

Part No. 215660-B
July 2004

4655 Great America Parkway
Santa Clara, CA 95054

Using Web-based Management for the BayStack 420/425, 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.

Contents

Preface	17
Before you begin	17
Text conventions	18
Related publications	18
How to get help	19
Chapter 1	
Using the Web-based management interface	21
Requirements	21
Logging in to the Web-based management interface	22
Menu	23
Management page	25
Chapter 2	
Administering the switch	29
Viewing system information	29
Configuring system security	30
Setting console, Telnet, and Web passwords	31
Configuring remote dial-in access security	32
Accessing the management interface	33
Rebooting the BayStack 425-24T Switch	36
Changing the BayStack 425-24T Switch to system defaults	37
Logging out of the management interface	38
Chapter 3	
Viewing summary information	39
Viewing stack information	39
Viewing summary switch information	41

Changing stack numbering	42
Identifying unit numbers	44
Chapter 4	
Configuring the switch	45
Configuring BootP, IP, and gateway settings	46
Modifying system settings	48
About SNMP	50
Configuring SNMPv1	50
Configuring SNMPv3	52
Viewing SNMPv3 system information	52
Configuring user access to SNMPv3	55
Creating an SNMPv3 system user configuration	55
Deleting an SNMPv3 system user configuration	57
Configuring an SNMPv3 system user group membership	57
Mapping an SNMPv3 system user to a group	58
Deleting an SNMPv3 group membership configuration	59
Configuring SNMPv3 group access rights	60
Creating an SNMPv3 group access rights configuration	60
Deleting an SNMPv3 group access rights configuration	62
Configuring an SNMPv3 management information view	63
Creating an SNMPv3 management information view configuration	63
Deleting an SNMPv3 management information view configuration	65
Configuring an SNMPv3 system notification entry	66
Creating an SNMPv3 system notification configuration	66
Deleting an SNMPv3 system notification configuration	67
Configuring an SNMPv3 management target address	68
Creating an SNMPv3 target address configuration	68
Deleting an SNMPv3 target address configuration	70
Configuring an SNMPv3 management target parameter	70
Creating an SNMPv3 target parameter configuration	70
Deleting an SNMPv3 target parameter configuration	72
Configuring an SNMP trap receiver	73
Creating an SNMP trap receiver configuration	73
Deleting an SNMP trap receiver configuration	74

Viewing learned MAC addresses by VLAN	75
Locating a specific MAC address	76
Configuring switch port autonegotiation speed	77
Configuring high speed flow control	80
Downloading switch images	81
Storing and retrieving a switch configuration file from a TFTP server	84
Requirements for storing and retrieving configuration parameters on a TFTP server	85
Configuring port communication speed	86
Chapter 5	
Configuring Remote Network Monitoring	89
Configuring RMON fault threshold parameters	89
Creating an RMON fault threshold	89
Deleting an RMON threshold configuration	92
Viewing the RMON fault event log	93
Viewing the system log	94
Viewing RMON Ethernet statistics	97
Viewing RMON history	99
Chapter 6	
Viewing system statistics	101
Viewing port statistics	101
Zeroing ports	104
Viewing interface statistics	105
Viewing Ethernet error statistics	106
Viewing transparent bridging statistics	109
Chapter 7	
Configuring application settings	111
Configuring port mirroring	111
Configuring MAC address-based security	113
Configuring MAC address-based security	114
Configuring ports	116
Adding MAC addresses	118

Clearing ports	120
Enabling security on ports	121
Deleting ports	123
Filtering MAC destination addresses	123
Deleting MAC DAs	124
Creating and managing VLANs	125
Port-based VLANs	125
Configuring VLANs	125
Creating a port-based VLAN	127
Modifying a port-based VLAN	128
Selecting a management VLAN	130
Deleting a VLAN configuration	131
Configuring broadcast domains	131
Viewing VLAN port information	132
Managing Spanning Tree Protocol	134
Changing Spanning Tree bridge switch settings	136
Configuring MultiLink Trunk members	140
Monitoring MLT traffic	142
Chapter 8	
Support menu	145
Using the online Help option	145
Downloading technical publications	147
Upgrade option	148
Index	149

Figures

Figure 1	Web-based management interface home page	22
Figure 2	Menu Page	23
Figure 3	Console page	26
Figure 4	System Information page	30
Figure 5	Console password setting page	31
Figure 6	RADIUS page	33
Figure 7	Web-based management interface log on page	34
Figure 8	System Information page	35
Figure 9	Reset page	36
Figure 10	Reset to Default page	37
Figure 11	Stack Information page	40
Figure 12	Switch Information page	41
Figure 13	Stack Numbering Setting page	43
Figure 14	Identify Unit Numbers page	44
Figure 15	IP page	46
Figure 16	System page	49
Figure 17	SNMPv1 page	51
Figure 18	System Information page	53
Figure 19	User Specification page	55
Figure 20	Group Membership page	58
Figure 21	Group Access Rights page	61
Figure 22	Management Information View page	64
Figure 23	Notification page	66
Figure 24	Target Address page	68
Figure 25	Target Parameter page	71
Figure 26	SNMP Trap Receiver page	73
Figure 27	MAC Address Table page	75
Figure 28	Find MAC Address Table page	77
Figure 29	Port Management page	78

14 Figures

Figure 30	High Speed Flow Control page	80
Figure 31	Software Download page	82
Figure 32	Configuration File Download/Upload page	84
Figure 33	Console/Communication Port page	87
Figure 34	RMON Threshold page	90
Figure 35	RMON Event Log page	94
Figure 36	System Log page	95
Figure 37	RMON Ethernet page	97
Figure 38	RMON History page	99
Figure 39	Port page	102
Figure 40	Interface page	105
Figure 41	Ethernet Errors page	107
Figure 42	Transparent Bridging page	109
Figure 43	Port Mirroring page	112
Figure 44	Security Configuration page	114
Figure 45	Port Lists page	116
Figure 46	Port List View, Port List page	117
Figure 47	Port List View, Learn by Ports page	118
Figure 48	Security Table Page	119
Figure 49	Port List View, Clear by Ports page	121
Figure 50	Port Configuration page	122
Figure 51	DA MAC Filtering page	123
Figure 52	VLAN Configuration page	126
Figure 53	VLAN Configuration: Port Information page	128
Figure 54	VLAN Configuration: Port Configuration page	129
Figure 55	Port Configuration page	132
Figure 56	Port Information page	133
Figure 57	Port Configuration page	135
Figure 58	Bridge Information page	137
Figure 59	Group page	140
Figure 60	Utilization page	142
Figure 61	Online help menu	146
Figure 62	Nortel Networks Technical Documentation Web site	147

Tables

Table 1	Main headings and options	24
Table 2	Menu icons	25
Table 3	Page icons	27
Table 4	System Information page items	30
Table 5	Console page fields	32
Table 6	RADIUS page fields	33
Table 7	User levels and access levels	35
Table 8	Stack Information page fields	40
Table 9	Switch Information page fields	42
Table 10	Stack Numbering Setting page fields	43
Table 11	IP page items	47
Table 12	System page items	49
Table 13	SNMPv1 page items	51
Table 14	System Information section fields	53
Table 15	SNMPv3 Counters section fields	54
Table 16	User Specification Table section items	56
Table 17	User Specification Creation section items	56
Table 18	Group Membership page items	59
Table 19	Group Access Rights page items	61
Table 20	Management Information View page fields	65
Table 21	Notification page items	67
Table 22	Target Address page items	69
Table 23	Target Parameter page items	71
Table 24	SNMP Trap Receiver page fields	74
Table 25	MAC Address Table page fields	76
Table 26	Port Management page items	79
Table 27	High Speed Flow Control page items	81
Table 28	Software Download page fields	82
Table 29	LED Indications during the software download process	83

Table 30	Configuration File Download/Upload page items	85
Table 31	Parameters not saved to the configuration file	86
Table 32	Console/Communication Port page items	87
Table 33	RMON Threshold page items	90
Table 34	RMON Event Log page fields	94
Table 35	System Log page fields	96
Table 36	RMON Ethernet page items	98
Table 37	RMON History page items	99
Table 38	Port page items	102
Table 39	Interface page items	106
Table 40	Ethernet Errors page items	108
Table 41	Transparent Bridging page items	110
Table 42	Port Mirroring page items	112
Table 43	Port-based monitoring modes	113
Table 44	Security Configuration page items	115
Table 45	Ports Lists page items	117
Table 46	Security Table page items	119
Table 47	Port Configuration page items	122
Table 48	DA MAC Filtering page items	124
Table 49	VLAN Configuration page items	127
Table 50	VLAN Configuration: Port Information page items	128
Table 51	Port Configuration page items	129
Table 52	Port Information page items	133
Table 53	Port Configuration page items	135
Table 54	Bridge Information page items	138
Table 55	Group page items	141
Table 56	Utilization page items	143

Preface

Welcome to *Using Web-based Management for the BayStack 420/425, Software Release 3.1*.

Default values are defined for all Nortel Networks* BayStack* Switch features that allow the switch to begin forwarding packets as soon as it is powered up and connected to compatible devices.

The Web-based management interface is one of many tools specifically designed to assist the network manager in creating complex standalone or network configurations. For information on the default values defined within the [Product Name (short)], or for information on additional products available to configure your switch, refer to *Using the Baystack 420/425 Switch, Software Release 3.1* (part number 215661-B).

This guide describes how to use the Web-based management interface to configure and maintain your [Product Name (short)] and the devices connected within its framework.

Before you begin

This guide is intended for network managers who are responsible for configuring BayStack switches. This guide assumes prior knowledge and understanding of the terminology, theories, and practices and specific knowledge about the networking devices, protocols, and interfaces that comprise your network.

You should have working knowledge of the Microsoft* Windows* operating system, Graphical User Interfaces (GUIs), and Web browsers.

Text conventions

This guide uses the following text conventions:

<i>italic text</i>	Indicates new terms and book titles.
separator (>)	Shows menu paths. Example: Configuration > Port Management identifies the Port Management option on the Configuration menu.

Related publications

You can print selected technical manuals and release notes free, directly from the Internet. Go to www.nortelnetworks.com/documentation. 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 www.adobe.com to download a free copy of the Adobe Acrobat Reader.

For more information about using the Web-based management interface and the [Product Name (short)], refer to the following publications:

- *Release Notes for the BayStack 420/425 Switch, Software Release 3.1* (216078-B)
Documents important changes about the software and hardware that are not covered in other related publications.
- *Using the Baystack 420/425 Switch, Software Release 3.1* (215661-B)
Describes how to use the BayStack 420/425 switch.
- *Installing the Baystack 425 Switch* (215658-B)
Describes how to install the BayStack 425 switches.
- *Reference for the BayStack 420/425 Command Line Interface, Software Release 3.1* (215659-B)

Describes how to use Command Line Interface (CLI) commands to configure and manage the BayStack 420/425 switch.

- *Reference for BayStack 420/425 Switch Management Software, Software Release 3.1 (215662-C)*

Describes how to use the Java-based device-level software management application, Device Manager (DM)

- *Getting Started with the BayStack 420/425 Switch Management Software, Software Release 3.1 (215663-B)*

Describes how to install the Java-based device level software management application.

How to get help

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

If you purchased a Nortel Networks service program, contact Nortel Networks Technical Support. To obtain contact information online, go to the www.nortelnetworks.com/cgi-bin/comments/comments.cgi URL, then click on Technical Support.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, you can call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

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 <http://www.nortelnetworks.com/help/contact/erc/index.html> URL.

Chapter 1

Using the Web-based management interface

This chapter describes the requirements for using the Web-based management interface and how to use it as a tool to configure your BayStack 425-24T Switch.

Requirements

To use the Web-based management interface, you need the following items:

- A computer connected to any of the network ports
- One of the following Web browsers installed on the computer:
 - Microsoft* Internet Explorer, version 4.0 or later on Windows 95, Windows 98, or Windows NT*
 - Netscape Navigator*, version 4.51 or later on Windows 95, Windows 98, Windows NT, and UNIX*)
- The IP address of the policy switch



Note: The Web-based management interface Web pages may load at different speeds depending on the Web browser you use.



Note: In order to use the BayStack 425-24T Switch Web-based management functionality, such as downloading software, you must connect your console terminal to a BayStack 425-24T Switch port within your stack.

Logging in to the Web-based management interface

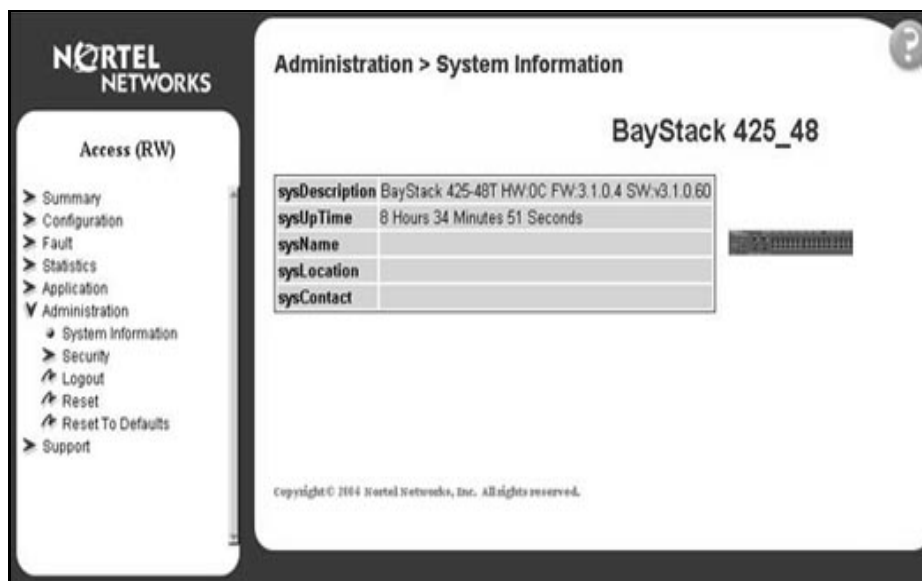
Before you log in to the Web-based management interface, use the console interface to verify the VLAN port assignments and to ensure that your switch CPU and your computer are assigned to the same VLAN. If the devices are not connected to the same VLAN, the IP address of the switch will not open the home page.

To log in to the Web-based management interface:

- 1 Start your Web browser.
- 2 In the Web address field, type the IP address for your host switch, for example, `http://10.30.31.105`, and press [Enter].

The home page opens (Figure 1).

Figure 1 Web-based management interface home page

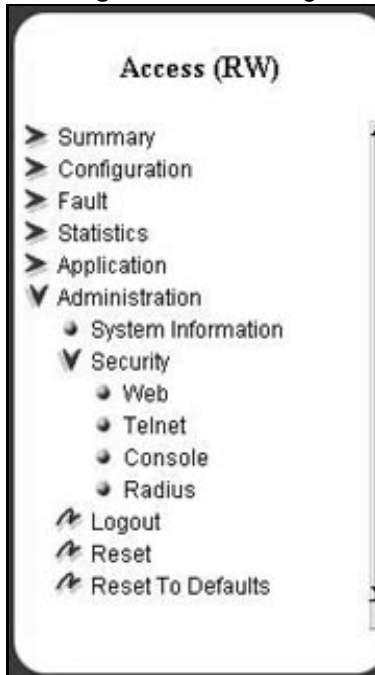


Network security does not yet exist the first time you access the Embedded Web Server. As the system administrator, you must create access parameters and passwords to protect the integrity of your network configuration(s).

Menu

The menu (Figure 2) is the same for all pages. It contains a list of seven main headings.

Figure 2 Menu Page



To navigate the Web-based management interface menu, click a menu title and then click one of its options. When you click an option, the corresponding page opens.

The first six headings provide options for viewing and configuring switch parameters. The Support heading provides options to open the online Help file and the Nortel Networks Web site.

[Table 1](#) lists the main headings in the Web-based management user interface and their associated options.

Table 1 Main headings and options

Main menu titles	Option
Summary	Stack Information (stack mode only) Switch Information Identify Unit Numbers (stack mode only) Stack Numbering (stack mode only)
Configuration	IP System SNMPv1 SNMPv3 SNMP Trap MAC Address Table Find MAC Address Port Management High Speed Flow Control Software Download Configuration File Console/Comm Port
Fault	RMON Threshold RMON Event Log System Log
Statistic	Port Interface Ethernet Errors Transparent Bridging RMON Ethernet RMON History
Application	Port Mirroring MAC Address Security VLAN Spanning Tree Multilink Trunk
Administration	System Information Security Logout Reset Reset to Defaults
Support	Help Release Notes Manuals Upgrades






Tools are provided in the menu to assist you in navigating the Web-based management interface.



Caution: Web browser capabilities such as page bookmarking, refresh, and page forward and page back, function as they would in any other Web site. However, these capabilities do not enhance the functionality of the Web-based management interface. Nortel Networks recommends that you use only the navigation tools provided in the management interface.

Table 2 describes the icons that appear on the menu.

Table 2 Menu icons

Button or icon	Description
	This icon identifies a menu title. Click on this icon to display its options.
	This icon identifies a menu title option. Click on this icon to display the corresponding page.
	This icon identifies a menu title option with a hyperlink to related pages.
	This icon is linked to an action, for example, logout, reset, or reset to system defaults.
	Clicking on the Nortel Networks logo opens the corporate home page in a new Web browser.

Management page

When you click a menu option, the corresponding management page opens. Figure 3 shows the page displayed for the Administration > Security > Console option.

Figure 3 Console page

The screenshot shows a web-based management interface for the Console page. The breadcrumb navigation is "Administration > Security > Console". There are two main sections: "Console Switch Password Setting" and "Console Stack Password Setting". Each section contains a dropdown menu for "Password Type" (set to "None"), a "Read-Only" password field (masked with "AAAA"), and a "Read-Write" password field (masked with "AAAAAA"). A "Submit" button is located at the bottom left of the form area.





A page is composed of one or more of the following elements:

- Tables and input forms
The gray cells in a page are display only, and white cells are input fields.
- Check boxes
You enable or disable a selection by clicking a check box. When a check mark is displayed in the box, that selection is enabled. You disable a selection by clicking the checked box.
- Icons and buttons

Icons and buttons perform an action concerning the displayed page or the switch. Some pages include a button that opens another page or updates the values shown on the current page.

[Table 3](#) describes the icons that allow you to modify information in a statistical table.

Table 3 Page icons

Icon	Name	Description
	Modify	Accesses a modification page for the selected row.
	View	Accesses a view only statistics page for the selected row.
	Delete	Deletes a row.
	Help	Accesses the Help menu in a new Web browser.
		Note: Text within a table that is highlighted blue and underlined is a hyperlink to a related management page.

#

28 Logging in to the Web-based management interface

Chapter 2

Administering the switch

The administrative options available to you are:

- [“Viewing system information,”](#) next
- [“Configuring system security”](#) on page 30
- [“Accessing the management interface”](#) on page 33
- [“Rebooting the BayStack 425-24T Switch”](#) on page 36
- [“Changing the BayStack 425-24T Switch to system defaults”](#) on page 37
- [“Logging out of the management interface”](#) on page 38

Viewing system information

You can view an image of the BayStack 425 switches switch or an image of your entire stack configuration, information about the host device (or stack) and, if provided, the contact person or manager for the switch. The System Information page is also the Web-based management interface home page.

To view system information:

- ➔ From the main menu, choose Administration > System Information.

The System Information page opens ([Figure 4](#)).



Note: You may create or modify existing system information parameters using the System page. For more information on configuring system information, see [“Modifying system settings”](#) on page 48.

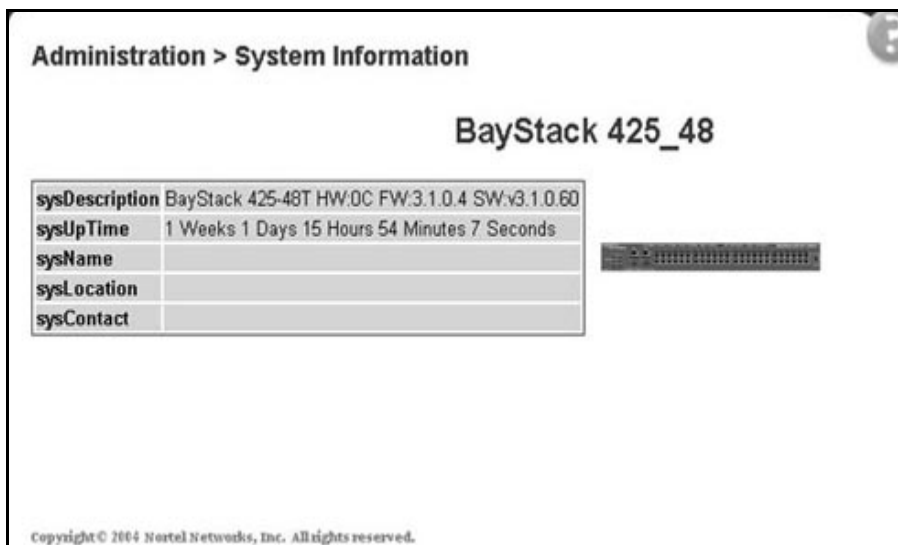
Figure 4 System Information page

Table 4 describes the items on the System Information page.

Table 4 System Information page items

Item	Description
sysDescription	The default description of the BayStack 425-24T Switch.
sysUpTime	The elapsed time since the last network management portion of the system was last re-initialized.
sysName	The name created by the network administrator to identify the switch, for example Finance Group.
sysLocation	The location name created by the network administrator to identify the switch location, for example, first floor.
sysContact	The name, email address and telephone number of the person to contact about switch operation.

Configuring system security

This section describes the steps you use to build and manage security using the Web-based management interface.

Setting console, Telnet, and Web passwords

To set console, Telnet, and Web passwords:

- 1 From the main menu, choose Administration > Security and Console, Telnet, or Web.

The selected password page opens (Figure 5).



Note: The title of the page corresponds to the menu selection you choose. In Figure 5, the network administrator selected Administration > Security > Console.

Figure 5 Console password setting page

Administration > Security > Console

Console Switch Password Setting	
Console Switch Password Type	None
Read-Only Switch Password	*****
Read-Write Switch Password	*****

Console Stack Password Setting	
Console Stack Password Type	None
Read-Only Stack Password	*****
Read-Write Stack Password	*****

Submit

[Table 5](#) describes the items on the Console page.

Table 5 Console page fields

Section	Fields	Setting	Description
Note: Console, Telnet, and Web settings share the same switch and stack password type and password.			
Console Switch Password Setting	Console Switch Password Setting Type	(1) None (2) Local Password (3) RADIUS Authentication	Displays the switch password types. Note: The default is None.
	Read-Only Switch Password	1..15	Type the read-only password setting for the read-only access user.
	Read-Write Switch Password	1..15	Type the read-write password setting for the read-write access user.
Console Stack Password Setting	Console Stack Password Setting Type	(1) None (2) Local Password (3) RADIUS Authentication	Displays the switch password types. Note: The default is None.
	Read-Only Stack Password	1..15	Type the read-only password setting for the read-only access user.
	Read-Write Stack Password	1..15	Type the read-write password setting for the read-write access user.

- 2 Type the information, or make a selection from the list.
- 3 Click Submit.

Configuring remote dial-in access security

To configure remote dial-in access security parameters:

- 1 From the main menu, choose Administration > Security > RADIUS.
The RADIUS page opens ([Figure 6](#)).

Figure 6 RADIUS page

Administration > Security > Radius

RADIUS Authentication Setting

Primary RADIUS Server	0.0.0.0
Secondary RADIUS Server	0.0.0.0
UDP RADIUS Port	1645
RADIUS Shared Secret	

Submit

[Table 6](#) describes the items on the RADIUS page.

Table 6 RADIUS page fields

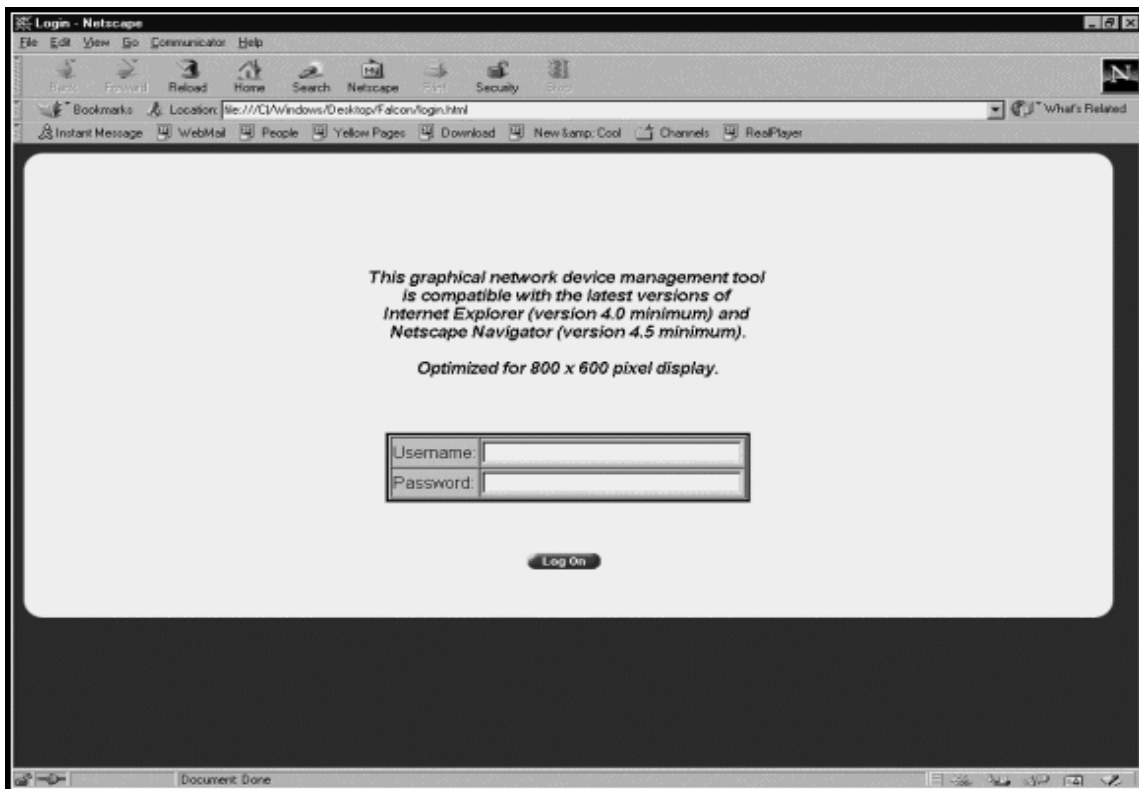
Field	Setting	Description
Primary RADIUS Server	XXX.XXX.XXX.XXX	Type a Primary RADIUS server IP address in the appropriate format.
Secondary RADIUS Server	XXX.XXX.XXX.XXX	Type a Secondary RADIUS server IP address in the appropriate format.
UDP RADIUS Port	Integer	Type the UDP RADIUS port number.
RADIUS Shared Secret	1..16	Type a unique character string to create a secret password.

- 2 Type the information.
- 3 Click Submit.

Accessing the management interface

Once switch and stack passwords and RADIUS authentication settings are integrated into the Web-based management user interface, anyone who attempts to use the application is presented with a log on page ([Figure 7](#)).

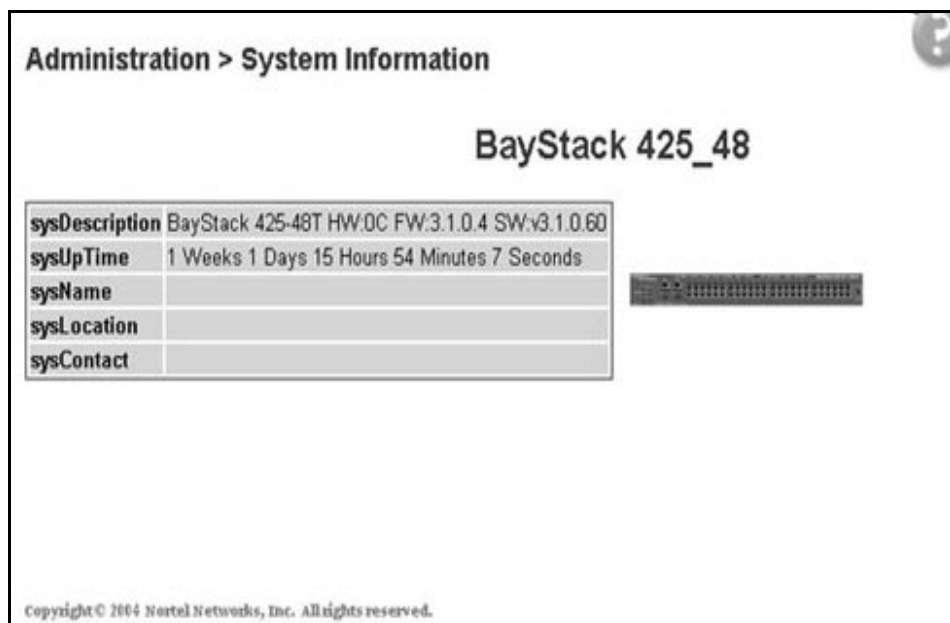
Figure 7 Web-based management interface log on page



To log on to the Web-based management interface:

- 1 In the Username text box, type **RO** (upper-case) for read-only access or **RW** (upper-case) for read-write access.
- 2 In the Password text box, type your password.
- 3 Click Log On.

The System Information page opens ([Figure 8](#)).

Figure 8 System Information page

With Web access enabled, the switch can support up to four concurrent Web page users. Two pre-defined user levels are available and each user level has a corresponding username and password.

[Table 7](#) shows an example of the two pre-defined user levels available and their access level within the Web-based management user interface.

Table 7 User levels and access levels

User level	User name for each level	Password for each user level	Access Level
Read-only	RO	XXXXXXXX	Read only
Read/write	RW	XXXXXXXX	Full read/write access

Rebooting the BayStack 425-24T Switch

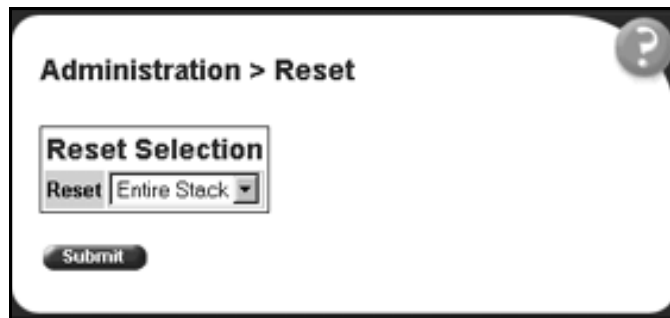
You can reboot a standalone switch or an entire stack without erasing any configured switch parameters. While rebooting, the switch initiates a self-test that comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

To reboot the BayStack 425-24T Switch without making changes (since your last Submit request):

- 1 From the main menu, choose Administration > Reset.

The Reset page opens (Figure 9).

Figure 9 Reset page



- 2 Click Submit. If you do not click Submit, any changes you make will be lost.



Note: If you have not configured system password security, a reset returns you to the home page, as shown in [Figure 1 on page 22](#). If you have configured system password security, a reset returns you to a log on page, as shown in [Figure 7 on page 34](#).

Changing the BayStack 425-24T Switch to system defaults

You can change a standalone switch, a specific unit in a stack configuration, or an entire stack, replacing all configured switch parameters with the factory default values.



Caution: If you choose change to default settings, all configured settings are replaced with factory default settings when you click Submit. For more information on factory default settings, see *Using the Baystack 420/425 Switch, Software Release 3.1 (215661-B)*.

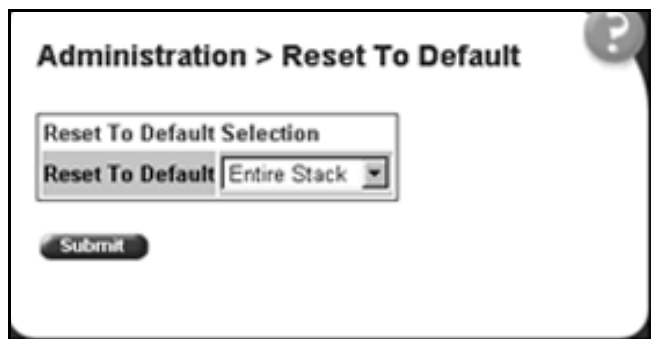
During the process of changing to default settings, the switch initiates a self-test that comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

To change the BayStack 425-24T Switch to system defaults:

- 1 From the main menu, choose Administration > Reset to Default.

The Reset to Default page opens (Figure 10).

Figure 10 Reset to Default page



- 2 Click Submit.

Logging out of the management interface



Note: If you have not configured system password security, a reset returns you to the home page, as shown in [Figure 1 on page 22](#). If you have configured system password security, a reset returns you to a log on page, as shown in [Figure 7 on page 34](#).

To log out of the Web-based management user interface:

- 1** From the main menu, choose Administration > Logout.
A message opens prompting you to confirm your request
- 2** Do one of the following:
 - Click OK to log out.
 - Click Cancel to return to the Web-based management interface home page.

Chapter 3

Viewing summary information

The summary information options are:

- [“Viewing stack information,”](#) next
- [“Viewing summary switch information”](#) on page 41
- [“Changing stack numbering”](#) on page 42
- [“Identifying unit numbers”](#) on page 44

Viewing stack information

You can view a summary of your stack framework, for example, the current version of the running software and the IP address of the Web-based management interface.



Note: The Web-based management user interface automatically detects the operational mode of your system. If the system is in standalone mode, the Stack Information page is not an option listed in the menu.

To view stack information:

- 1 From the main menu, choose Summary > Stack Information.
The Stack Information page opens ([Figure 11](#)).

Figure 11 Stack Information page

Stack Information	
System Description	BayStack 425-24T HW:0B FW:3.1.0.5 SW:v3.1.0.00
Software Version	v3.1.0.00
MAC Address	00-09-97-A2-9C-5F
IP Address	134.177.224.104
Manufacturing Date Code	20030523
Serial #	SACC25003M
Operational State	Normal

Stack Inventory		
Unit	Description	Operational State
1	BayStack 425-24T 24 10/100BaseTX plus 2 shared 10/100/1000TX-MiniGbic	Normal
2	BayStack 420 24 10/100BaseTX plus 1 GBIC slot and 1 Cascade Slot	Normal

Table 8 describes the fields on the Stack Information and Stack Inventory sections of the Stack Information page.

Table 8 Stack Information page fields

Section	Field	Description
Stack Information	System Description	The name created in the configuration process to identify the stack.
	Software Version	The version of the running software.
	MAC Address	The MAC address of the stack.
	IP Address	The IP address of the stack.
	Manufacturing Date Code	The date of manufacture of the board in ASCII format: YYYYMMDD.
	Serial Number	The serial number of the base unit.
	Operational State	The current operational state of the device. The operational states are: Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured
Stack Inventory	Unit	The unit number assigned to the device by the network manager. For more information on stack numbering, see page 42 .

Table 8 Stack Information page fields (continued)

Section	Field	Description
	Description	The description of the device or its subcomponent.
	Operational State	The current operational state of the stack. The operational states are: Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured.

- 2 In the upper-left corner of the Stack Information page, click the number of the device you want to view.

The Stack Information page is updated with information about the selected switch.

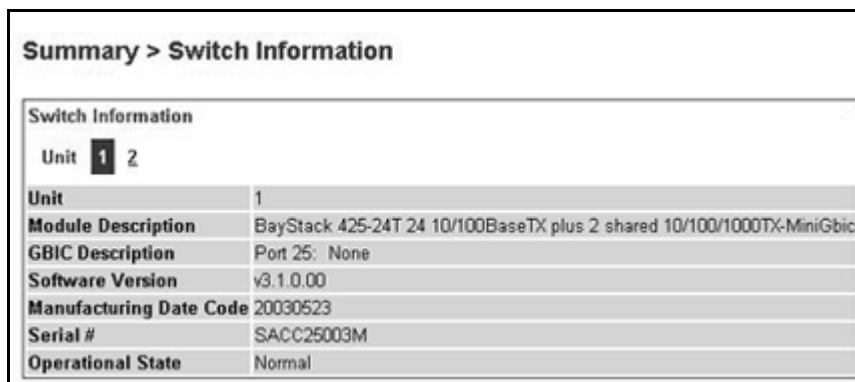
Viewing summary switch information

You can view summary information about the switch, for example, the unit number and its corresponding physical description and serial number.

To view summary switch information:

- 1 From the main menu, choose Summary > Switch Information.

The Switch Information page opens (Figure 12).

Figure 12 Switch Information page


The screenshot shows a web interface titled "Summary > Switch Information". Below the title is a "Switch Information" section with a "Unit" selector set to "2". A table below lists various attributes of the switch:

Switch Information	
Unit	2
Unit	1
Module Description	BayStack 425-24T 24 10/100BaseTX plus 2 shared 10/100/1000TX-MiniGbic
GBIC Description	Port 25: None
Software Version	v3.1.0.00
Manufacturing Date Code	20030523
Serial #	SACC25003M
Operational State	Normal

[Table 9](#) describes the fields on the Switch Information page.

Table 9 Switch Information page fields

Item	Description
Unit	Select the number of the device on which to view summary information. The page is updated with information about the selected switch.
Module Description	The factory set description of the policy switch.
GBIC Description	The factory set description of the sub-component/GBIC.
Software Version	The version of the running software.
Manufacturing Data Code	The date of manufacture of the board in ASCII format.
Serial Number	The serial number of the policy switch.
Operational State	The current operational state of the device. The operational states are: Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured.

- 2 In the upper-left corner of the Switch Information page, click the number of the device you want to view.

The Switch Information page is updated with information about the selected switch.

Changing stack numbering

If your system is set to “stack” operational mode, you can view existing stack numbering information and renumber the devices in your stack framework.

To view or renumber devices within the stack framework:



Note: The unit number does not affect the base unit designation.

- 1 From the main menu, choose Summary > Stack Numbering.

The Stack Numbering Setting page opens ([Figure 13](#)).

Figure 13 Stack Numbering Setting page

Stack Numbering Setting		
Current Unit Number	MAC Address	New Unit Number
1	00-09-97-A2-9C-40	1
2	00-09-97-38-99-40	2

Submit

Table 10 describes the fields on the Stack Numbering Setting page.

Table 10 Stack Numbering Setting page fields

Item	Range	Description
Current Unit Number	1..8	Unit number previously assigned to the policy switch. 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).
MAC Address	XX.XX.XX.XX.XX.XX	MAC address of the corresponding unit listed in the Current Unit Number field.
New Unit Number	1..8, None	Choose a new number to assign to your selected policy switch. Note: If you leave the field blank, the system automatically selects the next available number.

2 Choose the new number to assign to your switch.

3 Click Submit.

A message opens prompting you to confirm your request.

4 Do one of the following:

- Click OK to renumber the stack.
- Click Cancel to return to the Stack Numbering page without making changes.

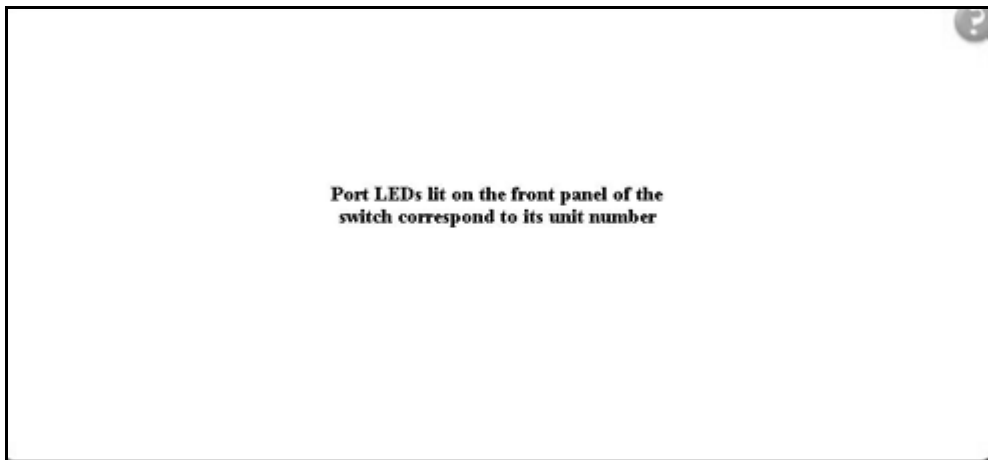
Identifying unit numbers

You can identify the unit numbers of the switches participating in a stack configuration by viewing the LEDs on the front panel of each switch.

To identify unit numbers in your configuration:

- 1 From the main menu, choose Summary > Identify Unit Numbers.
The Identify Unit Numbers page opens (Figure 14).

Figure 14 Identify Unit Numbers page



- 2 To continue viewing summary information or to start the configuration process, choose another option from the main menu.

Chapter 4

Configuring the switch

The switch configuration options available to you are:

- [“Configuring BootP, IP, and gateway settings”](#), (next)
- [“Modifying system settings”](#) on page 48
- [“About SNMP”](#) on page 50
- [“Configuring SNMPv1”](#) on page 50
- [“Configuring SNMPv3”](#) on page 52
- [“Viewing learned MAC addresses by VLAN”](#) on page 75
- [“Configuring switch port autonegotiation speed”](#) on page 77
- [“Configuring high speed flow control”](#) on page 80
- [“Downloading switch images”](#) on page 81
- [“Storing and retrieving a switch configuration file from a TFTP server”](#) on page 84
- [“Configuring port communication speed”](#) on page 86



Note: In order to use all the BayStack 425-24T Switch management features, you must connect your console terminal into a BayStack 425-24T Switch port within your stack.

Configuring BootP, IP, and gateway settings

You can configure the BootP mode settings, create and modify the in-band stack and in-band switch IP addresses and in-band subnet mask parameters, and configure the IP address of your default gateway.



Note: Settings take effect immediately when you click Submit.

To configure BootP, IP, and gateway settings:

- 1 From the main menu, choose Configuration > IP.
The IP page opens (Figure 15).

Figure 15 IP page

Configuration > IP

Boot Mode Setting
BootP Request Mode

IP Setting

	Configurable	In Use	Last BootP
In-Band Stack IP Address	<input type="text" value="0.0.0.0"/>	0.0.0.0	0.0.0.0
In-Band Switch IP Address	<input type="text" value="134.177.224.102"/>	134.177.224.102	0.0.0.0
In-Band Subnet Mask	<input type="text" value="255.255.255.0"/>	255.255.255.0	0.0.0.0

Gateway Setting
Default Gateway

Table 11 describes the items on the IP page.

Table 11 IP page items

Section	Item	Range	Description
Boot Mode Setting	BootP Request Mode	BootP When Needed	Choose this mode to inform the switch to send a BootP request when the switch IP address stored in nonvolatile memory is the factory default value. If the stored IP address differs from the factory default value, the switch uses the stored network parameters. If the switch cannot find a BootP server, it tries five more times to find one and then defaults to the factory settings
		BootP Always	Choose this mode to inform the switch, each time the switch boots, to ignore any stored network parameters and send a BootP request. If the BootP request fails, the switch boots with the factory default IP configuration. This setting disables remote management if no BootP server is set up for the switch, but it allows the switch to boot normally.
		BootP Disabled	Choose this mode to inform the switch, each time the switch boots, to use the IP configuration parameters stored in non-volatile memory. If a BootP configuration is in progress when you issue this command, the BootP configuration stops.
		BootP or Last Address	Choose this mode to inform the switch, at each startup, to obtain its IP configuration using BootP. If the BootP request fails, the switch uses the network parameters stored in its non-volatile memory. Note: Valid parameters obtained in using BootP always replace current information stored in the non-volatile memory.
			Note: Whenever the switch is broadcasting BootP requests, the BootP process times out if a reply is not received within (approximately) 7 minutes. When the process times out, the BootP request mode automatically changes to BootP Disabled mode. To restart the BootP process, change the BootP request mode to any of the three following modes: BootP When Needed, BootP Always, or to BootP or Last Address.
IP Setting	In-Band Stack IP Address	XXX.XXX.XXX.XX X	Type a new stack IP address in the appropriate format.

Table 11 IP page items (continued)

Section	Item	Range	Description
	In-Band Switch IP Address	XXX.XXX.XXX.XX X	Type a new switch IP address in the appropriate format. Note: When the IP address is entered in the In-Band IP Address field, and the In-Band Subnet Mask field value is not present, the software provides an <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.
	In-Band Subnet Mast	XXX.XXX.XXX.XX X	Type a new subnet mask in the appropriate format.
	In-Use		The column header for the read-only fields in this screen. The data displayed in this column represents data that is currently in use.
	Last BootP		The column header for the read-only fields in this screen. The read-only data displayed in this column represents data obtained from the last BootP reply received.
Gateway Setting	Default Gateway	XXX.XXX.XXX.XX X	Type an IP address for the default gateway in the appropriate format.

- 2 Type information in the text boxes, or select from a list.
- 3 Click Submit.

Modifying system settings

You can create or modify the system name, system location, and network manager contact information.



Note: The configurable parameters on the System page are displayed in a read only format on the System Information home page.

To configure system settings:

- 1 From the main menu, choose Configuration > System.
The System page opens (Figure 16).

Figure 16 System page

Configuration > System

System Characteristics Setting	
System Description	BayStack 425-48T HW:0C FW:3.1.0.4 SW:v3.1.0.60
System Object ID	1.3.6.1.4.1.45.3.57.1
System Up Time	10:10:35:6
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>

[Table 12](#) describes the items on the System page.

Table 12 System page items

Item	Range	Description
System Description		The factory set description of the hardware and software versions.
System Object ID		The character string that the vendor created to uniquely identify this device.
System Up Time		The elapsed time since the last network management portion of the system was last re-initialized. Note: This field is updated only when the screen is redisplayed.
System Name	0..56	Type a character string to create a name to identify the switch, for example Finance Group.
System Location	0..56	Type a character string to create a name for the switch location, for example, First Floor.
System Contact	0..56	Type a character string to create the contact information for the network manager or the selected person to contact regarding switch operation, for example, mcarlson@company.com Note: To operate correctly with the Web interface, the system contact should be an e-mail address.

2 Type information in the text boxes.

- 3 Click Submit.

About SNMP

Simple Network Management Protocol (SNMP) is the standard for network management that uses a common software agent to manage local and wide area network equipment from different vendors; part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite and defined in RFC1157. SNMPv1 is version one, or the original standard protocol. SNMPv3 is a combination of proposal updates to SNMP, most of which deal with security.

Configuring SNMPv1

You can configure SNMPv1 read/write and read-only community strings, enable or disable trap mode settings, and/or enable or disable the autotopology feature. The autotopology feature, when enabled, performs a process that recognizes any device on the managed network and defines and maps its relation to other network devices in real time.

To configure the community string, trap mode, and autotopology settings and features:

- 1 From the main menu, choose Configuration > SNMPv1.

The SNMPv1 page opens ([Figure 17](#)).

Figure 17 SNMPv1 page

The screenshot shows the 'Configuration > SNMPv1' page. It contains three distinct configuration sections, each with a 'Submit' button:

- Community String Setting:** Contains two text input fields. The first is labeled 'Read-Only Community String' and contains the text 'public'. The second is labeled 'Read-Write Community String' and contains the text 'private'.
- Trap Mode Setting:** Contains a dropdown menu labeled 'Authentication Trap' with the value 'Enabled' selected.
- AutoTopology Setting:** Contains a dropdown menu labeled 'AutoTopology' with the value 'Enabled' selected.

Table 13 describes the items on the SNMPv1 page.

Table 13 SNMPv1 page items

Section	Item	Range	Description
Community String Setting	Read-Only Community String	1..32	Type a character string to identify the community string for the SNMPv1 read-only community, for example, public or private. The default value is public.
	Read-Write Community String	1..32	Type a character string to identify the community string for the SNMPv1 read-write community, for example, public or private. The default value is private.
Trap Mode Setting	Authentication Trap	(1) Enable (2) Disable	Choose to enable or disable the authentication trap.
AutoTopology Setting	AutoTopology	(1) Enable (2) Disable	Choose to enable or disable the autotopology feature.

- 2 Type information in the text boxes, or select from a list.
- 3 Click Submit in any section to save your changes.

Configuring SNMPv3

This section describes the steps to build and manage SNMPv3 in the Web-based management user interface.

Viewing SNMPv3 system information

You can view information about the SNMPv3 engine that exists and the private protocols that are supported in your network configuration. You can also view information about packets received by the system having particular errors, such as unavailable contexts, unknown contexts, decrypting errors, or unknown user names.

To view SNMPv3 system information:

- 1 From the main menu, choose Configuration > SNMPv3 > System Information.

The System Information page opens ([Figure 18](#)).

Figure 18 System Information page

Configuration > SNMPv3 > System Information

System Information	
SNMP Engine ID	80-00-02-32-80-02-00-0b-53-41-43-43-32-36-30-30
SNMP Engine Boots	1
SNMP Engine Time	0:2:30:22
SNMP Engine Maximum Message Size	2048
SNMP Engine Dialects	SNMPv1, SNMPv2c, SNMPv3
Authentication Protocols Supported	HMAC MD5
Private Protocols Supported	None

SNMPv3 Counters	
Unavailable Contexts	0
Unknown Contexts	0
Unsupported Security Levels	0
Not In Time Windows	0
Unknown User Names	0
Unknown Engine IDs	0
Wrong Digests	0
Decryption Errors	0

Table 14 describes the fields on the System Information section of the SNMPv3 System Information page.

Table 14 System Information section fields

Item	Description
SNMP Engine ID	The SNMP engine's identification number.
SNMP Engine Boots	The number of times that the SNMP engine has re-initialized itself since its initial configuration.
SNMP Engine Time	The number of seconds since the SNMP engine last incremented the snmpEngineBoots object.
SNMP Engine Maximum Message Size	The maximum length, in octets, of an SNMP message which this SNMP engine can send or receive and process determined as the minimum of the maximum message size values supported among all transports available to and supported by the engine.
SNMP Engine Dialects	The SNMP dialect the engine recognizes. The dialects are:SNMP1v1, SNMPv2C, and SNMPv3.

Table 14 System Information section fields

Item	Description
Authentication Protocols Supported	The registration point for standards-track authentication protocols used in SNMP Management Frameworks. The registration points are: None, HMAC MD5, HMAC SHA, HMAC MD5. Note: The BayStack 425-24T Switch supports only the MD5 authentication protocol.
Private Protocols Supported	The registration point for standards-track privacy protocols used in SNMP Management Frameworks. The registration points are: None or CBC-DES. Note: The BayStack 425-24T Switch does not support privacy protocols.

[Table 15](#) describes the fields on the SNMPv3 Counters section of the SNMPv3 System Information page.

Table 15 SNMPv3 Counters section fields

Item	Description
Unavailable Contexts	The total number of packets dropped by the SNMP engine because the context contained in the message was unavailable.
Unknown Contexts	The total number of packets dropped by the SNMP engine because the context contained in the message was unknown.
Unsupported Security Levels	The total number of packets dropped by the SNMP engine because they requested a security level that was unknown to the SNMP engine or otherwise unavailable.
Not in Time Windows	The total number of packets dropped by the SNMP engine because they appeared outside of the authoritative SNMP engine's window.
Unknown User Names	The total number of packets dropped by the SNMP engine because they referenced an unknown user.
Unknown Engine IDs	The total number of packets dropped by the SNMP engine because they referenced an snmpEngineID that was not known to the SNMP engine.
Wrong Digests	The total number of packets dropped by the SNMP engine because they did not contain the expected digest value.
Decryption Errors	The total number of packets dropped by the SNMP engine because they could not be decrypted.

Configuring user access to SNMPv3

You can view a table of all current SNMPv3 user security information such as authentication/privacy protocols in use, and create or delete SNMPv3 system user configurations.

Creating an SNMPv3 system user configuration

To create an SNMPv3 system user configuration:

- 1 From the main menu choose Configuration > SNMPv3 > User Specification.
The User Specification page opens (Figure 19).

Figure 19 User Specification page

The screenshot shows a web-based management interface for configuring SNMPv3 users. The page title is "Configuration > SNMPv3 > User Specification". Below the title is a table titled "User Specification Table" with the following columns: Action, User Name, Auth Protocol, Private Protocol, and Entry Storage. Below the table is a "User Specification Creation" form with the following fields: User Name (text input), Authentication Protocol (dropdown menu with "None" selected), Authentication Password (text input), and Entry Storage (dropdown menu with "Volatile" selected). A "Submit" button is located at the bottom of the form.

Table 16 describes the items on the User Specification Table section of the User Specification page.

Table 16 User Specification Table section items


Item and MIB association	Description
	Deletes the row.
User Name (usmUserSecurityName)	The name of an existing SNMPv3 user.
Authentication Protocol (usmUserAuthProtocol)	Indicates whether the message sent on behalf of this user to/from the SNMP engine identified UserEngineID can be authenticated by the MD5 authentication protocol.
Private Protocol (usmUserPrivProtocol)	Displays whether or not messages sent on behalf of this user to or from the SNMP engine identified by usmUserEngineID can be protected from disclosure, and if so, the type of privacy protocol which is used.
Entry Storage	The current storage type for this row. If "Volatile" is displayed, information is dropped (lost) when you turn the power off. If non-volatile is displayed, information is saved in NVRAM when you turn the power off

Table 17 describes the items on the User Specification Creation section of the User Specification page.

Table 17 User Specification Creation section items

Item and MIB association	Range	Description
User Name	1..32	Type a string of characters to create an identity for the user.
Authentication Protocol (usmUserAuthProtocol)	None MD5	Choose whether or not the message sent on behalf of this user to/from the SNMP engine identified UserEngineID can be authenticated with the MD5 protocol.
Authentication Password (usmUserAuthPassword)	1..32	Type a string of character to create a password to use in conjunction with the authorization protocol.

Table 17 User Specification Creation section items

Item and MIB association	Range	Description
Creation Mode	Create Entry	Choose to create a new, unique user specification entry.
Entry Storage (usmUserStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the User Specification Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new configuration is displayed in the User Specification Table ([Figure 19 on page 55](#)).

Deleting an SNMPv3 system user configuration

To delete an existing SNMPv3 user configuration:

1 From the main menu, choose Configuration > SNMPv3 > User Specification.

The User Specification page opens ([Figure 19 on page 55](#).)

2 In the User Specification Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the SNMPv3 user configuration.
- Click Cancel to return to the User Specification page without making changes.

Configuring an SNMPv3 system user group membership

You can view a table of existing SNMPv3 group membership configurations and map or delete an SNMPv3 user to group configuration.

Mapping an SNMPv3 system user to a group

To map an SNMPv3 system user to a group:

- 1 From the main menu, choose Configuration > SNMPv3 > Group Membership.

The Group Membership page opens (Figure 20).

Figure 20 Group Membership page

Configuration > SNMPv3 > Group Membership

Group Membership Table				
Action	Security Name	Security Model	Group Name	Entry Storage
<input type="checkbox"/>	s5AgTrpRcvrComm0	SNMPv1	communitySnmpNotify	Read Only
<input type="checkbox"/>	s5AgTrpRcvrComm1	SNMPv1	communitySnmpNotify	Read Only
<input type="checkbox"/>	s5AgTrpRcvrComm2	SNMPv1	communitySnmpNotify	Read Only
<input type="checkbox"/>	s5AgTrpRcvrComm3	SNMPv1	communitySnmpNotify	Read Only
<input type="checkbox"/>	read_only_community	SNMPv1	communitySnmpRead	Read Only
<input type="checkbox"/>	read_write_community	SNMPv1	communitySnmpWrite	Read Only
<input type="checkbox"/>	s5AgTrpRcvrComm0	SNMPv2c	communitySnmpNotify	Read Only
<input type="checkbox"/>	s5AgTrpRcvrComm1	SNMPv2c	communitySnmpNotify	Read Only
<input type="checkbox"/>	s5AgTrpRcvrComm2	SNMPv2c	communitySnmpNotify	Read Only
<input type="checkbox"/>	s5AgTrpRcvrComm3	SNMPv2c	communitySnmpNotify	Read Only
<input type="checkbox"/>	read_only_community	SNMPv2c	communitySnmpRead	Read Only
<input type="checkbox"/>	read_write_community	SNMPv2c	communitySnmpWrite	Read Only
<input type="checkbox"/>	nncli	NNCLI	nncli	Read Only

Group Membership Creation

Security Name (i.e. User Name)


Security Model

Group Name

Entry Storage

Table 18 describes the items on the Group Membership page.

Table 18 Group Membership page items

Item and MIB association	Range	Description
		Deletes the row.
Security Name (vacmSecurityToGroupStatus)	1..32	Type a string of character to create a security name for the principal which is mapped by this entry to a group name.
Security Model (vacmSecurityToGroupStatus)	(1) SNMPv1 (2) SNMPv2c (3) USM	Choose the security model within which the security name to group name mapping is valid.
Group Name (vacmGroupName)	1..32	Type a string of character to specify the group name.
Entry Storage (vacmSecurityToGroupStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the Group Membership Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry is displayed in the Group Membership Table ([Figure 20 on page 58](#)).

Deleting an SNMPv3 group membership configuration

To delete an SNMPv3 group membership configuration:

1 From the main menu, choose Configuration > SNMPv3 > Group Membership.

The Group Membership page opens ([Figure 20 on page 58](#)).

2 In the Group Membership Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the group membership configuration.
- Click Cancel to return to the Group Membership page without making changes.



Note: This Group Membership Table section of the Group Membership page contains hyperlinks to the SNMPv3 User Specification and Group Access Rights pages. For more information on these pages, see [“Configuring user access to SNMPv3” on page 55](#) and [“Configuring SNMPv3 group access rights” on page 60](#).

Configuring SNMPv3 group access rights

You can view a table of existing SNMPv3 group access rights configurations, and you can create or delete a group’s SNMPv3 system-level access rights.

Creating an SNMPv3 group access rights configuration

To create a group’s SNMPv3 system-level access right configuration:

1 From the main menu, choose Configuration > SNMPv3 > Group Access Rights.

The Group Access Rights page opens ([Figure 21](#)).

Figure 21 Group Access Rights page

Configuration > SNMPv3 > Group Access Rights

Group Access Table						
Action	Group Name	Security Model	Security Level	Read View	Write View	Notify View
<input checked="" type="checkbox"/>	nncli	NNCLI	noAuthNoPriv	nncli	nncli	-- null --
<input checked="" type="checkbox"/>	communitySnmpRead	SNMPv1	noAuthNoPriv	snmpv1Obj	-- null --	-- null --
<input checked="" type="checkbox"/>	communitySnmpRead	SNMPv2c	noAuthNoPriv	snmpv1Obj	-- null --	-- null --
<input checked="" type="checkbox"/>	communitySnmpWrite	SNMPv1	noAuthNoPriv	snmpv1Obj	snmpv1Obj	-- null --
<input checked="" type="checkbox"/>	communitySnmpWrite	SNMPv2c	noAuthNoPriv	snmpv1Obj	snmpv1Obj	-- null --
<input checked="" type="checkbox"/>	communitySnmpNotify	SNMPv1	noAuthNoPriv	-- null --	-- null --	snmpv1Obj
<input checked="" type="checkbox"/>	communitySnmpNotify	SNMPv2c	noAuthNoPriv	-- null --	-- null --	snmpv1Obj

Group Access Creation	
Group Name	<input type="text"/>
Security Model	SNMPv1
Security Level	noAuthNoPriv
Read View	<input type="text"/>

Table 19 describes the items on the Group Access Rights page.

Table 19 Group Access Rights page items

Item and MIB association	Range	Description
<input checked="" type="checkbox"/>		Deletes the row.
Group Name (vacmAccessToGroupStatus)	1..32	Type a character string to specify the group name to which access is granted.
Security Model (vacmAccessSecurityModel)	(1) SNMPv1 (2) SNMPv2c (3) USM	Choose the security model to which access is granted.
Security Level (vacmAccessSecurityLevel)	(1) noAuthNoPriv (2) authNoPriv	Choose the minimum level of security required in order to gain the access rights allowed to the group.
Read View (vacmAccessReadViewName)	1..32	Type a character string to identify the MIB view of the SNMP context to which this entry authorizes read access.

Table 19 Group Access Rights page items (continued)

Item and MIB association	Range	Description
Write View (vacmAccessWriteViewName)	1..32	Type a character string to identify the MIB view of the SNMP context to which this entry authorizes write access.
Notify View (vacmAccessNotifyViewName)	1..32	Type a character string to identify the MIB view to which this entry authorizes access to notifications.
Entry Storage (vacmSecurityToGroupStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

- 2 In the Group Access Creation section, type information in the text boxes, or select from a list.
- 3 Click Submit.

The new entry is displayed in the Group Access Table ([Figure 21 on page 61](#)).

Deleting an SNMPv3 group access rights configuration

To delete a n SNMPv3 group access configuration:

- 1 From the main menu, choose Configuration > SNMPv3 > Group Access Rights.
The Group Access Rights page opens ([Figure 21 on page 61](#)).
- 2 In the Group Access Table, click the Delete icon for the entry you want to delete.
A message opens prompting you to confirm your request.
- 3 Do one of the following:
 - Click Yes to delete the group access configuration.

- Click Cancel to return to the Group Access Rights page without making changes.



Note: This Group Access Table section of the Group Access Rights page contains hyperlinks to the Management Information View page.

Configuring an SNMPv3 management information view

You can view a table of existing SNMPv3 management information view configurations, and you can create or delete SNMPv3 management information view configurations.



Note: A view may consist of multiple entries in the table, each with the same view name, but a different view subtree.

Creating an SNMPv3 management information view configuration

To create an SNMPv3 management information view configuration:

- 1 From the main menu, choose Configuration > SNMPv3 > Management Info View.

The Management Information View page opens ([Figure 22](#)).

Figure 22 Management Information View page


Configuration > SNMPv3 > Management Information View

Management Information Table					
Action	View Name	View Subtree	View Mask	View Type	Entry Storage
<input type="checkbox"/>	nncli	1.3	all ones	Included	Read Only
<input type="checkbox"/>	nncli	1.0.8802	all ones	Included	Read Only
<input type="checkbox"/>	snmpv1Objs	1.3	all ones	Included	Read Only
<input type="checkbox"/>	snmpv1Objs	1.0.8802	all ones	Included	Read Only
<input type="checkbox"/>	snmpv1Objs	1.3.6.1.6	all ones	Excluded	Read Only
<input type="checkbox"/>	snmpv1Objs	1.3.6.1.6.3.10	all ones	Included	Read Only
<input type="checkbox"/>	snmpv1Objs	1.3.6.1.6.3.12	all ones	Included	Read Only
<input type="checkbox"/>	snmpv1Objs	1.3.6.1.6.3.13	all ones	Included	Read Only
<input type="checkbox"/>	snmpv1Objs	1.3.6.1.6.3.1.1.4	all ones	Included	Read Only
<input type="checkbox"/>	snmpv1Objs	1.3.6.1.6.3.1.1.5	all ones	Included	Read Only
<input type="checkbox"/>	webSnmpObjs	1.3	all ones	Included	Read Only
<input type="checkbox"/>	webSnmpObjs	1.0.8802	all ones	Included	Read Only

Management Information Creation	
View Name	<input type="text"/>
View Subtree	<input type="text"/> (e.g., 1.3.6.1)
View Mask	<input type="text"/> (e.g., FF:CO/null [zero length])
View Type	Include <input type="button" value="v"/>
Entry Storage	Volatile <input type="button" value="v"/>

Table 20 describes the fields on the Management Information View page.

Table 20 Management Information View page fields

Fields and MIB association	Range	Description
		Deletes the row.
View Name (vacmViewTreeFamilyViewName)	1..32	Type a character string to create a name for a family of view subtrees.
View Subtree (vacmViewTreeFamilySubtree)	X.X.X.X.X...	Type an object identifier (OID) to specify the MIB subtree which, when combined with the corresponding instance of vacmViewTreeFamilyMask, defines a family of view subtrees. Note: If no OID is entered and the field is blank, a default mask value consisting of "1s" is recognized.
View Mask (vacmViewTreeFamilyMask)	Octet String (0..16)	Type the bit mask which, in combination with the corresponding instance of vacmViewFamilySubtree, defines a family of view subtrees.
View Type (vacmViewTreeFamilyType)	(1) Include (2) Exclude	Choose to include or exclude a family of view subtrees.
Entry Storage (vacmSecurityToGroupStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

- 2 In the Management Information Creation section, type information in the text boxes, or select from a list.
- 3 Click Submit.

The new entry appears in the Management Information Table ([Figure 22 on page 64](#)).

Deleting an SNMPv3 management information view configuration

To delete an existing SNMPv3 management information view configuration:

- 1 From the main menu, choose Configuration > SNMPv3 > Management Info View.

The Management Information page opens ([Figure 22 on page 64](#)).

- 2 In the Management Information Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

- 3 Do one of the following:
 - Click Yes to delete the management information view configuration.
 - Click Cancel to return to the table without making changes.

Configuring an SNMPv3 system notification entry

You can view a table of existing SNMPv3 system notification configurations, and you can configure specific SNMPv3 system notification types with particular message recipients and delete SNMPv3 notification configurations.

Creating an SNMPv3 system notification configuration

To create an SNMPv3 system notification configuration:

- 1 From the main menu, choose Configuration > SNMPv3 > Notification.

The Notification page opens (Figure 23).

Figure 23 Notification page

Configuration > SNMPv3 > Notification

Action	Notify Name	Notify Tag	Notify Type	Entry Storage
<input type="checkbox"/>	inform	inform	Inform	Read Only
<input type="checkbox"/>	s5AgTrpRcvr	s5AgTrpRcvr	Trap	Read Only
<input type="checkbox"/>	trap	trap	Trap	Read Only

Notification Creation

Notify Name:


Notify Tag:

Notify Type:

Entry Storage:

Table 21 describes the items on the Notification page.

Table 21 Notification page items

Item and MIB association	Range	Description
		Deletes the row.
Notify Name (snmpNotifyRowStatus)	1..32	Type a character string to identify the entry.
Notify Tag (snmpNotifyTag)	1..32	Type a value which to use to select entries in the snmpTargetAddrTable. Any entry in the snmpTargetAddrTable which contains a tag value which is equal to the value of an instance of this object is selected. If this object carries a zero length, no entries are selected
Notify Type (snmpNotifyType)	(1) Trap (2) Inform	Choose the type of notification to generate.
Entry Storage (snmpNotifyStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

- 2 In the Notification Creation section, type information in the text boxes, or select from a list.
- 3 Click Submit.

The new entry is displayed in the Notification Table ([Figure 23](#)).



Note: This Notification Table section of the Notification page contains hyperlinks to the Target Parameter page.

Deleting an SNMPv3 system notification configuration

To delete an SNMPv3 notification configuration:

- 1 From the main menu, choose Configuration > SNMPv3 > Notification.
The Notification page opens ([Figure 23 on page 66](#)).

- 2 In the Notification Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

- 3 Do one of the following:
 - Click Yes to delete the notification configuration.
 - Click Cancel to return to the table without making changes.

Configuring an SNMPv3 management target address

You can view a table of existing SNMPv3 management target configurations, create SNMPv3 management target address configurations that associate notifications with particular recipients and delete SNMPv3 target address configurations.

Creating an SNMPv3 target address configuration

To create an SNMPv3 target address configuration:

- 1 From the main menu, choose Configuration > SNMPv3 > Target Address.
The Target Address page opens (Figure 24).


Figure 24 Target Address page

Configuration > SNMPv3 > Target Address

Target Address Table							
Action	Target Name	Target Domain	Target Address	Timeout	Retry Count	Tag List	Target Parameters
<div style="border: 1px solid gray; padding: 5px;"> <p>Target Address Creation</p> <p>Target Name <input style="width: 80%;" type="text"/></p> <p>Target Address <input style="width: 80%;" type="text"/> (e.g., 1.2.3.4:160)</p> <p>Target Timeout <input style="width: 40%;" type="text" value="1500"/> seconds (0 .. 2147483647)</p> <p>Target Retry Count <input style="width: 40%;" type="text" value="3"/> (0 .. 255)</p> <p>Target Tag List <input style="width: 80%;" type="text"/></p> <p>Target Param Entry <input style="width: 80%;" type="text"/></p> <p>Entry Storage <input style="width: 40%;" type="text" value="Volatile"/> <input type="button" value="v"/></p> </div>							

Table 22 describes the items on the Target Address page.

Table 22 Target Address page items

Item and MIB association	Range	Description
		Deletes the row.
Target Name (snmpTargetAddrName)	1..32	Type a character string to create a target name.
Target Domain (snmpTargetAddrTDomain)	1..32	The transport type of the address contained in the snmpTargetAddrTAddress object.
Target Address (snmpTargetAddrTAddress)	XXX.XXX.XXX.XXX: XXX	Type a transport address in the format of an IP address, colon, and UDP port number. For example: 10.30.31.99:162.
Target Timeout (snmpTargetAddrTimeout)	Integer	Type the number, in seconds, to designate as the maximum time to wait for a response to an inform notification before re-sending the "Inform" notification.
Target Retry Count (snmpTargetAddrRetryCount)	0..255	Type the default number of retries to be attempted when a response is not received for a generated message. An application may provide its own retry count, in which case the value of this object is ignored.
Target Tag List (snmpTargetAddrTagList)	1..20	Type the space-separated list of tag values to be used to select target addresses for a particular operation.
Target Parameter Entry (snmpTargetAddr)	1..32	Type a numeric string to identify an entry in the snmpTargetParamsTable. The identified entry contains SNMP parameters to be used when generated messages to be sent to this transport address
Entry Storage	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

- 2 In the Target Address Creation section, type information in the text boxes, or select from a list.
- 3 Click Submit.

The new entry is displayed in the Target Address Table ([Figure 24 on page 68](#)).



Note: This Target Address Table section of the Target Address page contains hyperlinks to the Target Parameter page.

Deleting an SNMPv3 target address configuration

To delete an SNMPv3 target address configuration:

- 1 From the main menu, choose Configuration > SNMPv3 > Target Address. The Target Address page opens ([Figure 24 on page 68](#)).
- 2 In the Target Address Table, click the Delete icon for the entry you want to delete. A message opens prompting you to confirm your request.
- 3 Do one of the following:
 - Click Yes to delete the target address configuration.
 - Click Cancel to return to the table without making changes.

Configuring an SNMPv3 management target parameter

SNMPv3 management target parameters are used during notification generation to specify the communication parameters used for exchanges with notification recipients.

You can view a table of existing SNMPv3 target parameter configurations, create SNMPv3 target parameters that associate notifications with particular recipients, and delete existing SNMPv3 target parameter configurations.

Creating an SNMPv3 target parameter configuration

To create an SNMPv3 target parameter configuration:

- 1 From the main menu, choose Configuration > SNMPv3 > Target Parameter.

The Target Parameter page opens (Figure 25).

Figure 25 Target Parameter page

Table 23 describes the items on the Target Parameter page.

Table 23 Target Parameter page items

Item	Range	Description
		Deletes the row.
Parameter Tag (snmpTargetParamsRowStatus)	1..32	Type a unique character string to identify the parameter tag.
Msg Processing Model (snmpTargetParamsMPModel)	(0) SNMPv1 (1) SNMPv2c (2) SNMPv3 / USM	Choose the message processing model to be used when generating SNMP messages using this entry
Security Name (snmpTargetParamsSecurityName)	1..32	Type the principal on whose behalf SNMP messages are generated using this entry

Table 23 Target Parameter page items

Item	Range	Description
Security Level (snmpTargetParamsSecuirtyLevel)	(1) noAuthNoPriv (2) authNoPriv	Choose the level of security to be used when generating SNMP messages using this entry
Entry Storage (snmpTargetParamsStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

- 2 In the Target Parameter Creation section, type information in the text boxes, or select from a list.
- 3 Click Submit.

The new entry appears in the Target Parameter Table ([Figure 25 on page 71](#)).

Deleting an SNMPv3 target parameter configuration

To delete an SNMPv3 target parameter configuration:

- 1 From the main menu, choose Configuration > SNMPv3 > Target Parameter.
The Target Parameter page opens ([Figure 25 on page 71](#)).
- 2 In the Target Parameter Table, click the Delete icon for the entry you want to delete.
A message opens prompting you to confirm your request.
- 3 Do one of the following:
 - Click Yes to delete the target parameter configuration.
 - Click Cancel to return to the table without making changes.

Configuring an SNMP trap receiver

You can configure the IP address and community string for a new SNMP trap receiver, view a table of existing SNMP trap receiver configurations, or delete an existing SNMP trap receiver configuration(s).



Note: The SNMP Trap Receiver Table is an alternative to using the SNMPv3 Target Table and SNMPv3 Parameter Table. However, only SNMPv1 traps are configurable using this table.

Creating an SNMP trap receiver configuration

To create an SNMP trap receiver configuration:


- 1 From the main menu, choose Configuration > SNMP Trap Receiver.
The SNMP Trap Receiver page opens (Figure 26).

Figure 26 SNMP Trap Receiver page

The screenshot shows the 'Configuration > SNMP Trap Receiver' page. At the top, there is a table titled 'Trap Receiver Table' with columns for 'Action', 'Index', 'IP Address', and 'Community'. Below this is a 'Trap Receiver Creation' form. The form includes a 'Trap Receiver Index' dropdown menu set to '1', an 'IP Address' text input field with a placeholder '(xxxxxx.xxxx.xxxx)', and a 'Community' text input field. A 'Submit' button is located at the bottom left of the form.

[Table 24](#) describes the fields on the Trap Receiver Table and Trap Receiver Creation sections of the SNMP Trap Receiver page.

Table 24 SNMP Trap Receiver page fields

Fields	Range	Description
		Deletes the row.
Trap Receiver Index	1..4	Choose the number of the trap receiver to create or modify.
IP Address	XXX.XXX.XXX.XX X	Type the network address for the SNMP manager that is to receive the specified trap.
Community	0..32	Type the community string for the specified trap receiver.

2 In the Trap Receiver Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry is displayed in the Trap Receiver Table ([Figure 26](#)).

Deleting an SNMP trap receiver configuration

To delete SNMP trap receiver configurations:

1 From the main menu, choose Configuration > SNMP Trap Receiver.

The SNMP Trap Receiver page opens ([Figure 26](#)).

2 In the Trap Receiver Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the SNMP trap receiver configuration.
- Click Cancel to return to the table without making changes.

Viewing learned MAC addresses by VLAN

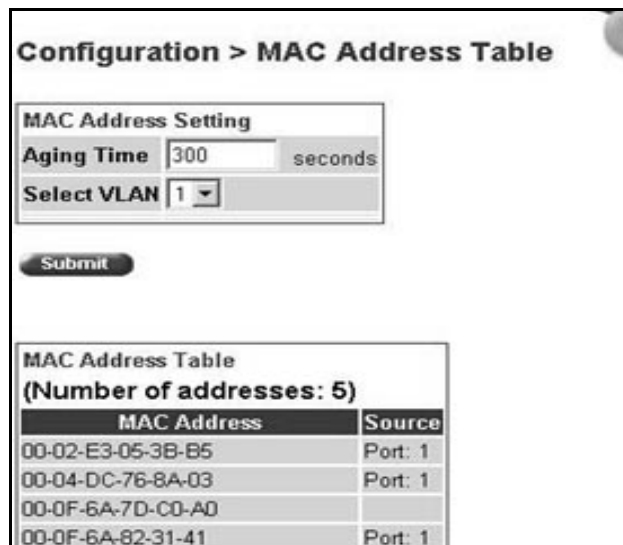
You can view MAC addresses and their associated port or trunk that the switch or stack configuration has learned, based on the VLAN you select.

To view learned MAC addresses and their associated port or trunk:

- 1 From the main menu, choose Configuration > MAC Address Table.

The MAC Address Table page opens (Figure 27).

Figure 27 MAC Address Table page



Configuration > MAC Address Table

MAC Address Setting

Aging Time seconds

Select VLAN

Submit

MAC Address Table
(Number of addresses: 5)

MAC Address	Source
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

[Table 25](#) describes the fields on the MAC Address Table page.

Table 25 MAC Address Table page fields

Section	Field	Range	Description
MAC Address Setting	Aging Time	10..1000000	Type the timeout period, in seconds, for aging out dynamically learned forwarding information. If the entry is inactive for a period of time that exceeds the specified aging time, the address is removed. Note: Nortel Networks recommends that you use the default value of 300 seconds.
	Select VLAN	1..255	Choose the VLAN on which to view learned MAC addresses.
MAC Address Table	MAC Address		The unicast MAC address for which the bridge has forwarding and/or filtering information.
	Source		The source of the discovered MAC address.

- 2 In the MAC Address Setting section, choose the aging time and VLAN you want to view learned MAC addresses on.
- 3 Click Submit.

Your request is displayed in the MAC Address Table ([Figure 27 on page 75](#)).

Locating a specific MAC address

You can search for a specific MAC address among all the MAC addresses learned from all the VLANs. This is a useful tool for finding whether or not a switch has learned a particular address.

To locate a specific MAC addresses:

- 1 From the main menu, choose Configuration > Find MAC Address.

The Find MAC Address Table page opens ([Figure 28](#)).

Figure 28 Find MAC Address Table page

Configuration > Find MAC Address Table

Find MAC Address Setting

Find MAC Address Not Found

Submit

MAC Address Table	
MAC Address	Source
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-C0-4F-0C-4E-24	Port: 1
08-00-20-7B-74-52	Port: 1

[Table 25 on page 76](#) describes the items on the MAC Address Table page fields.

- 2 In the MAC Address Setting section, type the MAC address you want to search for.
- 3 Click Submit to enter the request.

If the address is located, it is shown in the first row in the MAC Address Table section. If the address is not located, the system response “Not Found” is shown to the right of the Find MAC Address input field.

Configuring switch port autonegotiation speed

You can configure a specific switch port or all switch ports to autonegotiate for the highest available speed of the connected station or you can set the speed for selected switch ports (autonegotiation is not supported on 1000 Mb/s fiber optic ports).

To configure a switch port's autonegotiation speed:

- 1 From the main menu, choose Configuration > Port Management.
The Port Management page opens (Figure 29).

Figure 29 Port Management page

Configuration > Port Management

Port Management Setting						
Port	Trunk	Status	Link	Link Trap	Autonegotiation	Speed / Duplex
1		Enabled ▾	Up	On ▾	Enabled ▾	100Mbps / Full ▾
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 ▾	▾
Switch		Enable ▾ <input type="checkbox"/>		On ▾ <input type="checkbox"/>	Enable ▾ <input type="checkbox"/>	▾ <input type="checkbox"/>

Submit

[Ports 13 - 24](#)
 [Ports 25 - 36](#)
 [Ports 37 - 48](#)
 [Ports 49 - 50](#)

Table 26 describes the items on the Port Management page.

Table 26 Port Management page items

Item	Range	Description
Port		The switch port number of the corresponding row. The values that you set in each switch row affect all switch ports and, when the switch is part of a stack, the values that set in the stack row affect all ports in the entire stack (except the GBIC port or fiber optic ports when installed).
Trunk		The trunk group that the switch port belongs to as specified in the Trunk Member fields on the MultiLink Trunk page.
Status	(1) Enabled (2) Disabled	Choose to enable or disable the port. You can also use this field to control access to any switch port. The default setting is Enabled.
Link		The current link state of the corresponding port as follows: Up: The port is connected and operational Down: The port is not connected or is not operational.
Link/Trap	(1) On (2) Off	Choose to control whether link up/down traps are sent to the configured trap sink from the switch. The default setting is On.
Autonegotiation	(1) Enabled (2) Disabled	Choose to enable or disable the autonegotiation feature. Choosing to enable autonegotiation sets the corresponding port speed to match the best service provided by the connected station, up to 100Mb/s in full-duplex mode. Note: Autonegotiation also enables auto polarity on 10/100 ports. The default setting is Enabled.
Speed / Duplex	(1) 10Mbps / Half (2) 10Mbps / Full (3) 100Mbps / Half (4) 100Mbps / Full (5) 1000Mbps / Full	Choose the Ethernet speed you want the port to support. The default setting is 100Mbps/Half when autonegotiation is disabled and 1000 Mb/s full-duplex for gigabit ports only.

- 2 In the upper-left corner, click on the unit number of the BayStack 425 switch to manage.

The page is updated with the information for the selected switch.

- 3 In the port row of your choice, select from the lists.
- 4 Click Submit.

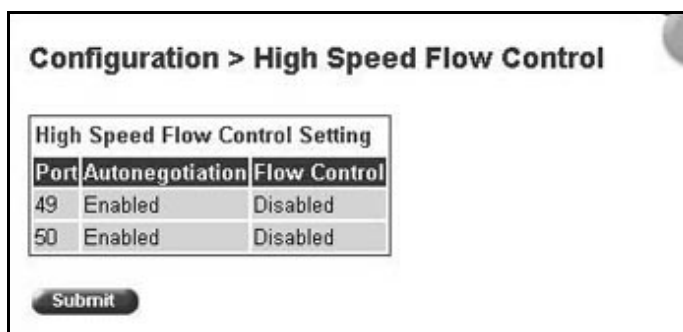
Configuring high speed flow control

You can set switch port parameters for GBICs when the switch is participating in a stack configuration.

To configure high speed flow control:

- 1 From the main menu, choose Configuration > High Speed Flow Control.
The High Speed Flow Control page opens (Figure 30).

Figure 30 High Speed Flow Control page



High Speed Flow Control Setting		
Port	Autonegotiation	Flow Control
49	Enabled	Disabled
50	Enabled	Disabled

Submit

Table 27 describes the items on the High Speed Flow Control page.

Table 27 High Speed Flow Control page items

Item	Range	Description
Autonegotiation	(1) Enabled (2) Disabled	Choose to enable or disable the autonegotiation feature. When enabled, the port advertises support only for 1000Mb/s operation in full-duplex mode.
Flow Control	(1) Enabled (2) Symmetric (3) Asymmetric	Choose your flow control preference to control traffic and avoid congestion on the GBIC port.

- 2 In the upper-left corner, click on the unit number of the GBIC to configure.
- 3 Select from the lists.
- 4 Click Submit.

Downloading switch images

You can download the BayStack 425-24T Switch software image that is located in non-volatile flash memory. To download the [Product Name (short)] software image, a properly configured Trivial File Transfer Protocol (TFTP) server must be present in your network, and the policy switch must have an IP address.

To learn how to configure the switch or stack IP address, refer to [“Configuring BootP, IP, and gateway settings” on page 46](#).



Caution: Do not interrupt power to the device during the software download process. A power interruption can corrupt the firmware image.

To download a switch image:

- 1 From the main menu, choose Configuration > Software Download.
The Software Download page opens ([Figure 31](#)).

Figure 31 Software Download page

Configuration > Software Download

Software Download Setting

Current Running Version v3.1.0.60

Local Store Version v3.1.0.60

Image Filename bs42x_31060.img

Diagnostics Filename

TFTP Server IP Address 134.177.152.102 (xxx.xxx.xxx.xxx)

Download Option No

Submit

Table 28 describes the fields on the Software Download page.

Table 28 Software Download page fields

Fields	Range	Description
Current Running Version		The version of the current running software.
Local Store Version		The local version of the software in the flash memory.
Image Filename	1..30	Type the software image load filename.
Diagnostics Filename	1..30	Type the diagnostics filename.
Image Filename	1..30	Type the image filename.
TFTP Server IP Address	XXX.XXX.XXX.XXX	Type the IP address of your TFTP load host.
Download Option	(1) No (2) Image (3) Diagnostics	Choose the software image to load.

- 2 Type information in the text boxes, or select from a list.
- 3 Click Submit.

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. Take care not to interrupt the download process until after it runs to completion (the process can take up to 10 minutes, depending on network conditions).

When the download process is complete, the switch automatically resets and the new software image initiates a self-test.

During the download process, the BayStack 425-24T Switch is not operational. You can monitor the progress of the download process by observing the LED indications.

[Table 29](#) describes the LED indications during the software download process.



Note: The LED indications described in [Table 29](#) apply to a 24-port switch model. Although a 12-port switch provides *similar* LED indications, the LED indication sequence is associated within the 12-port range.

Table 29 LED Indications during the software download process

Phase	Description	LED Indications
1	The switch downloads the new software image.	100 Mb/s port status LEDs (ports 18 to 24 only): The LEDs begin to turn on in succession beginning with port 24, which indicates the progress of the download process. When LEDs 18 to 24 are all on, the switch has received the new software image successfully.
2	The switch erases the flash memory.	100 Mb/s port status LEDs (ports 1 to 12 only): The LEDs begin to turn on in succession beginning with port 1, which indicates that various sectors of the switch's flash memory are being erased. When LEDs 1 to 12 are all on, the switch's flash memory has been erased.
3	The switch programs the new software image into the flash memory.	100 Mb/s port status LEDs (ports 1 to 8 only): The LEDs begin to turn on in succession beginning with port 1, which indicates that the new software image is being programmed into the switch's flash memory. When LEDs 1 to 8 are all on, the new software image has been programmed successfully into the switch's flash memory.
4	The switch resets automatically.	After the reset completes, the new software image initiates the switch self-test, which comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

Storing and retrieving a switch configuration file from a TFTP server

You can store switch and stack configuration parameters on a Trivial File Transfer Protocol (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.

To store a switch or stack configuration, you must set up the file on your TFTP server and set the filename read/write permission to enabled.

To download the BayStack 425-24T Switch configuration file, a properly configured TFTP server must be present in your network, and the BayStack 425 switch must have an IP address.

To learn how to configure the switch or stack IP address, refer to [“Configuring BootP, IP, and gateway settings”](#) on page 46.

To store or retrieve a switch or stack configuration file:

- 1 From the main menu, choose Configuration > Configuration File.

The Configuration File Download/Upload page opens ([Figure 32](#)).

Figure 32 Configuration File Download/Upload page

Configuration File Setting	
Configuration Image Filename	<input type="text"/>
TFTP Server IP Address	<input type="text" value="0.0.0.0"/> (xxx.xxx.xxx.xxx)
Copy Configuration Image to Server	<input type="button" value="No"/>
Retrieve Configuration Image from Server	<input type="button" value="No"/>

Table 30 describes the items on the Configuration File Download/Upload page.

Table 30 Configuration File Download/Upload page items

Item	Range	Description
Configuration Image Filename	1..32	Type the configuration file name.
TFTP Server IP Address	XXX.XXX.XXX.XXX	Type the IP address of the TFTP load host.
Copy Configuration Image to Server	(1) Yes (2) No	Choose whether or not to copy the configuration image to the server.
Retrieve Configuration Image from Server	(1) Yes (2) No	Choose whether or not to retrieve the configuration image from a server. If you choose Yes, the download process begins immediately and, when completed, causes the switch or stack to reset with the new configuration parameters.

- 2 Type information in the text boxes, or select from a list.
- 3 Click Submit.

Requirements for storing and retrieving configuration parameters on a TFTP server

The following requirements apply when storing and retrieving configuration parameters on a TFTP server:

- 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 .
- The configuration file also duplicates any settings that exist for any GBIC that is installed in the donor switch.
- If you use the configuration file to configure another switch that has the same GBIC model installed, the configuration file settings will also apply to and override the existing GBIC settings.

[Table 31](#) describes the parameters that are not saved to the configuration file.

Table 31 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	46
In-Band Switch IP Address		
In-Band Subnet Mask		
Default Gateway		
Configuration Image Filename	Configuration File Download/Upload	84
TFTP Server IP Address		
Console Read-Only Switch Password	Console/Comm Port Configuration	86
Console Read-Write Switch Password		
Console Read-Only Stack Password		
Console Read-Write Stack Password		

Configuring port communication speed

You can view the current console/communication port settings and configure the console port baud rate to match the baud rate of the console terminal.

To view current console/communication port settings and configure console port speed:

- 1 From the main menu, choose Configuration > Console/Comm Port.
The Console/Communication Port page opens ([Figure 33](#)).

Figure 33 Console/Communication Port page

Configuration > Console/Communication Port

Communication Port Setting	
Comm Port Data Bits	8 Data Bits
Comm Port Parity	No Parity
Comm Port Stop Bits	1 Stop Bit
Console Port Speed	9600

Submit

Table 32 describes the items on the Console/Communication Port page.

Table 32 Console/Communication Port page items

Item	Range	Description
Comm Port Data Bits		The current console communication port data bit setting.
Comm Port Parity		The current console communication port parity setting.
Comm Port Stop Bits		The current console communication port stop bit setting.
Console Port Speed	2400 4800 9600 19200 38400	Choose the console port speed baud rate. Note: The default setting is 9600. Caution: If you choose a baud rate that does not match your console terminal baud rate, you will lose communication with the configuration interface when you click Submit.

- 2 Select from the list.
- 3 Click Submit.

Chapter 5

Configuring Remote Network Monitoring

The Remote Network Monitoring (RMON) Management Information Base (MIB) is an interface between the RMON agent on a BayStack 420/425 Switch and RMON management applications such as the Web-based management user interface. It defines objects that are suitable for the management of any type of network. Some groups are specifically targeted for Ethernet networks.

The RMON agent continuously collects statistics and proactively monitors the switch.

This RMON options available to you are:

- [“Configuring RMON fault threshold parameters,”](#) next
- [“Viewing the RMON fault event log”](#) on page 93
- [“Viewing the system log”](#) on page 94
- [“Viewing RMON Ethernet statistics”](#) on page 97
- [“Viewing RMON history”](#) on page 99

Configuring RMON fault threshold parameters

Alarms are useful when you need to know when the value of some variable goes out of range. RMON alarms can be defined on any MIB variable that resolves to an integer value. String variables (such as system description) cannot be used as alarm variables.

Creating an RMON fault threshold

You can create the RMON threshold parameters for fault notification (alarms).

To create an RMON threshold:

- 1 From the main menu, choose Fault > RMON Threshold.

The RMON Threshold page opens (Figure 34).

Figure 34 RMON Threshold page

The screenshot shows the 'Fault > RMON Threshold' page. At the top, there is a table header for the 'RMON Threshold Table' with columns: Action, Index, Target, Parameter, Current Level, Rising Level, Rising Action, and Rising Event Index. Below this is a 'RMON Threshold Creation' form with the following fields:

- Alarm/Event Rising Index:
- Port:
- Parameter: Good-Bytes (dropdown)
- Rising Level:
- Rising Action: None (dropdown)
- Interval: seconds
- Alarm Sample: Absolute (dropdown)

Table 33 describes the items on the RMON Threshold page.

Table 33 RMON Threshold page items


Item	Range	Description
		Deletes the row.
Index/Alarm Index	1..10	Type the unique number to identify the alarm entry.
Target	Integer	The unit number and port number.
Unit	1..8	Choose the switch on which to configure port alarms.
Port	1..25	Choose the port on which to set an alarm.

Table 33 RMON Threshold page items (continued)

Item	Range	Description
Parameter	(1) Good-Bytes (2) Good-Packets (3) Multicast (4) Broadcast (5) CRC-Errors (6) Runts (7) Fragments (8) Frame-Too-Long (9) Collisions	Choose the sampled statistic.
Current Level	Integer	The value of the statistic during the last sampling period. Note: If the sample type is Delta, the value is the difference between the samples at the <i>beginning and end</i> of the period. If the sample type is Absolute, the value is the sampled value at the <i>end</i> of the period.
Rising Level	Integer	Type the event entry to be used when a rising threshold is crossed. Note: When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated. After a rising event is generated, another such event is not generated until the sampled value falls below this threshold and reaches the Falling Threshold.
Rising Action	(1) None (2) Log (3) SNMP Trap (4) Log and Trap	Choose the type of notification for the event. Selecting Log generates an entry in the RMON Event Log table for each event. Selecting SNMP Trap sends an SNMP trap to one or more management stations.

Table 33 RMON Threshold page items (continued)

Item	Range	Description
Interval		Type the time period (in seconds) to sample data and compare the data to the rising and falling thresholds.
Sample/Alarm Sample	(1) Absolute (2) Delta	Choose the sampling method. Absolute: <i>Absolute</i> alarms are defined on the current value of the alarm variable. An example of an alarm defined with absolute value is card operating status. Because this value is not cumulative, but instead represents states, such as card up (value 1) and card down (value 2), you set it for absolute value. Therefore, an alarm could be created with a rising value of 2 and a falling value of 1 to alert a user to whether the card is up or down. Delta: Most alarm variables related to Ethernet traffic are set to <i>delta</i> value. Delta alarms are defined based on the difference in the value of the alarm variable between the start of the polling period and the end of the polling period. Delta alarms are sampled twice per polling period. For each sample, the last two values are added together and compared to the threshold values. This process increases precision and allows for the detection of threshold crossings that span the sampling boundary. Therefore, if you keep track of the current values of a given delta-valued alarm and add them together, the result is twice the actual value. (This result is not an error in the software.)

- 2 In the RMON Threshold Creation section, type information in the text boxes, or select from a list.
- 3 Click Submit.

The new configuration is displayed in the RMON Threshold Table ([Figure 34 on page 90](#)).



Note: RMON threshold configurations are not modifiable. They must be deleted and the information recreated.

Deleting an RMON threshold configuration

To delete an existing RMON threshold configuration:

- 1 From the main menu, choose Fault > RMON Threshold.
The RMON Threshold page opens ([Figure 34 on page 90](#).)

- 2 In the RMON Threshold Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

- 3 Do one of the following:
 - Click Yes to delete the RMON threshold configuration.
 - Click Cancel to return to the RMON Threshold page without making changes.

Viewing the RMON fault event log

RMON events and alarms work together to notify you when values in your network go out of a specified range. When values pass the specified ranges, the alarm is triggered and “fires.” The event specifies how the activity is recorded.

An event specifies whether a trap, a log, or a trap and a log are generated to view alarm activity. When RMON is globally enabled, two default events are generated:

- Rising Event
- Falling Event

Default events specify that when an alarm goes out of range, the firing of the alarm is tracked in both a trap and a log. For example, when an alarm fires at the rising threshold, the rising event specifies that this information be sent to both a trap and a log. The RMON Event Log page works in conjunction with the RMON Threshold page to enable you to view a history of RMON fault events.

To view a history of RMON fault events:

- ➔ From the main menu, choose Fault > RMON Event Log.

The RMON Event Log page opens ([Figure 35](#)).

Figure 35 RMON Event Log page

[Table 34](#) describes the fields on the RMON Event Log page.

Table 34 RMON Event Log page fields

Field	Description
Time Stamp	The time the event occurred.
Description	An implementation dependent description of the event that activated this log entry.
Triggered By	A comment describing the source of the event.
ID	The event that generated this log entry.

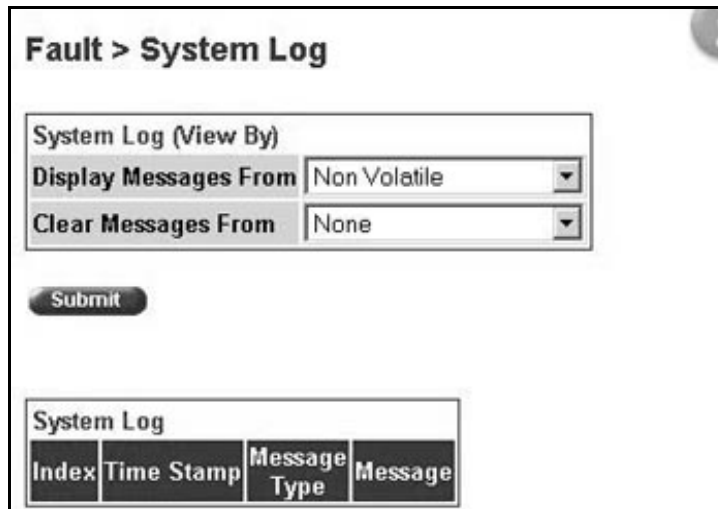
Viewing the system log

You can view a display of messages contained in Non-Volatile Random Access Memory (NVRAM) or Dynamic Random Access Memory (DRAM) and NVRAM.

To open the System Log page:

- 1 From the main menu, choose Fault > System Log.

The System Log page opens ([Figure 36](#)).

Figure 36 System Log page

The screenshot shows a web interface for viewing system logs. At the top, it says "Fault > System Log". Below this is a form with two dropdown menus: "Display Messages From" set to "Non Volatile" and "Clear Messages From" set to "None". A "Submit" button is located below the form. At the bottom, there is a table header for the "System Log" with columns: Index, Time Stamp, Message Type, and Message.

System Log			
Index	Time Stamp	Message Type	Message

[Table 35](#) describes the fields on the System Log page.

Table 35 System Log page fields

Section	Field	Range	Description
System Log (View By)	Display Unit	1..8	Choose the unit on which to display messages or clear messages.
System Log	Display Messages From	(1) Non Volatile (2) Volatile + Non Volatile	Choose to display messages from Non Volatile memory (NVRAM) or Volatile (DRAM) and Non Volatile memory. The default settings is Non Volatile.
	Clear Messages From	(1) Volatile (2) Volatile + Non Volatile (3) None	Choose to clear messages from Volatile memory or Volatile and Non Volatile memory. The default settings is None (do not clear messages)
System Log	Index		The number of the event.
	Time Stamp		The time, in hundreths of a second, between system initialization and the time the log messages entered the system.
	Message Type		The type of message. The options are (1) Critical, (2) Serious, and (3) Informational.
	Message		A character string that identifies the origin of the message and the reason why the message was generated.

2 In the System Log (View By) section do one or more of the following:

- Choose the number of the unit from which to display messages.
- Choose where to display messages from.
- Choose to clear messages from Volatile or Non Volatile memory.

3 Click Submit.

The results of your request are displayed in the System Log section ([Figure 36 on page 95](#)).

Viewing RMON Ethernet statistics

You can gather and graph RMON Ethernet statistics in a variety of formats.

To gather and graph RMON Ethernet statistics:

- 1 From the main menu, choose Statistics > RMON Ethernet.

The RMON Ethernet page opens (Figure 37).

Figure 37 RMON Ethernet page

Statistics > RMON Ethernet											
RMON Ethernet Statistics Table											
Port	Drop Events	Octets	Packets	Broadcast	Multicast	CRC Align Errors	Undersize	Oversize	Fragments	Collisions	Jabbers
1	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0

Table 36 describes the items on the RMON Ethernet page.

Table 36 RMON Ethernet page items

Item	Description
Port	The port number that corresponds to the selected switch.
Drop Events	The number of events in which packets were dropped by the interface due to a lack of resources.
Octets	The number of octets of data (including those in bad packets) received on the network (excluding framing bits, but including Frame Check Sequence (FCS) octets).
Packets	The number of packets received/transmitted on a port, including bad, broadcast and multicast packets.
Broadcast	The number of good packets received that were directed to the broadcast address. This <i>does not</i> include multicast packets.
Multicast	The number of good packets received that were directed to the multicast address. This <i>does not</i> include packets sent to the broadcast address.
CRC Align Errors	The number of packets received that had a length (excluding and 1518 octets, inclusive, but had either a bad Frame FCS with an integral number of octets (FCS errors) with a non-integral number of octets (alignment error).
Undersize	The number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.
Oversize	The number of packets received that were longer than 1518 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.
Fragments	The number of packets received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Collisions	The “best estimate” number of collisions on this Ethernet segment.
Jabbers	The number of packets received that were longer than 1518 octets in length (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Packets < = 64 bytes 65-127 bytes 128-255 bytes 256-511 bytes 512-1023 bytes 1024-1518 bytes	The number of octets received (including bad packets) in length (excluding framing bits, but including FCS octets).

- 2 In the upper-left hand corner, click on the unit number of the device to monitor.
- 3 Click Submit.

The RMON Ethernet Statistics Table is updated with information about the selected device ([Figure 37 on page 97](#)).

Viewing RMON history

You can view a periodic statistical sampling of data from various types of networks.

To view periodic statistical data:

- 1 From the main menu, choose Statistics > RMON History.

The RMON History page opens (Figure 38).

Figure 38 RMON History page

The screenshot shows the 'Statistics > RMON History' page. It features a form titled 'RMON History Statistics (View By)' with a 'Port' dropdown menu set to '1' and a 'Submit' button. Below the form is a table titled 'RMON History Statistics Table' with the following data:

Start	Drop Events	Octets	Packets	Broadcast	Multicast	CRC Align Errors
1 Weeks 1 Days 17 Hours 16 Minutes 6 Seconds	0	0	0	0	0	0
1 Weeks 1 Days 17 Hours 16 Minutes 36 Seconds	0	0	0	0	0	0
1 Weeks 1 Days 17 Hours 17 Minutes 6 Seconds	0	0	0	0	0	0
1 Weeks 1 Days 17 Hours 17 Minutes 36 Seconds	0	0	0	0	0	0
1 Weeks 1 Days 17 Hours 18 Minutes 6 Seconds	0	0	0	0	0	0
1 Weeks 1 Days 17 Hours 18 Minutes 36 Seconds	0	0	0	0	0	0
1 Weeks 1 Days 17 Hours 19 Minutes 6 Seconds	0	0	0	0	0	0
1 Weeks 1 Days 17 Hours 19 Minutes 36 Seconds	0	0	0	0	0	0
1 Weeks 1 Days 17 Hours 20 Minutes 6 Seconds	0	0	0	0	0	0
1 Weeks 1 Days 17 Hours 20 Minutes 36 Seconds	0	0	0	0	0	0
1 Weeks 1 Days 17 Hours 21 Minutes 6 Seconds	0	0	0	0	0	0

Table 37 describes the items on the RMON History page.

Table 37 RMON History page items

Section	Item	Description
RMON History Statistics Table (View By)	Unit	Choose the unit number to be monitored.
	Port	Choose the port number to be monitored.

Table 37 RMON History page items

Section	Item	Description
RMON History Statistics Table	Start	The value of the sysUptime at the start of the interval over which this sample was measured.
	Drop Events	The number of events in which packets were dropped by the interface due to a lack of resources.
	Octets	The number of octets of data (including those in bad packets) received on the network (excluding framing bits, but including Frame Check Sequence (FCS) octets).
	Packets	The number of packets received/transmitted on a port, including bad, broadcast and multicast packets.
	Broadcast	The number of good packets received that were directed to the broadcast address. This <i>does not</i> include multicast packets.
	Multicast	The number of good packets received that were directed to the multicast address. This <i>does not</i> include packets sent to the broadcast address.
	CRC Align Errors	The number of packets received that had a length (excluding and 1518 octets, inclusive, but had either a bad Frame FCS with an integral number of octets (FCS errors) with a non-integral number of octets (alignment error).
	Undersize	The number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.
	Oversize	The number of packets received that were longer than 1518 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.

- 2 In the Port Statistics section, choose the unit and port number to be monitored.
- 3 Click Submit.

The Port Statistics Table is updated with information about the selected device and port (Figure 38).

Chapter 6

Viewing system statistics

The options available to monitor system statistical data are:

- [“Viewing port statistics,”](#) next
- [“Viewing interface statistics”](#) on page 105
- [“Viewing Ethernet error statistics”](#) on page 106
- [“Viewing transparent bridging statistics”](#) on page 109

Viewing port statistics

You can view detailed statistics about a selected switch port in a stacked or standalone configuration. Both received and transmitted statistics are displayed so that you can compare throughput or other port parameters.

To view statistical data about a selected switch port:

- 1 From the main menu, choose Statistics > Port.

The Port page opens ([Figure 39](#)).

Figure 39 Port page

The screenshot shows a web interface titled "Statistics > Port". At the top, there is a section "Port Statistics (View By)" with a dropdown menu set to "Port" and a value of "1". Below this is a "Submit" button. The main content is a "Port Statistics Table" with two columns: "Received" and "Transmitted". Each row represents a different metric, with a counter (0) and a unit (0). The metrics include Packets, Multicasts, Broadcasts, Total Octets, Pause Frames, FCS Errors, Collisions, Undersized Packets, Single Collisions, Oversized Packets, Multiple Collisions, Discarded Packets, Excessive Collisions, Aged Packets, Deferred Packets, Frame Errors, and Late Collisions. Below the main table is a sub-section "Received/Transmitted" with three rows of byte ranges and their respective counts (0). At the bottom, there are three buttons: "Update", "Zero Port", and "Zero All Ports".

Port Statistics Table	
Received	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

Table 38 describes the items on the Port page.

Table 38 Port page items

Section	Item	Description
Port Statistics (View By)	Unit	Choose the number of the switch to monitor.
	Port	Choose the switch's port number to monitor.

Table 38 Port page items (continued)

Section	Item	Description
Port Statistics Table	Packets	The number of packets received/transmitted on this port, including bad packets, broadcast packets, and multicast packets.
	Multicast	The number of good multicast packets received/transmitted on this port, excluding broadcast packets.
	Broadcasts	The number of good broadcast packets received/transmitted on this port.
	Total Octets	The number of octets of data received/transmitted on this port, including data in bad packets and FCS octets, and framing bits.
	Pause Frames	The number of pause frames received/transmitted on this port.
	Lost Packets	The number of packets discarded on this port when the capacity of the port transmit buffer was exceeded.
	Packets = 64 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 65-127 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 128-255 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 256-511 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 512-1023 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 1024 or more bytes	The number of packets this size received/transmitted successfully on this port.
	FCS Errors	The number of valid-size packets received on this port with proper framing but discarded because of cyclic redundancy check (CRC) errors.
	Undersized Packets	The number of packets received on this port with fewer than 64 bytes and with proper CRC and framing (also known as short frames or runts).
	Oversized Packets	The number of packets that were received on this port with proper CRC and framing that meet the following requirements: <ul style="list-style-type: none"> • 1518 bytes if no VLAN tag exists • 1522 bytes if a VLAN tag exists
Filtered Packets	The number of packets filtered, but not forwarded on this port.	

Table 38 Port page items (continued)

Section	Item	Description
	Flooded Packets	The number of packets flooded (forwarded) through this port because the destination address was not recognized in the address database.
	Frame Errors	The number of valid-size packets received on this port but discarded because of CRC errors and improper framing.
Port Statistics Table, cont.	Collisions	The number of collisions detected on this port.
	Single Collisions	The number of packets that were transmitted successfully on this port after a single collision.
	Multiple Collisions	The number of packets that were transmitted successfully on this port after more than one collision.
	Excessive Collisions	The number of packets lost on this port due to excessive collisions.
	Deferred Packets	The number of frames that were delayed on the first transmission attempt, but never incurred a collision.
	Late Collisions	The number of packets collisions that occurred after a total length of time that exceeded 512 bit-times of packet transmission.

2 In the Port Statistics section, choose the unit number and its port number.

3 Click Submit.

The Port Statistics Table is updated with information about the selected device and port ([Figure 40 on page 105](#)).

4 To update the statistical information, click Update.

Zeroing ports

To clear the statistical information for the currently displayed port:

➔ Click Zero Port.

To clear the statistical information for all ports in a switch or stack configuration:

➔ Click Zero All Ports.

Viewing interface statistics

You can view selected switch interface statistics.

To view an interface's statistical information:

- 1 From the main menu, choose Statistics > Interface.

The Interface page opens (Figure 40).

Figure 40 Interface page

Statistics > Interface												
Interface Statistics Table												
Port	In Octets	Out Octets	In Unicast	Out Unicast	In Non-Unicast	Out Non-Unicast	In Discards	Out Discards	In Errors	Out Errors	In Unknown Protos	
1	0	0	0	0	0	0	0	0	0	0	0	
2	0	0	0	0	0	0	0	0	0	0	0	
3	0	0	0	0	0	0	0	0	0	0	0	
4	0	0	0	0	0	0	0	0	0	0	0	
5	0	0	0	0	0	0	0	0	0	0	0	
6	0	0	0	0	0	0	0	0	0	0	0	
7	0	0	0	0	0	0	0	0	0	0	0	
8	0	0	0	0	0	0	0	0	0	0	0	
9	0	0	0	0	0	0	0	0	0	0	0	
10	0	0	0	0	0	0	0	0	0	0	0	
11	0	0	0	0	0	0	0	0	0	0	0	
12	0	0	0	0	0	0	0	0	0	0	0	
13	0	0	0	0	0	0	0	0	0	0	0	
14	0	0	0	0	0	0	0	0	0	0	0	
15	0	0	0	0	0	0	0	0	0	0	0	

Table 39 describes the items on the Interface page.

Table 39 Interface page items

Item	Description
Port	The port number corresponding to the selected switch.
In Octets	The number of octets received on the interface, including framing characters.
Out Octets	The number of octets transmitted out of the interface, including framing characters.
In Unicast	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Out Unicast	The number of packets that higher-layer protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
In Non-Unicast	The number of non-unicast packets, for example, subnetwork-broadcast or subnetwork-multicast packets, delivered to a higher protocol.
Out Non-Unicast	The number of packets that higher-level protocols requested be transmitted to a non-unicast address. For example, a subnetwork-broadcast or a subnetwork multicast address, including those that were discarded or not sent.
In Discards	The number of inbound packets which were selected to be discarded even though no errors were detected to prevent their being delivered to a higher-layer protocol. Packet discarding is not arbitrary. One reason for discarding packets is to free buffer space.
Out Discards	The number of outbound packets which were selected to be discarded even though no errors were detected to prevent their being transmitted. Packet discarding is not arbitrary. One reason for discarding packets is to free buffer space.
In Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Out Errors	The number of outbound packets that could not be transmitted because of errors.
In Unknown Protocols	The number of packets received through the interface which were discards due to an unknown or unsupported protocol.

- 2 In the upper-left hand corner, click on the unit number of the device to monitor.

The page is updated with the information for the selected device ([Figure 40 on page 105](#)).

- 3 To update the statistical information, click Update.

Viewing Ethernet error statistics

You can view Ethernet error statistics for each monitored interface linked to the Business Policy Switch 2000.

To view Ethernet error statistics:

1 From the main menu, choose Statistics > Ethernet Errors.

The Ethernet Errors page opens (Figure 41).

Figure 41 Ethernet Errors page

Statistics > Ethernet Errors													
Ethernet Errors Statistics Table													
Port	Alignment Errors	FCS Errors	Internal MAC Transmit Errors	Internal MAC Receive Errors	Carrier Sense Errors	Frame Too Long	SOE Test Errors	Deferred Transmissions	Single Collisions Frames	Multiple Collisions Frames	Late Collisions	Excessive Collisions	
1	0	0	0	0	0	0	0	0	0	0	0	0	
2	0	0	0	0	0	0	0	0	0	0	0	0	
3	0	0	0	0	0	0	0	0	0	0	0	0	
4	0	0	0	0	0	0	0	0	0	0	0	0	
5	0	0	0	0	0	0	0	0	0	0	0	0	
6	0	0	0	0	0	0	0	0	0	0	0	0	
7	0	0	0	0	0	0	0	0	0	0	0	0	
8	0	0	0	0	0	0	0	0	0	0	0	0	
9	0	0	0	0	0	0	0	0	0	0	0	0	
10	0	0	0	0	0	0	0	0	0	0	0	0	
11	0	0	0	0	0	0	0	0	0	0	0	0	
12	0	0	0	0	0	0	0	0	0	0	0	0	
13	0	0	0	0	0	0	0	0	0	0	0	0	
14	0	0	0	0	0	0	0	0	0	0	0	0	
15	0	0	0	0	0	0	0	0	0	0	0	0	
16	0	0	0	0	0	0	0	0	0	0	0	0	
17	0	0	0	0	0	0	0	0	0	0	0	0	

Table 40 describes the items on the Ethernet Errors page.

Table 40 Ethernet Errors page items

Item	Description
Port	The port number corresponding to the selected switch.
Alignment Errors	The number of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check.
FCS Errors	The number of frames received on a particular interface that are an integral number of octets in length, but do not pass the FCS check.
Internal MAC Transmit Errors	The number of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame only is counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object.
Internal MAC Receive Errors	The number of frames for which reception on a particular interface fails due to an internal MAC sublayer transmit error. A frame only is counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object.
Carrier Sense Errors	The number of times that the carrier sense conditions was lost or never asserted when attempting to transmit a frame on a particular interface.
Frame Too Long	The number of frames received on a particular interface that exceed the maximum permitted frame size.
SQE Test Errors	The number of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985, and its generation is described in section 7.2.4.6 of the same document.
Deferred Transmissions	The number of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy.
Single Collision Frames	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Multiple Collision Frames	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by a single collision.
Late Collisions	The number of times a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.
Excessive Collisions	The number of frames for which transmission on a particular interface fails due to excessive collisions.

- 2 In the upper-left hand corner, click on the unit number of the device to monitor.

The table is updated with the information for the selected device.

- 3 To refresh the statistical information, click Update.

Viewing transparent bridging statistics

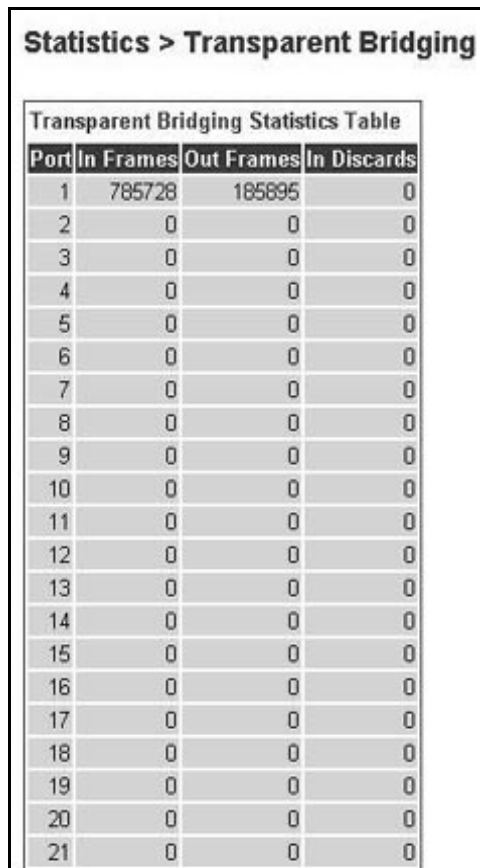
You can view the transparent bridging statistics measured for each monitored interface on the device.

To view transparent bridging statistics:

- 1 From the main menu, choose Statistics > Transparent Bridging.

The Transparent Bridging page opens (Figure 42).

Figure 42 Transparent Bridging page



The screenshot shows a web-based interface with the title "Statistics > Transparent Bridging". Below the title is a table titled "Transparent Bridging Statistics Table". The table has four columns: "Port", "In Frames", "Out Frames", and "In Discards". The first row shows port 1 with 785728 In Frames and 185895 Out Frames, while all other ports (2-21) show 0 for all three metrics.

Port	In Frames	Out Frames	In Discards
1	785728	185895	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0
8	0	0	0
9	0	0	0
10	0	0	0
11	0	0	0
12	0	0	0
13	0	0	0
14	0	0	0
15	0	0	0
16	0	0	0
17	0	0	0
18	0	0	0
19	0	0	0
20	0	0	0
21	0	0	0

Table 41 describes the items on the Transparent Bridging page.

Table 41 Transparent Bridging page items

Item	Description
Port	The port number that corresponds to the selected switch.
dot1dTpPortInFrames	The number of frames that have been received by this port from its segment. A frame received on the interface corresponding to this port is counted only if it is for a protocol being processed by the local bridging function, including bridge management errors.
dot1dTpPortOutFrames	The number of frames that have been transmitted by this port from its segment. A frame received on the interface corresponding to this port is counted only if it is for a protocol being processed by the local bridging function, including bridge management errors.
dot1dTpPortInDiscards	The number of valid frames received which were discarded by the forwarding process.

- 2 In the upper-left hand corner, click on the unit number of the device to monitor.

The page is updated with statistics about the selected device and its corresponding port number.

- 3 To refresh the statistical information, click Update.

Chapter 7

Configuring application settings

The options available to configure application settings are:

- [“Configuring port mirroring,”](#) next
- [“Configuring MAC address-based security”](#) on page 113
- [“Creating and managing VLANs”](#) on page 125
- [“Configuring VLANs”](#) on page 125
- [“Configuring broadcast domains”](#) on page 131
- [“Viewing VLAN port information”](#) on page 132
- [“Managing Spanning Tree Protocol”](#) on page 134
- [“Changing Spanning Tree bridge switch settings”](#) on page 136
- [“Configuring MultiLink Trunk members”](#) on page 140
- [“Monitoring MLT traffic”](#) on page 142

Configuring port mirroring

The BayStack 420/425 Switch supports port mirroring to analyze traffic. You can view existing port mirroring activity and you can configure a specific switch port to mirror up to two specified ports.

To configure port mirroring:

- 1 From the main menu, choose Application > Port Mirroring.
The Port Mirroring page opens ([Figure 43](#)).

Figure 43 Port Mirroring page

The screenshot shows a web interface for configuring port mirroring. The main heading is "Application > Port Mirroring". Below this is a "Port Mirroring Setting" box containing three dropdown menus: "Monitoring Mode" (currently set to "Disabled"), "Monitor Port", and "Port X". A "Submit" button is located below the settings. At the bottom of the page, there is a "Port Mirroring Active" status box, which also shows "Monitoring Mode" set to "Disabled".

Table 42 describes the items on the Port Mirroring page.

Table 42 Port Mirroring page items

Item	Range	Description
Monitoring Mode	(1) Disabled (2) --> Port X	The default setting is Disabled.
Port-based monitoring		
Monitor Port	1..24	Choose the switch port to designate as the monitor port.
Port X	1..24	Choose the switch port to be monitored by the designated monitor port. This port is monitored according to the value "X" in the Monitoring Mode field.

- 2 Type information in the text boxes, or select from a list.
- 3 Click Submit.

Table 43 describes the port-based monitoring modes.

Table 43 Port-based monitoring modes

Item	Description
Disabled	Choose this option to disable port-based monitoring. The default setting is Disabled.
--> Port X	Choose this option to monitor all traffic received by port X.

Configuring MAC address-based security

The MAC address-based security system allows you to specify a range of system responses to unauthorized network access to your switch with the Web-based management system.

The system response can range from sending a trap to disabling the port. The network access control is based on the MAC Source Addresses (SAs) of the authorized stations. You can specify a list of up to 448 MAC SAs that are authorized to access the switch. You can also specify the ports that each MAC SA is allowed to access. The options for allowed MAC SA port access include: NONE, ALL, and single or multiple ports that are specified in a list, for example, 1-4, 6, 9, and so forth. You must also include the MAC SA of any router connected to any secure ports.

When the switch software detects an SA security violation, the response can be to send a trap, turn on Destination Address (DA) filtering for all SAs, disable the specific port, or any combination of these three options.

You can configure the [Product Name (short)] to drop all packets having a specified MAC Destination Address (DA). You can create a list of up to 10 MAC DAs you want to filter. The packet with the specified MAC DA will be dropped regardless of the ingress port, Source Address (SA) intrusion, or VLAN membership.



Note: Ensure that you do not enter the MAC address of the switch or stack you are working on.



Note: After configuring the switch for MAC address-based security, you must enable the ports you want, using the Port Configuration page.

Configuring MAC address-based security

To configure MAC address-based security using the Web-based management system:

- 1 From the main menu, choose Application > MAC Address Security > Security Configuration.

The Security Configuration page opens (Figure 44).

Figure 44 Security Configuration page

Application > MAC Address Security > Security Configuration

MAC Address Security Setting	
MAC Address Security	Disabled ▾
MAC Address Security SNMP-Locked	Disabled ▾
Participation Port on Intrusion Detected	Disabled ▾
Participation Time	<input type="text" value=""/> (1 .. 65535)
DA Filtering on Intrusion Detected	Disabled ▾
Generate SNMP Trap on Intrusion	Disabled ▾



Submit

MAC Security Table			
	Action	Port List	Current Learning Mode
Clear by Ports	<input type="button" value=""/>		
Learn by Ports	<input type="button" value=""/>		Disabled ▾

Submit

Table 44 describes the items on the Security Configuration page.

Table 44 Security Configuration page items

Section	Item	Range	Description
MAC Address Security Setting	MAC Address Security	(1) Enabled (2) Disabled	Enables the MAC address security features.
	MAC Address Security SNMP-Locked	(1) Enabled (2) Disabled	Enables locking SNMP, so that you cannot use SNMP to modify the MAC address security features.
	Partition Port on Intrusion Detected	(1) Forever (2) Enabled (3) Disabled	Configures how the switch reacts to an intrusion event: Forever—The port is disabled and remains disabled (partitioned) until reset. The port does not reset after the Partition Time elapses. Enabled—The port is disabled, then automatically reset to enabled after the time specified in the Partition Time field elapses. Disabled—The port remains enabled, even if an intrusion event is detected.
	Partition Time	1 to 65535	Sets the time to partition a port on intrusion. Note: Use this field only if the Partition Port on Intrusion Detected field is set to Enabled.
	DA Filtering on Intrusion Detected	(1) Enabled (2) Disabled	Enables you to isolate the intruding node (discard) the packets.
	Generate SNMP Trap on Intrusion	(1) Enabled (2) Disabled	Enables generation of an SNMP when an intrusion is detected.
MAC Security Table/Clear by Ports	Action		Allows you to clear specific ports from participation in the MAC address security features.
	Port List		Will be blank.
	Current Learning Mode		Will be blank.
MAC Security Table/Learn by Ports	Action		Allows you to identify ports that will learn incoming MAC addresses. All source MAC addresses of any packets received on a specified port(s) are added to the MAC Security Table (maximum of 448 MAC addresses allowed).
	Port List		Displays all the ports that will learn incoming MAC address to detect intrusions (unallowed MAC addresses).
	Current Learning Mode	(1) Enabled (2) Disabled	Enables learning.

- 2 On the Security Configuration page, type information in the text boxes, or select from a list.
- 3 Click Submit.

Configuring ports

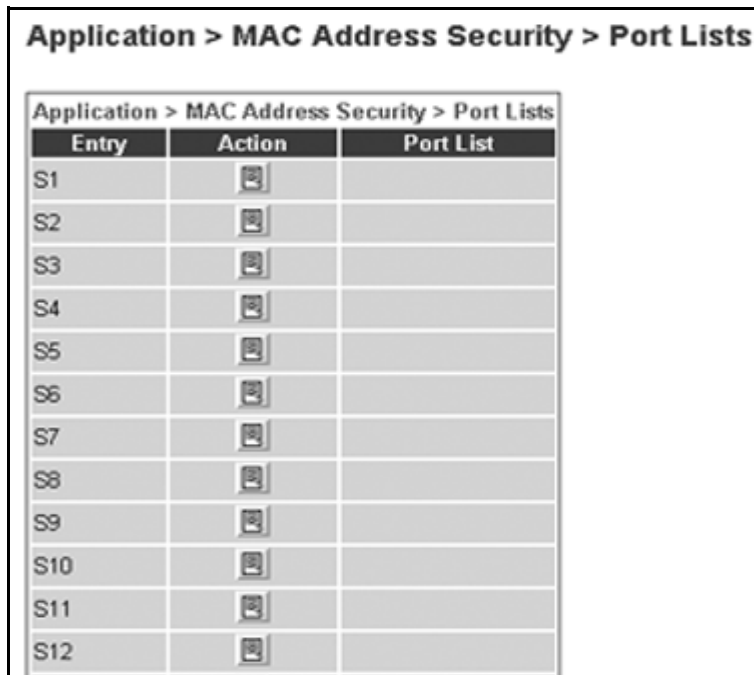
In this section, you create a list of ports, and you can add ports to or delete ports from each list.

To activate an entry or add or delete ports to a list:

- 1 From the main menu, choose Application > MAC Address Security > Port Lists.

The Port Lists page opens (Figure 45).

Figure 45 Port Lists page
















Application > MAC Address Security > Port Lists		
Entry	Action	Port List
S1		
S2		
S3		
S4		
S5		
S6		
S7		
S8		
S9		
S10		
S11		
S12		

Table 45 describes the items on the Ports Lists page.

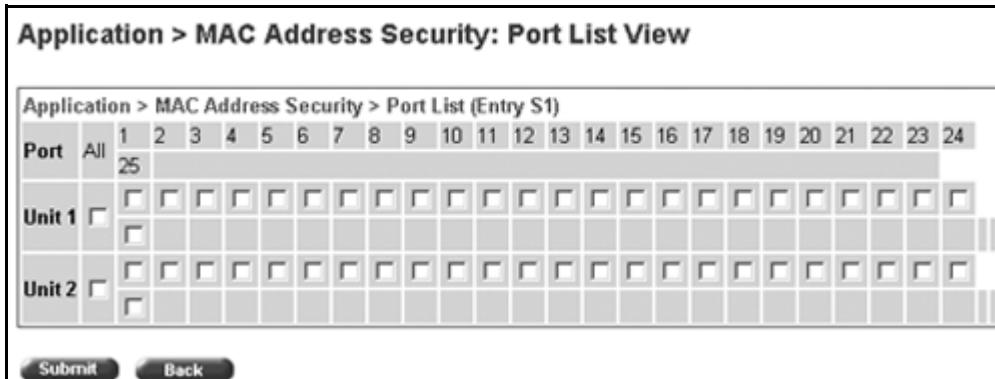
Table 45 Ports Lists page items

Item	Range	Description
Entry		These are the lists of ports.
Action		Allows you to add or delete ports to the lists.
Port List		Displays which ports are associated with each list.

- 2 To add or delete ports to a list, click the icon in the Action column in the list row you want.

The Port List View, Port List page opens (Figure 46).

Figure 46 Port List View, Port List page



- a Click the ports you want to add to the selected list or click None.
 - b To delete a port from a list, uncheck the box by clicking it.
 - c Click Submit.
- 3 From the main menu, choose Application > MAC Address Security > Security Configuration.
The Security Configuration page opens (Figure 44).
 - 4 In the MAC Security Table section, click the icon in the Action column of the Learn By Ports row.
The Port List View, Learn by Ports page opens (Figure 47).

Figure 47 Port List View, Learn by Ports page

Application > MAC Address Security: Port List View

Application > MAC Address Security > Port List (Entry S1)

Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Unit 1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unit 2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Submit Back

- a Click the ports through which you want the switch to learn MAC addresses or click None.
 - b If you want that port to no longer learn MAC addresses, click the checked box to uncheck it.
 - c Click Submit.
- 5 In the MAC Security Table section, choose Enabled in the Current Learning Mode column of the Learn By Ports row.
 - 6 Click Submit.



Note: You cannot include any of the port values you have chosen for the secure ports field.

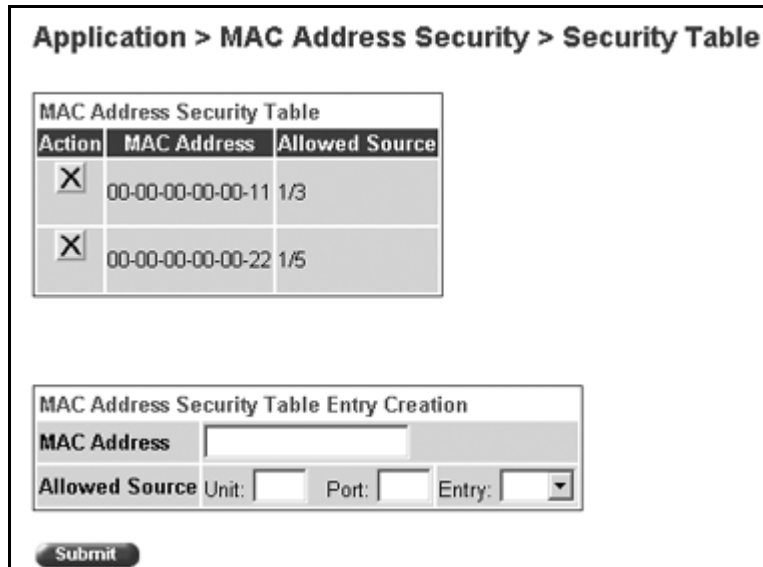
Adding MAC addresses

To add MAC address to the MAC address-based security system:

- 1 In the main menu, choose Applications > MAC Address Security > Security Table.

It may take awhile for the required addresses to be learned. Then, the Security Table page opens (Figure 48).

Figure 48 Security Table Page



Note: Using this page, you instruct the switch to allow the specified MAC address access *only* through the specified port or port list.

Table 46 describes the items on the Security Table page.

Table 46 Security Table page items

Section	Item	Range	Description
MAC Address Security Table	Action		Allows you to delete a MAC address.
	Address		Displays the MAC address.
	Allowed Source	(1) Unit/Port (2) Entry	Displays the entry through which the MAC address is allowed.

Table 46 Security Table page items (continued)

Section	Item	Range	Description
MAC Address Security Table Entry Creation	MAC Address		Enter the MAC address you want to allow to access the switch.
	Allowed Source		Select the unit and port through which the MAC address is allowed.
	Entry		Select the port list through which the MAC address is allowed.

- 2 Complete fields as described in the table.



Note: If you choose an Entry as the Allowed Source, you must have configured that specific entry on the Port View List, Port List page.

- 3 On the Security Table page, type information in the text boxes, or select from a list.
- 4 Click Submit.



Note: Be certain to include the MAC address for the default LAN router as an allowed source MAC address.

Clearing ports

You can clear all information from the specified port(s) for the list of ports that learn MAC addresses. If Learn by Ports is enabled, the specified ports will begin again to learn the MAC addresses.

To clear information from selected ports:

- 1 From the main menu, choose Application > MAC Address Security > Security Configuration.
The Security Configuration page opens ([Figure 44](#)).
- 2 In the MAC Security Table section, click the icon in the Action column of the Clear By Ports row.
The Port List View, Clear by Ports page opens ([Figure 49](#)).

Figure 49 Port List View, Clear by Ports page

Application > MAC Address Security: Port List View

Application > MAC Address Security > Port List (Entry S1)																									
Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
		25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
Unit 1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unit 2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- 3 Select the ports you want to clear or click None.
- 4 Click Submit.



Note: 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.

Enabling security on ports

To enable or disable MAC address-based security on the port:

- 1 From the main menu, choose Application > MAC Address Security > Port Configuration.

The Port Configuration page opens ([Figure 50](#)).

Figure 50 Port Configuration page

Application > MAC Address Security > Port Configuration

MAC Address Security > Port Configuration

Unit **1** 2

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 ▾

[Table 47](#) describes the items on the Port Configuration page.

Table 47 Port Configuration page items

Item	Range	Description
Unit	1 to 8	Displays the unit number of the ports shown in the table.
Port	1 to 26	Lists each port on the unit.
Trunk	Blank, 1 to 6	Displays the MultiLink Trunk that the port belongs to.
Security	(1) Enabled (2) Disabled	Enables MAC address-based security on that port. Note: You must configure the port for MAC address-based security before enabling the security.

Deleting ports

You can delete ports from the security system in a variety of ways:

- In the Ports List View, Port List page (Figure 46), click on the checkmark of a selected port to delete that port from the specified port list.
- In the Ports List View, Learn by Ports page (Figure 47), click on the checkmark of a selected port to remove that port from those that learn MAC addresses.
- In the Port Configuration page (Figure 50), click Disabled to remove that port from the MAC address-based security system; it will disable all MAC address-based security on that port.

Filtering MAC destination addresses

To drop all packets from a specified MAC Destination Address (DA):

- 1 From the main menu, choose Application > MAC Address Security > DA MAC Filtering.

The DA MAC Filtering page opens (Figure 51).

Figure 51 DA MAC Filtering page

The screenshot shows the DA MAC Filtering page with the following elements:


- Page title: **Application > MAC Address Security > DA MAC Filtering**
- Table: **Destination MAC Address Filtering Table**

Action	Index	MAC Address
- Form: **DA MAC Filtering Entry Creation**

DA MAC Address (xx.xx.xx.xx.xx.xx)

Table 48 describes the items on the DA MAC Filtering page.

Table 48 DA MAC Filtering page items

Section	Item	Range	Description
Destination MAC Address Filtering Table	Action		Allows you to delete a MAC DA you are filtering.
	MAC Address	1 -10	Displays list of MAC DAs you want filtered.
DA MAC Filtering Entry Creation	DA MAC Address	XX:XX:XX:XX:XX:XX	Enter the MAC DA you want to filter.



Note: Ensure that you do not enter the MAC address of the management station.

- 2 In the DA MAC Filtering Entry Creation area, enter the MAC DA you want to filter.

You can list up to 10 MAC DAs to filter.

- 3 Click Submit.

The system returns you to the DA MAC Filtering page ([Table 45](#)) with the new DA listed in the table.

Deleting MAC DAs

To delete a MAC DA:

- 1 From the main menu, choose Application > MAC Address Security > DA MAC Filtering.

The DA MAC Filtering page opens ([Figure 51](#)).

- 2 In the Destination MAC Address Filtering Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

- 3 Do one of the following:
 - Click Yes to delete the target parameter configuration.
 - Click Cancel to return to the table without making changes.

Creating and managing VLANs

A Virtual LAN(VLAN) is a collection of switch ports that make up a single broadcast domain. You can configure a VLAN for a single switch, or for multiple switches. When you create a VLAN, you can control traffic flow and ease the administration of moves, adds, and changes on the network, by eliminating the need to change physical cabling. Using the Web-based management interface, you can configure port-based VLANs.

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 on a switch, you assign a VLAN Identification Number (VLAN ID) and specify which ports belong to the VLAN. The VLAN ID is used to coordinate VLANs across multiple switches.

Configuring VLANs

You can create VLANs by assigning switch ports as VLAN members and you can designate an existing VLAN to act as the management VLAN.


To open the VLAN Configuration page:

- ➔ From the main menu, choose Application > VLAN > VLAN Configuration.

The VLAN Configuration page opens ([Figure 52](#)).

Figure 52 VLAN Configuration page

Application > VLAN > VLAN Configuration

VLAN Table			
Action	VLAN	VLAN Name	State
 	1	VLAN #1	Active

VLAN Creation

VLAN

VLAN Name

Create VLAN

VLAN Setting

Management VLAN

Submit



AutoPVID Setting

AutoPVID

Submit

Table 49 describes the items on the VLAN Configuration page.

Table 49 VLAN Configuration page items

Section	Item	Description
VLAN Table		Displays a modification page.
		Deletes the row.
VLAN Creation	VLAN	The number assigned to the VLAN when the VLAN was created.
	VLAN Name	The name assigned to the VLAN when the VLAN was created.
	State	The current operational state of the VLAN.
	VLAN	The number assigned to the VLAN.
VLAN Setting	VLAN Name	The name assigned to the VLAN.
	Management VLAN	Choose the VLAN to designate as the management VLAN.
Auto PVID Settings	AutoPVID	Choose Enabled to activate the Automatic PVID feature and to click Submit. Note: Use this <i>only</i> with port-based VLANs.

Creating a port-based VLAN

To create a port-based VLAN:

- 1 From the main menu choose Application > VLAN > VLAN Configuration.
The VLAN Configuration page opens ([Figure 52 on page 126](#)).
- 2 Type information in the text boxes, or select from a list.
The new port-based VLAN configuration appears in the VLAN Table on the VLAN Configuration page ([Figure 53 on page 128](#)).
- 3 Click Create VLAN.
The VLAN Configuration: Port Information page opens ([Figure 53](#)).

Figure 53 VLAN Configuration: Port Information page

Application > VLAN > Port Information

VLAN Port Information (View By)

Port	1
PVID	1
Port Name	Port 1

Submit

VLAN Port Information Table

VLAN	VLAN Name	VLAN Type
1	VLAN #1	Port

Table 50 describes the items on the VLAN Configuration: Port Information page.

Table 50 VLAN Configuration: Port Information page items

Item	Range	Description
VLAN	1..4094	The number assigned to the VLAN when the VLAN was created.
VLAN Name	1..16	Type a character string to create a unique name to identify the VLAN, for example, VLAN1.

Modifying a port-based VLAN

To modify an existing port-based VLAN:

- 1 From the main menu, choose Application > VLAN > VLAN Configuration.
The VLAN Configuration page opens (Figure 52 on page 126).
- 2 In the VLAN Table section, in the port-based VLAN row of your choice, click the Modify icon.
The VLAN Configuration: Port Configuration page opens (Figure 54).

Figure 54 VLAN Configuration: Port Configuration page

Port	Port Name	Filter Untagged Frames	PVID	Link Type
1	Port 1	No	1	Untagged Access
2	Port 2	No	1	Untagged Access
3	Port 3	No	1	Untagged Access
4	Port 4	No	1	Untagged Access
5	Port 5	No	1	Untagged Access
6	Port 6	No	1	Untagged Access
7	Port 7	No	1	Untagged Access
8	Port 8	No	1	Untagged Access
9	Port 9	No	1	Untagged Access
10	Port 10	No	1	Untagged Access
11	Port 11	No	1	Untagged Access
12	Port 12	No	1	Untagged Access

Submit

Ports 13 - 24 Ports 25 - 36 Ports 37 - 48 Ports 49 - 50

Table 51 describes the items on the VLAN Configuration: Port Configuration page.

Table 51 Port Configuration page items

Item	Range	Description
Port	1..25	The port number.
Port Name	1..16	Type character string to create a unique port name, for example, Unit 1, Port 1.
Filter Untagged Frames	(1) Yes (2) No	Choose how to process filter untagged frames. When a flag is set, the frames are discarded by the forwarding process. The default setting is No (no frames discarded).

Table 51 Port Configuration page items

Item	Range	Description
PVID	1..4094	Type the number of the VLAN ID to assign to untagged frames received on this trunk port. For example, a port with a PVID of 3 assigns all untagged frames received on this port to VLAN 3. The default setting is 1.
Link Type	(1) Untagged Access (2) Tagged Trunk	Choose the link type for each port.

- 3** Type information in the text boxes, or click the check box of a port to associate it with the VLAN or, if the port is already a member, click the check box to deselect it as a member of the VLAN.
- 4** Do one of the following:
 - Click Submit.
 - Click Back to return to the VLAN Configuration page without making changes.

The modified VLAN configuration is displayed in the VLAN Table ([Figure 52 on page 126](#)).

Selecting a management VLAN

You can select any VLAN to perform 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.

To select a VLAN as the management VLAN:

- 1** From the main menu, choose Application > VLAN > VLAN Configuration.
The VLAN Configuration page opens ([Figure 52 on page 126](#)).
- 2** In the VLAN Setting section, choose the VLAN to assign as your management VLAN.
- 3** Click Submit.

Deleting a VLAN configuration

To delete a VLAN configuration:

- 1 From the main menu, choose Application > VLAN > VLAN Configuration.
The VLAN Configuration page opens ([Figure 52 on page 126](#)).
- 2 In the VLAN Table, click the Delete icon for the entry you want to delete.
A message opens prompting you to confirm your request.
- 3 Do one of the following:
 - Click Yes to delete the VLAN configuration.
 - Click Cancel to return to the VLAN Configuration page without making changes.

Configuring broadcast domains

You can configure specified VLAN switch ports with the appropriate PVID/VLAN association that enables the creation of broadcast domains. You can configure specified switch ports to filter (discard) all received tagged frames, untagged frames, or unregistered frames. You can also prioritize the order in which the switch forwards untagged packets, on a per-port basis.

To configure broadcast domains:

- 1 From the main menu, choose Application > VLAN > Port Configuration.
The Port Configuration page opens ([Figure 55](#)).

Figure 55 Port Configuration page

Application > VLAN > Port Configuration

VLAN Port Setting

Port	Port Name	Filter Untagged Frames	PVID	Link Type
1	Port 1	No	1	Untagged Access
2	Port 2	No	1	Untagged Access
3	Port 3	No	1	Untagged Access
4	Port 4	No	1	Untagged Access
5	Port 5	No	1	Untagged Access
6	Port 6	No	1	Untagged Access
7	Port 7	No	1	Untagged Access
8	Port 8	No	1	Untagged Access
9	Port 9	No	1	Untagged Access
10	Port 10	No	1	Untagged Access
11	Port 11	No	1	Untagged Access
12	Port 12	No	1	Untagged Access

Submit

Ports 13 - 24 Ports 25 - 36 Ports 37 - 48 Ports 49 - 50

- 2 In the upper-left hand corner, click on the unit number of the switch to monitor.
- 3 Type information in the text boxes, or select from a list.
- 4 Click Submit.

Viewing VLAN port information

You can view VLAN information about a selected switch port.

To view VLAN port information:

- 1 From the main menu, choose Application > VLAN > Port Information.

The Port Information page opens (Figure 56).

Figure 56 Port Information page

Table 52 describes the items on the Port Information page.

Table 52 Port Information page items

Section	Item	Range	Description
VLAN Port Information (View By)	Unit	1..8	Choose the number of the switch to view.
	Port	1..25	Choose the number of the switch's port to view.
VLAN Port Information Table	PVID		The PVID assigned when the VLAN port was created.
	Port Name		The port name assigned when the VLAN port was created.
VLAN Port Information Table	VLAN		The number assigned to the VLAN when it was created.
	VLAN Name		The name assigned to the VLAN when it was created.

- 2 In the VLAN Port Information (View By) section, enter the unit and port number of the VLAN you want to view.
- 3 Click Submit.

The results of your request are displayed in the VLAN Port Information Table ([Figure 56 on page 133](#)).

Managing Spanning Tree Protocol

You can configure system parameters for Spanning Tree Protocol (STP), the industry standard for avoiding loops in switched networks. You can configure individual switch ports or all switch ports for participation in the Spanning Tree Algorithm (STA).



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

To configure switch ports for Spanning Tree participation:

- 1 From the main menu, choose Application > Spanning Tree > Port Configuration.

The Port Configuration page opens ([Figure 57](#)).

Figure 57 Port Configuration page

Application > Spanning Tree > Port Configuration

Spanning Tree - Port Setting					
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
Switch		Normal Learning ▾	<input type="checkbox"/>		

Ports 13 - 24 Ports 25 - 36 Ports 37 - 48 Ports 49 - 50

Table 53 describes the items on the Port Configuration page.

Table 53 Port Configuration page items

Item	Description/Command
Port	The port number of the currently displayed unit.
Trunk	The trunk that corresponds to the switch ports specified as MLT members. For more information on MLT, see "Type information in the text boxes, or select from a list." on page 142.

Table 53 Port Configuration page items

Item	Description/Command
Participation	<p>Choose any (or all) of the switch ports for Spanning Tree participation. Your options are:</p> <p>(1) Normal Learning (2) Fast Learning (3) Disabled</p> <p>Note: When an individual port is a trunk member, changing this setting for one of the trunk members changes the setting for all members of that trunk. Consider the effect changing this value has in your network topology before making changes.</p> <p>The default settings is Normal Learning.</p>
Priority	The 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).
Path Cost	The bridge spanning tree parameter that determines the lowest path cost to the root.
State	<p>The current state of the port as defined by application of the Spanning Tree Protocol. This state controls what action a port takes on reception of a frame.</p> <p>Note: If the bridge has detected a port that is malfunctioning, it will place that port into the broken (6) state. For ports which are disabled, this object will have a value of disabled (1).</p>

- 2 In the port row(s) of your choice, choose to enable STP (normal learning or fast learning) or disable STP.
- 3 Click Submit.

The results of your request are displayed in the Spanning Tree Port configuration page ([Figure 57 on page 135](#)).

Changing Spanning Tree bridge switch settings

You can view and configure existing Spanning Tree switch settings.

To configure Spanning Tree switch settings:

- 1 From the main menu, choose Application > Spanning Tree > Bridge Information.

The Bridge Information page opens ([Figure 58](#)).

Figure 58 Bridge Information page

Application > Spanning Tree > Bridge Information

Spanning Tree - Bridge Information	
Bridge Priority	<input type="text" value="0x8000"/> (0 - 0xFFFF)
Designated Root	7f-f1-00-e0-7b-cc-7e-81
Root Port	Port 1
Root Path Cost	30
Hello Time	2 seconds
Maximum Age Time	20 seconds
Forward Delay	15 seconds
Bridge Hello Time	<input type="text" value="2"/> seconds (1 .. 10)
Bridge Maximum Age Time	<input type="text" value="20"/> seconds (6 .. 40)
Bridge Forward Delay	<input type="text" value="15"/> seconds (4 .. 30)

Table 54 describes the items on the Bridge Information page.

Table 54 Bridge Information page items

Item	Range	Description
Bridge Priority	0..65535	<p>Type the 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>The default setting is 8000.</p>
Designated Root	XXXXXXXXXXXXX X	The bridge ID of the root bridge, as determined by the STA.
Root Port	1..25	The port number of the port which offers the lowest cost past from this bridge to the root bridge.
Root Path Cost	Integer	The cost of the path to the root as seen from this bridge.
Hello Time	1..10 seconds	<p>The actual Hello Interval, the amount of time between transmissions of configuration Bridge Protocol Data Units (BPDUs) that the root bridge is currently using.</p> <p>Note: Bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. See also Bridge Hello Time.</p>
Maximum Age Time	6..40 seconds	<p>The Maximum Age Time parameter value that the root bridge is currently using. This value specifies the maximum age that a Hello message can attain before it is discarded.</p> <p>Note: 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>
Forward Delay	4..30 seconds	<p>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: 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>

Table 54 Bridge Information page items (continued)

Item	Range	Description
Bridge Hello Time	1..10 seconds	<p>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: 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>The default setting is 2 seconds.</p>
Bridge Maximum Age Time	6..40 seconds	<p>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: 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>The default setting is 20 seconds.</p>
Bridge Forward Delay	4..30 seconds	<p>The amount of time that the bridge ports remains in the Listening and Learning states before entering the Forwarding state.</p> <p>Note: All bridges participating in the spanning tree network use the root bridge's Forward Delay parameter value. See also Forward Delay.</p> <p>The default setting is 15 seconds.</p>

- 2** Type information in the text boxes, or select from a list.
- 3** Click Submit.

The bridge information is displayed in the Spanning Tree Bridge Information page ([Figure 58 on page 137](#)).

Configuring MultiLink Trunk members

You can configure groups of links between the [Product Name (short)] and another switch or a server to provide higher bandwidth with active redundant links. Trunked ports can span multiple units of the stack for fail-safe connectivity to mission-critical servers and the network center.

You can configure two to four switch ports together as members of a trunk to a maximum of six trunks.

To configure MultiLink Trunk (MLT) members:

- 1 From the main menu, choose Application > MultiLink Trunk > Group.

The Group page opens (Figure 59).

Figure 59 Group page

Application > MultiLink Trunk > Group

MultiLink Trunk Group Setting							
Trunk	Trunk Members				STP Learning	Trunk Mode	Trunk Name
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Normal ▾	Basic	Trunk #1
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Normal ▾	Basic	Trunk #2
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Normal ▾	Basic	Trunk #3
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Normal ▾	Basic	Trunk #4
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Normal ▾	Basic	Trunk #5
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Normal ▾	Basic	Trunk #6

MultiLink Trunk Group Setting	
Trunk	Trunk Status
1	Disabled ▾
2	Disabled ▾
3	Disabled ▾
4	Disabled ▾
5	Disabled ▾
6	Disabled ▾

Table 55 describes the items on the Group page.

Table 55 Group page items

Section	Item	Range	Description
MultiLink Trunk Group Setting	Trunk	1..6	This 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 on the following management pages: Port Configuration and Spanning Tree Configuration. There are no default settings.
	Trunk Port Members	Unit: 1..8 Port: 1..25	Type the switch and port numbers to associate with the corresponding trunk. Note: You can configure two to four switch ports together as members of a trunk to a maximum of six trunks. Switch ports can only be assigned a member of a single trunk. There are no default settings.
	STP Learning	(1) Normal (2) Fast (3) Disabled	Choose the parameter that allows the specified trunk to participate in the spanning tree. This setting overrides those of the individual trunk members. Selecting Fast shortens the state transition timer by two seconds. The default setting is Normal.
	Trunk Mode	Basic	The default operating mode of the switch. When in Basic mode, source MAC addresses are dynamically assigned to specific trunk members for flooding and forwarding. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.
	Trunk Name	1..16	Type a character string to create a unique name to identify the trunk, for example, Trunk1. The name, if chosen carefully, can provide meaningful information to you. For example, S1:T1 to FS2 indicates that Trunk1, in Switch1 connects to File Server 2.
	MultiLink Trunk Group Setting	Trunk Status	(1) Enabled (2) Disabled

- 2 Type information in the text boxes, or select from a list.
- 3 Click Submit in any section to save your changes.

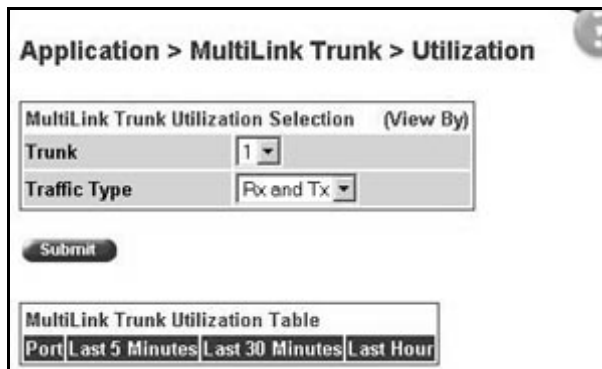
Monitoring MLT traffic

You can monitor the bandwidth usage for the MultiLink Trunk member ports within each trunk in your configuration by selecting the traffic type to monitor.

To monitor MultiLink Trunk traffic:

- 1 From the main menu, choose Application > MultiLink Trunk > Utilization.
The Utilization page opens ([Figure 60](#)).

Figure 60 Utilization page



Application > MultiLink Trunk > Utilization

MultiLink Trunk Utilization Selection (View By)

Trunk 1

Traffic Type Rx and Tx

Submit

MultiLink Trunk Utilization Table

Port Last 5 Minutes Last 30 Minutes Last Hour

[Table 56](#) describes the items on the Utilization page.

Table 56 Utilization page items

Section	Item	Range	Description
MultiLink Trunk Utilization Selection (View By)	Trunk	1..6	Choose the trunk to be monitored.
	Traffic Type	(1) RX and TX (2) RX (3) TX	Choose the traffic type to be monitored for percentage of bandwidth utilization.
MultiLink Trunk Utilization Table	Unit/Port		A list of the trunk member switch ports that correspond to the trunk specified in the Trunk column.
	Last 5 Minutes%		The percentage of packets (of the type specified in the Traffic Type field) used by the port in the last five minutes. This field provides a running average of network activity, and is updated every 15 seconds.
	Last 30 Minutes%		The percentage of packets (of the type specified in the Traffic Type field) used by the port in the last 30 minutes. This field provides a running average of network activity, and is updated every 15 seconds.
	Last Hour%		The percentage of packets (of the type specified in the Traffic Type field) used by the port in the last 60 minutes. This field provides a running average of network activity, and is updated every 15 seconds.

- 2 In the MultiLink Trunk Utilization Selection section, type the Trunk number and traffic type to be monitored.
- 3 Click Submit.

The results of your request are displayed in the MultiLink Trunk Utilization Table ([Figure 60 on page 142](#)).

Chapter 8

Support menu

The customer support options available to you are:

- [“Using the online Help option,”](#) next
- [“Downloading technical publications”](#) on page 147
- [“Upgrade option”](#) on page 148

Using the online Help option

You can read information about Web-based management user interface functions in the online Help menu embedded in the Web-based management interface.

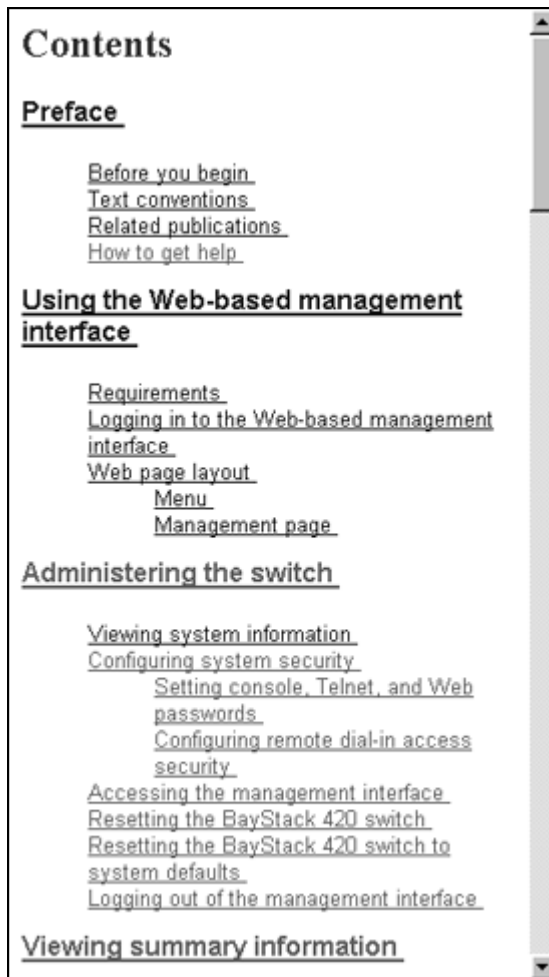
To open online Help:

- 1 From the main menu, choose Support > Help or click the Help icon located in the upper right corner of any management page.



The Online Help menu opens in a separate Web browser ([Figure 61](#)).

Figure 61 Online help menu



- 2** Click on any content item to read information about the topic. If you clicked the Help icon on a management page, information about that page is immediately displayed.
- 3** Click Return to Top to return to the Content index.
- 4** Close the Web browser.

Downloading technical publications

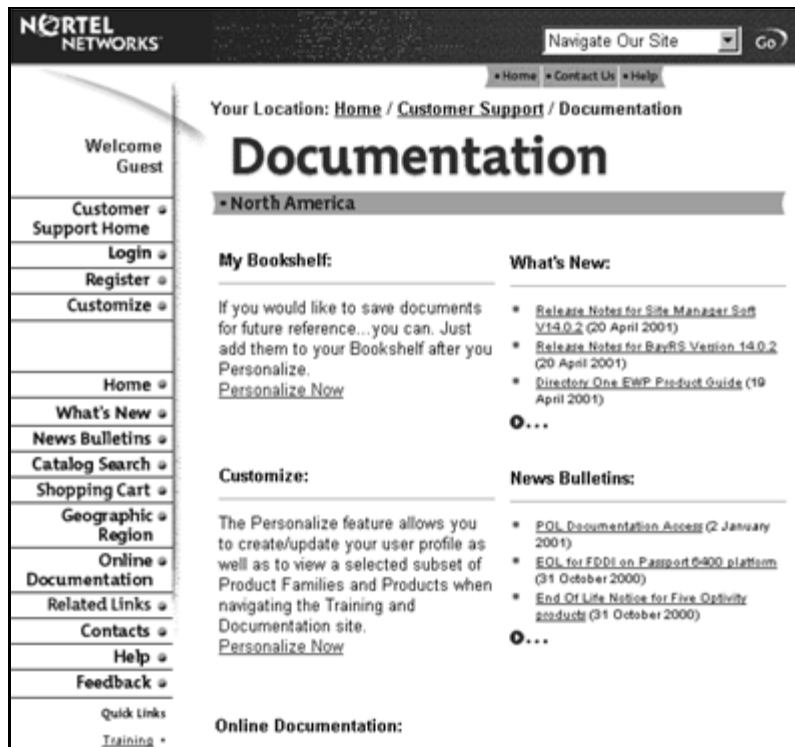
You can download current documentation about the Web-based management user interface from Nortel Networks Technical Documentation Web site.

To download current documentation:

- 1 From the main menu, choose Support > Release Notes.

Nortel Networks Technical Documentation Web site opens in a separate Web browser (Figure 62).

Figure 62 Nortel Networks Technical Documentation Web site



- 2 Locate your product, and click the document you want to download.
- 3 Click on the PDF icon to start the download process. You need Adobe Acrobat 3.0 or later to view or print documents from this site.
- 4 Follow the prompts to download the documentation.

- 5 Close the Web browser.

Upgrade option

You can upgrade your Web-based management user interface to the most recent software release.

To upgrade to the most recent software release:

- 1 From the main menu, choose Support > Upgrade.
Nortel Networks Technical Documentation Web site opens in a separate Web browser ([Figure 62](#)).
- 2 Follow the prompts to download the software release.
- 3 Close the Web browser.

Index

A

access

SNMP 114

administrative options

logging on 33

logging out 38

resetting the switch/stack 36

resetting to system defaults 37

security, configuring

passwords 30

remote dial-in access 32

alarms, configuring 93

Allowed Source field 119

application setting options

broadcast domains 131

MultiLink Trunking (MLT) 140

port mirroring 111

Spanning Tree Protocol 134

VLANs 125

authentication traps, enabling 50

autotopology, enabling 50

B

bootP

configuring 46

request modes 47

Bridge Information page 136

broadcast domains, configuring 131

C

check boxes, about 26

Clear by Ports page 121

community strings, configuring 50

Configuration File Download/Upload page 84

Console Password Setting page 31

Console/Communication Port page 86

conventions, text 18

Current Learning Mode field 115

customer support 19

D

DA Filtering on Intrusion Detected field 115

DA MAC Address field 124

DA MAC Filtering page 123

E

Entry field 117, 120

Ethernet error statistics

viewing 106

Ethernet Errors page 107

F

fault threshold parameters, configuring 89

Find MAC Address page 76

G

gateway addresses, configuring 46

Generate SNMP Trap on Intrusion field 115

Group Access Rights page 60

Group Membership page 58

Group page 140

H

High Speed Flow Control page 80

high speed flow control, configuring 80

I

icons, about 26

Identify Unit Numbers page 44

Interface page 105

interface statistics
viewing 105, 106

IP addresses, configuring 46

IP page 46

L

Learn by Ports page 117

logging on 33

logging out 38

M

MAC Address field 120, 124

MAC address security 114

allowed source 118

clearing 121

deleting ports 123

learn by ports 117

learning 115

MAC DA 113, 123

ports 121

security list 116

security table 118

MAC Address Security field 115

MAC Address Security SNMP-Locked field 115

MAC Address Table page 75

MAC addresses

locating a specific address 76

viewing learned addresses 75

MAC DA filtering 123

main menu

headings and options 24

icons 25, 27

Management Information View page 63

Microsoft Internet Explorer, software version
requirements 21

monitoring modes

port-based 113

MultiLink Trunking (MLT)

about 140

configuring 140

monitoring traffic 142

N

Netscape Navigator, software version
requirements 21

network administrator

contact information 48, 49

network security, protecting system integrity 22

Notification page 66

O

online help, accessing 145

P

Partition Port on Intrusion Detected field 115

Partition Time field 115

passwords, setting

console 31

remote dial-in access 32

Telnet 31

Web 31

port autonegotiation speed, configuring 77

port communication speed, configuring 86

Port Configuration page 121

Port Configuration page (STP) 134

Port Configuration page (VLAN) 131
Port Information page 132
Port List field 115, 117
Port List page 117
Port Lists page 116
Port Management page 78
port mirroring
 configuring 111
Port Mirroring page 111
Port page 101
port statistics
 viewing 101, 102
 zeroing ports 104
product support 19
publications
 hard copy 18
 related 18

R

Radius page 32
release notes, obtaining 23
remote dial-in access, configuring 32
Reset page 36
Reset to Defaults page 37
resetting the switch/stack 36
resetting the switch/stack, to system defaults 37
RMON
 Ethernet statistics
 viewing 97
 history statistics
 viewing 99
RMON Ethernet page 97
RMON Event Log page 93
RMON History page 99
RMON options
 fault event log, viewing 93
 fault threshold parameters
 configuring 89

 deleting 92
 history statistics
 viewing 99
RMON Threshold page 90
RMON, about 89

S

security
 MAC address-based 114
Security Configuration page 114
Security field 122
Security page 114
Security Table page 118
security, configuring
 passwords 30
 remote dial-in access 32
SNMP
 about 50
 MAC address security 115
 trap receivers
 configuring 73
 deleting 74
SNMP Trap Receiver page 73
SNMPv1
 about 50
 configuring 50
SNMPv1 page 50
SNMPv3
 about 50
 configuring 52
 group access rights
 configuring 60
 deleting 62
 group membership
 configuring 57
 deleting 59
 management information views
 configuring 63
 deleting 65
 system information, viewing 52

- system notification entries
 - configuring 66
 - deleting 67
- target addresses
 - configuring 68
 - deleting 70
- target parameters
 - configuring 70
 - deleting 72
- user access
 - configuring 55
 - deleting 57
- software download
 - LED indication descriptions 83
 - process 81, 82
- Software Download page 81
- software version requirements
 - Microsoft Internet Explorer 21
 - Netscape Navigator 21
- Spanning Tree Protocol
 - about 134
 - bridge switch settings, configuring 136
 - managing 134
- Stack Information page 39
- stack information, viewing 39
- Stack Numbering page 42
- stack numbering, configuring 42
- summary options
 - changing stack numbering 42
 - identifying unit numbers 44
 - viewing
 - stack information 39
 - switch information 41
- Support heading 23
- Support menu
 - online help 145
 - technical publications, downloading 147
 - user interface, upgrading 148
- support, Nortel Networks 19
- switch configuration files
 - not-saved parameters 86
 - retrieving from a TFTP server 84
 - storing on a TFTP server 84
- switch configuration options
 - autotopology feature 50
 - bootP settings 46
 - community string settings 50
 - gateway settings 46
 - high speed flow control 80
 - IP settings 46
 - MAC addresses, finding 76
 - MAC addresses, viewing 75
 - network manager contact 48
 - port autonegotiation speed 77
 - port communication speed 86
 - retrieving from a TFTP server 84
 - SNMP trap receivers 73
 - SNMPv3
 - group access rights 60
 - management information views 63
 - management target addresses 68
 - management target parameters 70
 - system information, viewing 52
 - system notification entries 66
 - user access 55
 - user group membership 57
 - storing on a TFTP server 84
 - switch images, downloading 81
 - system location 48
 - system name 48
 - trap mode settings 50
- switch images, downloading 81
- switch information
 - viewing 41
- Switch Information page 41
- switch port autonegotiation speed, configuring 77
- system default settings, resetting to 37
- System Information page 34, 52
- system location, naming 48
- system log, viewing 94
- system name, configuring 48
- System page 48

- system settings
 - modifying 48
 - system contact 49
 - system location 49
 - system name 49
- system statistics options, viewing
 - Ethernet error statistics 106
 - interface statistics 105
 - port statistics 101
 - transparent bridging statistics 109

T

- tables and input forms, about 26
- Target Address page 68
- Target Parameter page 70
- technical publications 18
- technical publications, downloading 147
- technical support 19
- Telnet Password Setting page 31
- text conventions 18
- Transparent Bridging page 109
- transparent bridging statistics
 - viewing 109, 110

U

- unit numbers, identifying 44
- user interface, upgrading 148
- Utilization page 142

V

- VLAN Configuration
 - Port Based modification page 128
 - Port Based Setting page 127
- VLAN Configuration page 125
- VLANs
 - about 125
 - broadcast domains, configuring 131
 - configuring 125

- deleting 131
- MAC SA-based
 - configuring 130
- port information
 - viewing 132
- port-based
 - about 125
 - configuring 127
- selecting a management VLAN 130

W

- Web browser, requirements 21
- Web Help file, accessing 23
- Web Password Setting page 31
- Web-based management interface
 - home page, graphic 22
 - logging in 22
 - main menu, icons 25, 27
 - management page 25
 - navigating the menu 23
 - requirements to use 21