9	Stack up configuration example	64
Figure 10	Stack down configuration example	65
Figure 11	Port-based VLAN example	67
Figure 12	Default VLAN settings	69
Figure 13	Port-based VLAN assignment	70
Figure 14	802.1Q tagging (after port-based VLAN assignment)	70
Figure 15	802.1Q tag assignment	71
Figure 16	802.1Q tagging (after 802.1Q tag assignment)	71
Figure 17	VLANs spanning multiple 802.1Q tagged switches	72
Figure 18	VLANs spanning multiple untagged switches	73
Figure 19	Possible problems with VLANs and Spanning Tree Protocol	74
Figure 20	Multiple VLANs sharing resources	75
Figure 21	VLAN broadcast domains within the switch	76
Figure 22	Default VLAN Configuration screen example	77
Figure 23	VLAN Configuration screen example	78
Figure 24	Default VLAN Port Configuration screen example	79
Figure 25	VLAN Port Configuration screen example	80
Figure 26	VLAN configuration spanning multiple switches	81
Figure 27	Switch-to-switch trunk configuration example	83
Figure 28	Switch-to-server trunk configuration example	84
Figure 29	Client/server configuration example	85

Figure 30	Choosing the MultiLink Trunk Configuration Menu screen	86
Figure 31	MultiLink Trunk Configuration screen for Switch S1	87
Figure 32	MultiLink Trunk Configuration screen for Switch S2	89
Figure 33	MultiLink Trunk Configuration screen for Switch S3	91
Figure 34	MultiLink Trunk Configuration screen for Switch S4	93
Figure 35	Path Cost arbitration example	96
Figure 36	Example 1: correctly configured trunk	97
Figure 37	Example 2: detecting a misconfigured port	98
Figure 38	Port Mirroring Configuration port-based screen example	100
Figure 39	Map of console interface screens	103
Figure 40	Console interface main menu	105
Figure 41	IP Configuration/Setup screen	108
Figure 42	SNMP Configuration screen	113
Figure 43	System Characteristics screen	116
Figure 44	Switch Configuration Menu screen	118
Figure 45	describes the MAC Address Table screen fields.	121
Figure 46	MAC Address Security Configuration Menu screen	123
Figure 47	MAC Address Security Configuration screen	125
Figure 48	MAC Security Port Configuration screen (1 of 2)	128
Figure 49	MAC Security Port Configuration screen (2 of 2)	129
Figure 50	MAC Address Security Port Lists screens	130
Figure 51	MAC Address Security Port Lists screen	131
Figure 52	MAC Address Security Table screens	134
Figure 53	MAC Address Security Table screen	135
Figure 54	VLAN Configuration Menu screen	137
Figure 55	VLAN Configuration screen	139
Figure 56	VLAN Port Configuration screen	142
Figure 57	VLAN Display by Port screen	144
Figure 58	Port Configuration screen (1 of 2)	146
Figure 59	Port Configuration screen (2 of 2)	147
Figure 60	High Speed Flow Control Configuration	149
Figure 61	MultiLink Trunk Configuration Menu screen	152
Figure 62	MultiLink Trunk Configuration screen	153
Figure 63	MultiLink Trunk Utilization screen (1 of 2)	155
Figure 64	MultiLink Trunk Utilization screen (2 of 2)	156



---

Figure 65	Port Mirroring Configuration screen	158
Figure 66	Port Statistics screen	160
Figure 67	System Log screen	164
Figure 68	Console/Comm Port Configuration screen	166
Figure 69	Renumber Stack Units screen	172
Figure 70	Hardware Unit Information screen	174
Figure 71	Spanning Tree Configuration Menu screen	175
Figure 72	Spanning Tree Port Configuration screen (1 of 2)	176
Figure 73	Spanning Tree Port Configuration screen (2 of 2)	177
Figure 74	Spanning Tree Switch Settings screen	179
Figure 75	TELNET Configuration screen	182
Figure 76	Software Download screen for a BayStack 420/425 stack	186
Figure 77	Configuration File Download/Upload screen	188
Figure 78	LED display panel	192
Figure 79	Types of GBICs	202
Figure 80	Nortel label on a GBIC	202
Figure 81	Installing a GBIC	210
Figure 82	Removing a GBIC	210
Figure 83	Configuring MultiLink Trunks	212
Figure 84	RJ-45 (8-pin modular) port connector	213
Figure 85	MDI-X to MDI cable connections	215
Figure 86	MDI-X to MDI-X cable connections	216
Figure 87	DB-9 Console port connector	216



---

## Tables

---

Table 1	Components of the BayStack 425 front panel .....	28
Table 2	BayStack 425 Switch LED descriptions .....	31
Table 3	Components on the BayStack 425 Switch back panel .....	33
Table 4	International power cord specifications .....	34
Table 5	SNMP MIB support .....	47
Table 6	Support SNMP traps .....	49
Table 7	Port states of Spanning Tree .....	52
Table 8	Path Cost Values .....	54
Table 9	Stack up configuration description .....	64
Table 10	Stack down configuration description .....	65
Table 11	Console interface main menu options .....	105
Table 12	IP Configuration/Setup screen fields .....	109
Table 13	SNMP Configuration screen fields .....	114
Table 14	System Characteristics screen fields .....	116
Table 15	Switch Configuration Menu options .....	119
Table 16	MAC Address Table screen fields .....	121
Table 17	MAC Address Security Configuration Menu options .....	124
Table 18	MAC Address Security Configuration screen fields .....	125
Table 19	MAC Security Port Configuration screen fields .....	129
Table 20	MAC Address Security Port Lists screen fields .....	131
Table 21	MAC Address Security Table screen fields .....	135
Table 22	VLAN Configuration Menu options .....	137
Table 23	VLAN Configuration screen fields .....	139
Table 24	VLAN Port Configuration screen fields .....	142
Table 25	VLAN Display by Port screen fields .....	144
Table 26	Port Configuration screen fields .....	147
Table 27	High Speed Flow Control Configuration screen fields .....	149
Table 28	MultiLink Trunk Configuration Menu options .....	152
Table 29	MultiLink Trunk Configuration screen fields .....	154

Table 30	MultiLink Trunk Utilization screen fields	156
Table 31	Port Mirroring Configuration screen fields	158
Table 32	Monitoring modes	159
Table 33	Port Statistics screen fields	161
Table 34	System Log screen fields	164
Table 35	Console/Comm Port Configuration screen fields	166
Table 36	Renumber Stack Units screen fields	173
Table 37	Spanning Tree Configuration Menu options	175
Table 38	Spanning Tree Port Configuration screen fields	177
Table 39	Spanning Tree Switch Settings parameters	180
Table 40	TELNET Configuration screen fields	183
Table 41	Software Download screen fields	186
Table 42	Configuration File Download/Upload screen fields	189
Table 43	Parameters not saved to the configuration file	190
Table 44	BayStack 425 Switch LED descriptions	192
Table 45	SFP GBIC Port LEDs on the BayStack 425 Switch	193
Table 46	Corrective actions	195
Table 47	Environmental specifications	197
Table 48	Electrical parameters	197
Table 49	Physical dimensions	198
Table 50	Performance specifications	198
Table 51	Nortel Networks GBIC models	203
Table 52	GBIC specifications	203
Table 53	Model 1000BASE-SX GBIC specifications	204
Table 54	Model 1000BASE-LX GBIC specifications	205
Table 55	Model 1000ASE-XD GBIC specifications	206
Table 56	Model 1000BASE-ZX GBIC specifications	207
Table 57	RJ-45 port connector pin assignments	214
Table 58	DB-9 Console port connector pin assignments	217
Table 59	Factory default settings	219

## Preface

---

This guide describes the Nortel Networks\* BayStack\* 425-24T/48T Switch features and uses. The terms “BayStack 425-24T Switch” and “BayStack 425-48T Switch” are used synonymously in this document.

You can use the BayStack 425 Switch in:

- A standalone switch configuration.
- A stack switch configuration.

## Before you begin

This guide is intended for network managers and administrators with the following background:

- Basic knowledge of networks, Ethernet\* bridging, and IP and IPX routing
- Familiarity with networking concepts and terminology
- Specific knowledge about the networking devices, protocols, topologies, and interfaces that comprise your network
- Experience with windowing systems, graphical user interfaces (GUIs), or Web browsers

## Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicates that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is: <code>ping &lt;ip_address&gt;</code> , you enter: <code>ping 192.32.10.12</code>
<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.
braces ({} )	Indicates required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is: <code>show ip {alerts   routes}</code> , you must enter either: <code>show ip alerts</code> or <code>show ip routes</code> , but not both.
brackets ([ ])	Indicates optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is: <code>show ip interfaces [-alerts]</code> , you can enter either: <code>show ip interfaces</code> or <code>show ip interfaces -alerts</code> .
ellipsis points (...)	Indicates that you repeat the last element of the command as needed. Example: If the command syntax is: <code>ethernet/2/1 [&lt;parameter&gt; &lt;value&gt;] . . .</code> , you enter <code>ethernet/2/1</code> and as many parameter-value pairs as needed.

<i>italic text</i>	<p>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.</p> <p>Example: If the command syntax is:</p> <pre><b>show at &lt;valid_route&gt;</b></pre> <p><i>valid_route</i> is one variable and you substitute one value for it.</p>
screen text	<p>Indicates system output, for example, prompts and system messages.</p> <p>Example: Set Trap Monitor Filters</p>
separator ( > )	<p>Shows menu paths.</p> <p>Example: Protocols &gt; IP identifies the IP option on the Protocols menu.</p>
vertical line (   )	<p>Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command.</p> <p>Example: If the command syntax is:</p> <pre><b>show ip {alerts   routes}</b>, you enter either: <b>show ip alerts</b> or <b>show ip routes</b>, but not both.</pre>

## Related publications

For more information about using the BayStack 425 Switch, refer to the following publications:

- *Using the BayStack 420/425 Switch, Software Release 3.1* (part number 215661-B)  
Describes how to use the BayStack 425 Switch for network configuration.
- *Using Web-Based Management for the BayStack 420/425, Software Release 3.1* (part number 215660-B)  
Describes how to use the Web-based management tool to configure switch features.
- *Installing the BayStack 425 Switch* (part number 215658-B)  
Describes how to install the BayStack 425 Switch.
- *Release Notes for the BayStack 420/425 Switch, Software Release 3.1* (part number 216078-B)  
Documents important changes about the software and hardware that are not covered in other related publications.
- *Getting Started with the BayStack 420/425 Switch Management Software, Software Release 3.1* (part number 215663-B)  
Describes how to install the Java-based device level software management application.
- *Reference for the BayStack 420/425 Switch Management Software, Software Release 3.1*(part number 215662-C)  
Describes how to use the Java-based device level software management application.
- *Reference for the BayStack 420/425 Command Line Interface, Software Release 3.1* (part number 215659-B)  
Describes how to use the Command Line Interface.



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

## How to get help

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

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

Technical Solutions Center	Telephone
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 4NORTEL or (800) 466-7835
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the [www12.nortelnetworks.com/](http://www12.nortelnetworks.com/) URL and click ERC at the bottom of the page.



---

# Chapter 1

## BayStack 425 Switch

---

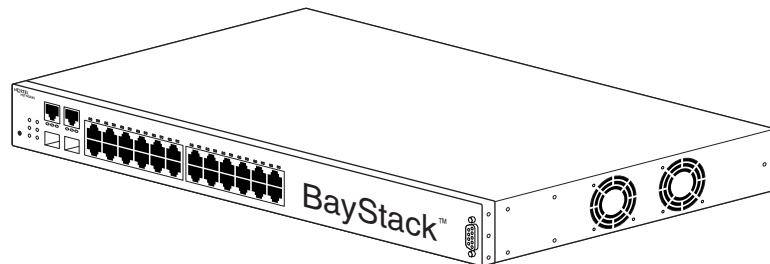
This chapter introduces the BayStack 425 Switch and covers the following topics:

- [“Physical description,”](#) next
- [“Features”](#) on page 37

### Physical description

[Figure 1](#) shows the front and side views of the BayStack 425 Switch.

**Figure 1** BayStack 425 Switch



11107FA

## Front panel

Figure 2 shows the configuration of the front panel on the BayStack 425 Switch.

For descriptions of the back panel BayStack 425 Switch components, see “[Back panel](#)” on page 33.

**Figure 2** BayStack 425 Switch front panel

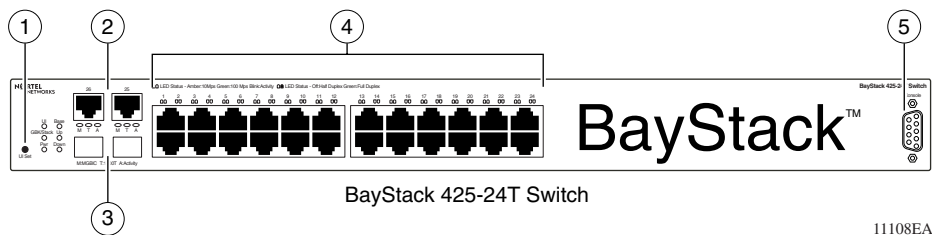


Table 1 describes the components on the front panel.

**Table 1** Components of the BayStack 425 font panel

Item	Description
1	User interface reset button
2	10/100/1000BaseT (copper) port 25 and 26
3	Gigabit Interface Converter (GBIC) ports 25 and 26
4	10/100BaseT ports 1 to 24
5	Console port

### User Interface reset button

The User Interface button on the BayStack 425-24T allows you to:

- Set the switch as the base unit in stacking mode
- Set the switch as a non-base unit in stacking mode

- Reset a stack or unit
- Put the switch in standalone mode

On the BayStack 425-48T, the User Interface button allows you to reset the unit.

## Console port

The Console port allows you to access the console interface (CI) screens and customize your network using the supplied menus and screens (see [Chapter 3, “Using the console interface,”](#) on page 101).

The Console port is a DB-9, RS-232-D male serial port connector. You can use this connector to connect a management station or console/terminal to the BayStack 425 Switch by using a straight-through DB-9 to DB-9 standard serial port cable. You must use a VT100/ANSI-compatible terminal (for cursor control and to enable cursor and functions keys) to use the console port. See *Installing the BayStack 425 Switch* for more information.



**Note:** The console port is configured as a data communications equipment (DCE) connector. Ensure that your RS-232 cable pinouts are configured for DCE connections (see [Appendix D, “Connectors and pin assignments,”](#) on page 213).

---

The Console port default settings are: 9600 baud with eight data bits, one stop bit, and no parity as the communications format, with flow control set to enabled.

## Gigabit Interface Converter

Gigabit Interface Converters (GBICs) are hot-swappable input/output enhancement components designed for use with Nortel Networks products to allow Gigabit Ethernet ports to link with fiber optic networks.

## Port connectors

The BayStack 425 Switch uses 10BASE-T/100BASE-TX RJ-45 (8-pin modular) port connectors.

The 10BASE-T/100BASE-TX port connectors are configured as MDI-X (media-dependent interface-crossover). These ports connect over straight cables to the network interface card (NIC) in a node or server, similar to a conventional Ethernet repeater hub. If you are connecting to an Ethernet hub or Ethernet switch, use a crossover cable unless an MDI connection exists on the associated port of the attached device (see [“Appendix D, “Connectors and pin assignments,” on page 213](#)).

The BayStack 425 Switch uses autosensing ports designed to operate at 10 Mb/s (megabits per second) or at 100 Mb/s, depending on the connecting device. These ports support the IEEE 802.3u autonegotiation standard, which means that when a port is connected to another device that also supports the IEEE 802.3u standard, the two devices negotiate the best speed and duplex mode.

The 10BASE-T/100BASE-TX switch ports also support half- and full-duplex mode operation (refer to *Installing the BayStack 425 Switch*).

The 10BASE-T/100BASE-TX RJ-45 ports can connect to 10 Mb/s or 100 Mb/s Ethernet segments or nodes.



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

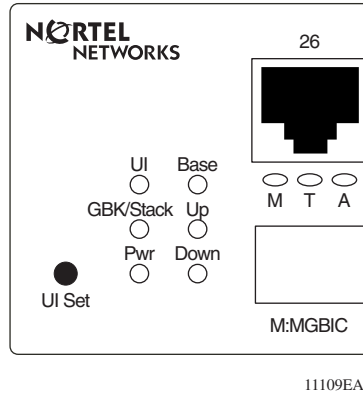
---

See [Appendix D, “Connectors and pin assignments,” on page 213](#) for more information about the RJ-45 port connectors.

## LED display panel

Figure 3 shows the BayStack 425 Switch LED display panel. See Table 2 for a description of the LEDs.

**Figure 3** BayStack 425 Switch LED display panel



**Table 2** BayStack 425 Switch LED descriptions

Label	Type	Color	State	Meaning
UI	Power status	Green	Blinking	Indicates the switch is in cmd mode.
			On	ON for about 3 seconds when executing a cmd, then goes OFF.
			Off	The UI LED should be off, unless active.
GBIC/Stack	Stack Mode	Green	On	The switch is in standalone mode.
			Off	The switch is in stack mode.

**Table 2** BayStack 425 Switch LED descriptions (continued)

Label	Type	Color	State	Meaning
Power On	Power status	Green	On	DC power is available to the switch's internal circuitry.
			Off	No AC power to switch or power supply failed.
Cascade Up	Stack mode	Green	Off	The switch is in standalone mode.
			On	The switch is connected to the <i>upstream</i> unit'.
Cascade Down	Stack mode	Green	Off	The switch is in standalone mode.
			On	The switch is connected to the <i>downstream</i> unit.
Base	Base mode	Green	On	The switch is configured as the stack base unit.
			Off	The switch is <i>not</i> configured as the stack base unit (or is in standalone mode).
		Amber		Due to a stack error, the unit is unable to maintain the stack connection.
10/100 Link/	10/100 Mb/s port speed indicator	Green	On	The corresponding port is set to operate at 100 Mb/s, and the link is good.
			Amber	On
			Off	The link connection is bad, or there is no connection to this port.
Activity	Port activity	Green	Blinking	Indicates network activity for the corresponding port. A high level of network activity can cause the LEDs to appear to be on continuously.
HD/FD	Duplex Mode	Green	On	The port is configured to full duplex.
			Off	The port is configured to half duplex.



## Back panel

Figure 4 shows the back panel of the switch.

**Figure 4** BayStack 425 Switch back panel

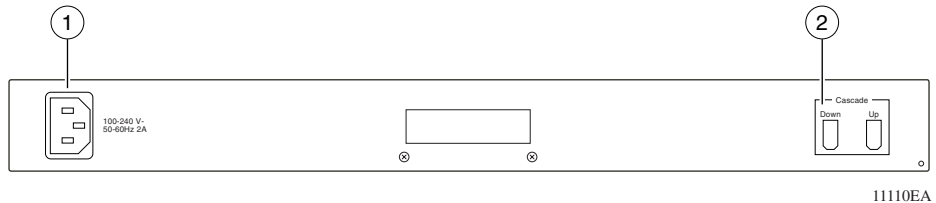


Table 3 describes the components on the back panel.

**Table 3** Components on the BayStack 425 Switch back panel

Item	Description
1	AC power receptacle
2	Cascade Up and Down Connectors

### Cascade Up and Down connectors

The Cascade Up and Down connectors allow the switch to be connected to the *upstream* unit's Cascade Up connector, or to the downstream unit's Cascade Down connector (see “[Stack configurations](#)” on page 63.)

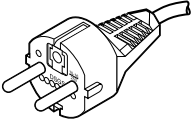
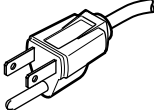
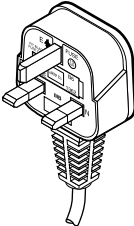
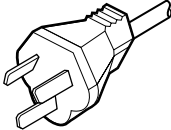
### Cooling fans

Two cooling fans are located on one side of the BayStack 425 Switch to provide cooling for the internal components. (See [Figure 1 on page 27.](#)) When you install the switch, be sure to allow enough space on *both sides* of the switch for adequate air flow. See *Installing the BayStack 425 Switch* for detailed information.

## AC power receptacle

The AC power receptacle accepts the AC power cord (supplied). For installation outside of North America, make sure that you have the proper power cord for your region. Any cord used must have a CEE-22 standard V female connector on one end and must meet the IEC 320-030 specifications. [Table 4](#) lists specifications for international power cords.

**Table 4** International power cord specifications

Country/Plug description	Specifications	Typical plug
Continental Europe: CEE7 standard VII male plug Harmonized cord (HAR marking on the outside of the cord jacket to comply with the CENELEC Harmonized Document HD-21)	220 or 230 VAC 50 Hz Single phase	 228FA
U.S./Canada/Japan: NEMA5-15P male plug UL recognized (UL stamped on cord jacket) CSA certified (CSA label secured to the cord)	100 or 120 VAC 50–60 Hz Single phase	 227FA
United Kingdom: BS1363 male plug with fuse Harmonized cord	240 VAC 50 Hz Single phase	 229FA
Australia: AS3112-1981 Male plug	240 VAC 50 Hz Single phase	 230FA

**Caution: Please read immediately.**

*Inspect this power cord and determine if it provides the proper plug and is appropriately certified for use with your electrical system. Immediately discard this cord if it is inappropriate for your country's electrical system and obtain the proper cord as required by your national electrical codes or ordinances.*

*Refer to this product's technical documentation for detailed installation procedures to be followed by qualified service personnel.*

---

**Vorsicht: Bitte sofort lesen.**

*Sehen Sie nach, ob dieses Netzkabel über den richtigen Stecker verfügt und für die Verwendung in Ihrem Stromversorgungsnetz zertifiziert ist. Falls dieses Kabel nicht für das Stromversorgungsnetz in Ihrem Land geeignet ist, darf es nicht verwendet werden. Besorgen Sie sich ein Kabel, das die Vorschriften der Zulassungsbehörden in Ihrem Land erfüllt.*

*Die technische Dokumentation dieses Produkts enthält ausführliche Installationsanweisungen, die nur von qualifiziertem Kundendienstpersonal ausgeführt werden dürfen.*

---

**Attention: Lisez ceci immédiatement.**

*Examinez ce cordon d'alimentation pour déterminer s'il dispose de la fiche appropriée et s'il est bien agréé pour utilisation sur votre installation électrique. Débarrassez-vous en immédiatement s'il ne convient pas à l'utilisation sur le secteur électrique en usage dans votre pays et procurez-vous un cordon conforme à la réglementation nationale en vigueur.*

*Reportez-vous à la documentation technique de ce produit pour obtenir des instructions détaillées d'installation, destinées à un technicien qualifié.*

---

**Attenzione: Leggere attentamente.**

*Controllare questo cavo di alimentazione, verificarne il collegamento con la presa appropriata nonché la certificazione per l'uso nell'impianto elettrico posseduto. Non utilizzare assolutamente in caso tale cavo non sia adatto al sistema elettrico del paese in cui viene utilizzato e richiederne un altro certificato dall'ente nazionale di fornitura elettrica.*

*Per le procedure di installazione che devono essere seguite dal personale di servizio, consultare questa documentazione tecnica del prodotto.*

---



**Advertencia: Sírvase leer inmediatamente.**

*Inspeccione este cable de alimentación eléctrica y determine si viene con el enchufe apropiado y está debidamente certificado para el uso con su sistema eléctrico. Si no cumple con los reglamentos del sistema eléctrico de su país, despójese de este cable de alimentación inmediatamente y obtenga el cable requerido, según las ordenanzas y códigos eléctricos nacionales.*

*Refiérase a la documentación técnica de este producto para recibir información detallada sobre los procedimientos que el personal calificado de reparaciones deberá seguir.*

---



**Caution:**

**注意：最初にお読み下さい。**

本電源コードが、ご使用になる電力規格に適したプラグ部で、且つ適正な規格証明がついているかどうかをお確かめ下さい。

もし本電源コードがご使用の電力規格に不適格な場合はただちに使用を中止し、ご使用の国家規格・法令に定められた適切な電源コードをご使用下さい。

本製品の取付方法につきましては、取扱技術説明書をご覧のうえ資格認定を受けたサービス・スタッフの指示に従って下さい。

---



**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。

## Features

The BayStack 425 Switch provides wire-speed switching that allows high-performance, low-cost connections to full-duplex and half-duplex 10/100/1000 Mb/s Ethernet local area networks (LANs). The BayStack 425 Switch provides the following features.

### Virtual Local Area Networks

In a traditional shared-media network, traffic generated by a station is transmitted to all other stations on the local segment. Therefore, for any given station on the shared Ethernet, the local segment is the *collision domain* because traffic on the segment has the potential to cause an Ethernet collision. The local segment is also the *broadcast domain* because any broadcast is sent to all stations on the local segment. Although Ethernet switches and bridges divide a network into smaller collision domains, they do not affect the broadcast domain. In simple terms, a virtual local area network provides a mechanism to fine-tune broadcast domains.

BayStack 425 Switch allows you to create port-based Virtual Local Area Networks (VLANs):

- IEEE 802.1Q port-based VLANs

A port-based VLAN is a VLAN in which the ports are explicitly configured to be in the VLAN. When you create a port-based VLAN, you assign a Port VLAN Identifier (PVID) and specify which ports belong to the VLAN. The PVID is used to coordinate VLANs across multiple switches.

- Auto PVID

When Auto PVID is active, a port that is assigned to a numbered VLAN has the same number for its PVID. For example, if the VLAN is 2, the PVID is 2.

## VLAN Support

The 3.1 release of BayStack 425 supports 255(bs425 only)/32(mixed environments) port-based VLANs, under the 802.1D bridging model. However, this version does not support protocol VLANs, MAC source-based VLANs or subnet-based VLANs.

PVIDs can be assigned on a per port basis. The AutoPVID option automatically assigns a PVID to all the ports. These ports are the members of the VLAN that has just been created.

Tagging will be available on per port basis. You can configure tagged and untagged ports on the same VLAN. By default, packets will be tagged internally. All ports will tag untagged ingress traffic so it can be handled by the CPU and forwarding database. Upon egress, the packet will either strip the tag or keep the tag unchanged with the egress port tag, depending on the state of the egress port.

Ports may be grouped into broadcast domains by assigning them to the same VLAN. For frame forwarding, all IP subnet-based or MAC-based VLANs must be a subset of port-based VLANs.

When the BayStack 425 switch is installed for the first time, all the ports will be in default VLAN (PVID = 1). The default management VLAN is VLAN 1.

You can configure the VLANs on each port through the user Interface or the configuration file. BayStack 425 supports CLI and ASCII configuration files. You can also configure VLANs using both SNMP and ASCII scripts.

## 802.1Q Tagging

BayStack 425 will allow per port basis tagging on all ports only if VLAN is associated with the protocols supported by the port.

Tagging status applies on all ports of a multi-link trunk (a port member in a MLT cannot be configured independently of the other members in the same MLT). You can configure tagged frame dropping on a per-port basis.

BayStack 425 supports the Independent VLAN Learning (IVL) model. IVL allows duplicate MAC address to be present in different sets, but not in the same set or VLAN.

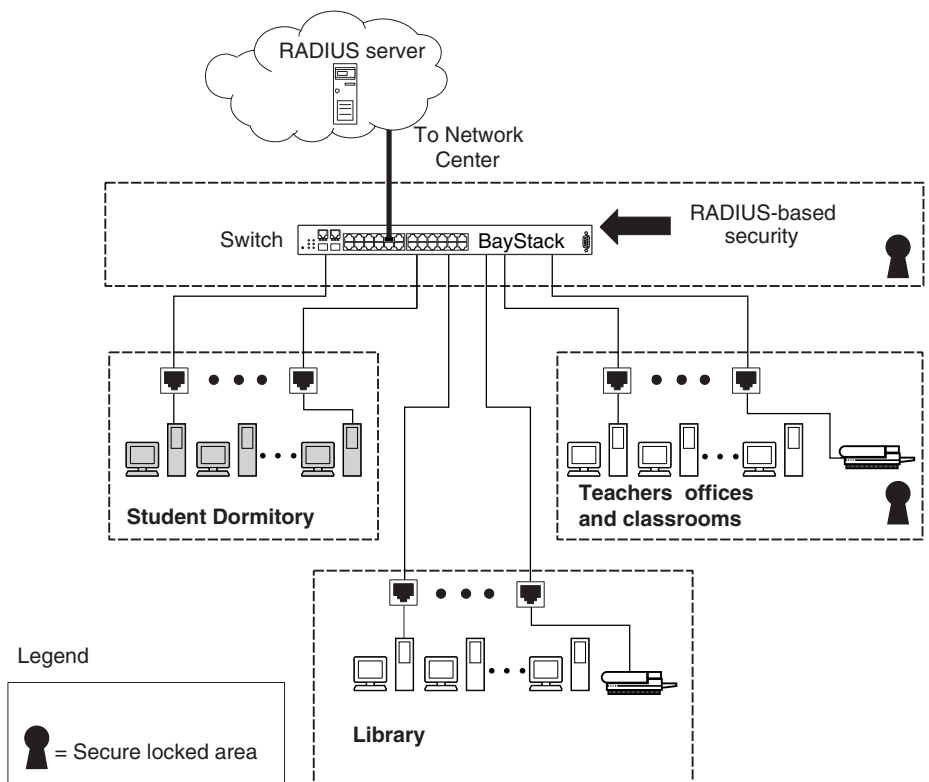
## Security

The BayStack 425 Switch security features provide two levels of security for your local area network (LAN):

- RADIUS-based security—limits administrative access to the switch through user authentication
- MAC address-based security—limits access to the switch based on allowed source MAC addresses

[Figure 5](#) shows a typical campus configuration using the BayStack 425 Switch security features. This example assumes that the switch, the teachers' offices and classrooms, and the library are physically secured. The student dormitory may (or may not be) physically secure.

Figure 5 BayStack 425 Switch security feature



11111EA



In this configuration example, the following security measures are implemented:

- The switch
  - RADIUS-based security is used to limit administrative access to the switch through user authentication (see [“RADIUS-based network security” on page 42](#)).
  - MAC address-based security is used to allow up to 448 authorized stations (MAC addresses) access to one or more switch ports (see [“MAC address-based security” on page 42](#)).
  - The switch is located in a locked closet, accessible only by authorized Technical Services personnel.
- Student dormitory

Dormitory rooms are typically occupied by two students and have been prewired with two RJ-45 jacks. Only students who are authorized (as specified by the MAC address-based security feature) can access the switch on the secured ports.
- Teachers’ offices and classrooms

The PCs that are located in the teachers’ offices and in the classrooms are assigned MAC address-based security that is specific for each classroom and office location. The security feature logically locks each wall jack to the specified station and prevents unauthorized access to the switch should someone attempt to connect a personal laptop PC into the wall jack. The printer is assigned as a single station and is allowed full bandwidth on that switch port.

It is assumed that all PCs are password protected and that the classrooms and offices are physically secured.
- Library

The wall jacks in the library are set up so that the PCs can be connected to any wall jack in the room. This arrangement allows the PCs to be moved anywhere in the room. The exception is the printer, which is assigned as a single station with full bandwidth to that port.

It is assumed that all PCs are password protected and that access to the library is physically secured.

## RADIUS-based network security

The RADIUS-based security feature allows you to set up network access control, using the Remote Authentication Dial-In User Services (RADIUS) security protocol. The RADIUS-based security feature uses the RADIUS protocol to authenticate local console and Telnet logins.

You will need to set up specific user accounts (user names and passwords, and Service-Type attributes) on your RADIUS server before the authentication process can be initiated. This provides you with appropriate levels of access to the switch, set the following username attributes on your RADIUS server:

- Read-write access—Set the Service-Type field value to Administrative.
- Read-only access—Set the Service-Type field value to NAS-Prompt.

For detailed instructions to set up your RADIUS server, refer to your RADIUS server documentation.

For instructions to use the console interface (CI) to set up the RADIUS-based security feature, see [Chapter 3, “Using the console interface,”](#) on page 101.

## MAC address-based security

The MAC address-based security feature allows you to set up network access control, based on source MAC addresses of authorized stations.

You can:

- Create a list of up to 448 MAC addresses and specify which addresses are authorized to connect to your switch or stack configuration. The 448 MAC addresses can be configured within a single standalone switch, or they can be distributed in any order among the units in a single stack configuration.
- Specify which of your switch ports each MAC address is allowed to access.  
The options for allowed port access include: NONE, ALL, and single or multiple ports that are specified in a list, for example, 1/1-4,1/6,2/9 (see [“Port list syntax”](#) on page 132).
- Specify optional actions to be exercised by your 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.

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.

For instructions to use the console interface (CI) to set up the RADIUS-based security feature, see [Chapter 3, “Using the console interface,”](#) on page 101.

## Flash memory storage

### Switch software image storage

The BayStack 425 Switch uses flash memory to store the switch software image. The flash memory allows you to update the software image with a newer version without changing the switch hardware (see [“Software Download screen”](#) on [page 184](#)). An in-band connection between the switch and the TFTP load host is required to download the software image.

### Configuration parameters storage

All configuration parameters are stored in flash memory. These parameters are updated every 10 seconds (if a change occurs) or whenever a reset command is executed.



**Warning:** Do not power off the switch within 10 seconds of changing any configuration parameters. Powering down the switch within 10 seconds of changing configuration parameters can cause the changed configuration parameters to be lost.

---

## Multi-Link Trunking

The MultiLink Trunking (MLT) feature allows you to group multiple ports, two or four together, when forming a link to another switch or server. This increases the aggregate throughput of the interconnection between two devices, up to 800 Mb/s in full-duplex mode.

The BayStack 425 Switch can be configured with up to six MultiLink Trunks in a stack. The trunk members can only be configured within a single unit in the stack.

The MLT feature also helps you to build a higher bandwidth port from multiple physical links, with the traffic load balanced across the physical ports.

Trunking can be described in the following terms:

- Network Trunk (NT) - A NT is attached to another internetworking device, yielding multiple addresses, which is seen on each of the trunk members. The same source addresses can be seen on one or more of the trunk members.
- Server Trunk (ST) - A ST is attached to a server that utilizes the same MAC address on each of its links.
- Bounded Trunk - All ports of a trunk group that exists on the same module.
- Distributed Trunk – All members of a trunk are distributed across the modules in a stack.

The two basic switching requirements of MLTS are:

- The ability to treat multiple links as a single one for the purposes of learning and migration.
- The ability to select one of the member paths as the destination for a forwarding function without sending any duplicate packets.

## **MLT Operation**

BayStack 425 supports a maximum of 6 trunks, scaling up to 4 ports per trunk. The MLT operation is based on the concept of trunk groups. A trunk group is a collection of ports that represent a single link for learning, forwarding and other bridge functions.

## **Forwarding Model**

The trunk forwarding function is based on the following:

- Destination Address (DA)
- Source Address (SA).

Maximum of four ports will be assigned to a trunk. The source address is associated with the trunk group rather than the individual port it was learned on. From here, the forwarding function points the packets to that particular trunk group.

For proper network operation, packets cannot be replicated to more than one port of a trunk group. The operation that creates this selection is based on the SA. SA selects one of the possible egress ports that is a member of the trunk group. For any DA, the egress path will always be defined by the SA.

Packets to a certain DA can appear on any member link of the trunk. Packets with the same SA always appear on the same egress port irrespective of DA. The exception to this is when the BCAST/MCAST/DLF traffic is sent out using the same port within the MLT regardless of the SA.

For more information on MultiLink Trunking feature, see [“MultiLink Trunk Configuration Menu screen” on page 151](#).

## Port mirroring

Port mirroring feature also referred to as *conversation steering* allows you to allocate a single switch port or monitor port as a traffic monitor for another switch port or mirror port. All incoming traffic on the mirrored port and all segment associated with local traffic is copied to the monitor port. This operation excludes traffic forwarded by the switch. This feature is helpful in network trouble shooting.

You can specify *port-based* monitoring for ingress to a specific port. You can also attach a probe device such as a Nortel Networks StackProbe, or equivalent to the designated monitor port. When a port is operating as a monitor port, forwarding is not allowed on that port.

For more information on port mirroring feature, see [“Port Mirroring Configuration screen” on page 157](#).

## Autosensing, autonegotiation, and autopolarity

The BayStack 425 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 switch to select the best of both speed and duplex modes.
- The term *autopolarity* refers to automatic detection of transmit and receive twisted pairs.

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 425 Switch reverts to half-duplex mode.

When autonegotiation-capable devices are attached to the BayStack 425 Switch, the ports negotiate down from 100 Mb/s speed and full-duplex mode until the attached device acknowledges a supported speed and duplex mode.

Autopolarity detects receive and transmit twisted pairs automatically. When autopolarity is active, any straight or crossover category 5 cable can be used to provide connection to a port. If the port is set to a fixed configuration, then autopolarity is not active.

For more information about autosensing and autonegotiation modes, see [Chapter 4, "Troubleshooting," on page 191](#).

### RFCs

For more information about networking concepts, protocols, and topologies, consult the following RFCs:

- RFC 1213 (MIB-II)
- RFC 1493 (Bridge MIB)
- RFC 1573 (Interface MIB)
- RFC 1643 (Ethernet MIB)

- RFC 1757 (RMON)
- RFC 1271 (RMON)
- RFC 1157 (SNMP)

## Standards

The following IEEE Standards also contain information germane to the BayStack 425 Switch:

- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.3 (Ethernet)
- IEEE 802.1Q (VLAN Tagging)

## SNMP MIB support

The BayStack 425 Switch supports an SNMP agent with industry standard MIBs, as well as private MIB extensions, which ensures compatibility with existing network management tools. The switch supports the MIB-II (RFC 1213), Bridge MIB (RFC 1493), 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 generate automatically for conditions such as an unauthorized access attempt or changes in a port's operating status. [Table 5](#) lists supported SNMP MIBs.

**Table 5** SNMP MIB support

Application	Standard MIBs	Proprietary MIBs
S5 Chassis MIB		s5cha127.mib
S5 Agent MIB		s5age140.mib
RMON	rfc1757.mib	
MLT		rcMLT
SNMPv3 MIBs	RFCs 2571, 2572, 2573, 2574, 2575, 2576	
MIB2	rfc1213.mib	
IF-MIB	rfc2233.mib	

**Table 5** SNMP MIB support (continued)

Etherlike MIB	rfc1643.mib	
Interface Extension MIB		s5ifx100.mib
Switch Bay Secure		s5sbs102.mib
System Log MIB		bnlog.mib
S5 Autotopology MIB		s5emt104.mib
VLAN		rcVlan
Entity MIB	RFC 2037	
Spanning Tree	RFC1493 Bridge MIB	

## Management Agent

The SNMP agent is trilingual and supports exchanges using SNMPv1, SNMPv2c and SNMPv3. SNMPv1 communities provides support for SNMPv2c by introducing standards-based GetBulk retrieval capability. SNMPv3 support provides MD5 and SHA-based user authentication and message security as well as DES-based message encryption.

Modules that support MIB are:

### Standard MIBs

- MIB II (RFC 1213)
- Bridge MIB (RFC 1493) and proposed VLAN extensions.
- 802.1Q Bridge MIB
- 802.1p
- Ethernet MIB (RFC 1643)
- RMON MIB (RFC 1757)
- SMON MIB
- High Capacity RMON
- Interface MIB (RFC2233)
- Entity MIB (RFC2037)
- SNMPv3 MIBs (RFC 2271 – RFC 2275)

### Proprietary MIBs



- s5Chassis MIB
- s5Agent MIB
- Interface Extension MIB
- s5 Multi-segment topology MIB
- s5 Switch BaySecure MIB
- System Log MIB
- RapidCity Enterprise MIB
  - rcDiag (Conversation steering) MIB
  - rcVLAN MIB
  - rcMLT MIB

## SNMP trap support

The BayStack 425 Switch supports an SNMP agent with industry standard SNMPv1 traps, as well as private SNMPv1 trap extensions ([Table 6](#)).

**Table 6** Support SNMP traps

Trap name	Configurable	Sent when
<b>RFC 1215 (industry standard):</b>		
linkUp	Per port	A port's link state changes to up.
linkDown	Per port	A port's link state changes to down.
authenticationFailure	System wide	There is an SNMP authentication failure.
coldStart	Always on	The system is powered on.
warmStart	Always on	The system restarts due to a management reset.
<b>s5CtrMIB (Nortel proprietary traps):</b>		
s5CtrUnitUp	Always on	A unit is added to an operational stack.
s5CtrUnitDown	Always on	A unit is removed from an operational stack.
s5CtrHotSwap	Always on	A unit is hot-swapped in an operational stack.
s5CtrProblem	Always on	An assigned base unit fails.
s5EtrSbsMacAccessViolation	Always on	A MAC address violation is detected.

## BootP automatic IP configuration/MAC address

The BayStack 425 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 425 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 information about a stack MAC address, see [“Stack MAC address” on page 63](#).

For more information and an example of a BootP configuration file, see [Appendix F, “Sample BootP configuration file,” on page 225](#).

## Configuration and switch management

The BayStack 425 Switch is shipped directly from the factory ready to operate in any 10BASE-T or 100BASE-TX standard network.

You must assign an IP address to the switch or stack, depending on the mode of operation. You can set both addresses by using the console port or BootP, which resides on the switch. You can manage the switch using:

- Console interface

The console interface allows you to configure and manage the switch locally or remotely. Access the CI menus and screens locally through a console terminal attached to your BayStack 425 Switch, remotely through a dial-up modem connection, or in-band through a Telnet session.

For information about the console interface, see [Chapter 3, “Using the console interface,” on page 101](#).

- Web-based management

You can manage the network from the World Wide Web. Access the Web-based graphical user interface (GUI) through the Embedded Web Server (EWS), the HTML-based browser located on your network. The GUI allows you to configure, monitor, and maintain your network through Web browsers. You can also download software using the Web.

For information about Web-based management, refer to *Using Web-based Management for the BayStack 420/425, Software Release 3.1*.

- Java-based Device Manager

Device Manager is a Java-based set of graphical network management applications used to configure and manage a BayStack 425 Switch. See *Reference for the BayStack 420/425 Switch Management Software, Software Release 3.1* for more information.

- Any generic SNMP-based network management software.

You can use any generic SNMP-based network management software to configure and manage a BayStack 425 Switch.

- Nortel Networks Optivity\* network management software

Optivity network management software consists of views, most of which are maps that illustrate the interconnections between the segments, rings, and nodes of your network. The views allow you to analyze network performance and fault conditions on the individual segments and specific areas in your network. They can also alert you when a problem has occurred in a specific location. For further information about Optivity, contact your Nortel Networks sales representative.

## 802.1p Class of Service support

BayStack 425 enables 802.1p Traffic Class by mapping the 8 priority levels into 4 internal CoS queues. The priorities can range from 'Low' to 'Highest'. You can specify this mapping through a console screen.

CoS queues are scheduled based on any of the following policies:

- Strict Priority Based Scheduling
- Weighted Round-Robin Scheduling

You can change the policy at runtime. Also, for Weighted Round-Robin Scheduling, you can adjust the minimum bandwidth or the number of packets per queue.

## 802.1p COS Remarking

BayStack 425 also implements the 802.1 remarking option. This forces all incoming ethernet packets to the ingress port priority instead of 802.1p for tagged packets within the TAG field.

## Spanning Tree

The BayStack 425-24T switch supports transparent bridging by implementing the IEEE 802.1D standard. This is also known as the Spanning Tree Protocol (STP) and Algorithm (STA) standards. STP runs on all ports to provide automatic network configuration of a loop-free topology. This allows you to configure redundant links to provide network fault tolerance.

### Port States

The port will always be in one of the following 5 states:

[Table 7](#) describes the port states of Spanning Tree

**Table 7** Port states of Spanning Tree

State	Rx BPDUs	Tx BPDUs	Learn Addresses	Forward Frames
Disabled	X	X	X	X
Blocking	✓	X	X	X
Listening	✓	✓	X	X
Learning	✓	✓	✓	X
Forwarding	✓	✓	✓	✓

After a switch or a stack is powered-up or reset and the initialization process is completed, all the ports are transformed from the Disabled state to the Blocking state.

If a port is not connected, the port will stay in the Blocking state.

If you connect a station to a port, the port will not start forwarding packets immediately. You will have to wait for the port to transit through the Listening and Learning states to have access to any resources located on another segment.

If you connect a hub or another bridging device to a port, it creates a loop in the network topology and a broadcast storm may occur. This is because one of the ports causing the loop might be in the Blocking state instead of the Forwarding state. The loop should be eliminated once this port receives a BPDU frame from a higher priority port.

The MIB variable `dot1dStpPortEnable` allows you to disable or enable a port. A port is enabled by default. In this mode of operation, the port is in one of the following STP states:

- Blocking
- Listening
- Learning
- Forwarding.

If you disable a port, it will not forward any frames and will not participate in the Spanning Tree Algorithm and Protocol.

## **Aging of Dynamic Entries in FDB**

Dynamic MAC address entries are automatically removed from the Filtering Database after a specified time.

If the network topology has not undergone any change, the aging time-out value is specified by the `dot1dTpAgingTime` MIB variable. This can be configured through the user interface console. The range of applicable values specified in the IEEE standard is 10-106 seconds, whereas the default value recommended is 300 seconds.

If the root bridge notifies topology changes to other bridging devices, a short aging time-out value is used. The time-out value is set equal to the Forward Delay parameter contained in BPDUs originating from the root. The range of values for the Forward Delay parameter specified in the IEEE standard is 4 - 30 seconds. The recommended default value is 15 seconds.

## Port Path Cost

The path cost associated with a port can either be automatically calculated by the switch or it can be assigned by you. By default the path cost is automatically calculated. Also by default, the cost of a given link is originally specified [IEEE90] to be inversely proportional to the data rate of the link: Thus, a 10 Mb/s Ethernet has a “link costs” of 100. This formula does not work well for Gigabit ethernet or even for emerging technologies such as packets-over-sonet at OC-48 rates and above.

[Table 8](#) describes a range of values for a given data rate, and a recommended value that has a non-linear relationship between link cost and data rate for very high-speed LANs.

**Table 8** Path Cost Values

Data Rate	Recommended Link Cost Range	Recommended Link Cost Value
10 Mbps	50-600	100
100 Mbps	10-60	19
1 Gbps	3-10	4
10 Gbps	1-5	2

The valid range for path cost values is between 0 and 65535. If you enter a value between 1 and 65535, the port’s path cost will be set to the new value. If you enter 0, the port’s path cost will be auto-calculated.

## IGMP Snooping

IP multicast is directly mapped to broadcast transmissions in a bridged Ethernet environment. In a layer 2 device such as the Ethernet switch, every IP multicast packet is forwarded on all the links. These IP multicast packets are delivered to all the segments of an extended LAN. As the network carries more broadcast traffic, the Network performance degrades. End stations are indiscriminately offered the same load as the rest of the network, even though they are not interested in particular IP multicast streams.

IGMP is a protocol used by the IP hosts. IGMP is used to report the multicast group memberships of the IP hosts to any of their immediately neighboring multicast routers.

When multicasting is used on more than one physical network and multicast data grams have to pass through routers, the IGMP protocol is useful.

IGMP snooping is supported by BayStack 425 for both, version 1 and 2 of the IGMP protocol. The IGMP snooping technique enables the switch to selectively forward multicast traffic only on those ports where particular IP multicast streams are expected.

By “snooping” for IGMP communication between routers and hosts, a switch can identify those ports.

The IGMP v1 and v2 ‘proxy’ functionality is also implemented by BayStack 425. This is done by generating single IGMP reports on behalf of all the IGMP hosts in a multicast group.

## **Banner Display Control**

You can customize the opening banner that appears when you connect to the switch console port or Telnet to the switch. The part you can customize is the “BAYSTACK,” written in asterisks when it is opened the first time. You cannot customize the portion that displays “Enter Ctrl-Y to begin”

The Banner Control feature provides you with an option to specify banner display. If you do not choose to display the banner, the system will enter the command mode through default command interface without you entering CTRL-Y.

You can select the display of the banner to appear at the beginning of the console or telnet connection. The selection details are stored in NVRAM and its value is reflected to all the units in a stack configuration. This selection also determine if the agent banner is displayed or not.

Besides telnet sessions, the selected behavior is also used for subsequent console sessions. For executing the new mode in the console, you have to logout, whereas in telnet all the subsequent sessions will use the selected mode.





---

## Chapter 2

# Network configuration

---

Use BayStack 425 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 connected to the switch or by creating a virtual LAN (VLAN) through the switch.

This chapter covers the following topics:

- [“Network configuration examples,”](#) next
- [“BayStack 425 Switch stack operation”](#) on page 61
- [“IEEE 802.1Q VLAN workgroups”](#) on page 66
- [“MultiLink Trunks”](#) on page 82
- [“Port mirroring”](#) on page 99

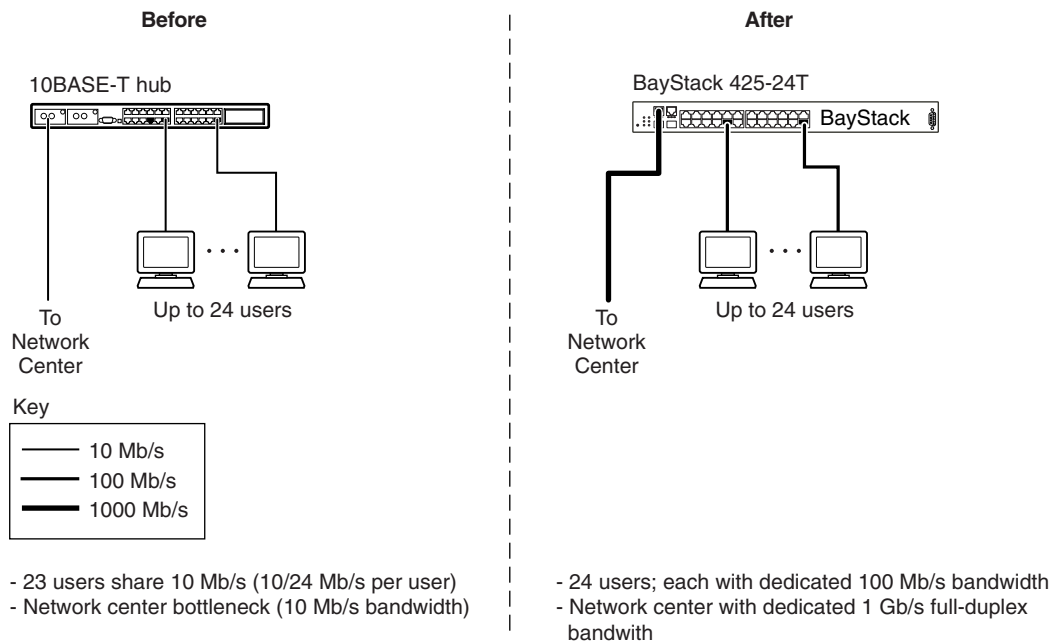
## Network configuration examples

This section provides four network configuration examples using BayStack 425 switch. In these examples, the packet classification feature can be used to prioritize the traffic of the network to ensure uninterrupted traffic of critical applications. The examples are:

- [Desktop switch application](#) (next)
- [Segment switch application](#) (page 58)
- [High-density switched workgroup application](#) (page 60)

### Desktop switch application

[Figure 6](#) shows a BayStack 425 Switch used as a desktop switch, where desktop workstations are connected directly to switch ports.

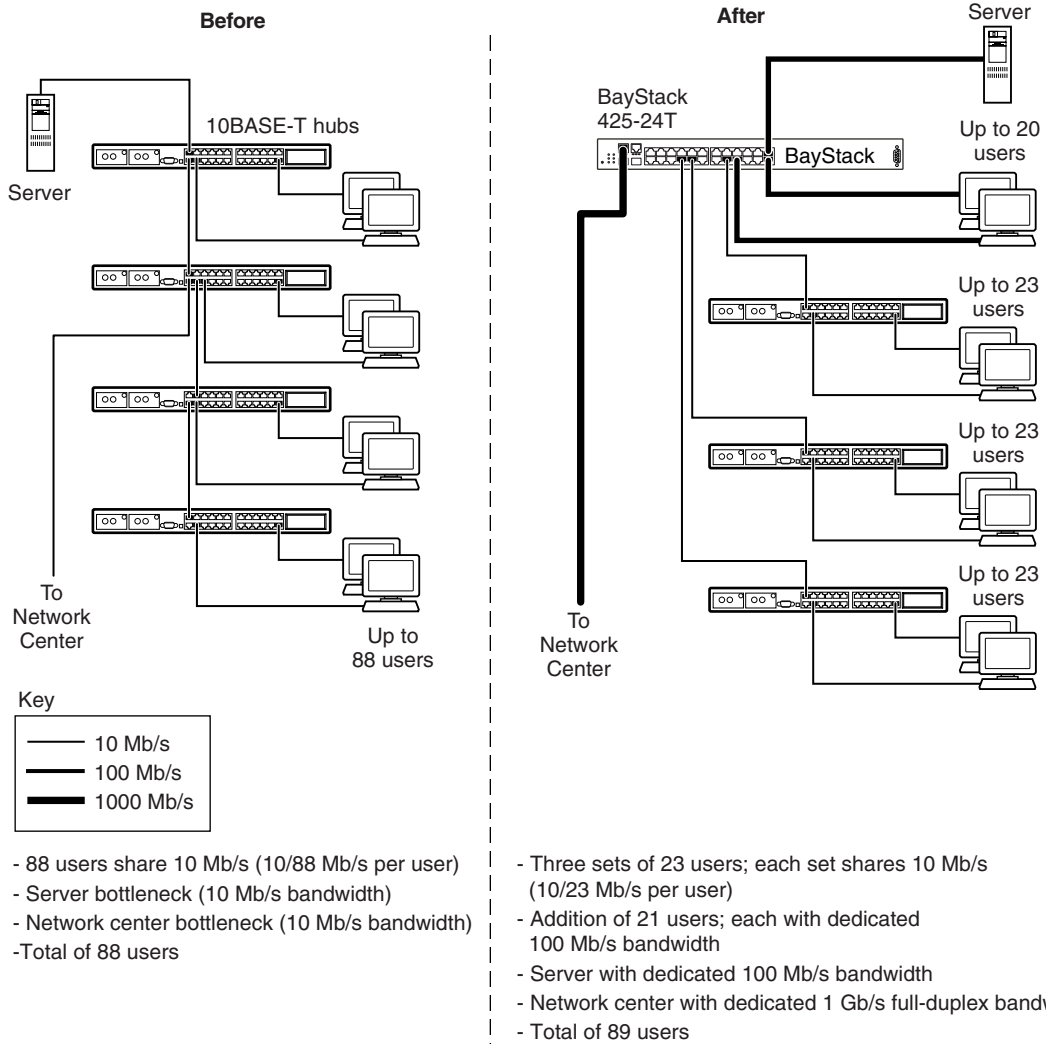
**Figure 6** BayStack 425 Switch used as a desktop switch

11112EA

## Segment switch application

**Figure 7** shows a BayStack 425 Switch used as a segment switch to alleviate user contention for bandwidth and eliminate server and network bottlenecks. Before segmentation, 88 users had a total bandwidth of only 10 Mb/s available. After segmentation, 92 users have 40 Mb/s, four times the previous bandwidth, while adding 22 dedicated 100 Mb/s connections. This configuration can be extended to add more segments without degrading performance.

**Figure 7** BayStack 425 Switch used as a segment switch



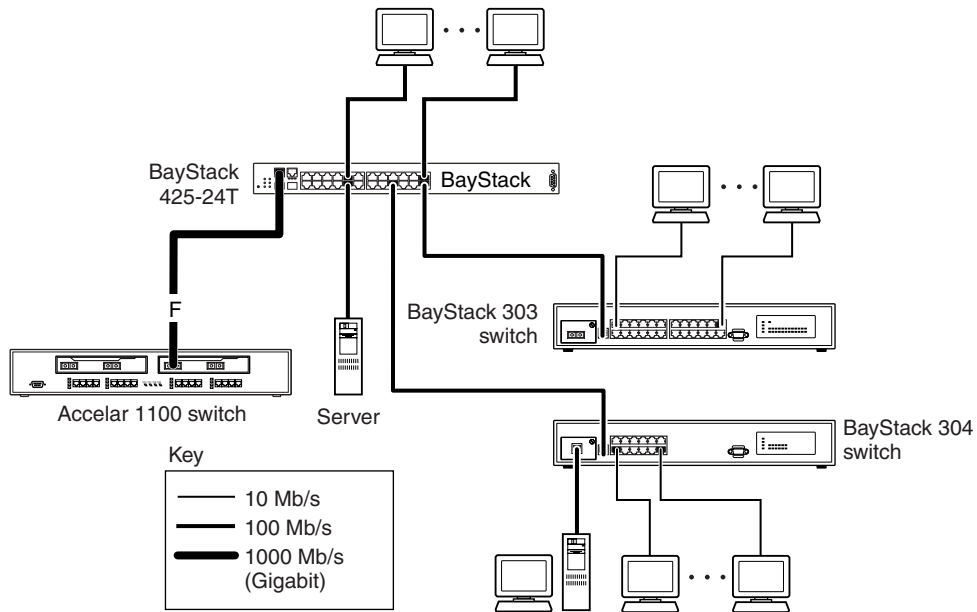
11113EA

## High-density switched workgroup application

**Figure 8** shows an example of using a BayStack 425 Switch with a high-speed (gigabit) connection to a Nortel Networks Passport\* 8600 switch. BayStack 303 and BayStack 304 switches are also shown in this example of a high-density switched workgroup.

As shown in **Figure 8**, the Passport 8600 switch is used as a backbone switch, connecting to the BayStack 425 Switch with an optional (1000BASE-SX) GBIC for maximum bandwidth. The BayStack 303 and BayStack 304 switches have 100 Mb/s connections to the BayStack 425 Switch, a 100BASE-TX hub, and a 100 Mb/s server as well as 10 Mb/s connections to DTE (data terminal equipment).

See the Nortel Networks library Web page [www.nortelnetworks.com/documentation](http://www.nortelnetworks.com/documentation) for online documentation about the Nortel Networks Passport 8600 switch and the BayStack 303 and BayStack 304 switches.

**Figure 8** Configuring power workgroups and a shared media hub

11114EA

## BayStack 425 Switch stack operation

You can connect up to eight BayStack 425-24T switches to provide uninterrupted connectivity for up to 192 ports. The entire stack can be managed as a single unit. This will also have a single IP and MAC address.

You can select the base unit by using the momentary switch mechanism. It is recommended that you use only one base unit in a stack and the selection of the same should be done before powering the stack.

BayStack 425 does not support stack redundancy. In case of cable or unit failure, all the units will go standalone. However, the stack will automatically reform once the missing cable is re-inserted or the bad unit is replaced.

BayStack units in a stack are interconnected through FireWire cables. Ensure that the downlink connection on a unit should always be connected to the Up link of the next unit in the ring.

## Unit Select switch

The Unit Select push-button switch (in = Base) determines the *base unit* for the stack configuration (see [“Base unit” on page 62](#)). The Unit Select switch status is displayed on the BayStack 425 Switch LED display panel. When the Unit Select switch is in the Base (in) position, all other Unit Select switches in the stack configuration must be set to Off (out).

## Base unit

The base unit is the unique stack unit that you configure with the Unit Select switch on the front panel. One BayStack 425 Switch in the stack *must* be configured as the base unit; all other units in the stack *must* have their Unit Select switch set to Off (see [“Unit Select switch” on page 62](#)). You can assign any single BayStack 425 Switch as the base unit.

The physical ordering of all of the other units in the stack is determined by the position of the base unit within the stack. This is important for network management applications that view the physical ordering of the units within the stack.

Some characteristics of the base unit are described in the following sections.

### Initial installation

During the *initial installation* of the stack, the software automatically determines the physical order of all units in the stack according to the position of the base unit within the stack. Thereafter, the individual units maintain their original unit numbering, even if you change the position of one or more units in the stack (you can renumber the units using the Renumber Stack Units screen; see [“Renumber Stack Units screen” on page 172](#)).

For example, when you initially power up the stack, the base unit becomes unit 1 and the unit that the base unit connects to becomes unit 2 (and the next unit is unit 3 and so on), until the maximum stack configuration (up to 8 units) is reached. If you change the base unit to another unit in the stack, the new base unit keeps its original unit number in the stack.

## Stack MAC address

When the switch is participating in a stack configuration, a stack MAC address is automatically assigned during the stack initialization. The base unit's MAC address, with a software offset, is used for the stack MAC address.

For example, if the base unit's MAC address is 00-00-82-99-44-00, and the stack software offset is 1F, then the stack MAC address becomes:

00-00-82-99-44-1F

If another unit in the stack is assigned as the base unit, the MAC address of the *new* base unit (with offset) now applies to the stack configuration. The original stack IP address still applies to the new base unit.

## Removing a unit from the stack

If a unit is removed from the stack (therefore operating in standalone mode), the following switch configuration settings revert back to the settings configured before the unit became a member of the stack:

- IP address
- Console password
- Telnet password
- SNMP community strings

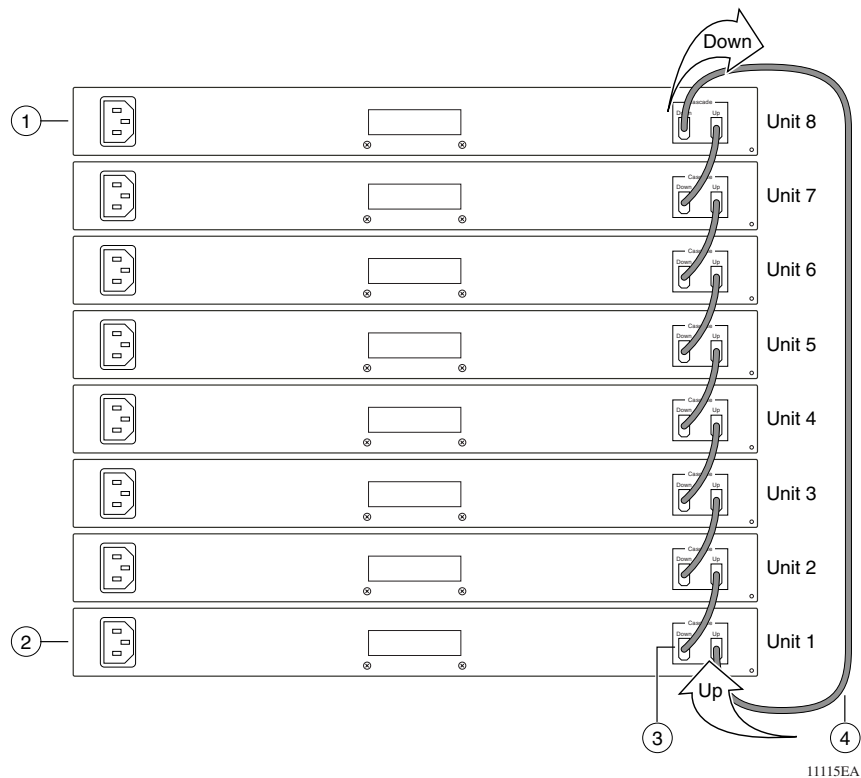
## Stack configurations

As shown in [Figure 9](#), the cable connectors provide the ability to stack up to eight switches. Because stack parameters are associated with the base unit (see “[Base unit](#)” on page 62), the physical stack order depends on the base unit's position and whether the stack is configured *stack up* or *stack down*.

## Stack up configurations

In [Figure 9](#), data flows from the base unit (unit 1) to the next switch, which is assigned as unit 2, and continues until the last switch in the stack is assigned as unit 8. The physical order of the switches is *from bottom to top* (unit 1 to unit 8).

**Figure 9** Stack up configuration example



[Table 9](#) describes the stack up configuration illustration references.

**Table 9** Stack up configuration description

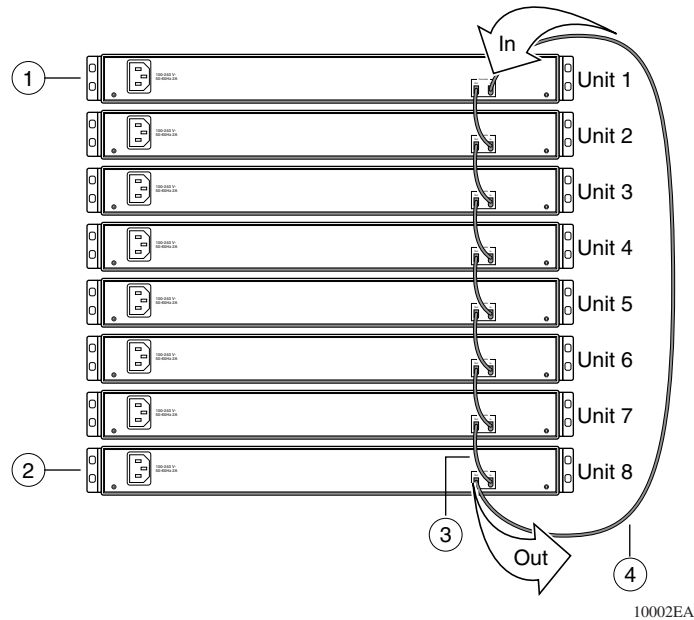
Item	Description
1	Last unit
2	Base unit
3	Stacking cable 30 cm (order number AL 2018005)
4	Stacking cable 1 m (order number AL 2018006)



## Stack down configurations

In [Figure 10](#), data flows from the base unit (unit 1) to the next switch, which is assigned as unit 2, and continues until the last switch in the stack is assigned as unit 8. The physical order of the switches is *from top to bottom* (unit 1 to unit 8).

**Figure 10** Stack down configuration example



[Table 10](#) describes the stack down configuration illustration references.

**Table 10** Stack down configuration description

Item	Description
1	Base unit
2	Last unit
3	Stacking cable 30 cm (order number AL 2018005)
4	Stacking max-return cable 1 m (part number AL 2018006)

Certain network management station (NMS) applications assume a stack down configuration for the graphical user interface (GUI) that represents the stack (see [Figure 10](#)). For this reason, Nortel Networks recommends that you always configure the top unit in the stack as the base unit.

In any stack configuration, the following applies:

- When you apply power to the stack, the base unit initializes and the entire stack powers up as a single logical unit.
- You can attach an RS-232 communications cable to the console port of any switch in the stack.
- You can downline upgrade the entire stack from any switch in the stack from the console interface, a Telnet session, the Web-based management interface, or any generic SNMP-based network management software.
- You can access and manage the stack using a Telnet connection, the Web-based management interface, or any generic SNMP management tool through any switch port that is part of the stack configuration.
- When you stack three or more switches, use the longer (1-meter) stacking max-return cable to complete the link from the last unit in the stack to the base unit.

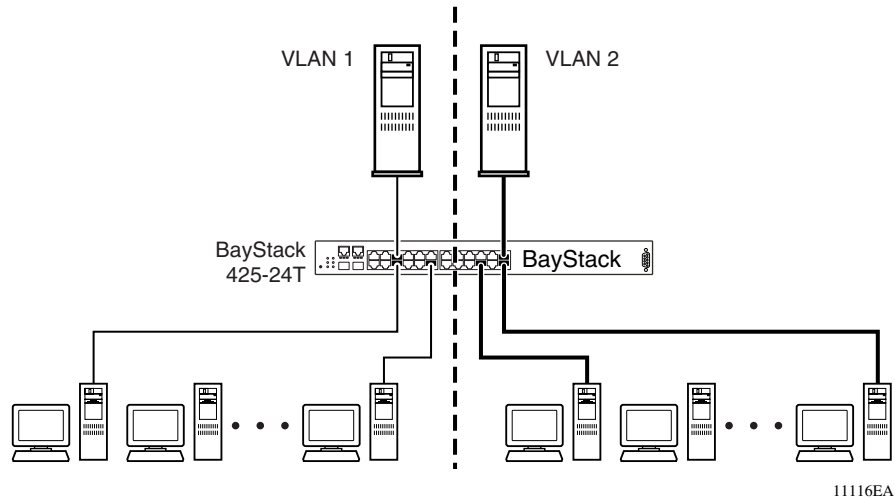
## IEEE 802.1Q VLAN workgroups

BayStack 425 switch supports up to 255 VLANs in a pure stack or standalone and 32 VLANs in a mixed stack of BayStack 425 and 420, or even an aggregation switch with IEEE 802.1Q tagging available per port. Ports are grouped into broadcast domains by assigning them to the same VLAN. Frames received in one VLAN can only be forwarded within that VLAN, and multicast frames and unknown unicast frames are flooded only to ports in the same VLAN.

Setting up virtual LANs (VLANs) is a way to segment networks to increase network capacity and performance without changing the physical network topology ([Figure 11](#)). With network segmentation, each switch port connects to a segment that is a single broadcast domain. When a switch port is configured to be a member of a VLAN, it is added to a group of ports (workgroup) that belong to one broadcast domain.

The BayStack 425 Switch allows you to assign ports to VLANs using the console, Telnet, Web-based management, or an appropriate SNMP-based application. You can assign different ports (and therefore the devices attached to these ports) to different broadcast domains. This feature allows network flexibility because you can reassign VLANs to accommodate network moves, additions, and changes, eliminating the need to change physical cabling.

**Figure 11** Port-based VLAN example



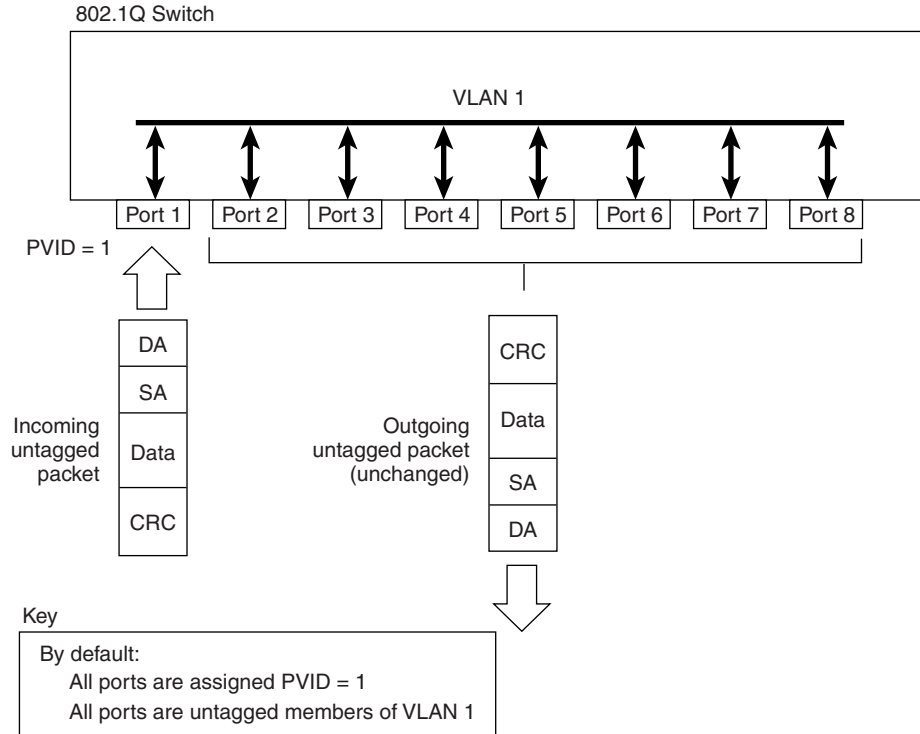
## IEEE 802.1Q tagging

BayStack 425-24T switches operate in accordance with the IEEE 802.1Q tagging rules. Important terms used with the 802.1Q tagging feature are:

- **VLAN identifier (VID)**—the 12-bit portion of the VLAN tag in the frame header that identifies an explicit VLAN. When other types of VLANs are enabled, this default value can be overridden by the values enabled in the Web-based management interface. Refer to *Using Web-based Management for the BayStack 420/425, Software Release 3.1*.
- **Port VLAN identifier (PVID)**—a classification mechanism that associates a port with a specific VLAN. For example, a port with a PVID of 3 (PVID =3) assigns all untagged frames received on this port to VLAN 3.

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

The default configuration settings for BayStack 425-24T switches have all ports set as untagged members of VLAN 1 with all ports configured as PVID = 1. Every VLAN is assigned a unique VLAN identifier (VID) that distinguishes it from all other VLANs. In the default configuration example shown in [Figure 12](#), all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID =1). Untagged packets enter and leave the switch unchanged.

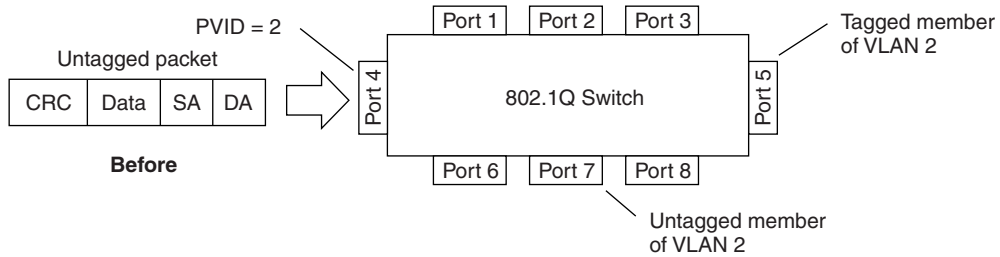
**Figure 12** Default VLAN settings

BS45010A

When you configure VLANs, you configure the switch ports as *tagged* or *untagged* members of specific VLANs (see [Figure 13](#) through [Figure 21](#)).

In [Figure 13](#), untagged incoming packets are assigned directly to VLAN 2 (PVID = 2). Port 5 is configured as a *tagged* member of VLAN 2, and port 7 is configured as an *untagged* member of VLAN 2.

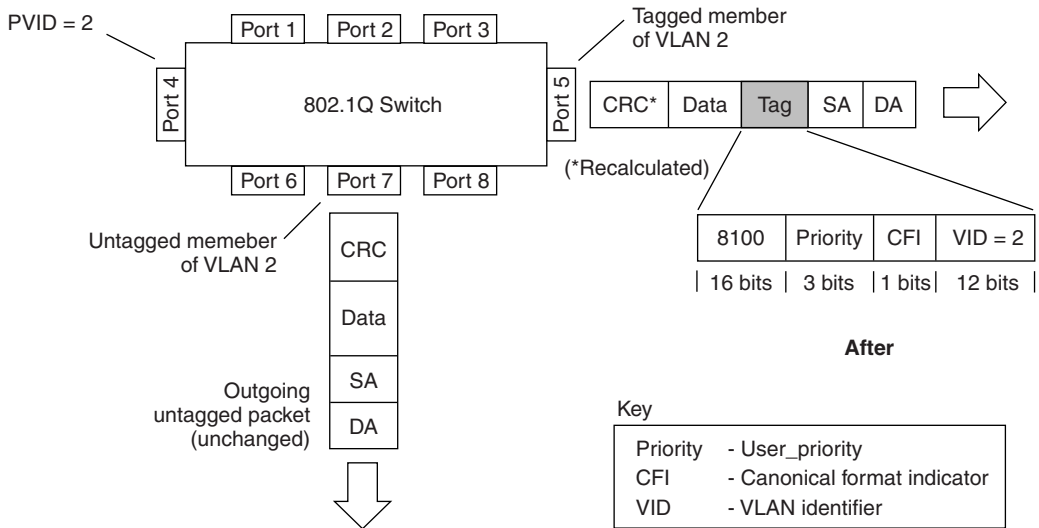
**Figure 13** Port-based VLAN assignment



BS45011A

As shown in Figure 14, the untagged packet is marked (tagged) as it leaves the switch through port 5, which is configured as a tagged member of VLAN 2. The untagged packet remains unchanged as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.

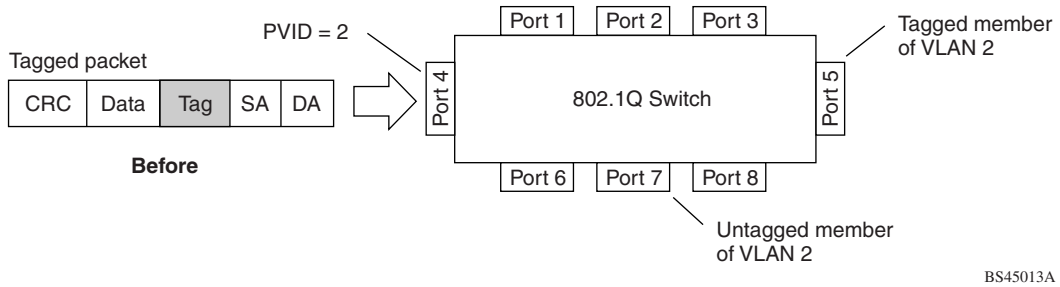
**Figure 14** 802.1Q tagging (after port-based VLAN assignment)



BS45012A

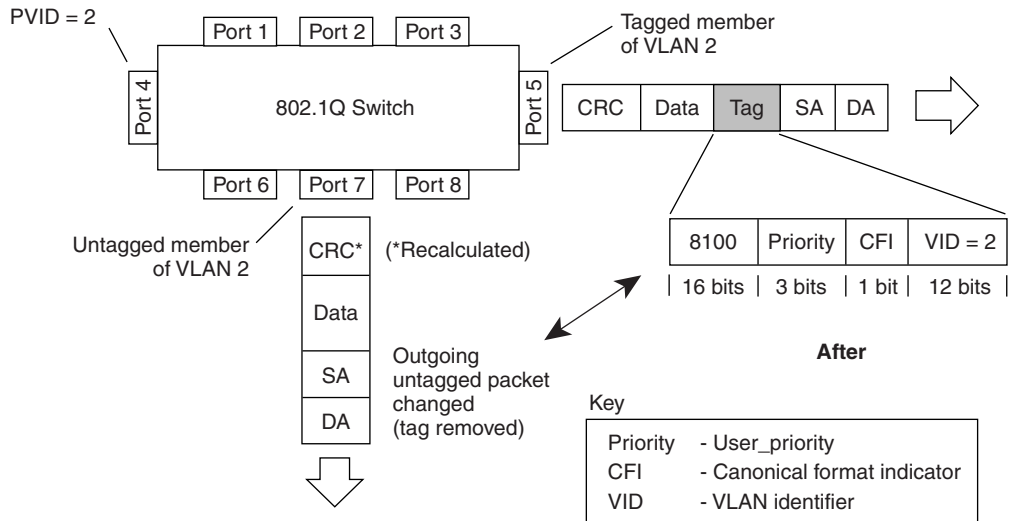
In [Figure 15](#), tagged incoming packets are assigned directly to VLAN 2 because of the tag assignment in the packet. Port 5 is configured as a *tagged* member of VLAN 2, and port 7 is configured as an *untagged* member of VLAN 2.

**Figure 15** 802.1Q tag assignment



As shown in [Figure 16](#), the tagged packet remains unchanged as it leaves the switch through port 5, which is configured as a tagged member of VLAN 2. However, the tagged packet is stripped (untagged) as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.

**Figure 16** 802.1Q tagging (after 802.1Q tag assignment)



## VLANs spanning multiple switches

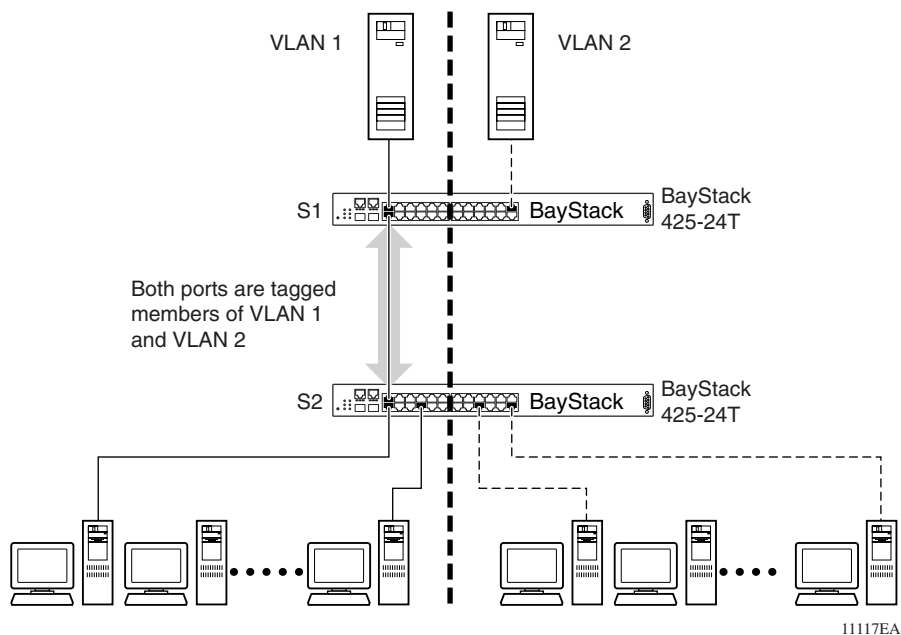
You can use VLANs to segment a network within a switch. When you connect multiple switches, it is possible to connect users of one VLAN with users of that same VLAN in another switch. However, the configuration guidelines depend on whether both switches support 802.1Q tagging.

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

### VLANs spanning multiple 802.1Q tagged switches

Figure 17 shows VLANs spanning two BayStack 425-24T switches. The 802.1Q tagging is enabled on S1, port 2 and on S2, port 1 for VLAN 1 and VLAN 2. Both ports are tagged members of VLAN 1 and VLAN 2.

**Figure 17** VLANs spanning multiple 802.1Q tagged switches





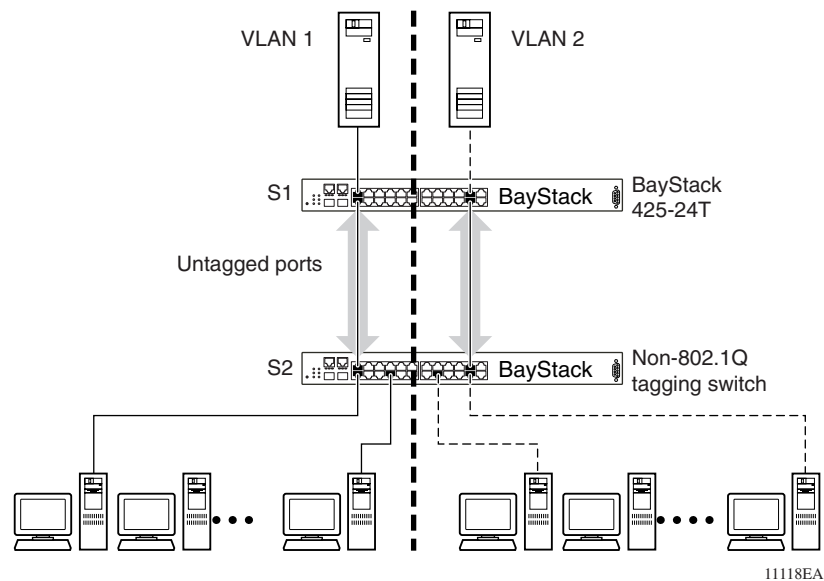
Because there is only one link between the two switches, the Spanning Tree Protocol (STP) treats this configuration as any other switch-to-switch connection. For this configuration to work properly, both switches must support the 802.1Q tagging protocol.

## VLANS spanning multiple untagged switches

Figure 18 shows VLANs spanning multiple untagged switches. In this configuration, Switch S2 does not support 802.1Q tagging and you must use a single switch port on each switch for each VLAN.

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

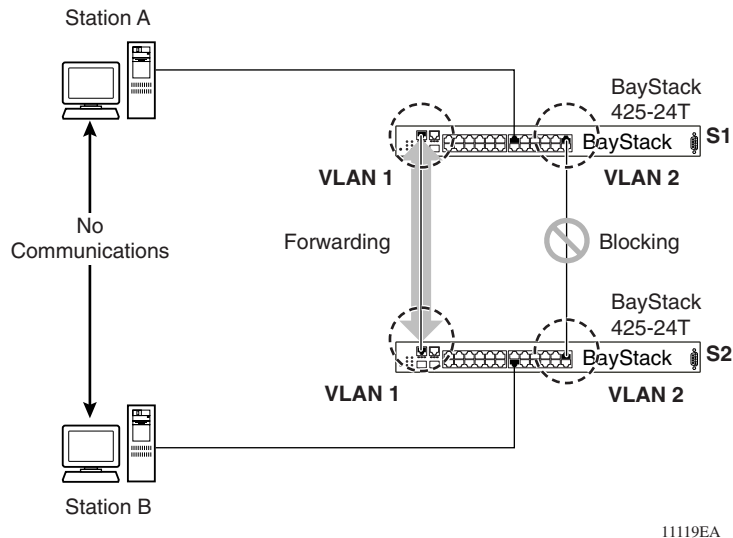
**Figure 18** VLANs spanning multiple untagged switches



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

To connect multiple VLANs across switches with redundant links, you must disable the STP on all participating switch ports. [Figure 19](#) shows possible consequences of enabling the STP when using VLANs between untagged (non-802.1Q tagged) switches.

**Figure 19** Possible problems with VLANs and Spanning Tree Protocol



As shown in [Figure 19](#), with STP enabled, only one connection between Switch S1 and Switch S2 is forwarding at any time. Communications failure occurs between VLAN 2 of S1 and VLAN 2 of S2, blocking communications between Stations A and B.

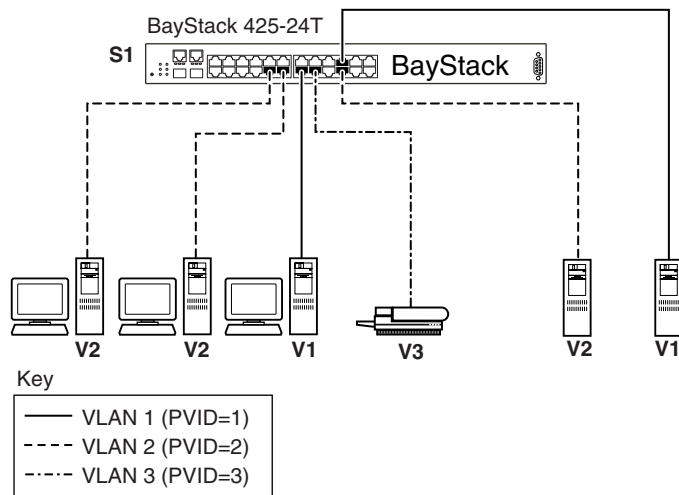
The STP selects the link connecting VLAN 1 on Switches S1 and S2 as the forwarding link based on port speed, duplex-mode, and port priority. Because the other link connecting VLAN 2 is in Blocking mode, stations on VLAN 2 in Switch S1 cannot communicate with stations in VLAN 2 on Switch S2. With multiple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

## Shared servers

BayStack 425-24T switches allow ports to exist in multiple VLANs for shared resources, such as servers, printers, and switch-to-switch connections. It is also possible to have resources exist in multiple VLANs on one switch as shown in [Figure 20](#).

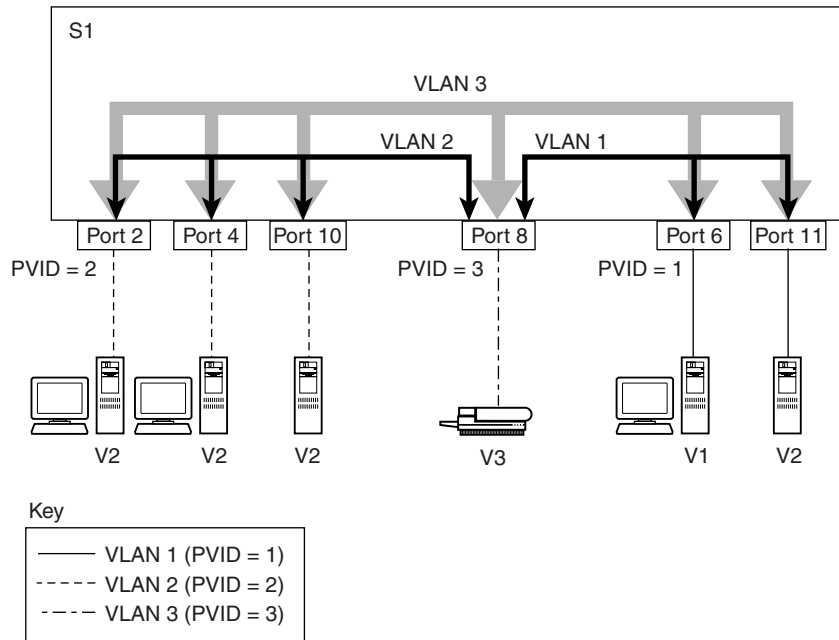
In this example, clients on different broadcast domains share resources. The broadcasts from ports configured in VLAN 3 can be seen by all VLAN port members of VLAN 3.

**Figure 20** Multiple VLANs sharing resources



11120EA

In the above configuration, all of the switch ports are set to participate as VLAN port members. This arrangement allows the switch to establish the appropriate broadcast domains within the switch ([Figure 21](#)).

**Figure 21** VLAN broadcast domains within the switch

BS45019A

For example, to create a broadcast domain for each VLAN shown in [Figure 21](#), configure each VLAN with a port membership, and each port with the appropriate PVID/VLAN association:

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

The following steps show how to use the VLAN configuration screens to configure the VLAN 3 broadcast domain shown in [Figure 21](#).

To configure the VLAN port membership for VLAN 1:

- 1 Select Switch Configuration from the BayStack 425 Switch Main Menu (or press w).
- 2 From the Switch Configuration Menu, select VLAN Configuration (or press v).
- 3 From the VLAN Configuration Menu select VLAN Configuration (or press v).

The default VLAN Configuration screen opens (Figure 22).

**Figure 22** Default VLAN Configuration screen example

```

                                VLAN Configuration

Create VLAN:      [ 1 ]
Delete VLAN:     [   ]
VLAN Name:       [ VLAN #1 ]
Management VLAN: [ Yes ] Now: 1      VLAN State:      [ Active ]

                                Port Membership
                                1-6    7-12  13-18  19-24  25-30  31-36  37-42  43-48  49-50
                                -----
Unit #1  ++++++ ++++++ ++++++ ++++++ ++++++ ++++++ ++++++ ++++++ ++

KEY: + = A Member of This VLAN, - = Not a Member of This VLAN
Use space bar to display choices or enter text.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

```

The VLAN Configuration screen settings shown in Figure 22 are default settings with all switch ports classified as *untagged* members of VLAN 1.

Figure 23 shows the VLAN Configuration screen after it is configured to support the VLAN 3 broadcast domain shown in Figure 21 on page 76 (VLAN Name is optional).

Ports 2, 4, 6, 8, 10, and 11 are now untagged members of VLAN 3 as shown in Figure 21 on page 76.

**Figure 23** VLAN Configuration screen example

```

                                VLAN Configuration

Create VLAN:      [ 1 ]
Delete VLAN:     [   ]
VLAN Name:       [ VLAN #1 ]
Management VLAN: [ Yes ] Now: 1      VLAN State:      [ Active ]

                                Port Membership
                                1-6    7-12  13-18  19-24  25-30  31-36  37-42  43-48  49-50
                                -----
Unit #1  ++++++ ++++++ ++++++ ++++++ ++++++ ++++++ ++++++ ++++++ ++

KEY: + = A Member of This VLAN, - = Not a Member of This VLAN
Use space bar to display choices or enter text.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

```

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

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

The default VLAN Port Configuration screen opens (Figure 24).

The VLAN Port Configuration screen settings shown in [Figure 24](#) are default settings.

**Figure 24** Default VLAN Port Configuration screen example

```
VLAN Port Configuration

Port: [ 1 ]
Filter Untagged Frames: [ No ]
Port Name: [ Port 1 ]
PVID: [ 1 ]
Port Priority: [ 0 ]
Tagging: [ Untagged Access ]

AutoPVID (all ports): [ Disabled ]

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

[Figure 25](#) shows the VLAN Port Configuration screen after it is configured to support the PVID assignment for port 8, as shown in [Figure 21 on page 76](#) (Port Name is optional).

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

**Figure 25** VLAN Port Configuration screen example

```
VLAN Port Configuration

Port:                               [ 1 ]
Filter Untagged Frames:            [ No ]
Port Name:                          [ Port 1 ]
PVID:                               [ 1 ]
Port Priority:                      [ 0 ]
Tagging:                            [ Untagged Access ]

AutoPVID (all ports):              [ Disabled ]

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

## VLAN workgroup summary

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

As shown in [Figure 26](#), Switch S1 (BayStack 425 Switch) is configured with multiple VLANs:

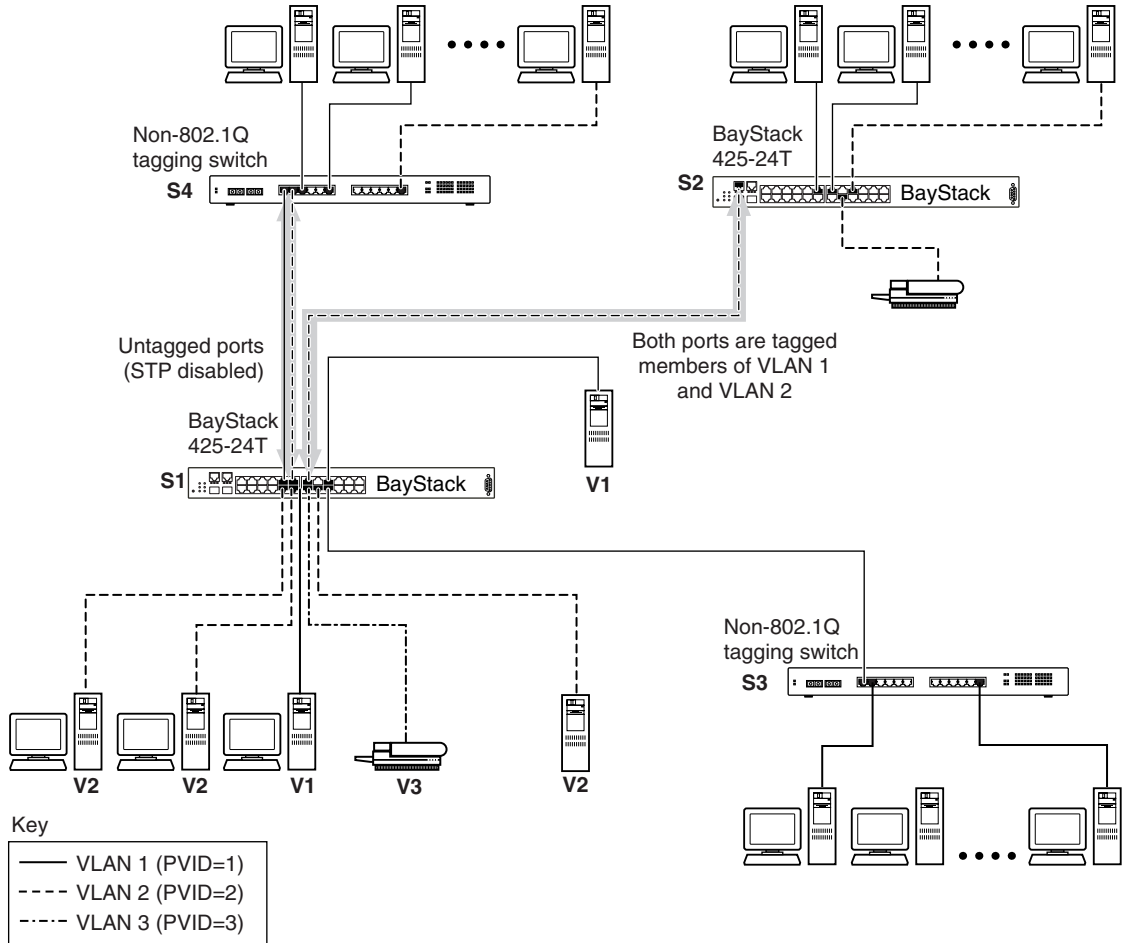
- Ports 1, 6, 11, and 12 are in VLAN 1.
- Ports 2, 3, 4, 7, and 10 are in VLAN 2.
- Port 8 is in VLAN 3.

Because S4 does not support 802.1Q tagging, a single switch port on each switch must be used for each VLAN (see [“VLANs spanning multiple untagged switches” on page 73](#)).

The connection to S2 requires only one link between the switches because S1 and S2 are both BayStack 425-24T switches that support 802.1Q tagging (see [“VLANs spanning multiple 802.1Q tagged switches” on page 72](#)).



Figure 26 VLAN configuration spanning multiple switches



11122EA

## VLAN configuration rules

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

- All ports that are involved in port mirroring must have memberships in the same VLANs. If a port is configured for port mirroring, the port's VLAN membership cannot be changed.
- If a port is a trunk group member, all trunk members are added or deleted from the VLAN.
- All ports involved in trunking and port mirroring must have the same VLAN configuration. If a port is on a trunk with a mirroring port, the VLAN configuration cannot be changed.
- Auto PVID can be activated by creating a VLAN and enabling Auto PVID for it.

For more information about configuring VLANs, see [“VLAN Configuration Menu screen” on page 136](#).

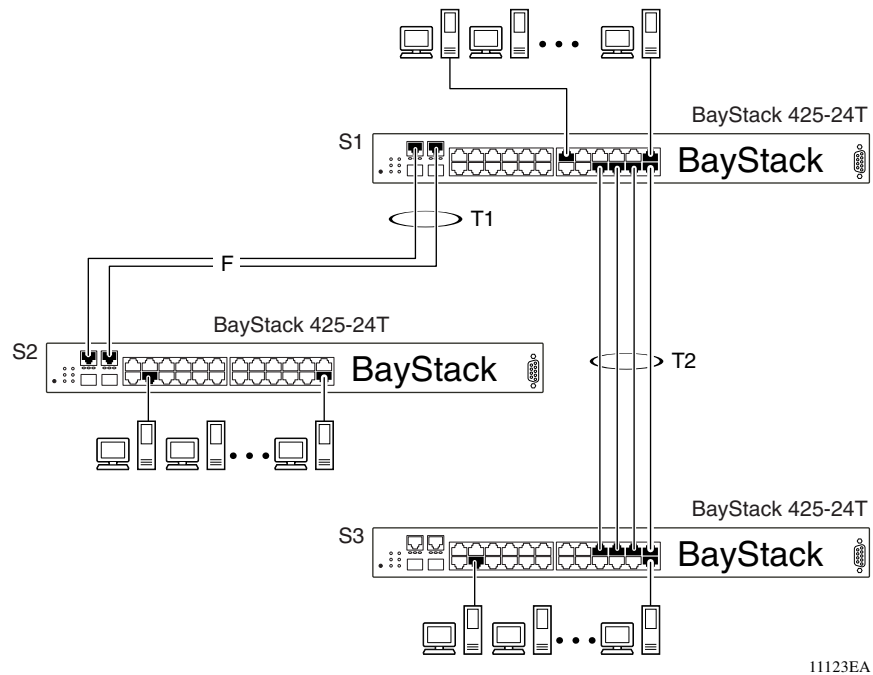
See also [Appendix C, “Quick configuration for MultiLink Trunking,” on page 211](#) for configuration flowcharts that can help you use this feature.

## MultiLink Trunks

MultiLink Trunks allow you to group from two to four switch ports together to form a link to another switch or server, thus increasing aggregate throughput of the interconnection between the devices (up to 800 Mb/s in full-duplex mode). You can configure up to six MultiLink Trunks. The trunk members can only reside on a single unit. MultiLink Trunking software detects misconfigured (or broken) trunk links and redirects traffic on the misconfigured or broken trunk link to other trunk members within that trunk.

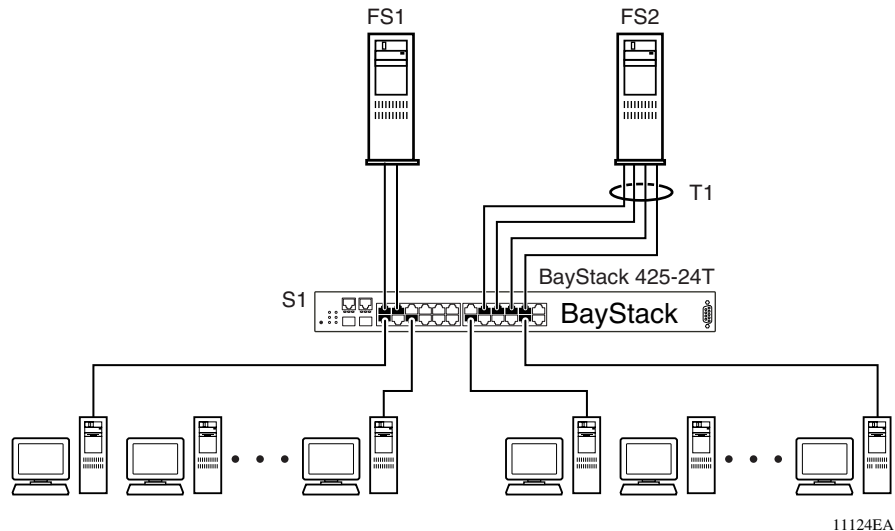
You can use the Trunk Configuration screen to create switch-to-switch and switch-to-server MultiLink Trunk links ([Figure 27](#) and [Figure 28](#)).

[Figure 27](#) shows two trunks (T1 and T2) connecting Switch S1 to switches S2 and S3.

**Figure 27** Switch-to-switch trunk configuration example

You can configure each of the trunks shown in [Figure 27](#) with up to four switch ports to provide up to 800 Mb/s aggregate bandwidth through each trunk, in full-duplex mode. As shown in this example, when traffic between switch-to-switch connections approaches single port bandwidth limitations, creating a MultiLink Trunk can supply the additional bandwidth required to improve the performance.

[Figure 28](#) shows a typical switch-to-server trunk configuration. In this example, file server FS1 uses dual MAC addresses, using one MAC address for each network interface card (NIC). For this reason, FS1 does not require a trunk assignment. FS2 is a single MAC server (with a four-port NIC) and is set up as trunk configuration T1.

**Figure 28** Switch-to-server trunk configuration example

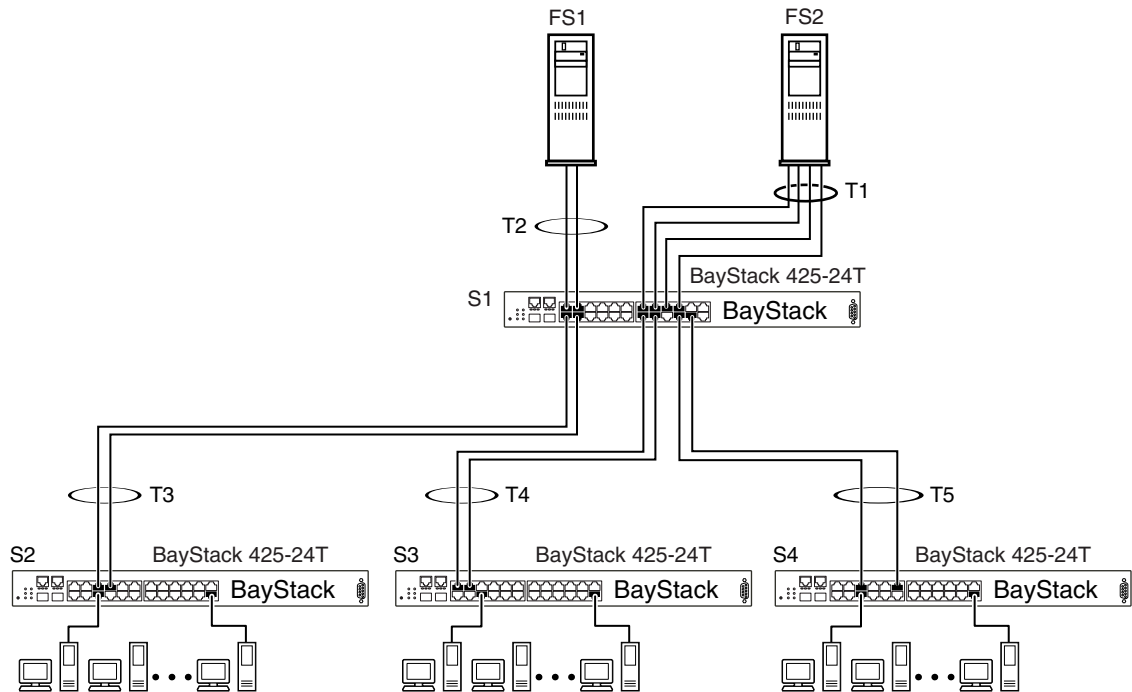
11124EA

## Client/server configuration using MultiLink Trunks

Figure 29 shows an example of how MultiLink Trunking can be used in a client/server configuration. In this example, both servers connect directly to Switch S1. FS2 is connected through a trunk configuration (T1). The switch-to-switch connections are through trunks (T2, T3, T4, and T5).

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

With spanning tree *enabled*, one of the trunks (T2 or T3) acts as a redundant (backup) trunk to Switch S2. With spanning tree *disabled*, you must configure trunks T2 and T3 into separate VLANs for this configuration to function properly. Refer to “IEEE 802.1Q VLAN workgroups” on page 66 for more information.

**Figure 29** Client/server configuration example

11125EA

The trunk configuration screens for switches S1 to S4 are shown in [“Trunk configuration screen examples”](#) following this section. For detailed information about configuring trunks, see [“MultiLink Trunk Configuration screen”](#) on page 153.

## Trunk configuration screen examples

This section shows examples of the MultiLink Trunk configuration screens for the client/server configuration example shown in [Figure 29](#). The screens show how you could set up the trunk configuration screens for switches S1 to S4. See [“Spanning tree considerations for MultiLink Trunks”](#) on page 95, and [“MultiLink Trunk Configuration screen”](#) on page 153 for more information.

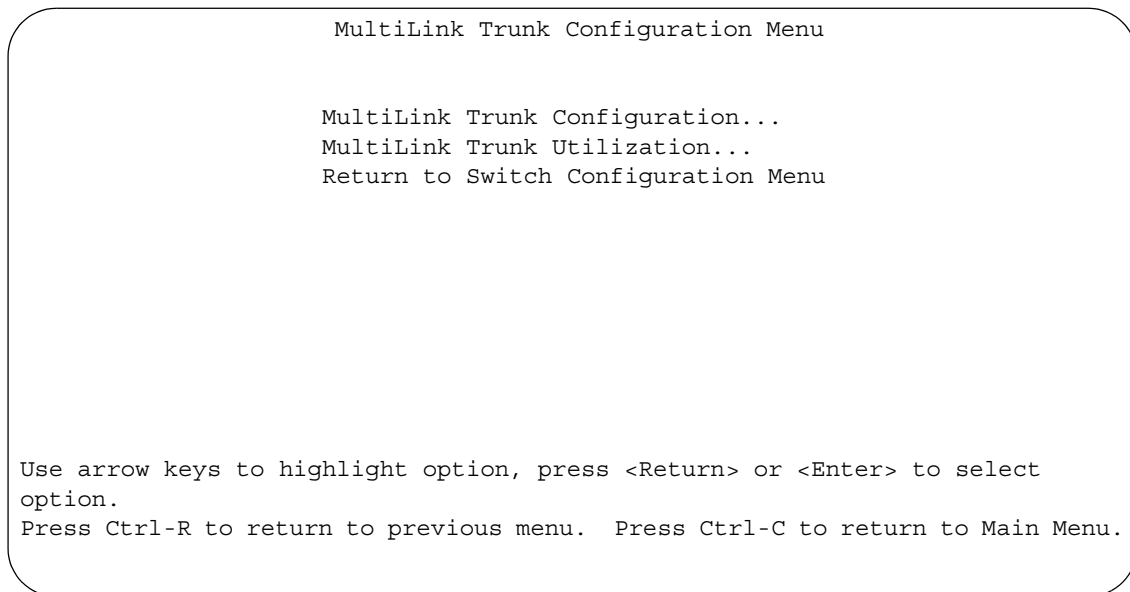
## Trunk configuration screen for Switch S1

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

To set up the S1 trunk configuration:

- Choose MultiLink Trunk Configuration (or press t) from the MultiLink Trunk Configuration Menu screen ([Figure 30](#)).

**Figure 30** Choosing the MultiLink Trunk Configuration Menu screen



The MultiLink Trunk Configuration Menu screen opens ([Figure 31](#)).

**Figure 31** MultiLink Trunk Configuration screen for Switch S1

```

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

Trunk      Trunk Name
-----
 1 [ Trunk #1 ]
 2 [ Trunk #2 ]
 3 [ Trunk #3 ]
 4 [ Trunk #4 ]
 5 [ Trunk #5 ]
 6 [ Trunk #6 ]

Use space bar to display choices or enter number. Enter 0 to delete.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

```

Switch S1 is configured as follows:

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



**Note:** The Unit value (in the Unit/Port field) is not configurable when the switch is operating standalone.

- Ports 15, 17, 19, and 21 are assigned as trunk members of trunk 1.
- Ports 25 and 26 are assigned as trunk members of trunk 2.
- Ports 2 and 4 are assigned as trunk members of trunk 3.
- Ports 14 and 16 are assigned as trunk members of trunk 4.
- Ports 22 and 24 are assigned as trunk members of trunk 5.

For detailed information about the MultiLink Trunk Configuration screen fields, see [“MultiLink Trunk Configuration screen” on page 153](#).

- **STP Learning** indicates the spanning tree participation setting for each of the trunks:
  - Trunks 1 through 4 are enabled for Normal STP Learning.
  - Trunk 5 is enabled for Fast STP Learning.

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

The Trunk Mode field values for trunks 1 to 5 are set to Basic. Source MAC addresses are statically assigned to specific trunk members for flooding and forwarding, which allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.

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

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

## Trunk configuration screen for Switch S2

As shown in [Figure 29 on page 85](#), Switch S2 is set up with two trunk configurations (T2 and T3). Both trunks connect directly to Switch S1.

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



Figure 32 shows the MultiLink Trunk Configuration screen for Switch S2.

**Figure 32** MultiLink Trunk Configuration screen for Switch S2

```

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

Trunk      Trunk Name
-----
1  [ Trunk #1 ]
2  [ Trunk #2 ]
3  [ Trunk #3 ]
4  [ Trunk #4 ]
5  [ Trunk #5 ]
6  [ Trunk #6 ]

Use space bar to display choices or enter number. Enter 0 to delete.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

```

Switch S2 is configured as follows:

- **Trunk** (read only) indicates the trunks (1 to 6) that correspond to the switch ports specified in the Trunk Members fields.
- **Trunk Members (Unit/Port)** indicates the ports that can be configured, in each row, to create the corresponding trunk:
  - Ports 25 and 26 are assigned as trunk members of trunk 1.
  - Ports 1 and 3 are assigned as trunk members of trunk 2.
- **STP Learning** indicates the spanning tree participation setting for each of the trunks. Trunks 1 and 2 are enabled for Normal STP Learning.

- **Trunk Mode** (read only) indicates the Trunk Mode for each of the trunks. The Trunk Mode field values for trunks 1 and 2 are set to Basic. Source MAC addresses are statically assigned to specific trunk members for flooding and forwarding, which allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.
- **Trunk Status** indicates the Trunk Status for each of the trunks. When set to Enabled, the configuration settings for that specific trunk are activated.
- **Trunk Name** indicates optional fields for assigning names to the corresponding configured trunks.

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

### Trunk Configuration screen for Switch S3

As shown in [Figure 29 on page 85](#), Switch S3 is set up with one trunk configuration (T4). This trunk connects directly to Switch S1.

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

[Figure 33](#) shows the MultiLink Trunk Configuration screen for Switch S3.

**Figure 33** MultiLink Trunk Configuration screen for Switch S3

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

Use space bar to display choices or enter number. Enter 0 to delete.  
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

Switch S3 is configured as follows:

- **Trunk** (read only) indicates the trunk (1 to 6) that corresponds to the switch ports specified in the Trunk Members fields.
- **Trunk Members (Unit/Port)** indicates the ports that can be configured, in each row, to create the corresponding trunk. Ports 1 and 3 are assigned as trunk members of trunk 1.
- **STP Learning** indicates the spanning tree participation setting for each of the trunks. Trunk 1 is enabled for Normal STP Learning.

- **Trunk Mode** (read only) indicates the Trunk Mode for each of the trunks. The Trunk Mode field value for trunk 1 is set to Basic. Source MAC addresses are statically assigned to specific trunk members for flooding and forwarding, which allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.
- **Trunk Status** indicates the Trunk Status for each of the trunks. When set to Enabled, the configuration settings for that specific trunk are activated.
- **Trunk Name** indicates optional fields for assigning names to the corresponding configured trunks.

### Trunk Configuration screen for Switch S4

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

As shown in [Figure 34](#), Switch S4 is set up with one trunk configuration (T5). This trunk connects directly to Switch S1.

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

[Figure 34](#) shows the MultiLink Trunk Configuration screen for Switch S4.

**Figure 34** MultiLink Trunk Configuration screen for Switch S4

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

Use space bar to display choices or enter number. Enter 0 to delete.  
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

Switch S4 is configured as follows:

- **Trunk** (read only) indicates the trunk (1 to 6) that corresponds to the switch ports specified in the Trunk Members fields.
- **Trunk Members (Unit/Port)** indicates the ports that can be configured, in each row, to create the corresponding trunk. Ports 5 and 11 are assigned as trunk members of trunk T1.
- **STP Learning** indicates the spanning tree participation setting for each of the trunks. Trunk 1 is enabled for Normal STP Learning.

- **Trunk Mode** (read only) indicates the Trunk Mode for each of the trunks. The Trunk Mode field value for trunk 1 is set to Basic. Source MAC addresses are statically assigned to specific trunk members for flooding and forwarding, which allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.
- **Trunk Status** indicates the Trunk Status for each of the trunks. When it is set to Enabled, the configuration settings for that specific trunk are activated.
- **Trunk Name** indicates optional fields for assigning names to the corresponding configured trunks.

The names chosen for this example provide meaningful information to the user (for example, S4:T5 to S1 indicates that Trunk 1, in Switch S4, connects to Switch 1).

## Before you configure trunks

When you create and enable a trunk, the trunk members (switch ports) take on certain settings necessary for correct operation of the MultiLink Trunking feature.

Before you configure your MultiLink Trunk, you must consider these settings, along with specific configuration rules, as follows:

- 1 Read the configuration rules provided in the next section, [“Spanning tree considerations for MultiLink Trunks” on page 95](#).
- 2 Determine which switch ports (up to four) are to become *trunk members* (the specific ports making up the trunk). A minimum of two ports are required for each trunk.

Ensure that the chosen switch ports are set to Enabled, using either the Port Configuration screen (see [“Port Configuration screen” on page 145](#)) or network management.

Trunk member ports must have the same VLAN configuration.

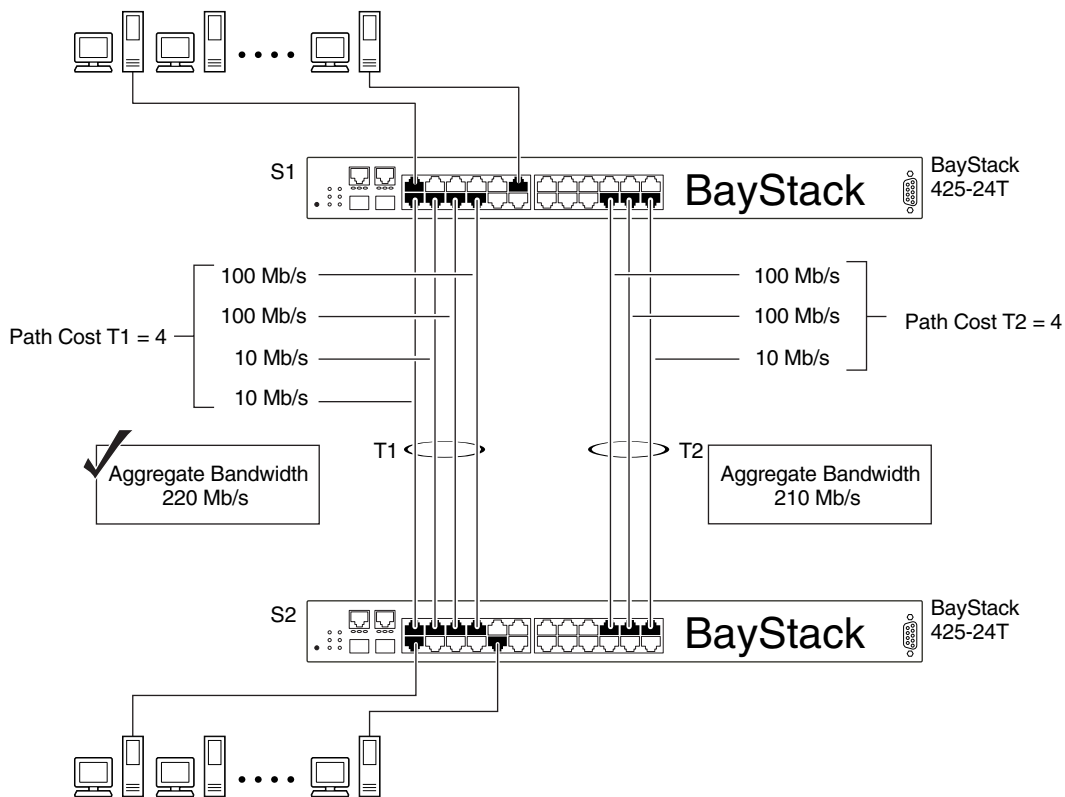
- 3 All network cabling should be complete and stable before configuring any trunks, to avoid configuration errors.
- 4 Consider how the existing spanning tree will react to the new trunk configuration (see [“Spanning tree considerations for MultiLink Trunks” on page 95](#)).

- 5 Consider how existing VLANs will be affected by the addition of a trunk.
- 6 After completing the above steps, see [“MultiLink Trunk Configuration screen” on page 153](#) for screen examples and field descriptions that will help you configure your MultiLink Trunks.

## Spanning tree considerations for MultiLink Trunks

The spanning tree Path Cost parameter is recalculated based on the aggregate bandwidth of the trunk. For example, [Figure 35](#) shows a four-port trunk (T1) with two port members operating at 100 Mb/s and two at 10 Mb/s. Trunk T1 provides an aggregate bandwidth of 220 Mb/s. The Path Cost for T1 is 4 (Path Cost = 1000/LAN speed, in Mb/s). Another three-port trunk (T2) is configured with an aggregate bandwidth of 210 Mb/s, with a comparable Path Cost of 4. When the Path Cost calculations for both trunks are equal, the software chooses the trunk with the larger aggregate bandwidth (T1) to determine the most efficient path.

Figure 35 Path Cost arbitration example



11126EA

The switch can also detect trunk member ports that are physically misconfigured. For example, in [Figure 36](#), trunk member ports 2, 4, and 6 of Switch S1 are configured *correctly* to trunk member ports 7, 9, and 11 of Switch S2. The Spanning Tree Port Configuration screen for each switch shows the port state field for each port in the Forwarding state.



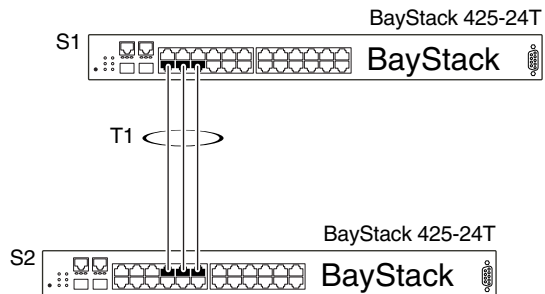
Figure 36 Example 1: correctly configured trunk

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

More...

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

S1 Port Configuration screen



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

More...

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

S2 Port Configuration screen

11127EA

If Switch S2's trunk member port 11 is physically disconnected and then reconnected to port 13, the Spanning Tree Port Configuration screen for Switch S1 changes to show port 6 in the Blocking state (Figure 37).

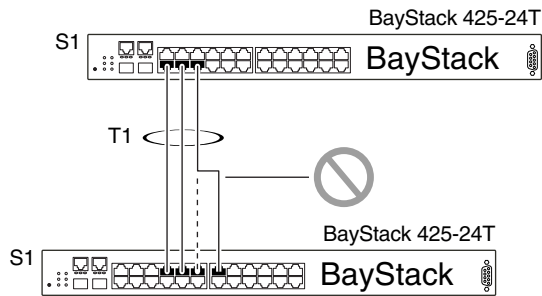
Figure 37 Example 2: detecting a misconfigured port

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

More...

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

S1 Port Configuration screen



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

More...

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

S2 Port Configuration screen

11128EA

## Additional tips about the MultiLink Trunking feature

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

All configured trunks are indicated in the Spanning Tree Configuration screen. The 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 you set the Trunk Status field to Enabled.

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

For more information about using the MultiLink Trunking feature, see [“MultiLink Trunk Configuration Menu screen” on page 151](#).

See also [Appendix C, “Quick configuration for MultiLink Trunking,” on page 211](#) for a configuration flowchart that can help you use this feature.

## Port mirroring

You can designate one of your switch ports to monitor ingress traffic on a single specified switch port (port-based).



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

---

[Figure 38](#) provides a sample Port Mirroring Configuration screen. Note that the displayed screens do not show all of the screen prompts that precede some actions.

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

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

**Figure 38** Port Mirroring Configuration port-based screen example

```
Port Mirroring Configuration

Monitoring Mode: [ Disabled ]
Monitor Unit/Port: [ / ]

Unit/Port X: [ / ]

Currently Active Port Mirroring Configuration
-----
Monitoring Mode: Disabled

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

---

## Chapter 3

# Using the console interface

---

This chapter describes how to configure and manage the BayStack 420/425 using the menu-driven console interface (CI).

This chapter covers the following topics:

- [“Accessing the CI menus and screens,”](#) next
- [“Using the CI menus and screens”](#) on page 102
- [“Main menu”](#) on page 104

## Accessing the CI menus and screens

You can access the CI menus and screens locally through a console terminal attached to your BayStack 425 Switch, remotely through a dial-up modem connection, or in-band through a Telnet session (see [“Console port”](#) on page 29). You can connect your console cable into any unit in a BayStack 425 Switch-only stack for a unified stack interface. For the mixed stack management functions to become fully operational, you must connect your console terminal into a BayStack 425 Switch port within your mixed stack.



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

---

For information about SNMP, see your network management documentation.

## Using the CI menus and screens

The CI menus and screens provide options that allow you to configure and manage BayStack 425 switches. 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.

The Console port default settings are: 9600 baud with eight data bits, one stop bit, and no parity as the communications format, with flow control set to disabled.

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

### Navigating the CI menus and screens

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

To select a menu option:

- 1 Use the arrow keys to highlight the option name.
- 2 Press [Enter].

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

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

To toggle between values in a form:

- 1 Use the spacebar to highlight the value.
- 2 Press [Enter].

To clear a string field:

- 1 Position the cursor in the string field.
- 2 Press [Ctrl]-K.

To return to the previous menu, press [Ctrl]-R.

To go to the next screen in a series, press [Ctrl]-N.

To return to the main menu at any time, press [Ctrl]-C.

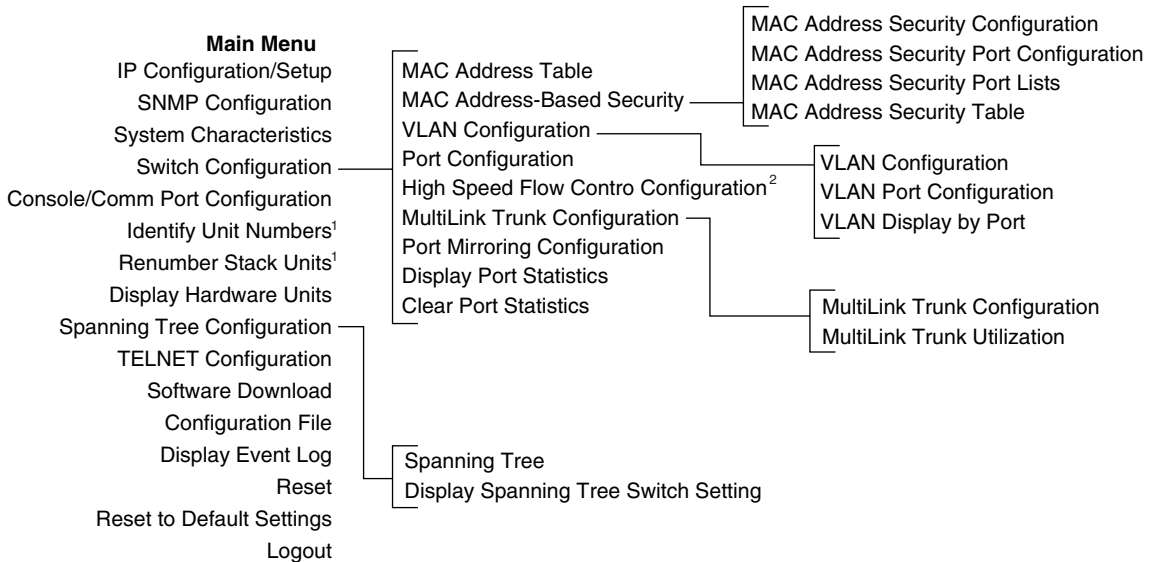
Press [Backspace] to delete entered text.

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

## Screen fields and descriptions

Figure 39 shows a map of the CI screens. The remainder of this chapter describes the CI screens and their fields, beginning with the main menu.

**Figure 39** Map of console interface screens



<sup>1</sup> Only appears when the switch is participating in a stack configuration.

<sup>2</sup> Only appears when a gigabit MDA is installed in one or more units in a stack configuration.

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



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

---

## Main menu

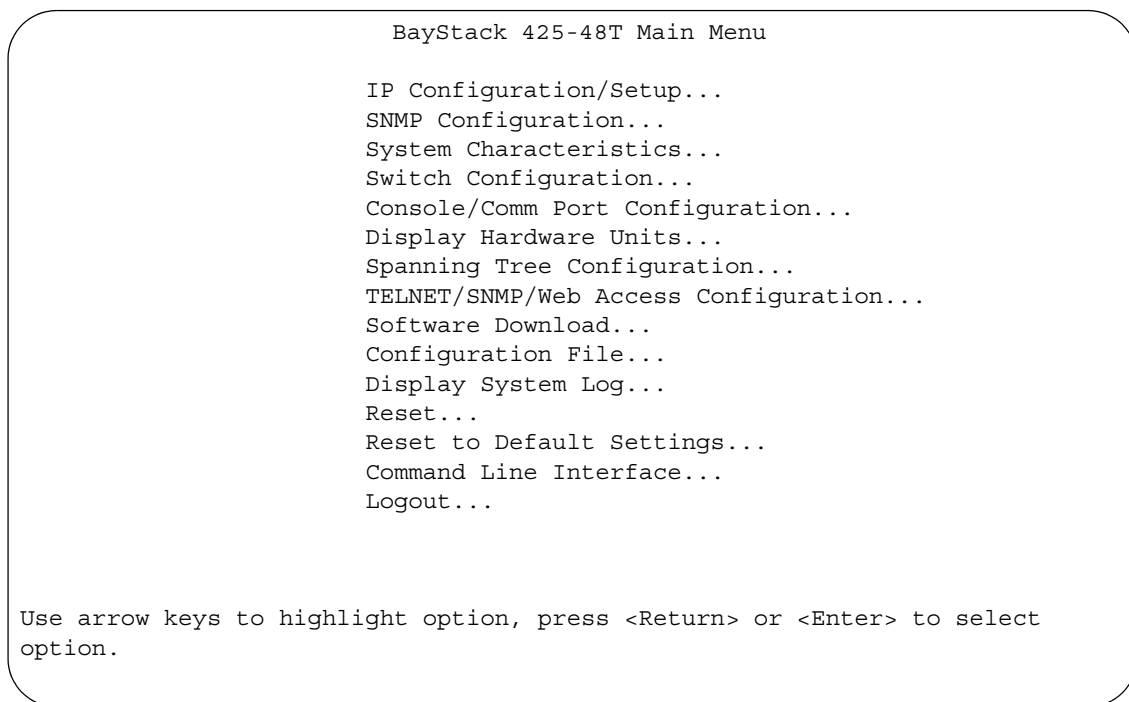
This section describes the options available from the CI main menu ([Figure 40](#)). The CI screens and submenus for these options are described in the following sections.



**Note:** Some menu options shown in this main menu example and in other screen examples in this chapter may not appear on your screen, depending on the switch options installed. However, the full menu options are shown in the screen examples and described in the following sections.

---



**Figure 40** Console interface main menu

[Table 11](#) describes the CI main menu options.







**Table 11** Console interface main menu options

Option	Description
<b>IP Configuration/Setup...</b>	Displays the IP Configuration/Setup screen (see <a href="#">“IP Configuration/Setup screen” on page 108</a> ). This screen allows you to set or modify IP configuration parameters.
<b>SNMP Configuration...</b>	Displays the SNMP Configuration screen (see <a href="#">“SNMP Configuration screen” on page 113</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 and the link Up/down trap, set the IP address of trap receivers, and set the trap community strings.

**Table 11** Console interface main menu options (continued)

Option	Description
<b>System Characteristics...</b>	Displays the System Characteristics screen (see <a href="#">“System Characteristics screen” on page 115</a> ). This screen allows you to view switch characteristics, including number of resets, power status, hardware and firmware version, and MAC address. This screen also contains three user-configurable fields: sysContact, sysName, and sysLocation. When the switch is part of a stack configuration, this screen also displays the base unit identification, the number of units configured in the stack, and the local unit stack number.
<b>Switch Configuration...</b>	Displays the Switch Configuration Menu screen (see <a href="#">“Switch Configuration Menu screen” on page 118</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, Display Port Statistics, Clear All Port Statistics, Display System Log, and Stack Operational Mode.
<b>Console/Comm Port Configuration...</b>	Displays the Console/Comm Port Configuration screen (see <a href="#">“Console/Comm Port Configuration screen” on page 165</a> ). This screen allows you to configure and modify the console/Comm port parameters, including the console port speed and password settings for the switch and stack operation.
<b>Spanning Tree Configuration...</b>	Displays the Spanning Tree Configuration Menu (see <a href="#">“Spanning Tree Configuration Menu screen” on page 174</a> ). This menu provides the following options: Spanning Tree Port Configuration, Display Spanning Tree Switch Settings.
<b>TELNET Configuration...</b>	Displays the TELNET Configuration screen (see <a href="#">“TELNET Configuration screen” on page 182</a> ). This screen allows you to set your switch to enable a user at a remote console terminal to communicate with the BayStack 420/425 as if the console terminal were directly connected to it. You can have up to four active Telnet sessions running at one time in either a standalone switch or a stack configuration.
<b>Software Download...</b>	Displays the Software Download screen (see <a href="#">“Software Download screen” on page 184</a> ). This screen allows you to revise the BayStack 420/425 software image that is located in nonvolatile flash memory.
Configuration File	Displays the Configuration File Download/Upload screen (see <a href="#">“Configuration File Download/Upload screen” on page 187</a> ). This screen allows you to store your switch/stack configuration parameters on a TFTP server. You can retrieve the configuration parameters for automatically configuring a replacement switch or stack with the same configuration when required.
<b>Display System Log</b>	Displays the System Log screen (see <a href="#">“System Log screen” on page 163</a> ).

**Table 11** Console interface main menu options (continued)

Option	Description
<b>Reset</b>	<p>Resets the switch with the current configuration settings. This option is followed by a screen prompt that precedes the action. Enter Yes to reset the switch; enter No to abort the option:</p> <ul style="list-style-type: none"> <li>• If the switch is participating in a stack configuration, you can reset the entire stack.</li> <li>• When you select this option, the switch resets, runs a self-test, then displays the Nortel Networks logo screen. Press [Ctrl]-Y to access the BayStack 420/425 main menu.</li> </ul>
<b>Reset to Default Settings</b>	<p>Resets the switch to the factory default configuration settings. This option is followed by a screen prompt that precedes the action. Enter Yes to reset the switch to the factory default configuration settings; enter No to abort the option:</p> <ul style="list-style-type: none"> <li>• If the switch is participating in a stack configuration, you can reset the entire stack.</li> <li>• When you select this option, the switch resets, runs a self-test, then displays the Nortel Networks logo screen. Press [Ctrl]-Y to access the BayStack 420/425 main menu.</li> </ul>
	<p> <b>Caution:</b> If you choose the Reset to Default Settings option, all of your configured settings will be replaced with factory default settings when you press [Enter]</p>
	<p> <b>Achtung:</b> 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.</p>
	<p> <b>Attention:</b> Si vous restaurez la configuration usine, votre configuration courante sera remplacée par la configuration usine dès que vous appuierez sur [Entrée].</p>
	<p> <b>Precaución:</b> Si selecciona el comando Restaurar valores predeterminados, todos los valores de configuración se sustituirán por los valores predeterminados en fábrica al pulsar [Intro].</p>
	<p> <b>Attenzione:</b> 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].</p>
	<p> 注意: 「デフォルトの設定にリセット」コマンドを選択すると、現在のコンフィグレーションされた設定は、[Enter]を押したとき、工場出荷時の設定に変更されます。</p>
<b>Logout</b>	<p>Allows a user in a Telnet session or a user working at a password-protected console terminal to terminate the session.</p>

## IP Configuration/Setup screen

The IP Configuration/Setup screen (Figure 41) allows you to set or modify the BayStack 420/425 IP configuration parameters. Data that you enter in the user-configurable fields takes effect as soon as you press [Enter].

To open the IP Configuration/Setup screen:

- ➔ Choose IP Configuration/Setup (or press i) from the main menu.

**Figure 41** IP Configuration/Setup screen

```

                                IP Configuration/Setup

                                BootP Request Mode: [ BootP Disabled ]

                                Configurable          In Use          Last BootP
                                -----
In-Band Stack IP Address: [ 0.0.0.0 ]           0.0.0.0           0.0.0.0
In-Band Switch IP Address: [ 134.177.224.102 ] 134.177.224.102  0.0.0.0
In-Band Subnet Mask:      [ 255.255.255.0 ]   255.255.255.0   0.0.0.0

Default Gateway:          [ 134.177.224.1 ]   134.177.224.1   0.0.0.0

IP Address to Ping:      [ 10.30.40.1 ]
Start Ping:              [ No ]

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


```

Table 12 describes the IP Configuration/Setup screen fields.



**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 110 for more information.)

**Table 12** IP Configuration/Setup screen fields

Field	Description
<b>BootP Request Mode</b>	<p>One of four modes of operation for BootP. (See <a href="#">“Choosing a BootP request mode”</a> on page 110 for details about the four modes.)</p> <p>Default Value      BootP Disabled</p> <p>Range                BootP Disabled, BootP When Needed, BootP Always, BootP or Last Address</p>
<b>Configurable</b>	Column header for the user-configurable IP configuration 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 IP configuration 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 IP configuration obtained from the last BootP reply received.
<b>In-Band Stack IP Address</b>	<p>The in-band <i>stack</i> IP address field. This field is not required for the operation of the standalone switch.</p> <p>Default Value      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, between 0 and 255, separated by a decimal point</p>
<b>In-Band Switch IP Address</b>	<p>The in-band IP address of the switch. This field is not required for the operation of the stack. This field can not use the same IP address used for the stack.</p> <p>Default Value      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, between 0 and 255, separated by a decimal point</p> <p> <b>Note:</b> When the IP address is entered in the In-Band IP Address field, and the In-Band Subnet Mask field value is not present, the software provides an <i>in-use</i> default value for the In-Band Subnet Mask field that is based on the class of the IP address entered in the In-Band IP Address field.</p>

**Table 12** IP Configuration/Setup screen fields (continued)

Field	Description
<b>In-Band Subnet Mask</b>	<p>The subnet address mask associated with the in-band IP address shown on the screen (see In-Band Switch IP address field). 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.</p> <p>Default Value      0.0.0.0 (no subnet mask assigned)</p> <p>Range                Four-octet dotted-decimal notation, where each octet is represented as a decimal value, between 0 and 255, separated by a decimal point</p>
<b>Default Gateway</b>	<p>The IP address of the default gateway.</p> <p>Default Value      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, between 0 and 255, separated by a decimal point</p>

## Choosing a BootP request mode

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

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



**Note:** Whenever the switch is broadcasting BootP requests, the BootP process will eventually time out if a reply is not received. When the process times out, the BootP request mode automatically changes to BootP Disabled mode. To restart the BootP process, change the BootP request mode to any of the three following modes:

- BootP When Needed
- BootP Always
- 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-use 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 switch 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 screen

The SNMP Configuration screen (Figure 42) allows you to set or modify the SNMP configuration parameters.

To open the SNMP Configuration screen:

- ➔ Choose SNMP Configuration (or press m) from the main menu.

**Figure 42** SNMP Configuration screen

```
SNMP Configuration

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

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

Authentication Trap:        [ Enabled ]
AutoTopology:                [ Enabled ]

Enter text, press <Return> or <Enter> when complete.
```

Table 13 describes the SNMP Configuration screen fields.

**Table 13** SNMP Configuration screen fields

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

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

## System Characteristics screen

The System Characteristics screen ([Figure 43](#)) allows you to view system characteristics and contains three user-configurable fields: sysContact, sysName, and sysLocation.

To open the System Characteristics screen:

- ➔ Choose System Characteristics (or press s) from the main menu.

**Figure 43** System Characteristics screen

```

                                System Characteristics

Operation Mode:  Stack, Unit # 1
Size Of Stack:  2
Base Unit:      1

MAC Address:    00-09-97-A2-9C-5F

Reset Count:    18
Last Reset Type: Management Reset
Power Status:   Primary Power
Local GBIC Type: port 25, None

sysDescr:       BayStack 425-24T HW:0B          FW:3.1.0.5    SW:v3.1.0.00
sysObjectID:    1.3.6.1.4.1.45.3.57.2
sysUpTime:      11 days, 09:33:29
sysServices:    3
sysContact:     [ Burke ]
sysName:        [ BayStack 425-24T ]
sysLocation:    [ ]

Enter text, press <Return> or <Enter> when complete.

```

**Table 14** System Characteristics screen fields

Field	Description
<b>Operation Mode</b>	Read-only field that indicates the operation mode of the unit, for example: <ul style="list-style-type: none"> <li>When the unit is part of a stack configuration, the (read-only) field indicates the unit is operational in a stack, and lists the current unit number of this switch. In this example (see <a href="#">Figure 43 on page 116</a>), the current unit number is Unit 2.</li> <li>When the unit is <i>not</i> part of a stack configuration (operating standalone), the read-only field indicates the unit is operating as a switch. When in this operation mode, the Size of Stack and Base Unit fields (see following description) do not appear.</li> </ul>
<b>Size of Stack</b>	This read-only field only appears when the switch is participating in a stack configuration. This field indicates the number of units configured in the stack configuration (1 to 8 units maximum).
<b>Base Unit</b>	This read-only field only appears when the switch is participating in a stack configuration. This field indicates the unit number of the switch that is currently operating as the base unit.

**Table 14** System Characteristics screen fields (continued)

Field	Description
<b>MAC Address</b>	The MAC address of the switch or, when the switch is participating in a stack configuration, the MAC address of the stack configuration.
<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 Value 1 Range 0 to $2^{32} - 1$ (4,294,967,295)
<b>Last Reset Type</b>	A read-only field that indicates the last type of reset. Default Value Power Cycle Range Power Cycle, Software Download, Management Reset, Management Factory Reset
<b>Power Status</b>	A read-only field that indicates the current power source (primary, RPSU, or both). Default Value Primary Power Range Primary Power, Redundant Power, Primary and Redundant Power
<b>Local GBIC Type</b>	A read-only field that indicates the GBIC type that is configured in this unit.
<b>sysDescr</b>	A read-only field that specifies hardware and software versions.
<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 Value 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 Value 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 Value 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 Menu screen

The Switch Configuration Menu screen ([Figure 44](#)) 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 ([Table 15](#)).

**Figure 44** Switch Configuration Menu screen

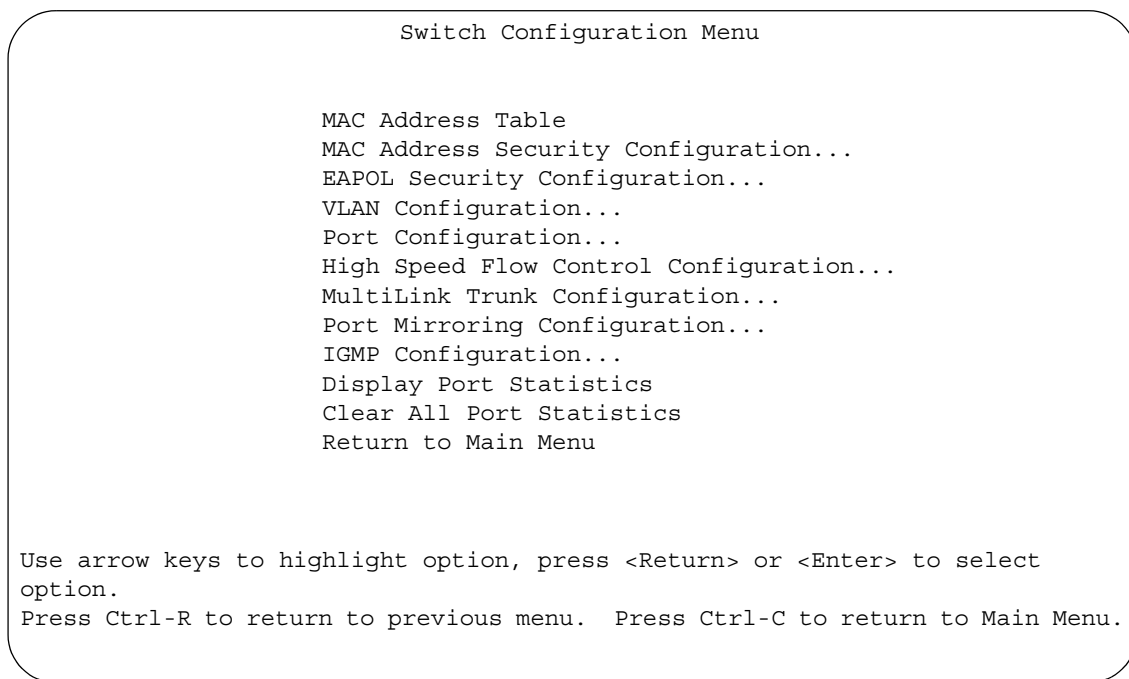


Table 15 describes the Switch Configuration Menu options.

**Table 15** Switch Configuration Menu options

Option	Description
<b>MAC Address Table</b>	Displays the MAC Address Table screen (see <a href="#">“MAC Address Table screen” on page 120</a> ). This screen allows you to view all MAC addresses and their associated port or trunk that the switch has learned, or to search for a particular MAC address (to see if the switch has learned the address).
<b>MAC Address Security Configuration...</b>	Displays the MAC Address Security Configuration menu (see <a href="#">“MAC Address Security Configuration Menu screen” on page 122</a> ). This screen allows you to set up the MAC address security feature and provides the following options: MAC Address Security Configuration, MAC Address Security Port Configuration, MAC Address Security Port Lists, and MAC Address Security Table. This menu allows you to enable and disable security features on the port and trunk levels.
<b>VLAN Configuration...</b>	Displays the VLAN Configuration Menu (see <a href="#">“VLAN Configuration Menu screen” on page 136</a> ). This menu provides the following options: VLAN Configuration, VLAN Port Configuration, VLAN Display by Port, MAC-SA, and Return to Switch Configuration Menu screen. This menu allows you to create and modify VLANs.
<b>Port Configuration...</b>	Displays the Port Configuration screen (see <a href="#">“Port Configuration screen” on page 145</a> ). This screen allows you to configure a specific switch port, all switch ports or, when in a stack configuration, all stack ports.
<b>High Speed Flow Control Configuration...</b>	Displays the High Speed Flow Control Configuration screen.
<b>MultiLink Trunk Configuration...</b>	Displays the MultiLink Trunk Configuration Menu (see <a href="#">“MultiLink Trunk Configuration Menu screen” on page 151</a> ). This menu provides the following options: MultiLink Trunk Configuration, MultiLink Trunk Utilization, and Return to Switch Configuration Menu screen. This menu allows you to create and modify trunks, and to monitor the bandwidth utilization of configured trunks.
<b>Port Mirroring Configuration...</b>	Displays the Port Mirroring Configuration screen (see <a href="#">“Port Mirroring Configuration screen” on page 157</a> ). This screen allows you to designate a single switch port as a traffic monitor for one specific port.
<b>Display Port Statistics</b>	Displays the Port Statistics screen (see <a href="#">“Port Statistics screen” on page 159</a> ). This screen allows you to view detailed information about any switch port.

**Table 15** Switch Configuration Menu options (continued)

Option	Description
<b>Clear All Port Statistics</b>	<p>Allows you to clear all port statistics.</p> <p>This option is followed by screen prompts that precede a choice of the actions:</p> <ul style="list-style-type: none"> <li>• If the switch is operating <i>standalone</i>, choose one of the following: <ul style="list-style-type: none"> <li>• Yes, to clear all port statistics for all switch ports</li> <li>• No, to abort the option</li> </ul> </li> <li>• If the switch is <i>participating in a stack configuration</i>, choose one of the following: <ul style="list-style-type: none"> <li>• Clear all port statistics for a specific unit in the stack</li> <li>• Clear all port statistics for the entire stack</li> <li>• No, to abort the option</li> </ul> </li> </ul>
<b>Display System Log</b>	<p>In a stack environment, displays the system log screen, which provides information obtained through volatile or nonvolatile RAM. See <a href="#">“System Log screen” on page 163</a>.</p>

## MAC Address Table screen

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

The MAC Address Table 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 screen” on page 157](#)).

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



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



**Figure 45** describes the MAC Address Table screen fields.

```

MAC Address Table

Aging Time:                [ 300 seconds ]
Find an Address:           [ 00-00-00-00-00-00 ]
Select VLAN ID:           [ 1 ]
Number of addresses:       7

00-00-A2-8D-58-50          Port: 1
00-02-E3-05-3B-B5          Port: 1
00-04-DC-76-8A-03          Port: 1
00-0F-6A-7D-C0-A0
00-0F-6A-82-31-41          Port: 1
00-A0-CC-58-EA-BE          Port: 1
00-C0-4F-0C-4E-24          Port: 1
08-00-20-7C-86-AD          Port: 1

No more addresses.
Enter number, press <Return> or <Enter> when complete.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

```

**Table 16** MAC Address Table screen fields

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

## MAC Address Security Configuration Menu screen

The MAC Address Security Configuration Menu screen (Figure 46) 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 448 MAC addresses that are authorized to access the switch. You can also specify the ports that each MAC address is allowed to access. The options for allowed port access include: NONE, ALL, and single or multiple ports that are specified in a list, for example, 1-4, 6, 9, etc. 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.

To open the MAC Address Security Configuration screen:

- ➔ Choose MAC Address Security Configuration from the Switch Configuration Menu.

**Figure 46** MAC Address Security Configuration Menu screen

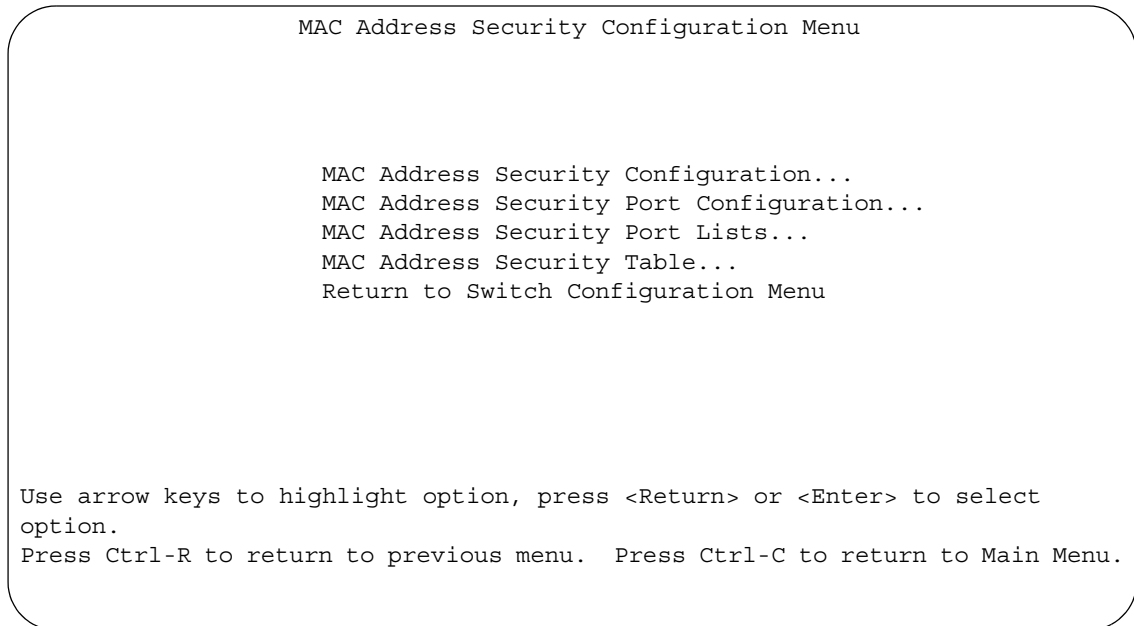


Table 17 describes the MAC Address Security Configuration Menu options.

**Table 17** MAC Address Security Configuration Menu options

Option	Description
<b>MAC Address Security Configuration...</b>	Displays the MAC Address Security Configuration screen (see <a href="#">“Table 17 describes the MAC Address Security Configuration Menu options.” on page 124</a> ). This screen allows you to Enable or Disable the MAC Address Security feature.
<b>MAC Address Security Port Configuration...</b>	Displays the MAC Address Security Port Configuration screen (see <a href="#">“MAC Address Security Port Configuration screen” on page 127</a> ”). This screen allows you to Enable or Disable MAC Security for each port.
<b>MAC Address Security Port Lists...</b>	Displays the MAC Address Security Port Lists screen (see <a href="#">“MAC Address Security Port Lists screens” on page 130</a> ). This screen allows you to create port lists that can be used as an <i>allowed source port list</i> for a MAC address in the MAC Address Security Table screen.
<b>MAC Address Security Table...</b>	Displays the MAC Address Security Table screen (see <a href="#">“MAC Address Security Table screens” on page 134</a> ). This screen allows you to specify the MAC addresses that are allowed to access the switch.
<b>Return to Switch Configuration Menu...</b>	Exits the MAC Address Security Configuration Menu screen and displays the Switch Configuration Menu screen.

The MAC Address Security Configuration screen ([Figure 47](#)) allows you to enable or disable the MAC address security feature and to specify the appropriate system responses to any unauthorized network access to your switch.

Choose MAC Address Security Configuration from the MAC Address Security Configuration Menu to open the MAC Address Security Configuration screen.

**Figure 47** MAC Address Security Configuration screen

```

MAC Address Security Configuration

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

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

MAC Security Table:

Clear by Ports: [   ]

Learn by Ports: [   ]

Current Learning Mode:                [ Disabled ]

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

```

[Table 18](#) describes the MAC Address Security Configuration screen fields.

**Table 18** MAC Address Security Configuration screen fields

Field	Description
<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. If the software detects a 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>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>

**Table 18** MAC Address Security Configuration screen fields (continued)

Field	Description
<b>Partition Port on Intrusion Detected:</b>	<p>This field value determines how the switch reacts to an intrusion event. When an intrusion even is detected (see MAC Address Security field description) the specified switch port is set to Disabled (partitioned from other switch ports).</p> <p>When the 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.</li> <li>• Forever - the port becomes disabled, and remains disabled (partitioned). The Partition Time field cannot be used 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 screen" on page 145</a>).</p> <p>Default            Disabled</p> <p>Range             Disabled, Enabled, Forever</p>
<b>Partition Time</b>	<p>This field appears only when the Partition Port on Intrusion Detected field is set to enabled. This field determines the length of time a partitioned port remains disabled. 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>
<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 Configuration screen" on page 113</a>).</p> <p>Default            Disabled</p> <p>Range             Disabled, Enabled</p>

**Table 18** MAC Address Security Configuration screen fields (continued)

Field	Description
<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 screens</a>” on page 134). 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 an 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, 1/1, 2/6, 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 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, 1/1-4, 2/6, 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 448 MAC address entries allowed). If you exceed the limit of 448 entries, the system prompts you with an alert message.</p> <p>Default            Disabled</p> <p>Range             Disabled, Enabled</p>

## MAC Address Security Port Configuration screen

The MAC Address Security Port Configuration screens ([Figure 48](#) and [Figure 49](#)) allow you to set or modify your MAC address port security configuration on a per port basis.

To open the MAC Address Security Port Configuration screen:

- ➔ Choose MAC Address Security Port Configuration from the MAC Address Security Configuration Menu.

**Figure 48** MAC Security Port Configuration screen (1 of 2)

```
MAC Security Port Configuration

Port      Trunk      Security
-----
 1         [ Disabled ]
 2         [ Disabled ]
 3         [ Disabled ]
 4         [ Disabled ]
 5         [ Disabled ]
 6         [ Disabled ]
 7         [ Disabled ]
 8         [ Disabled ]
 9         [ Disabled ]
10        [ Disabled ]
11        [ Disabled ]
12        [ Disabled ]
13        [ Disabled ]
14        [ Disabled ]

More...
```

Press Ctrl-N to display next screen.  
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 49** MAC Security Port Configuration screen (2 of 2)

MAC Security Port Configuration		
Port	Trunk	Security
15		[ Disabled ]
16		[ Disabled ]
17		[ Disabled ]
18		[ Disabled ]
19		[ Disabled ]
20		[ Disabled ]
21		[ Disabled ]
22		[ Disabled ]
23		[ Disabled ]
24		[ Disabled ]
25		[ Disabled ]
26		[ Disabled ]
27		[ Disabled ]
28		[ Disabled ]

More...

Press Ctrl-N to display next screen. Press Ctrl-P to display previous screen. 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.

[Table 19](#) describes the MAC Security Port Configuration screen fields.

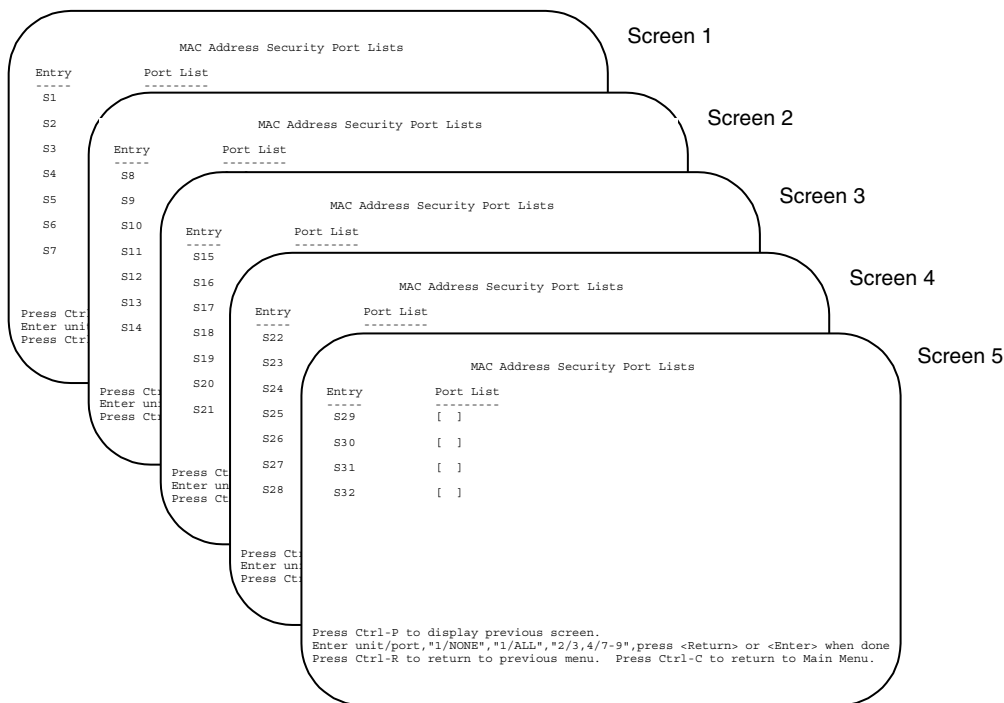
**Table 19** MAC Security Port Configuration screen fields

Field	Description
<b>Port</b>	Displays a numbered port list.
<b>Trunk</b>	Displays the trunk number if the port is a member of that trunk. Default          blank field
<b>Security</b>	This field value determines whether or not security is enabled or disabled on the port level or switch level. Default          Disabled Range            Disabled, Enabled

## MAC Address Security Port Lists screens

The MAC Address Security Port Lists screens allow you to create port lists that can be used as *allowed source port lists* for a specified MAC address in the MAC Address Security Table screen. You can create as many as 32 port lists, using up to five MAC Address Security Port Lists screens (see [Figure 50](#)).

**Figure 50** MAC Address Security Port Lists screens



To open the MAC Address Security Lists screen:

- ➔ Choose MAC Address Security Lists from the MAC Address Security Configuration Menu.

[Figure 51](#) shows the options allowed for port access, which includes: NONE, ALL, and ports that are specified in a list (for example, 1/1, 2/6, etc.). Refer to Port List syntax for more information.

**Figure 51** MAC Address Security Port Lists screen

MAC Address Security Port Lists	
Entry	Port List
S1	[ ]
S2	[ ]
S3	[ ]
S4	[ ]
S5	[ ]
S6	[ ]
S7	[ ]

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.

[Table 20](#) describes the MAC Address Security Port Lists screen fields.

**Table 20** MAC Address Security Port Lists screen fields

Field	Description
<b>Entry</b>	This field indicates the port list number (S1 to S32) that corresponds to the values you set in the Port List field.
<b>Port List</b>	This field allows you to create a port list that you can use as an “Allowed Source” in the MAC Address Security Table screen.

## Port list syntax

When you enter a port list in a stack configuration, you must specify either a unit/port list, NONE, or ALL. In a stack configuration, ALL indicates all of the stack port; whereas, in a standalone scenario, ALL indicates all of the switch ports.



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

---

A unit/port number list is composed of one or more list items, each of which can be a single number or a range of numbers (where the numbers represents one or more ports). If a list item is preceded by a number and then a slash (/), the number represents a stack unit.

For example, 1/1-7,2/1-7,2/9,3/1-4,4/12 is a valid unit/port number list (see entry S1 in [Figure 51 on page 131](#)). It represents the following port order:

- Unit 1: ports 1 to 7
- Unit 2: ports 1 to 7 and port 9
- Unit 3: ports 1 to 4
- Unit 4: port 12

## Accelerator keys for repetitive tasks

You can use certain keystrokes as “accelerator keys” to help speed up repetitive tasks. For example, suppose you want to modify the Port List field in the MAC Address Security Port List screen ([Figure 51 on page 131](#)). You can modify the port list in any of the following ways:

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

### *Adding a new port to an existing port number list*

In the example shown in [Figure 51 on page 131](#), S3 shows the Port List field values as:

1/3,2/7,3/1-4

If you want to add another port (for example, port **2/9**) to the existing port number list, you could highlight the field and then type another port list, including the new port number 1/3,2/7,**2/9**,3/1-4 [Return]. This method can be cumbersome.

As an alternative method instead, you can highlight the field and then enter +2/9 [Return]. The existing field keeps the previous list and adds the new port number (2/9) between ports 2/7 and 3/14.

(If you choose to add port 2/8 to the existing port number list, the field accepts the new port 2/8 but shows the new port number list field as: 1/3,2/7-8,3/1-4.)

### *Removing a port from an existing port number list*

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

### *Copying an existing field into an adjacent field*

You can use the period (.) character to copy a previously entered field value into the field directly next to it. For example, to copy the Allowed Source S3 (shown in [Figure 51 on page 131](#)) into the next field (entry 6):

- 1 Enter a MAC address into the next MAC address field.
- 2 Highlight the (blank) Allowed Source field.
- 3 Enter the period (.) character and click Return.

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





**Table 21** MAC Address Security Table screen fields (continued)

Field	Description
	Range A range of 6 Hex Octets, separated by dashes (multicast <sup>1</sup> and broadcast addresses are not allowed).
<b>Allowed Source</b>	Allows you to specify the ports that each MAC address is allowed to access. The options for the Allowed Source field include a single unit/port number or a port list value that you have previously configured in the MAC Address Security Port Lists screen.
	Default - (Blank field)
	Range A single unit/port or a port list value (for example, 1/3, 1/6, 3/4, S1, S5, etc.).

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

## VLAN Configuration Menu screen

The VLAN Configuration Menu screen ([Figure 54](#)) allows you to select the appropriate screen to configure up to 32 VLANs.

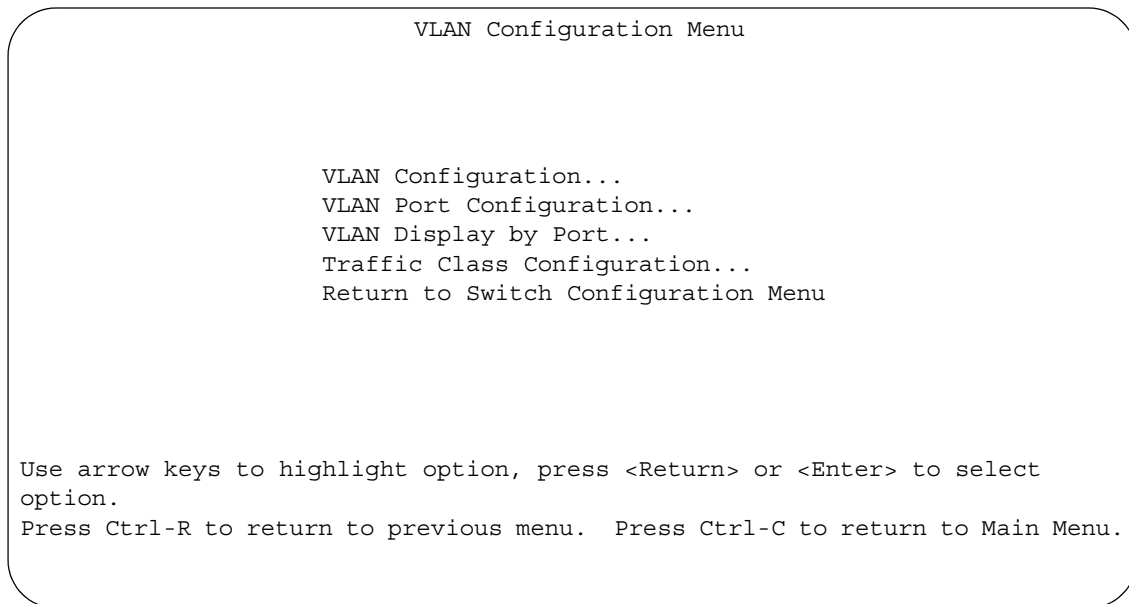
When you create VLANs, you can assign various ports (and therefore the devices attached to these ports) to different broadcast domains. Creating VLANs increases network flexibility by allowing you to reassign devices to accommodate network moves, additions, and changes, eliminating the need to change physical cabling.



To open the VLAN Configuration Menu:

- ➔ Choose VLAN Configuration (or press v) from the Switch Configuration Menu screen.

**Figure 54** VLAN Configuration Menu screen



[Table 22](#) describes the VLAN Configuration Menu options.

**Table 22** VLAN Configuration Menu options

Option	Description
<b>VLAN Configuration...</b>	Displays the VLAN Configuration screen (see <a href="#">“VLAN Configuration screen” on page 138</a> ). This screen allows you to set up VLAN workgroups.
<b>VLAN Port Configuration...</b>	Displays the VLAN Port Configuration screen (see <a href="#">“VLAN Port Configuration screen” on page 141</a> ). This screen allows you to set up a specific switch port.
<b>VLAN Display by Port...</b>	Displays the VLAN Display by Port screen (see <a href="#">“VLAN Display by Port screen” on page 143</a> ).
<b>Return to Switch Configuration Menu</b>	Exits the VLAN Configuration Menu screen and displays the Switch Configuration Menu screen.

## VLAN Configuration screen

The VLAN Configuration screen ([Figure 55](#)) allows you to create and assign VLAN port memberships to standalone or stacked unit ports. You can create port-based and policy-based VLANs for the following purposes:

- IEEE 802.1Q port-based VLANs allow you to explicitly configure switch ports as VLAN port members.

When you create a port-based VLAN, you assign a Port VLAN Identifier (PVID) manually, or use Auto PVID to assign it automatically.

When you configure ports as VLAN port members, they become part of a set of ports that form a broadcast domain for a specific VLAN. You can assign switch ports, whether standalone or stacked unit ports, as VLAN port members of one or more VLANs.

You can add or remove port members from a VLAN in accordance with the IEEE 802.1Q tagging rules. See [“IEEE 802.1Q VLAN workgroups”](#) on page 66 for a description of important terms used with 802.1Q VLANs.

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

To open the VLAN Configuration screen:

- ➔ Choose VLAN Configuration (or press v) from the VLAN Configuration Menu screen.

**Figure 55** VLAN Configuration screen

```

                                VLAN Configuration

Create VLAN:      [  1  ]
Delete VLAN:     [      ]
VLAN Name:       [ VLAN #1 ]
Management VLAN: [ Yes ] Now: 1      VLAN State:      [ Active ]

                                Port Membership
                                1-6      7-12    13-18   19-24   25-30   31-36   37-42   43-48   49-50
                                -----  -----  -----  -----  -----  -----  -----  -----  --
Unit #1  ++++++ ++++++ ++++++ ++++++ ++++++ ++++++ ++++++ ++++++ ++

KEY: + = A Member of This VLAN, - = Not a Member of This VLAN
Use space bar to display choices or enter text.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

```

[Table 23](#) describes the VLAN Configuration screen fields.

**Table 23** VLAN Configuration screen fields

Field	Description
<b>Create VLAN</b>	<p>Allows you to set up or view configured VLAN workgroups. Enter the number of the new VLAN you want to create or view, then press [Return]. The Port Membership fields indicate the corresponding VLAN workgroup configuration, if configured. Dashes (-) indicate no VLAN Members are configured. Alternatively, you can use the space bar to toggle through the various configured VLAN workgroups. You can create up to 255 different VLANs (except VLAN #1).</p> <p>Default            1</p> <p>Range             2 to 4094</p>
<b>Delete VLAN</b>	<p>Allows you to delete specified VLANs, except the assigned management VLAN (See Management VLAN field). Enter the number of the VLAN you want to delete, then press [Return], or use the space bar to toggle through the selection until you reach the VLAN you want to delete, then press [Return].</p>

**Table 23** VLAN Configuration screen fields (continued)

Field	Description
	<p>The specified VLAN is deleted as soon as you press [Return]. The software does not prompt you to reconsider this action. If you delete a VLAN, all configuration parameters that are associated with that VLAN are deleted also.</p> <p>You cannot delete VLAN 1. By default, all switch ports are assigned as untagged members of VLAN 1 with all ports configured as PVID = 1. See <a href="#">“IEEE 802.1Q VLAN workgroups” on page 66</a> for more information.</p>
	<p>Default            blank field</p> <p>Range             2 to 4094</p>
<b>VLAN Name</b>	<p>Allows you to assign a name field to configured VLANs.</p> <p>Default            VLAN # (<i>VLAN number</i>)</p> <p>Range             Any ASCII string of up to 16 printable characters</p>
Management VLAN	<p>Allows you to assign any VLAN as the management VLAN. VLAN 1 is the default management VLAN for the switch. To set this field, the VLAN State field value must be Active.</p> <p>Default            No</p> <p>Range             Yes, No</p>
VLAN State	<p>Allows you to activate your newly created VLAN.</p> <p>The following field values: VLAN Type, Protocol Id (PID), or User-defined PID must be configured appropriately before this field can be set to active. After you set the VLAN State field value to Active, you cannot change the VLAN State, VLAN Type, Protocol Id, or User-defined PID field values, unless you delete the VLAN.</p> <p>If you delete a VLAN, all configuration parameters that are associated with that VLAN are also deleted.</p> <p>Default            Inactive</p> <p>Range             Inactive, Active</p>
Port Membership	<p>Allows you to assign VLAN port memberships to <i>standalone</i> or <i>stacked unit</i> ports. The ports can be configured in one or more VLANs. To set this field, you must set the VLAN State field to Active. Certain restrictions apply for Gigabit and BayStack 410 ports.</p> <p>This field is dependent on the Tagging field value in the VLAN Port Configuration screen (see the Tagging field description in <a href="#">“VLAN Port Configuration screen fields” on page 142</a>).</p> <p>The Port Membership field is (+) if the port is a member of VLAN.</p> <p>The Port Membership field is (-) if the port is a non-member of VLAN.</p> <p>The Port Membership fields are displayed in six-port groups (for example, 1-6, 7-12, 13-18). The number of ports displayed depends on the switch model or type of optional GBIC installed in the Uplink Module slot.</p>

**Table 23** VLAN Configuration screen fields (continued)

Field	Description
Default U	All ports are assigned as untagged members of VLAN 1.
Range	U, T, and – : (+) and (-)

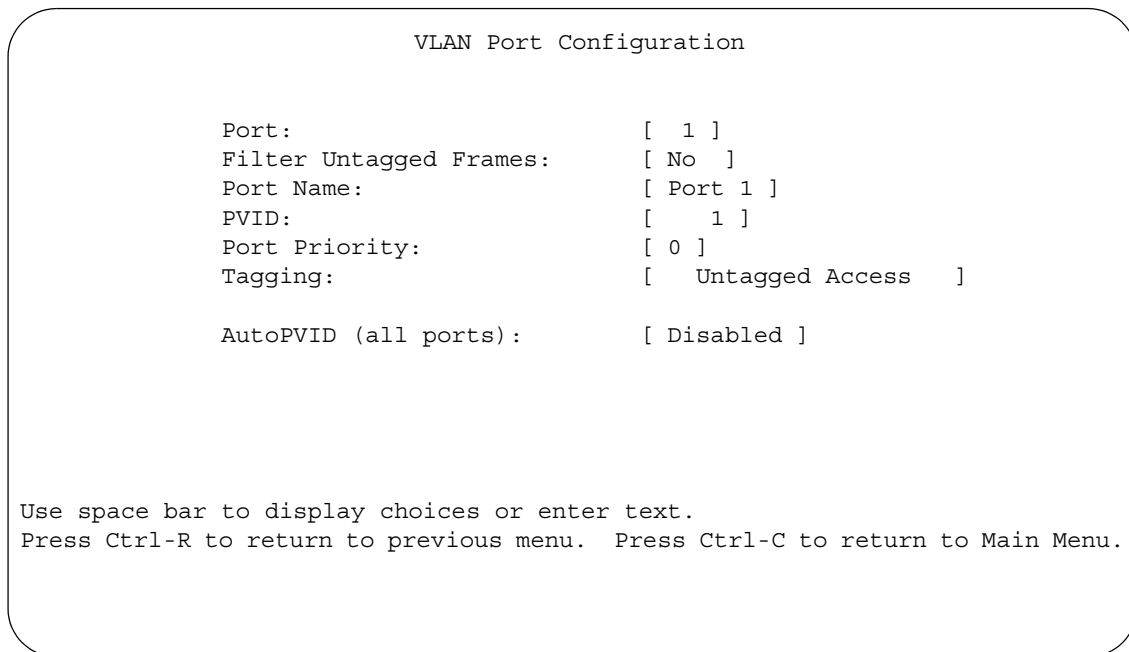
## VLAN Port Configuration screen

The VLAN Port Configuration screen ([Figure 56](#)) allows you to configure specified switch ports with the appropriate PVID/VLAN association that enables the creation of VLAN broadcast domains (see [“Shared servers” on page 75](#) for more information about setting up VLAN broadcast domains).

You can configure specified switch ports to filter (discard) all received untagged frames (see [“IEEE 802.1Q VLAN workgroups” on page 66](#)).

To open the VLAN Port Configuration screen.

- ➔ Choose VLAN Port Configuration (or press c) from the VLAN Configuration Menu screen.

**Figure 56** VLAN Port Configuration screen

[Table 24](#) describes the VLAN Port Configuration screen fields.

**Table 24** VLAN Port Configuration screen fields

Field	Description
Unit	Allows you to select a switch in your stack. To view another switch, type its switch number and press [Enter], or press the spacebar to toggle the switch numbers.
Port	Allows you to select the number of the port you want to view or configure. To view another port, type its port number and press [Enter], or press the spacebar to toggle the port numbers.
Filter Untagged Frames	Sets this port to filter (discard) all received untagged frames. Default        No Range         No, Yes
Port Name	The default port name (with associated stack unit number when configured) assigned to this port. You can change this field to any name that is up to 16 characters long. Default        Unit x, Port x Range         Any ASCII string of up to 16 printable characters

**Table 24** VLAN Port Configuration screen fields (continued)

Field	Description
PVID	<p>Associates this port to a specific VLAN. For example, a port with a PVID of 3 assigns all untagged frames received on this port to VLAN 3.</p> <p>Default        1</p> <p>Range         1 to 4094</p>
Tagging	<p>Assigns VLAN Port Membership tagging options to the given port, as follows:</p> <ul style="list-style-type: none"> <li>Untagged Access: Any VLAN that this port is a member of <i>will not</i> be 802.1Q tagged.</li> </ul> <p>Default        Untagged Access</p> <p>Range         Untagged Access, Tagged Trunk</p>
Auto PVID	Specifies the port VLAN identifier (PVID) automatically

### VLAN Display by Port screen

The VLAN Display by Port screen ([Figure 57](#)) allows you to view VLAN characteristics associated with a specified switch port.

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

**Figure 57** VLAN Display by Port screen

```

                                VLAN Display by Port

                                Port:      [ 1 ]
                                PVID:      1
                                Port Name:  Port 1

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

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

```

[Table 25](#) describes the VLAN Display by Port screen fields.

**Table 25** VLAN Display by Port screen fields

Field	Description
Unit	Displays the switch number. To view another switch, type the switch number and press [Enter], or press the spacebar to toggle the switch numbers.
Port	Displays the port number. To view another port, type the port number and press [Enter], or press the spacebar on your keyboard to toggle the port numbers.
PVID	Displays the PVID settings. This is a read-only field.
Port Name	Displays the specific port name. This is a read-only field.
VLANs	Displays a list of VLANs associated to the specified port. This is a read-only file.
VLAN Name	Displays a list of VLANs associated to the specified port. This is a read-only file.



## Port Configuration screen

The Port Configuration screen (Figures 58 and 59) allows you to configure specific switch ports or all switch ports. You can enable or disable the port status of specified switch ports, set the switch ports to autonegotiate for the highest available speed of the connected station, or set the speed for selected switch ports (autonegotiation is not supported on fiber optic ports).

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



**Note:** The Autonegotiation fields, the Speed fields, and the Duplex fields are independent of MultiLink Trunking, VLANs, and the STP.

---

To open the Port Configuration screen:

- ➔ Choose Port Configuration (or press p) from the Switch Configuration Menu screen.

**Figure 58** Port Configuration screen (1 of 2)

```

                                Port Configuration
  Port      Trunk      Status      Link      LnkTrap      Autonegotiation      Speed      Duplex
  ----      -
  1          [ Enabled ]      Down [ On ]      [ Enabled ]      [
  2          [ Enabled ]      Down [ On ]      [ Enabled ]      [
  3          [ Enabled ]      Down [ On ]      [ Enabled ]      [
  4          [ Enabled ]      Down [ On ]      [ Enabled ]      [
  5          [ Enabled ]      Down [ On ]      [ Enabled ]      [
  6          [ Enabled ]      Down [ On ]      [ Enabled ]      [
  7          [ Enabled ]      Down [ On ]      [ Enabled ]      [
  8          [ Enabled ]      Down [ On ]      [ Enabled ]      [
  9          [ Enabled ]      Down [ On ]      [ Enabled ]      [
  10         [ Enabled ]      Down [ On ]      [ Enabled ]      [
  11         [ Enabled ]      Down [ On ]      [ Enabled ]      [
  12         [ Enabled ]      Down [ On ]      [ Enabled ]      [
  13         [ Enabled ]      Down [ On ]      [ Enabled ]      [
  14         [ Enabled ]      Down [ On ]      [ Enabled ]      [
                                                    More...

Press Ctrl-N to display next screen.
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 59** Port Configuration screen (2 of 2)

Port Configuration							
Port	Trunk	Status	Link	LnkTrap	Autonegotiation	Speed	Duplex
15		[ Enabled ]	Down	[ On ]	[ Enabled ]	[	]
16		[ Enabled ]	Down	[ On ]	[ Enabled ]	[	]
17		[ Enabled ]	Down	[ On ]	[ Enabled ]	[	]
18		[ Enabled ]	Down	[ On ]	[ Enabled ]	[	]
19		[ Enabled ]	Down	[ On ]	[ Enabled ]	[	]
20		[ Enabled ]	Down	[ On ]	[ Enabled ]	[	]
21		[ Enabled ]	Down	[ On ]	[ Enabled ]	[	]
22		[ Enabled ]	Down	[ On ]	[ Enabled ]	[	]
23		[ Enabled ]	Down	[ On ]	[ Enabled ]	[	]
24		[ Enabled ]	Down	[ On ]	[ Enabled ]	[	]
25		[ Enabled ]	Down	[ On ]	[ Enabled ]	[	]
26		[ Enabled ]	Down	[ On ]	[ Enabled ]	[	]
27		[ Enabled ]	Down	[ On ]	[ Enabled ]	[	]
28		[ Enabled ]	Down	[ On ]	[ Enabled ]	[	]

More...

Press Ctrl-N to display next screen. Press Ctrl-P to display previous screen. 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.

[Table 26](#) describes the Port Configuration screen fields.

**Table 26** Port Configuration screen fields

Field	Description
Port	Indicates the switch port numbers that correspond to the field values in that row of the screen (for example, the field values in row 2 apply to switch port 2). The values that you set in the <i>Switch</i> row will affect all switch ports and, when the switch is part of a stack, the values that you set in the <i>Stack</i> row will affect all ports in the entire stack (except the GBIC ports or fiber optic ports).
Trunk	The read-only data displayed in this column indicates the trunks that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen (see <a href="#">"MultiLink Trunk Configuration Menu screen" on page 151</a> ).

**Table 26** 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 Value 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>LnkTrap</b>	Allows you to control whether link up/link down traps are sent to the configured trap sink from the switch. Default Value On Range On, Off
<b>Autonegotiation</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. This field is disabled for all fiber optic ports. Default Value Enabled Range Enabled, Disabled
<b>Speed/Duplex<sup>1</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. This field is set (by default) to 1000 Mb/s, full-duplex for Gigabit ports only. Default Value 100Mbps/Half (when Autonegotiation is Disabled) Range 10Mbps/Half, 10Mbps/Full, 100Mbps/Half, 100Mbps/Full

<sup>1</sup> Fiber optic ports can only be set to 100 Mb/s/Half or 100 Mb/s Full.

## High Speed Flow Control Configuration screen

The High Speed Flow Control Configuration screen ([Figure 60](#)) allows you to set the port parameters for the Gigabit Ethernet Interface.



**Note:** The GBIC module does not need to be installed to configure the port.

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

**Figure 60** High Speed Flow Control Configuration

High Speed Flow Control Configuration				
Port	Autonegotiation	Speed	Duplex	Flow Control
49	Enabled	1000Mbs	Full	Disabled
50	Enabled	1000Mbs	Full	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.

[Table 27](#) describes the High Speed Flow Control Configuration screen fields.

**Table 27** High Speed Flow Control Configuration screen fields

Field	Description
Unit	Allows you to select the unit number (when stacking is configured) to view or configure. To view or configure another unit, type its unit number and press [Enter], or press the spacebar to toggle the unit numbers (the system only displays a screen for units that are configured with a Gigabit MDA).

**Table 27** High Speed Flow Control Configuration screen fields (continued)

Field	Description
<b>Autonegotiation</b>	<p>When enabled, the port only advertises support for 1000 Mb/s operation, in full-duplex mode.</p> <p>Default Value    Enabled</p> <p>Range            Enabled, Disabled</p>
<b>Flow Control</b>	<p>Allows you to control traffic and avoid congestion on the Gigabit MDA port. Two modes are available (see <a href="#">“Choosing a high speed flow control mode,”</a> next, for details about the two modes). The Flow Control field cannot be configured unless you set the Autonegotiation field value to Disabled.</p> <p>Default Value    Disabled</p> <p>Range            Disabled, Symmetric, Asymmetric</p>

## Choosing a high speed flow control mode

The high speed flow control feature allows you to control traffic and avoid congestion on the Gigabit full-duplex link. If the receive port buffer becomes full, the BayStack 425 Switch issues a flow-control signal to the device at the other end of the link to suspend transmission. When the receive buffer is no longer full, the switch issues a signal to resume the transmission. You can choose Symmetric or Asymmetric flow control mode.

### Symmetric mode

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

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

### Asymmetric mode

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

In this mode, the GBIC port is disabled from transmitting pause frames to its link partner. Use this mode when the GBIC port is connected to a buffered repeater device.

## MultiLink Trunk Configuration Menu screen

The MultiLink Trunk Configuration Menu screen ([Figure 61](#)) allows you to select the appropriate screen to configure up to six MultiLink Trunks (you can group up to four switch ports together to form each trunk).

You can configure up to six MultiLink Trunks in each stack, with trunk members in either a single unit or distributed between units within the stack configuration (distributed trunking).

You can monitor the bandwidth usage for the trunk member ports within each trunk. For more information about configuring MultiLink Trunks, see [“MultiLink Trunks” on page 82](#).



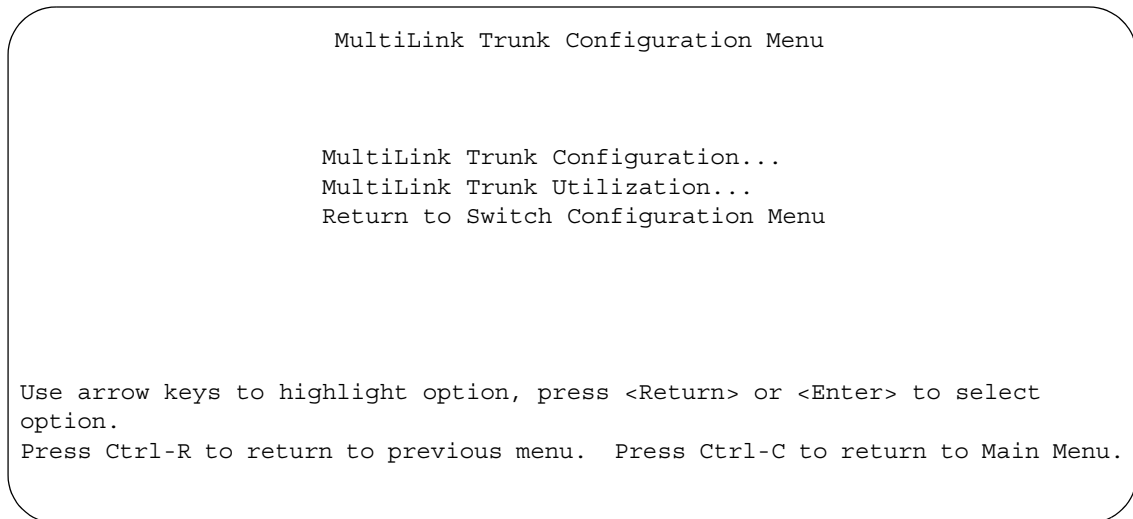
**Note:** When a trunk is not active (Trunk Status field set to Disabled), configuration changes do not take effect until you set the Trunk Status field to Enabled.

---

To open the MultiLink Trunk Configuration Menu screen:

- ➔ Choose MultiLink Trunk Configuration (or press t) from the Switch Configuration Menu screen.

**Figure 61** MultiLink Trunk Configuration Menu screen



[Table 28](#) describes the MultiLink Trunk Configuration Menu options.

**Table 28** MultiLink Trunk Configuration Menu options

Option	Description
<b>MultiLink Trunk Configuration...</b>	Displays the MultiLink Trunk Configuration screen ( <a href="#">Figure 62</a> ). This screen allows you to configure up to six MultiLink Trunks within a standalone switch or within a stack configuration. You can group up to four switch ports together to form each trunk.
<b>MultiLink Trunk Utilization...</b>	Displays the MultiLink Trunk Utilization screen ( <a href="#">Figure 63</a> and <a href="#">Figure 64</a> ). This screen allows you to monitor the bandwidth utilization of the configured trunks.
<b>Return to Switch Configuration Menu</b>	Exits the MultiLink Trunk Configuration Menu screen and displays the Switch Configuration Menu screen.



## MultiLink Trunk Configuration screen

The MultiLink Trunk Configuration screen (Figure 62) allows you to configure up to six trunks in a standalone switch or stack. In a stack configuration, trunk members can be distributed between any of the units within the same stack configuration.

To open the MultiLink Trunk Configuration screen:

- ➔ Choose Trunk Configuration (or press t) from the MultiLink Trunk Configuration Menu screen.

**Figure 62** MultiLink Trunk Configuration screen

```

MultiLink Trunk Configuration

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

Trunk      Trunk Name
-----
 1  [ Trunk #1 ]
 2  [ Trunk #2 ]
 3  [ Trunk #3 ]
 4  [ Trunk #4 ]
 5  [ Trunk #5 ]
 6  [ Trunk #6 ]

Use space bar to display choices or enter number. Enter 0 to delete.
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

```

Table 29 describes the MultiLink Trunk Configuration screen fields.

**Table 29** MultiLink 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 trunk (1 to 6) that corresponds to the switch ports specified in the user-configurable Trunk Members fields.
<b>Trunk Members (Unit/Port)</b>	<p>The Trunk Members column contains fields in each row that can be configured to create the corresponding trunk. The Unit value in the (Unit/Port) field is configurable only when the switch (unit) is part of a stack configuration. It indicates that the trunk members in this row are associated with the specified unit number configured in the Unit field. Each switch port can only be a member of a single trunk. The appropriate trunk number for each trunk member configured within this field is shown adjacent to the corresponding switch port in the following screens: Port Configuration screen, and Spanning Tree Configuration screen.</p> <p>Default Value      blank field</p> <p>Range                1 to 8 or 1 to 28 (depending on model type)</p>
STP Learning	<p>The STP Learning column contains a single field for each row that, when enabled, allows the specified trunk to participate in the spanning tree. This setting overrides those of the individual trunk members.</p> <p>Fast is the same as Normal, except that the state transition timer is shortened to two seconds.</p> <p>Default Value      Normal</p> <p>Range                Normal, Fast, Disabled</p>
Trunk Mode	<p>The Trunk Mode column contains a single read only field for each row that indicates the default operating mode for the switch.</p> <p><b>Basic:</b> Basic mode is the default mode for the switch. When in this mode, source MAC addresses are dynamically assigned to specific trunk members for flooding and forwarding, which allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.</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 Value      Disabled</p> <p>Range                Enabled, Disabled</p>
<b>Trunk Name</b>	The Trunk Name column contains a single optional field in each row that can be used to assign names to the corresponding configured trunks. The names chosen for this example can provide meaningful information to the user (for example, S1:T1 to FS2 indicates Trunk 1, in switch S1 connects to File Server 2).

## MultiLink Trunk Utilization screen

The MultiLink Trunk Utilization screen (Figure 63 and Figure 64) allows you to monitor the percentage of bandwidth used by configured trunk members. You can choose the type of traffic to monitor.

Figure 63 shows an *example* of bandwidth utilization rates for the trunk member ports configured in Figure 62. Because two screens are necessary to show all of the configured trunks (up to six), the screen prompts you to Press [Ctrl]-N to view trunks five and six.

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

**Figure 63** MultiLink Trunk Utilization screen (1 of 2)

MultiLink Trunk Utilization					
Trunk	Traffic Type	Unit/Port	Last 5 Minutes	Last 30 Minutes	Last Hour
1	[ Rx and Tx ]				
2	[ Rx and Tx ]				
3	[ Rx and Tx ]				
4	[ Rx and Tx ]				

More...

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

**Figure 64** MultiLink Trunk Utilization screen (2 of 2)

MultiLink Trunk Utilization					
Trunk	Traffic Type	Unit/Port	Last 5 Minutes	Last 30 Minutes	Last Hour
5	[ Rx and Tx ]				
6	[ Rx and Tx ]				

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

Table 30 describes the MultiLink Trunk Utilization screen fields.

**Table 30** MultiLink 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 trunk (1 to 6) that corresponds 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 Value Rx and Tx Range Rx and Tx, Rx, Tx
<b>Unit/Port</b>	Lists the trunk member ports that correspond to the trunk specified in the Trunk column. The (Unit/) extension to the Port column name only appears when the switch (unit) is part of a stack configuration. It indicates that the ports in this row are associated with the specified unit number configured in the Unit field.
<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 5 minutes. This field provides a running average of network activity and is updated every 15 seconds.

**Table 30** MultiLink Trunk Utilization screen fields (continued)

Field	Description
<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 30 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 60 minutes. This field provides a running average of network activity and is updated every 15 seconds.

## Port Mirroring Configuration screen

The Port Mirroring Configuration screen allows you to configure a specific switch port to monitor one specific port. You can specify port-based monitoring, and in a stack configuration, you can monitor ports that reside on different units within the stack.

For more information about the port mirroring feature, see [“Port mirroring” on page 45](#).

[Figure 65](#) shows an example of a Port Mirroring Configuration screen.

To open the Port Mirroring Configuration screen:

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

**Figure 65** Port Mirroring Configuration screen

```

Port Mirroring Configuration

Monitoring Mode: [ Disabled ]
Monitor Unit/Port: [ / ]

Unit/Port X: [ / ]

Currently Active Port Mirroring Configuration
-----
Monitoring Mode: Disabled

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

```

[Table 31](#) describes the Port Mirroring Configuration screen fields.

**Table 31** Port Mirroring Configuration screen fields

Field	Description
<b>Monitoring Mode</b>	<p>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 32 on page 159</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 Value Disabled</p> <p>Range See <a href="#">Table 32 on page 159</a></p>
<b>Monitor Unit/Port</b>	<p>Indicates the port number (of the specified unit) that is designated as the monitor port.</p> <p>Default Value Zero-length string</p> <p>Range 1 to 8/ 1 to 28 (depending on model type)</p>

**Table 31** Port Mirroring Configuration screen fields (continued)

Field	Description
<b>Unit/Port X</b>	Indicates one of the ports (of the specified unit) that will be monitored by the designated port monitor when one of the port-based monitoring modes is selected. This port will be monitored according to the value of Port X in the Monitoring Mode field (see <a href="#">Table 32</a> ).  Default Value      Zero-length string  Range                1 to 8/ 1 to 28 (depending on model type)

[Table 32](#) describes the various monitoring modes available from the Port Mirroring Configuration screen.

**Table 32** Monitoring modes

Field	Description
Port-based:	
Disabled	Default value for this feature.
-> Port X	Monitor all traffic received by Port X.

## Port Statistics screen

The Port Statistics screen ([Figure 66](#)) allows you to view detailed information about any switch or port in a stacked or standalone configuration. 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 10 seconds.

You can use the Port Statistics screen to clear (reset to zero) port counters for a specific switch or port. Alternatively, you can use the Clear All Port Statistics option to clear port counters for all switches or ports (see “[Switch Configuration Menu screen](#)” on page 118).

To open the Port Statistics screen:

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

**Figure 66** Port Statistics screen

Port Statistics			
Received		Port: [ 1 ]	
-----		-----	
Transmitted			
Packets:	0	Packets:	0
Multicasts:	0	Multicasts:	0
Broadcasts:	0	Broadcasts:	0
Total Octets:	0	Total Octets:	0
Pause Frames:	0	Pause Frames:	0
FCS Errors:	0	Collisions:	0
Undersized Packets:	0	Single Collisions:	0
Oversized Packets:	0	Multiple Collisions:	0
Discarded Packets:	0	Excessive Collisions:	0
Aged Packets:	0	Deferred Packets:	0
Frame Errors:	0	Late Collisions:	0
-----			
Received / Transmitted			
-----			
Packets 64 bytes:	0	Packets 256-511 bytes:	0
65-127 bytes	0	512-1023 bytes	0
128-255 bytes	0	1024-1518 bytes	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.			

[Table 33](#) describes the Port Statistics screen fields.



**Note:** In a stacked configuration, the Port Statistics screen appears in a slightly different format when the port selected in the Unit/Port field is configured with a GBIC.



**Table 33** Port Statistics screen fields

Field	Description
Unit	Only appears if the switch is participating in a stack configuration. The field allows you to select the number of the unit you want to view or configure. To view or configure another unit, type its unit number and press [Enter], or press the spacebar on your keyboard to toggle the unit numbers.
Port	Allows you to select the number of the port you want to view or reset to zero. To view another port, type its port number and press [Enter], or press the spacebar on your keyboard to toggle the port numbers.
Packets	Received column: Indicates the total number of packets received on this port, including bad packets, broadcast packets, and multicast packets. Transmitted column: Indicates the total number of packets transmitted successfully on this port, including broadcast packets and multicast packets.
Multicasts	Received column: Indicates the total number of good multicast packets received on this port, excluding broadcast packets. Transmitted column: Indicates the total number of multicast packets transmitted successfully on this port, excluding broadcast packets.
Broadcasts	Received column: Indicates the total number of good broadcast packets received on this port. Transmitted column: Indicates the total number of broadcast packets transmitted successfully on this port.
Total Octets	Received column: Indicates the total number of octets of data (including data in bad packets) received on this port, excluding framing bits but including FCS octets. Transmitted column: Indicates the total number of octets of data transmitted successfully on this port, including FCS octets.
Lost Packets	Received column: Indicates the total number of packets lost (discarded) when the capacity of the port receive buffer was exceeded. Transmitted column: Indicates the total number of packets lost (discarded) when the capacity of the port transmit buffer was exceeded.
Packets 64 bytes	Received column: Indicates the total number of 64-byte packets received on this port. Transmitted column: Indicates the total number of 64-byte packets transmitted successfully on this port.
65-127 bytes	Received column: Indicates the total number of 65-byte to 127-byte packets received on this port. Transmitted column: Indicates the total number of 65-byte to 127-byte packets transmitted successfully on this port.

**Table 33** Port Statistics screen fields (continued)

<b>Field</b>	<b>Description</b>
<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.
<b>Frame Errors</b>	Indicates the total number of valid-size packets that were received but discarded because of CRC errors and improper framing.
<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>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>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>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>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.
The following field values appear only when the port selected in the Unit/Port field is configured with a GBIC.	

**Table 33** Port Statistics screen fields (continued)

Field	Description
Pause Frames (Port 25 only)	<p>Transmitted column: Indicates the total number of pause frames transmitted on this port. Pause frames cause the transmitting port to temporarily suspend the transmission of packets when the receiving port's frame buffer is full (Gigabit ports only).</p> <p>Received column: Indicates the total number of pause frames received on this port. Pause frames cause the transmitting port to temporarily suspend the transmission of packets when the receiving port's frame buffer is full (Gigabit ports only).</p>

## System Log screen

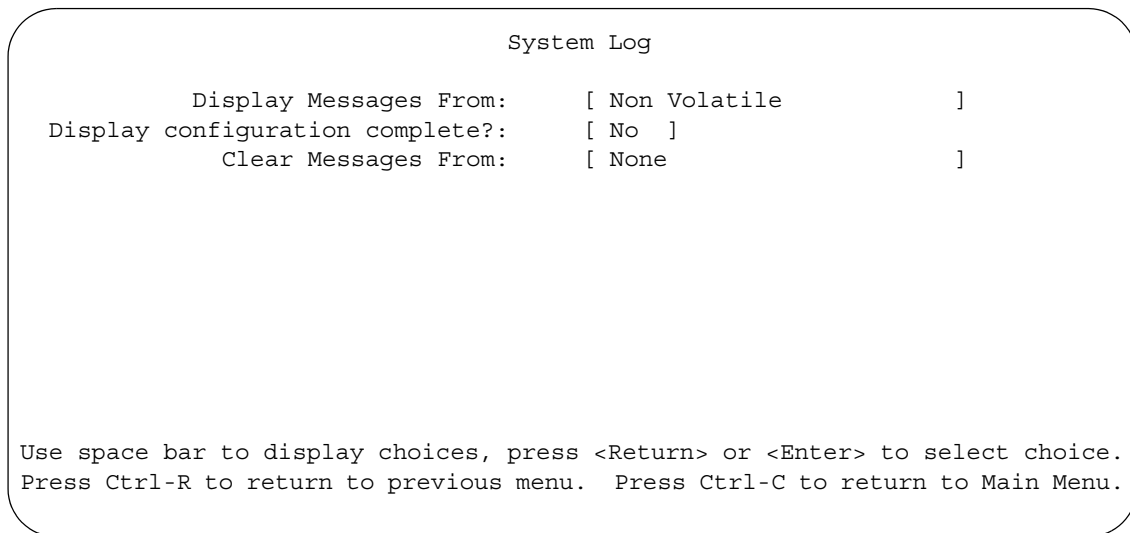
The System Log screen (Figure 67) displays or clears messages obtained from system nonvolatile random access memory (NVRAM) or dynamic random access memory (DRAM) and NVRAM. When the switch is part of a stack configuration, the System screen displays only the data for the BayStack 420/425 you are connected to through the Console/Comm port.

System Log messages operate as follows:

- NVRAM messages are retrievable after a system reset.
- DRAM messages can be viewed while the system is operational.
- All NVRAM and DRAM messages are time stamped.
- When you restart your system after a reset, the DRAM messages are deleted.
- After a reset, all messages stored in NVRAM are copied to DRAM (DRAM messages are not copied to NVRAM). The messages copied to DRAM are time stamped to zero (0).

To open the System Log screen:

- ➔ Choose Display System Log (or press y) from the main menu.

**Figure 67** System Log screen

[Table 34](#) describes the System Log screen fields.

**Table 34** System Log screen fields

Field	Description
Unit	This field only appears if the switch is participating in a stack configuration. The field allows you to select the unit number of the BayStack 420/425 you want to view. To view the log messages of another BayStack 420/425, type its unit number and press [Enter], or press the spacebar on your keyboard to toggle the unit numbers.
Display Messages From	This field allows you to select the RAM source your messages are obtained from. Choose Non Volatile (NVRAM) or Volatile (DRAM) + Non Volatile. Use the spacebar to toggle between the options. DefaultNon Volatile RangeNon Volatile, Volatile, Volatile + Non Volatile

**Table 34** System Log screen fields (continued)

Field	Description
Display configuration complete?	This field allows you to determine whether the configuration information received from NVRAM/DRAM (depending on what is selected in the Display Messages From field) is complete. Use the spacebar to toggle between the options. DefaultNo RangeNo, Yes
Clear Messages From	This field allows you to clear the information messages from DRAM, NVRAM or both. If you clear DRAM messages, existing NVRAM messages are copied into DRAM. After a system reset, all existing NVRAM messages are copied to DRAM. Use the spacebar to toggle between the options. DefaultNone RangeNone, NVRAM, DRAM + NVRAM

## Console/Comm Port Configuration screen

The Console/Comm Port Configuration screen ([Figure 68](#)) allows you to configure and modify the console/comm port parameters and security features of a standalone switch or any participating switch in a stack configuration.

To open the Console/Comm Port Configuration screen:

- ➔ Choose Console/Comm Port Configuration (or press o) from the main menu.

**Figure 68** Console/Comm Port Configuration screen

```

                                Console/Comm Port Configuration

Comm Port Data Bits:                8 Data Bits
Comm Port Parity:                   No Parity
Comm Port Stop Bits:                1 Stop Bit
Console Port Speed:                 [ 9600 Baud ]

Console Switch Password Type:       [ None           ]
Console Stack Password Type:        [ None           ]
Telnet/WEB Switch Password Type:    [ None           ]
Telnet/WEB Stack Password Type:     [ None           ]

Console Read-Only Switch Password:  [ user ]
Console Read-Write Switch Password: [ secure ]
Console Read-Only Stack Password:   [ user ]
Console Read-Write Stack Password:  [ secure ]

Primary RADIUS Server:              [ 0.0.0.0 ]
Secondary RADIUS Server:            [ 0.0.0.0 ]
UDP RADIUS Port:                    [ 1645 ]
RADIUS Shared Secret:               [ ]

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







```

[Table 35](#) describes the Console/Comm Port Configuration screen fields.

**Table 35** Console/Comm Port Configuration screen fields

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

**Table 35** Console/Comm Port Configuration screen fields (continued)






Field	Description
	 <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 service port setting.
	 <b>Achtung:</b> Bei Auswahl einer Baud rate, 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.
	 <b>Attention:</b> 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.
	 <b>Precaución:</b> 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.
	 <b>Attenzione:</b> 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.
	 <b>注意:</b> 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。

**Table 35** Console/Comm Port Configuration screen fields (continued)






Field	Description
<b>Console Switch Password Type</b>	<p>Enables password protection for accessing the console interface (CI) of a <i>standalone switch</i> through a console terminal.</p> <p>If you set this field to Required, you can use the Logout option to restrict access to the CI. Thereafter, you will need to specify the correct password at the console-terminal prompt. See Console Read-Only Switch Password and Console Read-Write Switch Password for more information.</p> <p>Default Value    None</p> <p>Range            None, Local Password, RADIUS Authentication</p>
<b>Console Stack Password Type</b>	<p>Enables password protection for accessing the console interface (CI) of <i>any participating switch in a stack configuration</i> through a console terminal.</p> <p>If you set this field to Required, you can use the Logout option to restrict access to the CI of any stack unit. Thereafter, you will need to specify the correct password at the console-terminal prompt when accessing the stack. See Console Read-Only Stack Password and Console Read-Write Stack Password for more information.</p> <p>Default Value    None</p> <p>Range            None, Local Password, RADIUS Authentication</p>
TELNET Switch Password Type	<p>Enables password protection for accessing the console interface (CI) of a <i>standalone switch</i> through a Telnet session.</p> <p>If you set this field to Required, you can use the Logout option to restrict access to the CI. Thereafter, you will need to specify the correct password at the console-terminal prompt. See Console Read-Only Switch Password and Console Read-Write Switch Password descriptions for more information.</p> <p>Default Value    None</p> <p>Range            None, Local Password, RADIUS Authentication</p>
TELNET Switch Password Type	<p>Enables password protection for accessing the console interface (CI) of <i>any participating switch in a stack configuration</i>, through a Telnet session.</p> <p>If you set this field to Required, you can use the Logout option to restrict access to the CI of any stack unit. Thereafter, you will need to specify the correct password at the console-terminal prompt when accessing the stack. See Console Read-Only Stack Password and Console Read-Write Stack Password for more information.</p> <p>Default Value    None</p> <p>Range            None, Local Password, RADIUS Authentication</p>





**Table 35** Console/Comm Port Configuration screen fields (continued)

Field	Description
<b>Console Read-Only Switch Password</b>	<p>When the Console Switch Password field is set to Required (for Telnet, for Console, or for Both), this field allows read-only password access to the CI of a <i>standalone switch</i>. Users can access the CI using the correct password (see default), but cannot change parameters or use the Reset option or Reset to Default option.</p> <p>Default Value    user</p> <p>Range            An ASCII string of up to 15 printable characters</p>
<b>Console Read-Write Switch Password</b>	<p>When the Console Switch Password field is set to Required (for Telnet, for Console, or for Both), this field allows read-write password access to the CI of a <i>standalone switch</i>. Users can log in to the CI using the correct password (see default) and can change any parameter, except the stack passwords.</p> <p>You can change the default passwords for read-only access and read-write access to a private password.</p> <p>Default Value:    secure</p> <p>Range:            Any ASCII string of up to 15 printable characters</p>
	<p> <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.</p>
	<p> <b>Achtung:</b> Wenn Sie die für das System standardmäßig eingestellten Paßwörter ändern, notieren Sie sich die neuen Paßwörter, und bewahren Sie sie an einem sicheren Ort auf. Falls Sie die neuen Paßwörter vergessen, können Sie nicht mehr auf die Konsolenschnittstelle zugreifen. Wenden Sie sich in diesem Fall an Nortel Networks, um Unterstützung zu erhalten.</p>
	<p> <b>Attention:</b> Si vous changez les mots de passe par défaut du système, assurez-vous de bien noter vos nouveaux mots de passe et de les conserver dans un endroit sûr. Si vous perdez vos nouveaux mots de passe, vous ne pourrez plus accéder à votre interface. Le cas échéant, veuillez contacter Nortel Networks.</p>
	<p> <b>Precaución:</b> Si modifica las contraseñas predeterminadas asignadas por el sistema, asegúrese de anotar las nuevas contraseñas y guárdelas en un lugar seguro. Si olvida las nuevas contraseñas, no podrá acceder al interfaz de la consola. En ese caso, póngase en contacto con Nortel Networks para obtener ayuda al respecto.</p>
	<p> <b>Attenzione:</b> In caso di modifica delle password predefinite nel sistema, assicurarsi di annotare le nuove password e di conservarle in un luogo sicuro. Nel caso in cui le nuove password vengano dimenticate, non sarà possibile accedere all'interfaccia della console. In tal caso, contattare la Nortel Networks per avere assistenza.</p>

**Table 35** Console/Comm Port Configuration screen fields (continued)

Field	Description
	<p>注意：システム装備したデフォルトのパスワードを変更する場合、必ず新しいパスワードを書き留めて安全な場所に保管してください。新しいパスワードを忘れてしまうと、コンソール・インタフェイスにアクセスできません。この場合は、Bay Networksまでご連絡ください。</p>
<b>Console Read-Only Stack Password</b>	<p>When the Console Switch Password field is set to Required (for Telnet, for Console, or for Both), this field allows read-only password access to the CI of <i>any participating switch in a stack configuration</i>. Users can access the CI using the correct password (see default), but cannot change any parameters or use the Reset option or Reset to Default option.</p> <p>Default Value    user</p> <p>Range            An ASCII string of up to 15 printable characters</p>
<b>Console Read-Write Stack Password</b>	<p>When the Console Switch Password field is set to Local Password (for Telnet, for Console, or for Both), this field allows read-write password access to the CI of <i>any participating switch in a stack configuration</i>. Users can log in to the CI using the correct password (see default), and can change any parameter, except the switch password.</p> <p>You can change the default passwords for read-only access and read-write access to a private password.</p> <p>Default Value:    secure</p> <p>Range:            Any ASCII string of up to 15 printable characters</p>
	<p><b>Caution:</b> When 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.</p>
	<p><b>Achtung:</b> Wenn Sie die für das System standardmäßig eingestellten Paßwörter ändern, notieren Sie sich die neuen Paßwörter, und bewahren Sie sie an einem sicheren Ort auf. Falls Sie die neuen Paßwörter vergessen, können Sie nicht mehr auf die Konsolenschnittstelle zugreifen. Wenden Sie sich in diesem Fall an Nortel Networks, um Unterstützung zu erhalten.</p>
	<p><b>Attention:</b> Si vous changez les mots de passe par défaut du système, assurez-vous de bien noter vos nouveaux mots de passe et de les conserver dans un endroit sûr. Si vous perdez vos nouveaux mots de passe, vous ne pourrez plus accéder à votre interface. Le cas échéant, veuillez contacter Nortel Networks.</p>
	<p><b>Precaución:</b> Si modifica las contraseñas predeterminadas asignadas por el sistema, asegúrese de anotar las nuevas contraseñas y guárdelas en un lugar seguro. Si olvida las nuevas contraseñas, no podrá acceder al interfaz de la consola. En ese caso, póngase en contacto con Nortel Networks para obtener ayuda al respecto.</p>

**Table 35** Console/Comm Port Configuration screen fields (continued)

Field	Description
	 <b>Attenzione:</b> In caso di modifica delle password predefinite nel sistema, assicurarsi di annotare le nuove password e di conservarle in un luogo sicuro. Nel caso in cui le nuove password vengano dimenticate, non sarà possibile accedere all'interfaccia della console. In tal caso, contattare la Nortel Networks per avere assistenza.
	注意: システム装備したデフォルトのパスワードを変更する場合、必ず新しいパスワードを書き留めて安全な場所に保管してください。新しいパスワードを忘れてしまうと、コンソール・インタフェイスにアクセスできません。この場合は、Bay Networksまでご連絡ください。
<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 UPD Port</b>	The user datagram protocol (UDP) port for the RADIUS server. Default            1645 Range             0 to 65536
<b>RADIUS 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

## Renumber Stack Units screen

The Renumber Stack Units screen (Figure 69) allows you to renumber the units configured in the stack. When selected, this option identifies the unit number of each unit in the stack configuration by lighting the corresponding number of (100 Mb/s port) LEDs on each unit for approximately 10 seconds. For example, unit 3 will display three LEDs.



**Note:** This menu option and screen appears only when the switch is participating in a stack configuration.

To open the Renumber Stack Units screen:

- ➔ Choose Renumber Stack Units (or press n) from the main menu.

**Figure 69** Renumber Stack Units screen

```

                                Renumber Stack Units

Current Unit Number          MAC Address          New Unit Number
-----
[ 1 ]                       00-60-fd-77-a6-0c          [ 1 ]
[ 2 ]                       00-60-fd-77-a5-f0          [ 2 ]
[ 3 ]                       00-60-fd-77-a4-4c          [ 3 ]
[ 4 ]                       00-60-fd-77-ab-84          [ 4 ]

Renumbering stack units will cause an automatic Reset to Current Settings to
occur across the entire stack. The current configuration will be adapted to
the new numbering scheme. Check the stack configuration after the reset to
confirm the desired configuration is set.

Are you sure you want to renumber switches with the new settings?   [ No ]

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

```

Table 36 describes the Renumber Stack Units screen fields.

**Table 36** Renumber Stack Units screen fields

Field	Description
<b>Current Unit Number</b>	Read-only fields listing the current unit number of each of the configured stack units. The entries in this column are displayed in order of their current physical cabling with respect to the base unit, and can show nonconsecutive unit numbering if one or more units were previously moved or modified. The entries can also include unit numbers of units that are no longer participating in the stack (not currently active).
<b>MAC Address</b>	Read-only field listing the MAC address of the corresponding unit listed in the Current Unit Number field.
New Unit Number	User-settable field showing the current unit number of each unit in the stack. You can change any of the fields, as required. You can also delete entries by typing zero (0) or using the space bar to clear the field.  Default Value      Current stack order Range                1 to 8
Renumber units with new setting?	Specifies whether to start the renumbering process (default is No). Use the spacebar to toggle the selection to Yes.  Renumbering resets the switch with the current configuration values. When you select this option, the switch resets, runs a self-test, then displays the Nortel Networks logo screen. After you press [Ctrl]-Y at the screen prompt, the console screen temporarily displays the (standalone) BayStack 420/425 main menu. Then, within 20 seconds, the console screen refreshes and displays the main menu screen for the stack configuration. The Unit LEDs display the new numbering order.  Default Value      No Range                No, Yes

## Hardware Unit Information screen

The Hardware Unit Information screen (Figure 70) lists the switch models, including any installed GBICs that are configured in your standalone or stack configuration.

To open the Hardware Unit Information screen:

- ➔ Choose Display Hardware Units (or press h) from the main menu.

**Figure 70** Hardware Unit Information screen

	Switch Model	GBIC1 Model	HW Version	SW Version
Unit #1	BayStack 425-24T	None	0B	v3.1.0.00
Unit #2	BayStack 420-24T	None	#1a	v3.1.0.00

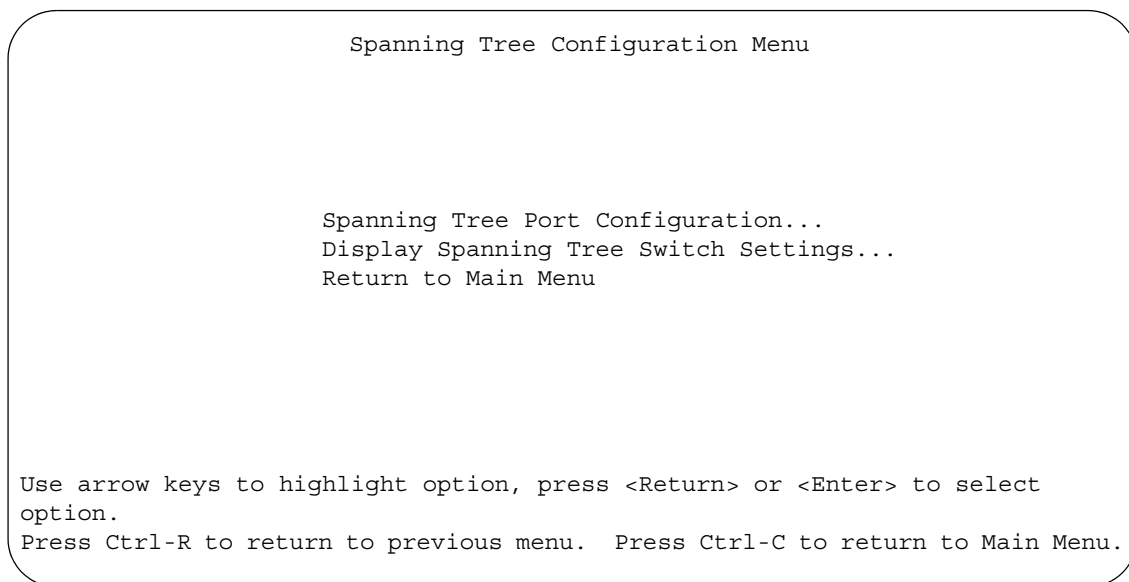
Press Ctrl-R to return to previous menu. Press Ctrl-C to return to Main Menu.

## Spanning Tree Configuration Menu screen

The Spanning Tree Configuration Menu screen (Figure 71) 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.

To open the Spanning Tree Configuration Menu screen:

- ➔ Choose Spanning Tree Configuration (or press p) from the main menu.

**Figure 71** Spanning Tree Configuration Menu screen

[Table 37](#) describes the Spanning Tree Configuration Menu options.

**Table 37** 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 screen” on page 175</a> ).
<b>Spanning Tree Switch Settings</b>	Displays the Spanning Tree Switch Settings screen (see <a href="#">“Spanning Tree Switch Settings screen” on page 179</a> ).
<b>Return to Main Menu</b>	Exits the Spanning Tree Configuration Menu and displays the main menu.

## Spanning Tree Port Configuration screen

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



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

Figure 72 and Figure 73 show sample port configurations for the two Spanning Tree Port Configuration screens.

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

Figure 72 Spanning Tree Port Configuration screen (1 of 2)

```
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

More...

Press Ctrl-N to display next screen.  
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 73** Spanning Tree Port Configuration screen (2 of 2)

```

Spanning Tree Port Configuration

Port      Trunk      Participation      Priority      Path Cost      State
-----
15        [ Normal Learning ]      128          10           Forwarding
16        [ Normal Learning ]      128          10           Forwarding
17        [ Normal Learning ]      128          10           Forwarding
18        [ Normal Learning ]      128          10           Forwarding
19        [ Normal Learning ]      128          10           Forwarding
20        [ Normal Learning ]      128          10           Forwarding
21        [ Normal Learning ]      128          10           Forwarding
22        [ Normal Learning ]      128          10           Forwarding
23        [ Normal Learning ]      128          10           Forwarding
24        [ Normal Learning ]      128          10           Forwarding
25        [ Normal Learning ]      128          10           Forwarding
26        [ Normal Learning ]      128          10           Forwarding
27        [ Normal Learning ]      128          10           Forwarding
28        [ Normal Learning ]      128          10           Forwarding
More...

Press Ctrl-N to display next screen. Press Ctrl-P to display previous screen.
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.

```

[Table 38](#) describes the Spanning Tree Port Configuration screen fields.

**Table 38** Spanning Tree Port Configuration screen fields

Field	Description
Unit	This field only appears if the switch is participating in a stack configuration. The field allows you to select the number of the unit you want to view. To view another unit, type its unit number and press [Enter], or press the spacebar on your keyboard to toggle the unit numbers.
Port	Indicates the switch port numbers that correspond to the field values in that row of the screen (for example, the field values in row 2 apply to switch port 2). Note that the values in the <i>Switch</i> row affect all switch ports and, when the switch is part of a stack, the values in the <i>Stack</i> row affect all ports in the entire stack.
Trunk	The read-only data displayed in this column indicates the trunks that correspond to the switch ports specified in the Trunk Members fields of the Trunk Configuration screen (see <a href="#">"MultiLink Trunk Configuration Menu screen" on page 151</a> ).

**Table 38** Spanning Tree Port Configuration screen fields (continued)

Field	Description
<b>Participation</b>	<p>Allows you to configure any (or all) of the switch ports for Spanning tree participation. When an individual port is a trunk member (see Trunk field), changing this setting for one of the trunk members changes the setting for all members of that trunk. You should consider how this can change your network topology before you change this setting.</p> <p>The Fast Learning parameter is the same as Normal Learning, except that the state transition timer is shortened to 2 seconds.</p> <p>Default Value      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 Value      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 Value      10 or 100 (1 for Gigabit port)</p> <p>                         Path Cost = 1000/LAN speed (in Mb/s)</p> <p>                         The higher the LAN speed, the lower the path cost.</p> <p>                         See also Priority.</p> <p>Range                1 to 65535</p>
<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 Value      Topology dependent</p> <p>Range                Disabled, Blocking, Listening, Learning, Forwarding</p>

## Spanning Tree Switch Settings screen

The Spanning Tree Switch Settings screen (Figure 74) allows you to view spanning tree parameter values for the BayStack 420/425.

To open the Spanning Tree Switch Settings screen:

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

**Figure 74** Spanning Tree Switch Settings screen

```
Spanning Tree Switch Settings

Bridge Priority:           8000
Designated Root:         800000001D0E6CFC
Root Port:                48
Root Path Cost:          133
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.
```

Table 39 describes the Spanning Tree Switch Settings parameters.

**Table 39** Spanning Tree Switch Settings parameters

Parameter	Description
<b>Bridge Priority</b>	<p>Indicates the management-assigned priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. The STA uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values compared first, followed by the hardware addresses.</p> <p>Default Value      8000</p> <p>Range                0 to 65535</p>
<b>Designated Root</b>	<p>Indicates the bridge ID of the root bridge, as determined by the STA.</p> <p>Default Value      8000 (bridge_id)</p> <p>Range                0 to 65535</p>
<b>Root Port</b>	<p>Indicates the switch port number that offers the lowest path cost to the root bridge.</p> <p>Default Value      0</p> <p>Range                Unit: 0 Port: 28</p>
<b>Root Path Cost</b>	<p>Indicates the path cost from this switch port to the root bridge.</p> <p>Default Value      0</p> <p>Range                Not applicable</p>
<b>Hello Time</b>	<p>Indicates the Actual Hello Interval, the amount of time between transmissions of configuration Bridge Protocol Data Units (BPDUs) that the root bridge is currently using. Note that all bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. See also Bridge Hello Time.</p> <p>Default Value      2 seconds</p> <p>Range                1 to 10 seconds</p>
<b>Maximum Age Time</b>	<p>Indicates the Maximum Age Time parameter value that the root bridge is currently using. This value specifies the maximum age that a Hello message can attain before it is discarded. Note that the root bridge's Maximum Age Time parameter value becomes the actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. See also Bridge Maximum Age Time.</p> <p>Default Value      20 seconds</p> <p>Range                6 to 40 seconds</p>

**Table 39** 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 Value      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 Value      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 Value      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 Value      15 seconds</p> <p>Range                4 to 30 seconds</p>

## TELNET Configuration screen

The TELNET Configuration screen (Figure 75) allows a user at a remote console terminal to communicate with the BayStack 420/425 as if the console terminal were directly connected to it. You can have up to four active Telnet sessions at one time.

To open the TELNET Configuration screen:

➔ Choose TELNET Configuration (or press t) from the main menu.

**Figure 75** TELNET Configuration screen

```

                                TELNET/SNMP/Web Access Configuration

TELNET:                          |                               Access:          Use List:
Login Timeout      : [ 1 minute ] | TELNET: [ Enabled ]   [ Yes ]
Login Retries      : [ 3 ]         | SNMP  : [ Enabled ]   [ Yes ]
Inactivity Timeout: [ 15 minutes ] | WEB   : [ Enabled ]   [ Yes ]
Event Logging      : [ All         ] |

#           Allowed Source IP Address           Allowed Source Mask
--           -----
1           [ 0.0.0.0 ]                          [ 0.0.0.0 ]
2           [ 255.255.255.255 ]                  [ 255.255.255.255 ]
3           [ 255.255.255.255 ]                  [ 255.255.255.255 ]
4           [ 255.255.255.255 ]                  [ 255.255.255.255 ]
5           [ 255.255.255.255 ]                  [ 255.255.255.255 ]
6           [ 255.255.255.255 ]                  [ 255.255.255.255 ]
7           [ 255.255.255.255 ]                  [ 255.255.255.255 ]
8           [ 255.255.255.255 ]                  [ 255.255.255.255 ]
9           [ 255.255.255.255 ]                  [ 255.255.255.255 ]
10          [ 255.255.255.255 ]                  [ 255.255.255.255 ]

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

```

Table 40 describes the TELNET Configuration screen fields.

**Table 40** TELNET Configuration screen fields

Field	Description
<b>TELNET Access</b>	Allows a user remote access to the CI through a Telnet session. Default Value: 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 Value: 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 Value: 3 Range: 1 to 100
<b>Inactivity Timeout</b>	Specifies the amount of time the session can be inactive before it is terminated. Default Value: 15 minutes Range: 0 to 60 minutes (0 indicates “no timeout”)
<b>Event Logging</b>	Specifies the types of events that will be displayed in the Event Log screen (see <a href="#">“System Log screen” on page 163</a> ). Default Value: All Range: All, None, Accesses, Failures Description: <i>All</i> : 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> <i>None</i> : Indicates that no Telnet events will be logged in the Event Log screen. <i>Accesses</i> : Logs only Telnet connect and disconnect events in the Event Log screen. <i>Failures</i> : Logs only failed Telnet connection attempts in the Event Log screen.

**Table 40** TELNET Configuration screen fields (continued)

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

## Software Download screen

The Software Download screens ([Figure 76](#) and [Figure 77](#)) allow you to revise the BayStack 420/425 software image that is located in nonvolatile flash memory.



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



**Achtung:** Unterbrechen Sie die Stromzufuhr zum Gerät nicht, während die Software heruntergeladen wird. Bei Unterbrechung der Stromzufuhr kann das Firmware-Image beschädigt werden.



**Attention:** Ne pas couper l'alimentation de l'appareil pendant le chargement du logiciel. En cas d'interruption, le programme résident peut être endommagé.





**Precaución:** No interrumpa la alimentación del dispositivo durante el proceso de descarga del software. Si lo hace, puede alterar la imagen de la programación (firmware).

---



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

---



**注意:** ソフトウェアをダウンロードしているとき、デ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。

---

To download the software image, you need a properly configured Trivial File Transfer Protocol (TFTP) server in your network, and an IP address for the switch (or stack, if configured). To learn how to configure the switch or stack IP address, refer to [“IP Configuration/Setup screen” on page 108](#).

To open the Software Download screen:

➔ Choose Software Download (or press f) from the main menu.

You can monitor the software download process by observing the LEDs (see [“LED Indications during the download process” on page 187](#)).

**Figure 76** Software Download screen for a BayStack 420/425 stack

```

                                Software Download

Software Image Filename:          [ bs42x_31060.img ]
Diagnostics Image Filename:      [   ]

TFTP Server IP Address:          [ 134.177.152.102 ]

Start TFTP Load of New Image:    [ No           ]

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

```

[Table 41](#) describes the Software Download screen fields.

**Table 41** Software Download screen fields

Field	Description
<b>BayStack 425-24T Image Filename</b>	<p>The BayStack 420/425 software image load file name.</p> <p><b>QRWH:</b> Certain software releases may require you to download two images: the boot code image and the agent image. For proper operation of the switch, the new boot code image must be downloaded before the agent image is downloaded.</p> <p>Default Value      Zero-length string</p> <p>Range                An ASCII string of up to 30 printable characters</p>
<b>BayStack 425-24T Diagnostics Filename</b>	<p>The BayStack 420/425 diagnostics file name.</p> <p>Default Value      Zero-length string</p> <p>Range                An ASCII string of up to 30 printable characters</p>

**Table 41** Software Download screen fields (continued)

Field	Description
<b>TFTP Server IP Address</b>	The IP address of your TFTP load host. Default Value      0.0.0.0 (no IP address assigned) Range                Four-octet dotted-decimal notation, where each octet is represented as a decimal value, separated by a decimal point
<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. Default Value      No Range                Yes, No

## LED Indications during the download process

The software download process automatically completes without user intervention. The process erases the contents of flash memory and replaces it with a new software image. Be careful not to interrupt the download process until after it runs to completion (the process can take up to 10 minutes, depending on network conditions).



**Note:** If problems occur during the software download process, the Software Download screen displays error codes that define the problem. The error codes are described in [Chapter 4, “Troubleshooting,”](#) on page 191.

## Configuration File Download/Upload screen

The Configuration File Download/Upload screen ([Figure 77](#)) allows you to store your switch/stack configuration parameters on a TFTP server.

You can retrieve the configuration parameters of a standalone switch or an entire stack and use the retrieved parameters to automatically configure a replacement switch or stack. Certain requirements apply when automatically configuring a switch or stack using this feature (see [“Requirements” on page 190](#)). 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 43 on page 190](#)).

To open the Configuration File Download/Upload screen:

➔ Choose Configuration File (or press g) from the main menu.

**Figure 77** Configuration File Download/Upload screen

```
Configuration File Download/Upload

Configuration Image Filename:      [ bs425-48T-20040609.cfg ]
TFTP Server IP Address:           [ 134.177.152.102 ]
Copy Configuration Image to Server: [ No ]
Retrieve Configuration Image from Server: [ No ]

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

Table 42 describes the Configuration File Download/Upload screen fields.

**Table 42** 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 Value    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 Value    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/stack parameters to the specified TFTP server (default is No).</p> <p>Use the spacebar to toggle the selection to Yes.</p> <p>Press [Enter] to initiate the process.</p> <p>Default Value    No</p> <p>Range            Yes, No</p>
<b>Retrieve Configuration Image from Server</b>	<p>Specifies whether to retrieve the stored switch/stack 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/stack to reset with the new configuration parameters.</p> <p>Use the spacebar to toggle the selection to Yes.</p> <p>Press [Enter] to initiate the process.</p> <p>Default Value    No</p> <p>Range            Yes, No</p>

## Requirements

The following requirements apply to the Configuration File feature:

- The Configuration File feature can only be used to copy *standalone switch configuration parameters to other standalone switches* or to copy *stack configuration parameters to other stack configurations*.

For example, you cannot duplicate the configuration parameters of a unit in a *stack* configuration and use it to configure a *standalone* switch.

- A configuration file obtained from a standalone switch can only be used to configure other standalone switches that have the same firmware revision and model type as the donor standalone switch.
- A configuration file obtained from a stack unit can only be used to configure other stacks that have the same number of switches, firmware version, model types, and physical IDs as the stack the donor stack unit resides in.

Reconfigured stacks are configured according to the unit order number of the donor unit. For example, the configuration file parameters from a donor unit with physical ID *x* are used to reconfigure the unit with physical ID *x*.

[Table 43](#) describes configuration file parameter information.

**Table 43** Parameters not saved to the configuration file

These parameters are not saved:	Used in this screen:	See page:
In-Band Stack IP Address	IP Configuration/Setup	<a href="#">108</a>
In-Band Switch IP Address		
In-Band Subnet Mask		
Default Gateway		
Console Read-Only Switch Password	Console/Comm Port Configuration	<a href="#">165</a>
Console Read-Write Switch Password		
Console Read-Only Stack Password		
Console Read-Write Stack Password		
Configuration Image Filename	Configuration File Download/Upload	<a href="#">187</a>
TFTP Server IP Address		

---

## Chapter 4

# Troubleshooting

---

This chapter describes how to isolate and diagnose problems with your BayStack 425 and covers the following topics:

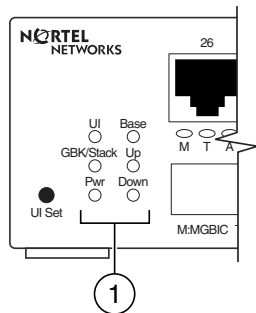
- [“Interpreting the LEDs,”](#) next
- [“Diagnosing and correcting problems”](#) on page 193
  - Normal power-up sequence
  - Port connection problems

The chapter topics lead you through a logical process for troubleshooting the BayStack 425. For example, because LEDs provide visual indications of certain problems, see [“Interpreting the LEDs”](#) on page 191 to understand the various states ([Table 44](#) and [Table 45](#)) that your switch LEDs can exhibit during normal operation.

For more help in determining the problem, [“”](#) on page 192 describes symptoms and corrective actions ([Table 46](#)) you can perform to resolve specific problems. Subsequent sections give step-by-step procedures to correct the problems.

## Interpreting the LEDs

[Figure 78](#) shows the BayStack 425 LED display panel. [Table 44](#) and [Table 45](#) describes the LEDs.

**Figure 78** LED display paneo

1 = Switch LEDs

11106EA

**Table 44** BayStack 425 Switch LED descriptions

Label	Color/Status	Meaning
UI	Green	The switch is operating normally.
	Amber	A flash error occurred.
	Off	The switch is inactive.
Base	Green	This switch is the active base unit in the stack.
	Amber	This switch is configured as the base unit, but is not currently the active base unit.
	Off	This switch is not the base unit, or is in a stand-alone configuration.
GBIC/Stack	Green	The GBIC port is linked. (Stacking is not available in this release).
	Off	The GBIC port is not linked.
Up	Green	A connection was detected to a unit through the stack up connector.
	Off	No connection was detected to a unit through the stack up connector.
Pwr	Green	Power is available to the switch.
	Off	No power is available to the switch.
Down	Green/steady	A connection was detected to a unit through the stack down connector.
	Off	No connection was detected to a unit through the stack down connector.



**Table 45** SFP GBIC Port LEDs on the BayStack 425 Switch

Label	Color/Status	Meaning
M (MGBIC)	Green	This port has a good connection (fiber).
	Off	This port does not have a good connection (fiber).
T (Copper)	Green	This port has a good connection (copper - at 1000 Mbps).
	Amber	This port has a good connection (copper - at 100 Mbps).
	Amber/Green	This port has a good connection (copper - at 10 Mbps)
	Off	This port does not have a good connection.
A (Activity)	Green (blinking)	There is activity on this port.
	Off	There is no activity on this port.

## Diagnosing and correcting problems

Before you perform the problem-solving steps in this section, cycle the power to the BayStack 425 (disconnect and then reconnect the AC power cord); then verify that the switch follows the normal power-up sequence.



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

---



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

---



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

---



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

---



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

---



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

---

## Normal power-up sequence

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


- 1 After power is applied to the switch, the Pwr (Power) LED turns on within 5 seconds.
- 2 The switch initiates a self-test, during which the port LEDs display various patterns to indicate the progress of the self-test.
- 3 After the self-test, the remaining port LEDs indicate their operational status, as described in [Table 46](#).

## Port connection problems

You can usually trace port connection problems to either a poor cable connection or an improper connection of the port cables at either end of the link. To remedy these types of problems, make sure that the cable connections are secure and that the cables connect to the correct ports at both ends of the link.

Port connection problems are also traceable to the autonegotiation mode or the port interface.

**Table 46** 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.
		 <b>Note:</b> Operating temperature for the switch must not exceed 40°C (104°F). Do not place the switch in areas where it can be exposed to direct sunlight or near warm air exhausts or heaters.
The Activity LED for a connected port is off or does not blink (and you have reason to believe that traffic is present).	The switch is experiencing a port connection problem. The switch's link partner is not autonegotiating properly.	See <a href="#">"Port connection problems"</a> next.

## 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 425 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 as follows:

- If the connected station uses a form of autonegotiation that is not compatible with the IEEE 802.3u autonegotiating standard, the BayStack 425 cannot negotiate a compatible mode for correct operation.
- If the autonegotiation feature is not present or not enabled at the connected station, the BayStack 425 may not be able to determine the correct duplex modes.

In both situations, the BayStack 425 “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:

- 1 Use the Port Configuration screen to disable autonegotiation for the suspect port (see [“Port Configuration screen” on page 145](#)).
- 2 Manually set the Speed/Duplex field to match the speed/duplex mode of the connected station (see [Table 26 on page 147](#)).

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

If the problem persists:

- 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 425 port.

### **Port interface**

Ensure that the devices are connected using the appropriate crossover or straight-through cable (see [Appendix D, “Connectors and pin assignments,” on page 213](#)), or that autonegotiation or autopolarity is active.

---

## Appendix A

# Technical specifications

---

This appendix provides technical specifications for the BayStack 420/425 Switch.

## Environmental

[Table 47](#) lists environmental specifications for the BayStack 425 Switch.

**Table 47** Environmental specifications

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

## Electrical

[Table 48](#) lists power electrical parameters for the BayStack 425 Switch.

**Table 48** Electrical parameters

Parameter	Electrical specification
Input Voltage	100 to 240 VAC @ 47 to 63 Hz
Input Power Consumption	50 W maximum
Input Volt Amperes Rating	65 VA maximum

**Table 48** Electrical parameters (continued)

Parameter	Electrical specification
Input current	1 A @ 100 VAC 0.5 A @ 240 VAC
Maximum thermal output	250 BTU/hr

## Physical dimensions

[Table 49](#) lists physical dimensions for the BayStack 425 Switch.

**Table 49** Physical dimensions

Parameter	Specifications
Height	1.75 in (4.5 cm)
Width	17.125 in (43.5 cm)
Depth	8.0 in (20.32 cm)
Weight	6.2 lb (2.82 kg)

## Performance specifications

[Table 50](#) lists performance specifications for the BayStack 425 Switch.

**Table 50** Performance specifications

Parameter	Specifications
Frame Forward Rate (64-byte packets)	Up to 3.2 million packets per second (pps) maximum, learned unicast traffic; 5.1 million packets per second (pps) in a stack configuration
Port Forwarding/Filtering Performance (64-byte packets)	<ul style="list-style-type: none"><li>• For 10 Mb/s: 14,880 pps maximum</li><li>• For 100 Mb/s: 148,810 pps maximum</li></ul>
Address Database Size	8,000 entries at line rate
Addressing	48-bit MAC address
Frame Length	64 to 1518 bytes (IEEE 802.1Q Untagged) 68 to 1522 bytes (IEEE 802.1Q Tagged)

## Network protocol and standards compatibility

The following are protocols and standards used by the BayStack 425 Switch:

- IEEE 802.3 10BASE-T (ISO/IEC 8802-3, Clause 14)
- IEEE 802.3u 100BASE-TX (ISO/IEC 8802-3, Clause 25)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1z (Gigabit)
- IEEE 802.1d (Spanning tree protocol)

## Safety agency certification

- The safety certifications follow for the BayStack 425 Switch:
- UL Listed (UL 1950)
- IEC 950/EN60950 (CB report) with all national deviations
- C22.2 No. 950 (CUL)
- UL-94-V1 flammability requirements for PC board
- NOM (NOM-019)

## Electromagnetic emissions

- The electromagnetic emission standards for the BayStack 425 Switch:
- US. CFR47, Part 15, Subpart B, Class A
- Canada. ICES-003, Issue 2, Class A
- Australia/New Zealand. AS/NZS 3548:1995, Class A
- Japan. V-3/97.04:1997, Class A
- Taiwan. CNS 13438, Class A
- EN55022:1995, Class A
- EN61000-3-2:1995
- EN61000-3-3:1994

## **Electromagnetic immunity**

The BayStack 425 Switch meets the EN50082-1:1997 standard.



---

## Appendix B

# Installing a Gigabit Interface Converter (GBIC)

---

This appendix describes how to install and remove a Gigabit Interface Converter (GBIC). It also provides a description of the GBIC, the GBIC label, and GBIC specifications.

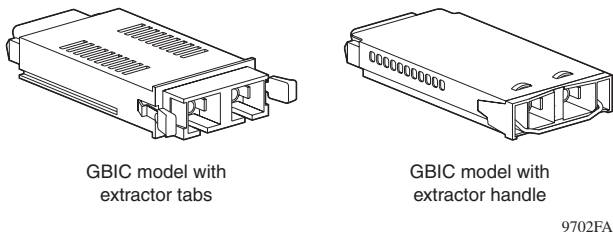
### Product description

GBICs are hot-swappable input/output enhancement components designed for use with Nortel Networks products to allow Gigabit Ethernet ports to link with fiber optic networks.

The following GBIC versions are available for the BayStack 425 Switch:

- 1000BASE-SX—uses multimode fiber over distances up to 550 meters
- 1000BASE-LX—uses multimode fiber over distances up to 550 meters or single-mode fiber over distances up to 10 kilometers
- 1000BASE-XD—uses single-mode fiber over distances up to 50 km
- 1000BASE-ZX—uses single-mode fiber over distances up to 70 km

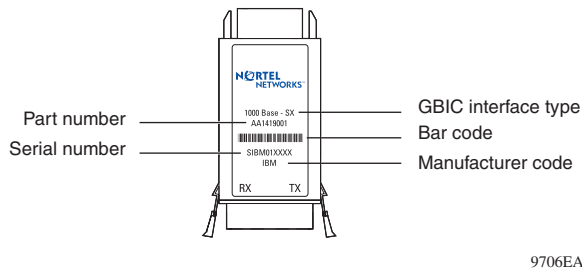
GBICs are available in different case styles. One type has two spring tabs at the front of the GBIC; the other type has an extractor handle on the front ([Figure 79](#)).

**Figure 79** Types of GBICs

GBICs are shipped with a protective rubber plug in the connectors. Leave the plug in place when no cables are connected to the GBIC.

## GBIC labeling

The Nortel Networks label on a typical GBIC ([Figure 80](#)) contains a Nortel Networks serial number, a bar code, a manufacturer's code, an interface type, and a part number.

**Figure 80** Nortel label on a GBIC

**Note:** You must have the Nortel Networks serial number, the manufacturer's code, the interface type, and the part number of your GBIC available when you contact a Nortel Networks service representative for troubleshooting purposes.

## GBIC Models

[Table 51](#) lists the available Nortel Networks GBIC models.

**Table 51** Nortel Networks GBIC models

Model number	Product number	Description
1000BASE-SX	AA1419001	Short wavelength 550 m
1000BASE-LX	AA1419002	Long wavelength 5 km
1000BASE-XD	AA1419003	Extended distance 50 km
1000BASE-ZX	AA1419004	Extended distance 70 km

## GBIC specifications

GBIC specifications are listed in [Table 52](#).

**Table 52** GBIC specifications

Specifications	Description
Dimensions (H x W x D)	0.39 x 1.18 x 2.56 inches (1 x 3 x 6.5 cm)
Connectors	Multimode fiber optic: SC Single-mode fiber optic: SC

## Standards, connectors, cabling, and distance

This section discusses GBIC standards, connectors, cabling, and distance. The tables provide specifications for GBICs to be installed in Gigabit Ethernet ports. All GBIC ports have SC-type connectors, and the minimum cable distance for all GBICs (multimode fiber and single-mode fiber) listed is 6.5 feet (2 m).

### 1000BASE-SX

The Model 1000BASE-SX GBIC provides 1000BASE-SX (850 nm, short wavelength, Gigabit Ethernet) connectivity using SC duplex multimode fiber connectors. The Model 1000BASE-SX GBIC supports full-duplex operation only.

Table 53 describes standards, connectors, cabling, and distance for the Model 1000BASE-SX GBIC.

**Table 53** Model 1000BASE-SX GBIC specifications

Type	Specifications
Standards	Conformity to the following standards: 802.3z, 1000BASE-SX
Connectors	Duplex SC fiber optic connector
Cabling	62.5 $\mu\text{m}$ MMF optic cable 50 $\mu\text{m}$ MMF optic cable
Distance	902 ft. (275 m) using 62.5 $\mu\text{m}$ MMF optic cable 1804 ft. (550 m) using 50 $\mu\text{m}$ MMF optic cable
Wavelength	850 nm
Optical budget	7 dB
<b>Laser Transmitter Characteristics</b>	
Minimum launch power	-10 dBm
Maximum launch power	-4 dBm
<b>Receiver Characteristics</b>	
Minimum receiver sensitivity	-17 dBm
Maximum input power	0 dBm

## 1000BASE-LX

The Model 1000BASE-LX GBIC provides 1000BASE-LX (1300 nm, wavelength, Gigabit Ethernet) connectivity using SC duplex fiber connectors. The long wavelength optical transceivers used in the LX model provide variable distance ranges using both multimode and single-mode fiber optic cabling. The Model 1000BASE-LX GBIC supports full-duplex operation only.

Table 54 describes standards, connectors, cabling, and distance for the Model 1000BASE-LX GBIC.

**Table 54** Model 1000BASE-LX GBIC specifications

Type	Specifications
Standards	Conformity to the following standards: 802.3z, 1000BASE-LX
Connectors	Duplex SC fiber optic connector
Cabling	62.5 $\mu\text{m}$ MMF optic cable 50 $\mu\text{m}$ MMF optic cable 10 $\mu\text{m}$ SMF optic cable
Distance	1804 ft. (550 m) using 62.5 $\mu\text{m}$ MMF optic cable 1804 ft. (550 m) using 50 $\mu\text{m}$ MMF optic cable 16405 ft. (5 km) using 10 $\mu\text{m}$ SMF optic cable
Wavelength	1300 nm
Optical budget	10.5 dB
<b>Laser Transmitter Characteristics</b>	
Minimum launch power	-9.5 dBm
Maximum launch power	-3 dBm
<b>Receiver Characteristics</b>	
Minimum receiver sensitivity	-20 dBm
Maximum input power	-3 dBm



**Note:** When multimode fiber is used in long distance applications, external, removable, mode-conditioning patch cords may be required to prevent differential mode delay (DMD). You can order mode conditioning patch cords through Nortel Networks:

- SC-SC Mode Conditioning Patch Cord 62.5/125—part number AA0018035
- SC-SC Mode Conditioning Patch Cord 50/125—part number AA0018036

## 1000BASE-XD

The Model 1000BASE-XD GBIC provides Gigabit Ethernet connectivity using SC duplex single-mode fiber connectors. High-performance optical transceivers enable Gigabit Ethernet link distances up to 50 kilometers (km) over single-mode fiber. The ports operate in full-duplex mode only.

[Table 55](#) describes standards, connectors, cabling, and distance for the Model 1000BASE-XD GBIC.

**Table 55** Model 1000BASE-XD GBIC specifications

Type	Specifications
Standards	Conformity to the following standards: 802.3z, Ethernet full duplex
Connectors	SC duplex single-mode fiber optic connector
Cabling	Single-mode fiber optic cable
Distance	Up to 50 km using single-mode fiber cable, depending on the quality of the fiber
Optical budget	17 dB
<b>Laser Transmitter Characteristics</b>	
Wavelength	1550 ± 10 nm
Maximum spectral width	0.2 nm
Maximum launch power	0 dBm or 1.0 mW
Minimum launch power into fiber	-5 dBm or 0.3 mW
Distance	50 km
<b>Receiver Characteristics</b>	
Wavelength	1200 to 1550 nm
Minimum receiver sensitivity	-22 dBm
Maximum input power	-3 dBm



**Note:** Nortel Networks recommends that you use an in-line attenuator for shorter link distances to avoid overloading the receiver.



**Note:** The Model 1000BASE-XD GBIC is based on proprietary signaling and is compatible with Accelar 1000 Series XD modules.

## 1000BASE-ZX

The Model 1000BASE-ZX GBIC provides Gigabit Ethernet connectivity using SC duplex single-mode fiber connectors. High-performance optical transceivers enable Gigabit Ethernet link distances up to 70 km over single-mode fiber cable. The ports operate in full-duplex mode only.

[Table 56](#) describes standards, connectors, cabling, and distance for the Model 1000BASE-ZX GBIC.

**Table 56** Model 1000BASE-ZX GBIC specifications

Type	Specifications
Standards	Conformity to the following standards: 802.3z, Ethernet full duplex
Connectors	SC duplex single-mode fiber optic connector
Cabling	Single-mode fiber optic cable
Distance	Up to 70 km using single-mode fiber optic cable, depending on the quality of the fiber
Optical budget	22 dB
<b>Laser Transmitter Characteristics</b>	
Wavelength	1550 ± 10 nm
Maximum spectral width	0.2 nm
Maximum launch power	3.0 mW ± 5 dBm
Minimum launch power into fiber	0 dBm
Distance	70 km
<b>Receiver Characteristics</b>	
Wavelength	1200 nm to 1550 nm
Minimum receiver sensitivity	-22 dBm
Maximum input power	-3 dBm



**Note:** When shorter lengths of single-mode fiber cable are used, there is a risk of overloading the receiver. It may be necessary to insert an in-line optical attenuator in the link to prevent overloading, as follows:

- Insert a 10dB in-line optical attenuator between the fiber optic cable plant and the receiving port on the 1000BASE-ZX GBIC, at each end of the link, if the fiber optic cable span is less than 25 km.
- Insert a 5dB in line optical attenuator between the fiber optic cable plant and the receiving port on the 1000BASE-ZX GBIC, at each end of the link, if the fiber optic cable span is less than 50 km.



**Note:** The 1000BASE-ZX GBIC is based on proprietary signaling. Nortel Networks recommends that this product be used only with other Nortel Networks 1000BASE-ZX GBICs.

---

## Handling, safety, and environmental guidelines

Before installing your GBIC, read the following handling, safety, and environmental guidelines:

- GBICs are static sensitive. To prevent damage from electrostatic discharge (ESD), follow your normal board and component handling procedures.
- GBICs are dust sensitive. When storing a GBIC, or when a GBIC is disconnected from a fiber optic cable, always keep the dust cover over a GBIC's optical bores.
- To clean contaminants from the optical bores of a GBIC, use an alcohol swab or equivalent to clean the ferrules of the optical connector.
- Dispose of this product according to all national laws and regulations.



## Installing a GBIC

GBIC bays are covered by spring-loaded filler panels that rotate out of the way as you push the GBIC into place. You can install or replace a GBIC in a BayStack 425 Switch without turning off power to the switch.



**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.

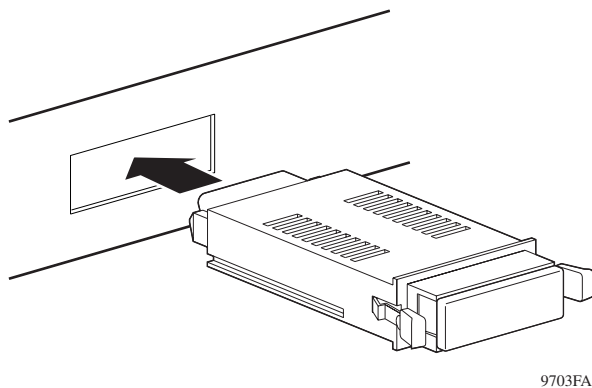


8769EA

To install a GBIC:

- 1 Remove the GBIC from its protective packaging.
- 2 Insert the GBIC into the slot on the BayStack switch (Figure 81).  
GBICs are keyed to prevent improper insertion. If the GBIC resists pressure, do not force it. Remove it, turn it over, and reinsert it.

**Figure 81** Installing a GBIC

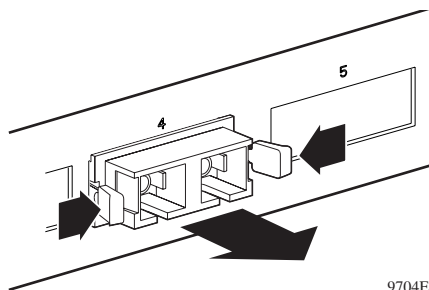


- 3 Press on the front of the GBIC until it snaps into place.
- 4 Remove the rubber plug to connect cables.

To remove an installed GBIC:

- 1 If the GBIC has spring tabs, press in on the tabs on each side of the GBIC as you pull the GBIC out of the bay (Figure 82).

**Figure 82** Removing a GBIC



- 2 If the GBIC has an extractor handle, grasp the handle and pull firmly to remove the GBIC from the bay.

---

## Appendix C

# Quick configuration for MultiLink Trunking

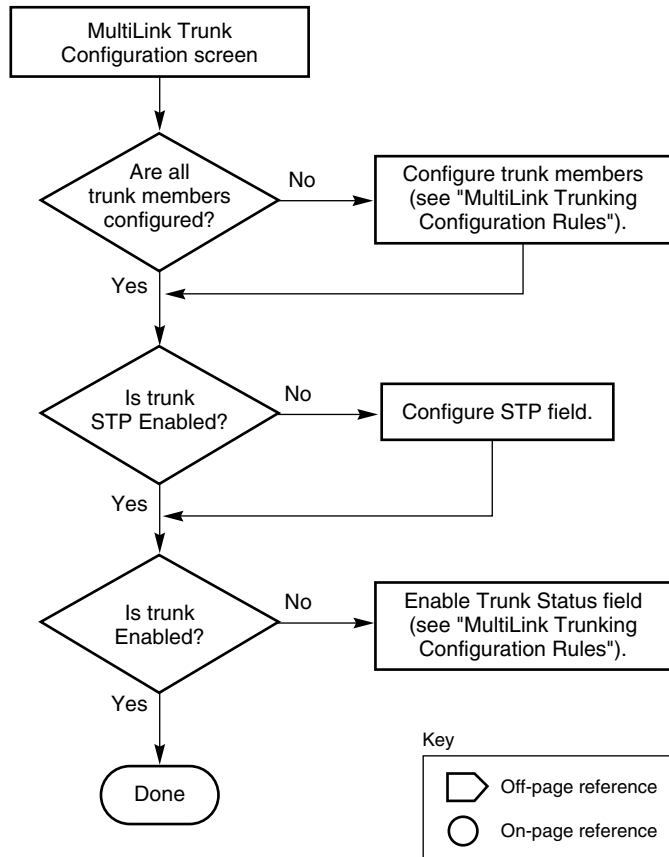
---

If you are a system administrator with experience configuring Baystack 420 Switch MultiLink Trunking, use the flowchart in [Figure 83 on page 212](#) as a quick configuration guide. The flowchart refers you to the “configuration rules” appropriate for this feature.

To open the MultiLink Trunk Configuration screen:

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

**Figure 83** Configuring MultiLink Trunks



BS45050A

---

## Appendix D

# Connectors and pin assignments

---

This appendix describes the Baystack 420 Switch port connectors and pin assignments.

### RJ-45 (10BASE-T/100BASE-TX) port connectors

The RJ-45 port connectors ([Figure 84](#)) are wired as MDI-X ports to connect end stations without using crossover cables. (See [“MDI and MDI-X devices” on page 214](#) 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 84** RJ-45 (8-pin modular) port connector

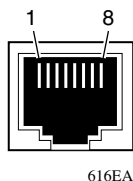


Table 57 lists the RJ-45 (8-pin modular) port connector pin assignments.

**Table 57** RJ-45 port connector pin assignments

Pin	Signal	Description
1	RX+	Receive Data +
2	RX-	Receive Data -
3	TX+	Transmit Data +
4	Not applicable	Not applicable
5	Not applicable	Not applicable
6	TX-	Transmit Data -
7	Not applicable	Not applicable
8	Not applicable	Not applicable

## MDI and MDI-X devices

Media dependent interface (MDI) is the IEEE standard for the interface to unshielded twisted pair (UTP) cable.

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

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



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

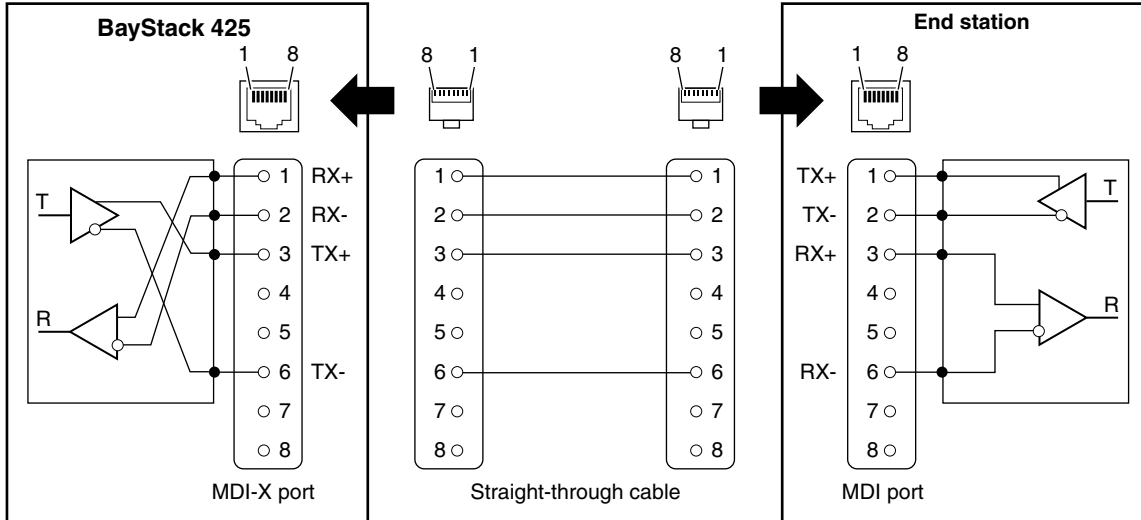
---

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

## MDI-X to MDI cable connections

BayStack 420 10/100/1000 Switch switches use MDI-X ports that allow you to connect directly to end stations without using crossover cables (Figure 85).

**Figure 85** MDI-X to MDI cable connections

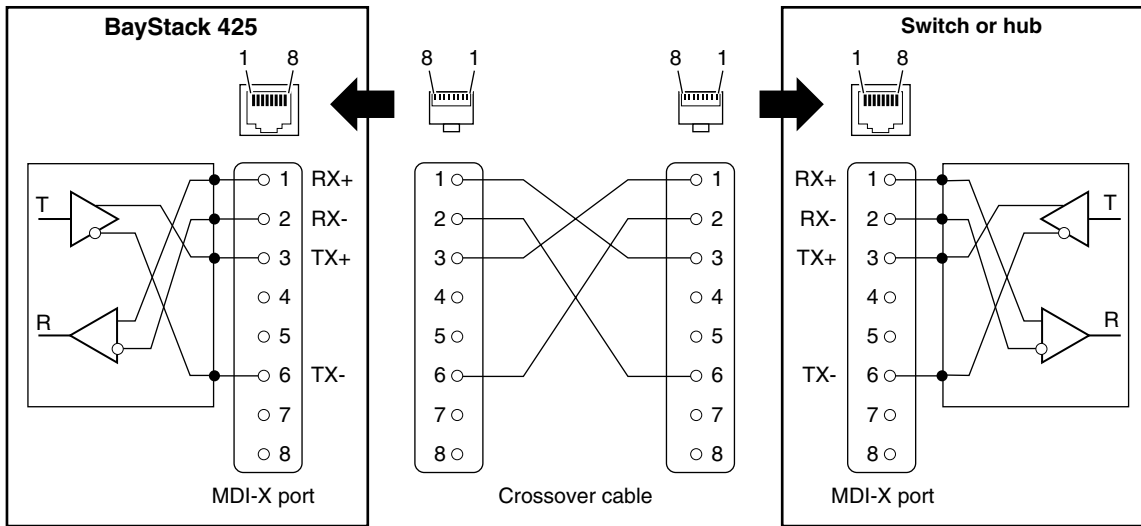


BS45056A

## MDI-X to MDI-X cable connections

If you are connecting the BayStack 420 10/100/1000 Switch to a device that also implements MDI-X ports, use a crossover cable (Figure 86).

**Figure 86** MDI-X to MDI-X cable connections

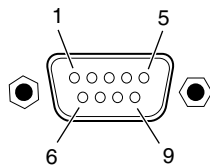


BS45057B

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

The DB-9 Console/Comm Port connector (Figure 87) 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 87** DB-9 Console port connector



619EA



Table 58 lists the DB-9 Console port connector pin assignments.

**Table 58** DB-9 Console 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	Not used
7	RTS	Request to send (not used)
8	CTS	Not used
9	RI	Ring indicator (not used)
Shell		Chassis ground



## Appendix E

### Default settings

Table 59 lists the factory default settings for the BayStack 425 Switch according to the console interface (CI) screens and fields for the settings.

**Table 59** Factory default settings

Field	Default setting	Appears in this CI screen
BootP Request Mode	BootP Disabled	"IP Configuration/Setup screen" on page 108
In-Band Stack IP Address	0.0.0.0 (no IP address assigned)	
In-Band Switch IP Address	0.0.0.0 (no IP address assigned)	
In-Band Subnet Mask	0.0.0.0 (no subnet mask assigned)	
Default Gateway	0.0.0.0 (no IP address assigned)	
Read-Only Community String	public	"SNMP Configuration screen" on page 113
Read-Write Community String	private	
Trap IP Address	0.0.0.0 (no IP address assigned)	
Community String	Zero-length string	
Authentication Trap	Enabled	
Link Up/Down Trap	Enabled	
sysContact	Zero-length string	"System Characteristics screen" on page 115
sysName	Zero-length string	
sysLocation	Zero-length string	

**Table 59** Factory default settings (continued)

Field	Default setting	Appears in this CI screen
Aging Time	300 seconds	"MAC Address Table screen" on page 120
Find an Address	00-00-00-00-00-00 (no MAC address assigned)	
MAC Address Security	Disabled	"MAC Address Security Configuration Menu screen" on page 122
MAC Address Security SNMP-Locked	Disabled	
Partition Port on Intrusion Detected:	Disabled	
Partition Time	0 seconds (the value 0 indicates forever)	
DA Filtering on Intrusion Detected:	Disabled	
Generate SNMP Trap on Intrusion	Disabled	
Clear by Ports	NONE	
Learn by Ports	NONE	
Current Learning Mode	Not Learning	
Trunk	blank field	"MAC Address Security Port Configuration screen" on page 127
Security	Disabled	
Port List	blank field	"MAC Address Security Port Lists screens" on page 130
Find an Address	blank field	"MAC Address Security Table screens" on page 134
MAC Address	- - - - - (no address assigned)	
Allowed Source	- (blank field)	
Display/Create MAC Address	00-00-00-00-00-00	
Create VLAN	1	"VLAN Configuration screen" on page 138
Delete VLAN	blank field	
VLAN Name	VLAN # ( <i>VLAN number</i> )	
Management VLAN	Yes, VLAN #1	
VLAN Type	Port-based	
VLAN State	Inactive	

**Table 59** Factory default settings (continued)

Field	Default setting	Appears in this CI screen
Subnet Addr	0.0.0.0.	
Subnet Mask	0.0.0.0.	
Port Membership	U (all ports assigned as untagged members of VLAN 1)	
Unit	1	<a href="#">"VLAN Port Configuration screen" on page 141</a>
Port	1	
Filter Untagged Frames	No	
Port Name	Unit 1, Port 1	
PVID	1	
Tagging	Untagged Access	
Unit	1	<a href="#">"VLAN Display by Port screen" on page 143</a>
Port	1	
PVID	1 (read only)	
Auto PVID	Disabled	
Port Name	Unit 1, Port 1 (read only)	
Unit	1	<a href="#">"Port Configuration screen" on page 145</a>
Status	Enabled (for all ports)	
Autonegotiation	Enabled (for all ports)	
Speed/Duplex	100Mbps/Half (when Autonegotiation is Disabled)	
Trunk	1 to 6 (depending on configuration status)	<a href="#">"MultiLink Trunk Configuration Menu screen" on page 151</a>
Trunk Members (Unit/Port)	Blank field	
STP Learning	Normal	
Trunk Mode	Basic	
Trunk Status	Disabled	
Trunk Name	Trunk #1 to Trunk #6	
Traffic Type	Rx and Tx	<a href="#">"MultiLink Trunk Utilization screen" on page 155</a>

**Table 59** Factory default settings (continued)

Field	Default setting	Appears in this CI screen
Monitoring Mode	Disabled	"Port Mirroring Configuration screen" on page 157
Monitor/Unit Port	Zero-length string	
Unit/Port X	Zero-length string	
Unit	1	"Port Statistics screen" on page 159
Port	1	
Console Port Speed	9600 Baud	"Console/Comm Port Configuration screen" on page 165
Console Switch Password	Not Required	
Console Stack Password	Not Required	
Console Read-Only Switch Password	user	
Console Read-Write Switch Password	secure	
Console Read-Only Stack Password	user	
Console Read-Write Stack Password	secure	
<b>Note:</b> The following two fields only appear when the switch is a participant in a stack configuration.		
New Unit Number	Current stack order	"Re-number Stack Units screen" on page 172
Re-number units with new setting?	No	
Unit	1	"Spanning Tree Port Configuration screen" on page 175
Participation	Normal Learning	
Priority	128	
Path Cost	10 or 100	
Bridge Priority	8000 (read only)	"Spanning Tree Switch Settings screen" on page 179
Designated Root	8000 (bridge_id) (read only)	
Root Port	0 (read only)	
Root Path Cost	0 (read only)	
Hello Time	2 seconds (read only)	
Maximum Age Time	20 seconds (read only)	

**Table 59** Factory default settings (continued)

Field	Default setting	Appears in this CI screen
Forward Delay	15 seconds (read only)	
Bridge Hello Time	2 seconds (read only)	
Bridge Maximum Age Time	20 seconds (read only)	
Bridge Forward Delay	15 seconds (read only)	
TELNET Access	Enabled	<a href="#">“TELNET Configuration screen” on page 182</a>
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	<a href="#">“Software Download screen” on page 184</a>
TFTP Server IP Address	0.0.0.0 (no IP address assigned)	
Start TFTP Load of New Image	No	
Configuration Image Filename	Zero-length string	<a href="#">“Configuration File Download/Upload screen” on page 187</a>
TFTP Server IP Address	0.0.0.0 (no IP address assigned)	
Copy Configuration Image to Server	No	
Retrieve Configuration Image from Server	No	





---

## Appendix F

# Sample BootP configuration file

---

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

A sample BootP configuration file follows:

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

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

bay1|ht=ethernet|ha=0060fd000000|ip=192.0.0.1|hd=c:\ezlan\images|bf= BS425-24T_100.img

# Where:
#   host name:                bay1
#   hardware type:           Ethernet
#   MAC address:             00-60-FD-00-00-00
#   IP address:              192.0.0.0
#   home directory of boot file: c:\ezlan\images
#   boot file:               BS425-24T_100.img
```

---

# Index

---

## A

Actual Hello Interval 180  
Aging Time field 121  
Allowed Source IP Address field 184  
Allowed Source Mask field 184  
Authentication Trap field 114  
autonegotiation  
    description 46  
    modes 194  
    troubleshooting 195  
Autonegotiation field 148  
autosense description 46

## B

BayStack 425 switch  
    connectors 213  
    default port settings for VLANs 68  
BootP  
    Always mode 111  
    BOOTPTAB.TXT file 225  
    Bootstrap Protocol  
        choosing a request mode 110  
    Disabled 112  
    Last Address setting 112  
    Last BootP field 109  
    Request Mode field 109  
    sample configuration file 225  
    When Needed mode 111  
BPS 2000 Image Filename field 186  
Bridge Forward Delay field 181  
Bridge Hello Time field 181  
Bridge Maximum Age Time field 181

Bridge Priority field 180  
Broadcasts field 161  
Business Policy Switch  
    front panel 28

## C

Clear All Port Statistics option 120  
Collisions field 162  
Comm Port Data Bits field 166  
Comm Port Parity field 166  
Comm Port Stop Bits field 166  
Community String field 114  
Configurable field 109  
configuration rules  
    VLANs 82  
connectors 213  
    DB-9 console/comm port connector 216  
    RJ-45 port connector 213  
console interface (CI)  
    main menu 104  
    menus, using 102  
Console Password field 168  
Console Port Speed field 166  
Console Read-Only Password field 169, 170  
Console Read-Write Password field 169, 170  
console/comm port  
    configuration screen 165  
    illustration 216  
    pin assignments 217  
Console/Comm Port Configuration options 106  
conventions, text 22

conversation steering 45

crossover cable 215

customer support 25

## D

DB-9 console/comm port connector 216

Default Gateway field 110

default settings 219

Deferred Packets field 162

Designated Root field 180

Display Event Log option 106

Display Port Statistics option 119

Display Spanning Tree Switch Settings option 175

## E

electrostatic discharge  
and GBICs 208

Event Logging field 183

Excessive Collisions field 162

## F

FCS Errors field 162

fiber optic networks  
linking with Gigabit Ethernet ports 29, 201

Filtered Packets field 162

Find an Address field 121

flash memory for software image upgrades 43

Flooded Packets field 162

Forward Delay field 181

Frame Errors field 162

## G

GBIC

cleaning 208

connectors 203

description 203

dimensions 203

disposal 208

handling 208

labels 202

Model

1000BASE-LX 203, 204

1000BASE-SX 203, 204

1000BASE-XD 203, 206

1000BASE-ZX 203, 207

specifications 203

storing 208

Gigabit Ethernet ports,  
linking with fiber optic networks 29, 201

## H

Hello Interval 180, 181

Hello Time field 180

## I

IEEE 802.1Q tagging important terms 67

IEEE 802.3u standard 46

In Use field 109

Inactivity Timeout field 183

In-Band IP Address field 109

In-Band Subnet Mask field 110

interoperability issues  
configuration requirements 202  
setting up your configuration 201

IP Configuration option 105

IP Configuration screen 108

## L

labels

reading 202

Late Collisions field 162

LEDs

descriptions 31

display panel 31, 192

Link field 148  
Login Retries field 183  
Login Timeout field 183  
Logout option 107  
Lost Packets field 161

## M

MAC Address Table option 119  
MAC Address Table screen 120  
MAC address-based network security 42  
main menu, console interface 104  
Maximum Age Time field 180  
MDI-X to MDI cable connections 215  
MDI-X to MDI-X cable connections 215  
MIBs SNMP MIB support 47  
Model  
    1000BASE-LX 203, 204  
    1000BASE-SX 203, 204  
    1000BASE-XD 203, 206  
    1000BASE-ZX 203, 207  
multimode fiber,  
    in long distance applications 205  
Multicasts field 161  
MultiLink Trunk Configuration option 119  
MultiLink Trunk Configuration screen 151  
MultiLink Trunking  
    configuration example 82  
    feature 43  
Multiple Collisions field 162

## N

network configuration  
    configuring power workgroups and a shared  
    media hub 61  
network protocol/standards compatibility 199

## O

optical attenuators,  
    when to use 208  
options  
    Clear All Port Statistics 120  
    Console/Comm Port Configuration 106  
    Display Event Log 106  
    Display Port Statistics 119  
    Display Spanning Tree Switch Settings 175  
    IP Configuration 105  
    Logout 107  
    MAC Address Table 119  
    MultiLink Trunk Configuration 119  
    Port Configuration 119  
    Port Mirroring Configuration 119  
    Reset 105, 107  
    Reset to Default Settings 107  
    SNMP Configuration 105  
    Software Download 106  
    Spanning Tree Configuration 106  
    Spanning Tree Port Configuration 175  
    Switch Configuration 106  
    System Characteristics 106  
    TELNET Configuration 106  
    VLAN Configuration 119  
Oversized Packets field 162

## P

Packets field 161  
Participation field 178  
patch cords,  
    for multimode fiber applications 205  
Path Cost field 178  
Port Configuration option 119  
Port Configuration screen 145  
port connections, troubleshooting 194  
Port field 147, 161, 177  
port mirroring  
    conversation steering 45  
    monitoring modes 159

- Nortel Networks StackProbe 45
- Port Mirroring Configuration option 119
- Port Mirroring Configuration screen 157
- Port Statistics screen 159
- power cord warnings (multilingual) 35
- power cords 34
- power-up sequence 194
- Priority field 178
- product support 25
- publications
  - related 24, 46

## R

- RADIUS-based network security 42
- Read-Only Community String field 114
- Read-Write Community String field 114
- request mode, choosing 110
- requirements
  - power cords 34
- Reset to Default Settings option 107
- RFC 46
- RJ-45 port connector
  - illustration 213
  - pin assignments 214
- Root Path Cost field 180
- Root Port field 180

## S

- Security
  - MAC address-based network security 42
  - RADIUS-based network security 42
- settings, default 219
- Single Collisions field 162
- SNMP Configuration option 105
- SNMP Configuration screen 113
- software
  - download process 187

- image upgrades 43
- Software Download option 106
- Spanning Tree Configuration Menu 174
- Spanning Tree Configuration option 106
- Spanning Tree Port Configuration option 175
- Spanning Tree Port Configuration screen 175
- Spanning Tree Switch Settings screen 179
- specifications
  - GBIC 203
- specifications,
  - Model
    - 1000BASE-LX 204
    - 1000BASE-SX 204
    - 1000BASE-XD 206
    - 1000BASE-ZX 207
- Speed/Duplex field 148
- stack MAC address 63
- stack up/down configurations 63
- stacking
  - cascade module slot 33
  - considerations 66
  - initial installation 62
  - overview 61
  - stack MAC address 63
  - stacking considerations 63
- standards 47
- Start TFTP Load of New Image field 187
- State field 178
- Status field 148
- support, Nortel Networks 25
- Switch Configuration Menu 118
  - options 119
- Switch Configuration option 106
- System Characteristics option 106
- System Characteristics screen 115
- System Characteristics screen fields
  - Base Unit 116
  - Last Reset Type 117

- Local MDA Type 117
- MAC Address 117
- Operational Mode 116
- Power Status 117
- Reset Count 117
- Size of Stack 116
- sysContact 117
- sysDescr 117
- sysLocation 117
- sysName 117
- sysObjectID 117
- sysServices 117
- sysUpTime 117

## T

- technical specifications 197
- technical support 25
- technical terms
  - port priority 68
  - port VLAN identifier (PVID) 67
  - tagged frame 68
  - tagged member 68
  - unregistered packet/frame 68
  - untagged frame 68
  - untagged member 68
  - user\_priority 68
  - VLAN identifier (VID) 67
  - VLAN port members 68
- TELNET Access field 183
- TELNET Configuration option 106
- TELNET Configuration screen 182
- text conventions 22
- TFTP Server IP Address field 187, 189
- Total Octets field 161
- Trap IP Address fields 114
- Trivial File Transfer Protocol (TFTP)
  - software download 185
- troubleshooting 202
  - port interface 195
  - power-up sequence 194

- tutorial
  - IEEE 802.1Q tagging 67
  - IEEE 802.1Q VLAN workgroups 66

## U

- Undersized Packets field 162
- Uplink/Expansion slot 28, 29

## V

- virtual LAN (VLAN)
  - configuration rules 82
  - network example 57
- VLANs
  - Configuration option 119
  - Configuration screen 137
  - port-based 37

