

Part No. 215662-C
July 2004

4655 Great America Parkway
Santa Clara, CA 95054

Reference for the BayStack 420/425 Switch Management Software, 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 | 23 |
| Before you begin | 23 |
| Text conventions | 23 |
| Related publications | 24 |
| How to get help | 25 |
| Chapter 1 | |
| Device Manager basics | 27 |
| Starting Device Manager | 27 |
| Setting the Device Manager properties | 28 |
| Opening a device | 31 |
| Device Manager window | 33 |
| Menu bar | 34 |
| Toolbar | 35 |
| Device view | 35 |
| Selecting objects | 36 |
| Selecting a single object | 36 |
| Selecting multiple objects | 37 |
| LEDs and ports | 39 |
| Shortcut menus | 40 |
| Status bar | 41 |
| Using the buttons in Device Manager dialog boxes | 41 |
| Editing objects | 43 |
| Working with statistics and graphs | 43 |
| Types of statistics | 44 |
| Types of graphs | 44 |
| Statistics for single and multiple objects | 47 |
| Viewing statistics as graphs | 48 |

| | |
|--|-----------|
| Telneting to a switch | 50 |
| Opening the Web-based management home page | 51 |
| Trap log | 52 |
| Online Help | 53 |
| Chapter 2 | |
| Configuring and graphing the switch | 55 |
| Viewing switch IP information | 55 |
| Globals tab | 55 |
| Addresses tab | 56 |
| ARP tab | 57 |
| Editing the chassis configuration | 59 |
| System tab | 59 |
| Base Unit Info tab | 62 |
| Stack Info tab | 64 |
| Agent tab | 66 |
| SNMP tab | 68 |
| Trap Receivers tab | 69 |
| Adding a Trap Receiver | 70 |
| Power Supply tab | 71 |
| Fan tab | 73 |
| Banner tab | 74 |
| Custom banner tab | 76 |
| Working with configuration files | 77 |
| ASCII config file | 79 |
| Graphing chassis statistics | 81 |
| SNMP tab | 81 |
| IP tab | 84 |
| ICMP In tab | 87 |
| ICMP Out tab | 89 |
| Switch Management | 90 |
| Ease of use and configuration | 90 |
| Momentary switch operation | 91 |

| | |
|--|------------|
| Chapter 3 | |
| Configuring and graphing ports | 93 |
| Viewing and editing a single port configuration | 93 |
| Interface tab for a single port | 94 |
| VLAN tab for a single port | 97 |
| STG tab for a single port | 99 |
| EAPOL tab for a single port | 101 |
| Viewing and editing multiple port configurations | 103 |
| Graphing multiple ports | 104 |
| Interface tab for multiple ports | 105 |
| VLAN tab for multiple ports | 108 |
| EAPOL tab for multiple ports | 109 |
| Graphing port statistics | 111 |
| Interface tab for graphing ports | 112 |
| Ethernet Errors tab for graphing ports | 114 |
| Bridge tab for graphing ports | 118 |
| RMON tab | 119 |
| EAPOL Stats tab for graphing ports | 122 |
| EAPOL Diag tab for graphing ports | 124 |
| | |
| Chapter 4 | |
| Setting up MultiLink Trunk ports | 127 |
| MultiLink Trunk (MLT) features | 127 |
| Setting up MLTs | 128 |
| Adding ports to a MultiLink Trunk | 129 |
| MultiLink Trunk statistics | 129 |
| MultiLink Trunk Ethernet error statistics | 131 |
| | |
| Chapter 5 | |
| Creating and managing VLANs | 135 |
| VLANs | 135 |
| VLAN Information | 135 |
| Creating VLANs | 137 |
| Creating a port-based VLAN | 138 |
| Accepting untagged frames | 139 |

Modifying and managing existing VLANs 140

Chapter 6

Setting up bridging 143

Base tab 143

Spanning Tree tab 144

Transparent tab 147

Forwarding tab 148

Spanning tree group (STG) 150

Configuration tab 151

Status tab 152

Ports tab 154

Chapter 7

Troubleshooting Device Manager 157

Topology tab 157

Topology Table tab 158

Chapter 8

RMON 161

Working with RMON information 161

Viewing statistics 161

Viewing history 165

Creating a history 166

Disabling history 171

Enabling Ethernet statistics gathering 172

Disabling Ethernet statistics gathering 174

Alarms 176

How RMON alarms work 176

Creating alarms 178

Alarm Manager example 179

Events 184

How events work 184

Viewing an event 184

Creating an event 186

| | |
|---|------------|
| Deleting an event | 187 |
| Log information | 187 |
| Chapter 9 | |
| Security parameters..... | 189 |
| General tab | 189 |
| SecurityList tab | 192 |
| Security, Insert SecurityList dialog box | 193 |
| AuthConfig tab | 194 |
| Security, Insert AuthConfig dialog box | 195 |
| AuthStatus tab | 197 |
| AuthViolation tab | 199 |
| SSH tab | 201 |
| SSH Sessions tab | 202 |
| Chapter 10 | |
| Working with SNMPv3..... | 205 |
| SNMPv3 Overview | 205 |
| Initial Login with an SNMPv3 User | 206 |
| User-based Security Model | 206 |
| Configuring the User-based Security Model | 207 |
| View-based Access Control Model | 211 |
| Defining Group Membership with VACM | 211 |
| Assigning Group Access Rights with VACM | 213 |
| Defining a MIB view | 215 |
| Creating a community | 217 |
| Management Targets | 219 |
| Creating a Management Target Address | 220 |
| Creating Target Parameters | 222 |
| The Notify Table | 224 |
| Index | 227 |

Figures

| | | |
|-----------|--|----|
| Figure 1 | Device Manager window | 28 |
| Figure 2 | Properties dialog box | 29 |
| Figure 3 | Open Device dialog box | 32 |
| Figure 4 | Device view | 33 |
| Figure 5 | Parts of the Device Manager window | 34 |
| Figure 6 | Objects in the device view | 36 |
| Figure 7 | Interface tab | 38 |
| Figure 8 | Color port legend | 39 |
| Figure 9 | Switch unit shortcut menu | 40 |
| Figure 10 | Port shortcut menu | 40 |
| Figure 11 | Line graph | 45 |
| Figure 12 | Area graph | 45 |
| Figure 13 | Bar graph | 46 |
| Figure 14 | Pie graph | 46 |
| Figure 15 | Interface statistics for a single port | 47 |
| Figure 16 | Interface statistics for multiple ports | 48 |
| Figure 17 | Statistics dialog box for a port | 49 |
| Figure 18 | Open home page icon | 51 |
| Figure 19 | Web-based management home page | 52 |
| Figure 20 | Globals tab | 56 |
| Figure 21 | Edit IP dialog box — IP Address tab | 57 |
| Figure 22 | Edit IP dialog box — ARP tab | 58 |
| Figure 23 | Edit Chassis dialog box — System tab | 60 |
| Figure 24 | Edit Chassis dialog box — Base Unit Info tab | 63 |
| Figure 25 | Edit Chassis dialog box — Stack Info tab | 64 |
| Figure 26 | Edit Chassis dialog box — Agent tab | 67 |
| Figure 27 | Edit Chassis dialog box — SNMP tab | 68 |
| Figure 28 | Trap Receivers tab | 69 |
| Figure 29 | Chassis, Insert Trap Receive dialog box | 70 |

| | | |
|-----------|--|-----|
| Figure 30 | Edit Chassis dialog box — Power Supply tab | 72 |
| Figure 31 | Edit Chassis dialog box — Fan tab | 73 |
| Figure 32 | Edit Chassis dialog box — banner tab | 75 |
| Figure 33 | Telnet window with default banner | 75 |
| Figure 34 | Edit Chassis dialog box — custom banner tab | 76 |
| Figure 35 | Telnet window with custom banner | 77 |
| Figure 36 | FileSystem - Config/Image/Diag File tab dialog box | 78 |
| Figure 37 | File system - ASCII Config File dialog box | 80 |
| Figure 38 | Graph Chassis dialog box — Chassis SNMP tab | 82 |
| Figure 39 | Graph Chassis dialog box — IP tab | 85 |
| Figure 40 | Graph Chassis dialog box — ICMP In tab | 88 |
| Figure 41 | Graph Chassis dialog box — ICMP Out tab | 89 |
| Figure 42 | Port dialog box — Interface tab | 95 |
| Figure 43 | Edit Port dialog box — VLAN tab | 98 |
| Figure 44 | Edit Port dialog box — STG tab | 99 |
| Figure 45 | Edit Port dialog box — EAPOL tab | 102 |
| Figure 46 | Port dialog box — Interface tab | 106 |
| Figure 47 | VLAN tab for multiple ports | 108 |
| Figure 48 | EAPOL tab for multiple ports | 110 |
| Figure 49 | Interface tab for graphing ports | 112 |
| Figure 50 | Graph Port dialog box — Ethernet Errors tab | 115 |
| Figure 51 | Graph Port dialog box — Bridge tab | 118 |
| Figure 52 | Graph Port dialog box — RMON tab | 120 |
| Figure 53 | Graph Port dialog box — EAPOL Stats tab | 123 |
| Figure 54 | Graph Port dialog box — EAPOL Diag tab | 125 |
| Figure 55 | MLT dialog box | 128 |
| Figure 56 | PortMembers dialog box | 129 |
| Figure 57 | MLT Statistics — Interface tab | 130 |
| Figure 58 | MLT Statics dialog box — Ethernet Errors tab | 132 |
| Figure 59 | VLAN - dialog box with the Basic tab displayed | 136 |
| Figure 60 | VLAN dialog box- Snoop tab | 137 |
| Figure 61 | VLAN, Insert Basic dialog box for a port-based VLANs | 138 |
| Figure 62 | VLAN tab | 139 |
| Figure 63 | VLAN dialog box | 140 |
| Figure 64 | Base tab | 144 |

| | | |
|-----------|--|-----|
| Figure 65 | Spanning Tree tab | 145 |
| Figure 66 | Transparent tab | 147 |
| Figure 67 | Forwarding tab | 149 |
| Figure 68 | Configuration tab | 151 |
| Figure 69 | Status tab | 153 |
| Figure 70 | Ports tab | 155 |
| Figure 71 | Diagnostics dialog box — Topology tab | 157 |
| Figure 72 | Diagnostics dialog box — Topology Table tab | 158 |
| Figure 73 | Port dialog box — RMON tab | 163 |
| Figure 74 | Port dialog box — RMON tab | 166 |
| Figure 75 | History tab | 167 |
| Figure 76 | RMONControl, Insert History dialog box | 169 |
| Figure 77 | RMONControl dialog box — Ether Stats tab | 172 |
| Figure 78 | RMONControl, Insert Ether Stats dialog box | 174 |
| Figure 79 | RMONControl, Insert Ether Stats dialog box port list | 174 |
| Figure 80 | How alarms fire | 177 |
| Figure 81 | Alarm example — threshold less than 260 | 178 |
| Figure 82 | Alarm Manager dialog box | 179 |
| Figure 83 | Alarm variable list | 180 |
| Figure 84 | RMONAlarms dialog box — Alarms tab | 182 |
| Figure 85 | RMONAlarms dialog box — Events tab | 185 |
| Figure 86 | Insert Events dialog box | 186 |
| Figure 87 | New event in the Events tab | 186 |
| Figure 88 | Log tab | 187 |
| Figure 89 | General tab | 190 |
| Figure 90 | SecurityList tab | 192 |
| Figure 91 | Security, Insert SecurityList dialog box | 193 |
| Figure 92 | AuthConfig tab | 194 |
| Figure 93 | Security, Insert AuthConfig dialog box | 196 |
| Figure 94 | AuthStatus tab | 198 |
| Figure 95 | AuthViolation tab | 200 |
| Figure 96 | SSH tab | 201 |
| Figure 97 | SSH Sessions tab | 203 |
| Figure 98 | USM dialog box | 208 |
| Figure 99 | USM, Insert USM Table dialog box | 209 |

| | | |
|------------|--|-----|
| Figure 100 | VACM dialog, Group Membership tab | 212 |
| Figure 101 | VACM, Insert Group Membership dialog box | 213 |
| Figure 102 | Group Access Right tab | 214 |
| Figure 103 | VACM, Insert Group Access Right dialog box | 215 |
| Figure 104 | MIB View tab | 216 |
| Figure 105 | VACM, Insert MIB View dialog box | 217 |
| Figure 106 | Community Table dialog box | 218 |
| Figure 107 | Community Table, Insert Community Table dialog box | 218 |
| Figure 108 | Target Table dialog box, Target Address Table tab. | 220 |
| Figure 109 | Target Table, Insert Target Address Table dialog box | 221 |
| Figure 110 | Target Params Table tab | 222 |
| Figure 111 | Target Table, Insert Target Params Table dialog box | 223 |
| Figure 112 | NotifyTable dialog box | 224 |
| Figure 113 | Notify Table, Insert Notify Table dialog box | 225 |

Tables

| | | |
|----------|--|----|
| Table 1 | Properties dialog box items | 30 |
| Table 2 | SNMP community string default values | 31 |
| Table 3 | Open Device dialog box fields | 32 |
| Table 4 | Menu bar commands | 34 |
| Table 5 | Toolbar buttons | 35 |
| Table 6 | Port color codes | 39 |
| Table 7 | Switch unit shortcut menu command | 40 |
| Table 8 | Port shortcut menu commands | 41 |
| Table 9 | Device Manager buttons | 41 |
| Table 10 | Types of statistics | 44 |
| Table 11 | Graph dialog box buttons | 50 |
| Table 12 | Help file locations | 53 |
| Table 13 | Globals tab items | 56 |
| Table 14 | IP Addresses tab items | 57 |
| Table 15 | ARP tab items | 58 |
| Table 16 | System tab items | 61 |
| Table 17 | Base Unit Info tab items | 63 |
| Table 18 | Stack Info tab fields | 65 |
| Table 19 | Agent tab fields | 67 |
| Table 20 | SNMP tab fields | 69 |
| Table 21 | Edit Chassis dialog box — Trap Receivers tab items | 70 |
| Table 22 | Power Supply tab fields | 72 |
| Table 23 | Fan tab fields | 74 |
| Table 24 | FileSystem Config/Image/Diag file dialog box items | 78 |
| Table 25 | FileSystem - ASCII Config File dialog box items | 80 |
| Table 26 | SNMP tab fields | 82 |
| Table 27 | Chassis IP tab fields | 85 |
| Table 28 | ICMP In tab fields | 88 |
| Table 29 | ICMP Out tab fields | 90 |

| | | |
|----------|--|-----|
| Table 30 | Interface tab items for a single port | 96 |
| Table 31 | VLAN tab items for a single port | 98 |
| Table 32 | STG tab items for a single port | 100 |
| Table 33 | EAPOL tab items for a single port | 102 |
| Table 34 | Interface tab fields for multiple ports | 106 |
| Table 35 | VLAN tab fields for multiple ports | 109 |
| Table 36 | EAPOL tab fields for multiple ports | 110 |
| Table 37 | Port Interface tab fields for multiple ports | 113 |
| Table 38 | Ethernet Errors tab fields | 116 |
| Table 39 | Bridge tab fields | 119 |
| Table 40 | RMON tab fields | 121 |
| Table 41 | EAPOL tab stats fields | 123 |
| Table 42 | EAPOL Diag tab fields | 125 |
| Table 43 | MLT dialog box fields | 128 |
| Table 44 | Interface tab fields | 130 |
| Table 45 | Ethernet Errors tab fields | 132 |
| Table 46 | VLAN Basic tab fields | 136 |
| Table 47 | VLAN - Snoop tab fields | 137 |
| Table 48 | VLAN dialog box fields | 140 |
| Table 49 | Base tab fields | 144 |
| Table 50 | Spanning Tree tab fields | 145 |
| Table 51 | Transparent tab items | 148 |
| Table 52 | Forwarding tab fields | 150 |
| Table 53 | Configuration tab fields | 151 |
| Table 54 | Status tab fields | 153 |
| Table 55 | Ports tab fields | 155 |
| Table 56 | Topology tab items | 158 |
| Table 57 | Topology Table tab fields | 159 |
| Table 58 | Port dialog box — RMON tab fields | 163 |
| Table 59 | Types of statistics | 165 |
| Table 60 | History tab fields | 169 |
| Table 61 | RMON History items | 170 |
| Table 62 | Ether Stats tab fields | 173 |
| Table 63 | RMON Insert Alarm dialog box fields | 181 |
| Table 64 | Describes the fields on the Alarms tab | 182 |

| | | |
|----------|---|-----|
| Table 65 | Events tab fields | 185 |
| Table 66 | Log tab fields | 188 |
| Table 67 | General tab items | 190 |
| Table 68 | SecurityList tab fields | 192 |
| Table 69 | Security, Insert AuthConfig dialog box fields | 193 |
| Table 70 | AuthConfig tab fields | 194 |
| Table 71 | Security, Insert AuthConfig dialog box fields | 196 |
| Table 72 | AuthStatus tab fields | 198 |
| Table 73 | AuthViolation tab fields | 200 |
| Table 74 | SSH tab fields | 202 |
| Table 75 | SSH Sessions tab fields | 203 |
| Table 76 | SNMPv3 user configuration method | 207 |
| Table 77 | USM dialog box fields | 208 |
| Table 78 | USM, Insert USM Table dialog box fields | 210 |
| Table 79 | View-based access control mapping tables | 211 |
| Table 80 | Group Membership tab fields | 212 |
| Table 81 | VACM dialog box—Group Access Right tab fields | 214 |
| Table 82 | VACM dialog box—MIB View tab fields | 216 |
| Table 83 | Community Table dialog box fields | 218 |
| Table 84 | Managment target tables | 220 |
| Table 85 | Target Address Table fields | 221 |
| Table 86 | Target Params Table dialog box fields | 223 |
| Table 87 | Notify Table dialog box fields | 224 |

Preface

Welcome to the Nortel Networks* Device Manager software, a set of graphical network management applications you can use to configure and manage the Nortel Networks BayStack* 420/425 Switch. This guide provides information about using the features and capabilities of the Java-based Device Manager graphical user interface (GUI) to perform network management operations for the switch.

Before you begin

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

- Basic knowledge of networks and Ethernet* bridging
- Familiarity with networking concepts and terminology
- Basic knowledge of network topologies
- Familiarity with GUIs

Text conventions

This guide uses the following text conventions:

| | |
|--------------------|--|
| <i>italic text</i> | Indicates book titles. |
| separator (>) | Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu. |

Related publications

For more information about using the BayStack 420/425 Switch, refer to the following publications:

- *Installing the BayStack 425 Switch* (part number 215658-B)
Describes how to install the BayStack 420/425 Switch.
- *Getting Started with BayStack 420/425 Switch Management Software, Software Release 3.1* (part number 215663-B)
Describes how to install the Device Manager software management application.
- *Using the BayStack 420/425 Switch, Software Release 3.1* (part number 215661-B)
Describes how to use the BayStack 420/425 Switch for network configuration.
- *Using Web-based Management for the BayStack 425 Switch, Software Version 3.1* (part number 215660-B)
Describes how to use the Web-based management tool to configure switch features.
- *Reference for the BayStack 420/425 Command Line Interface, Software Release 3.1* (part number 215659-B)
Describes how to use Command Line Interface (CLI) commands to configure and manage the BayStack 420/425 Switch.

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

How to get help

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

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

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

Chapter 1

Device Manager basics

This chapter describes basic procedures for using the Device Manager software. The chapter includes the following information:

- Instructions to start Device Manager, set the Device Manager properties, and open a device (next)
- A summary of the Device Manager user interface features and how to use them (starting on [page 33](#))
- Instructions to view statistics and display graphs ([page 43](#))
- Instructions to use Device Manager to Telnet to a switch ([page 50](#))
- Information about the trap log ([page 52](#))
- Information about online Help ([page 53](#))

Starting Device Manager

► Do one of the following, depending upon your operating system environment:

- In a Microsoft* Windows* environment, from the Windows taskbar choose Start > Programs > Nortel Networks Device Manager > DM.
- In a UNIX environment, verify that the Device Manager installation directory is in your search path; then enter:

```
./JDM
```

The initial Device Manager window opens ([Figure 1](#)).



Note: On startup, Device Manager performs a DNS lookup for the machine on which it is running. If the DNS lookup is slow or fails, the initial Device Manager window may take up to 30 seconds to open.

Figure 1 Device Manager window



Setting the Device Manager properties

Device Manager communicates with the BayStack 420/425 Switch using Simple Network Management Protocol (SNMP). The software is shipped with default values set for important communication parameters, such as the polling interval, timeout, and retry count. You can set the parameters before you open a device to manage.

To set the Device Manager properties:

- 1 Choose Device > Properties.

The Properties dialog box opens ([Figure 2](#)).

Figure 2 Properties dialog box

Device Manager 563b07 - Properties

Polling

Status Interval: 20 secs
(If Traps, Status Interval: 60 secs)
Hotswap Detect every: 1 intervals
 Enable

SNMP

Retry Count: 1 1..5
Timeout: 5 3..30 secs
 Trace
 Listen for Traps
Max Traps in Log: 500 1..10000
Trap Port: 162
 Confirm row deletion

Default Read Community: public
Default Write Community: private

Ok Close Help

- 2 Type information and select check boxes.
- 3 Click OK.

[Table 1](#) describes the Properties dialog box items.

Table 1 Properties dialog box items

| Area | Item | Description |
|-------------|-------------------------------|--|
| SR | Status Interval | Interval at which status information is gathered (default is 20 seconds). For a full stack, set this interval to 60 seconds. |
| | (If Traps, Status Interval:) | Interval at which statistics and status information are gathered when traps are enabled. The default is 60. |
| | Hotswap Poll Interval | The interval at which Device Manager polls for module information. The default is 1 interval. |
| | Enable | Enables (true) or disables (false) periodic polling of the device for updated status. If polling is disabled, the chassis status is updated only when you click Refresh on the Chassis tab. |
| VQPS | Retry Count | Number of times Device Manager sends the same polling request if a response is not returned to Device Manager. You may want to set this field to three or four. |
| | Timeout | Length of each retry of each polling waiting period. When you access the device through a slow link, you may want to increase the timeout interval and then change the Retransmission Strategy to superlinear. |
| | Trace | The trace field is used to enable and disable SNMP tracing. When Trace is selected, SNMP protocol data units (PDUs) are displayed in the Device > Log dialog box. |
| | Listen for Traps | When selected (enabled), Device Manager will listen for traps. |
| | Max Traps in Log | The specified number of traps that may exist in the trap log. The default is 500. |
| | Trap Port | Specifies the UDP port that Device Manager will listen to receive SNMP traps. |
| | Confirm row deletion | A dialog box displays when checked, before deleting a row. |
| | Default read community | Specifies the default read community. |
| | Default write community | Specifies the default write community. |

Opening a device

“Opening” a device displays the device view, a picture of the device. To open the device view, you must enter community strings that determine the access level granted to the device.

[Table 2](#) shows the default access community strings for the Device Manager software.

Table 2 SNMP community string default values

| Access level | Description |
|--------------|-------------|
| Read-only | public |
| Read/write | private |

To display the device view:

- 1 Do one of the following:
 - Choose Device > Open.
 - Choose Device > Open Last, and select an IP address from the list.
 - Click the folder icon in the Device Manager window.



- Press [Ctrl] + O.

The Open Device dialog box opens ([Figure 3](#)).

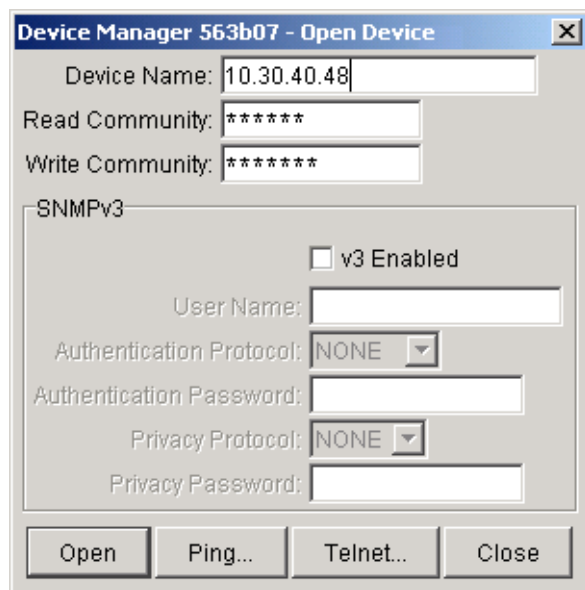
Figure 3 Open Device dialog box

Table 3 describes the Open Device dialog box fields.

Table 3 Open Device dialog box fields

| Field | Description |
|-------------------------|--|
| Device Name | Either an IP address or a DNS name for the device, entered by the user. |
| Read Community | SNMP read community string for the device. Default is <code>public</code> (displayed as <code>*****</code>). The entry is case-sensitive. |
| Write Community | SNMP write community string for the device. Default is <code>private</code> (displayed as <code>*****</code>). The entry is case-sensitive. |
| v3 Enable | When selected (enabled), Open Device dialog box will display SNMPv3 options. |
| User Name | Indicates the name of the user |
| Authentication Protocol | Identifies the authentication protocol used |
| Authentication Password | Specifies the current authentication password |
| Privacy Protocol | Identifies the privacy protocol |
| Privacy Password | Specifies the current privacy password |

- 2 In the Device Name text box, type the DNS name or IP address of the device.
- 3 In the Read Community and Write Community text boxes, type the proper community strings.



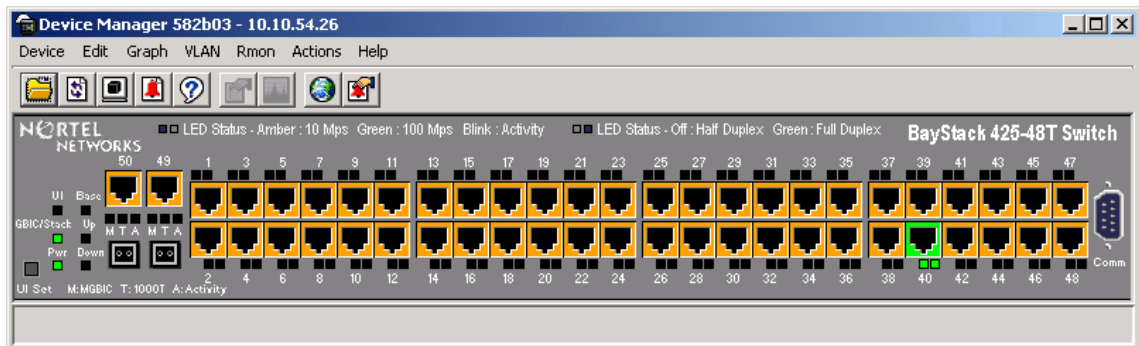
Note: To gain read/write access to a device in Device Manager, you must enter the read/write community string for both the Read Community and Write Community strings.

- 4 Click Open.

Device Manager automatically determines what version of software the selected device is running and displays the appropriate Device Manager dialog boxes.

The Device Manager window opens, showing a picture of the device (Figure 4) that represents the physical features of the device.

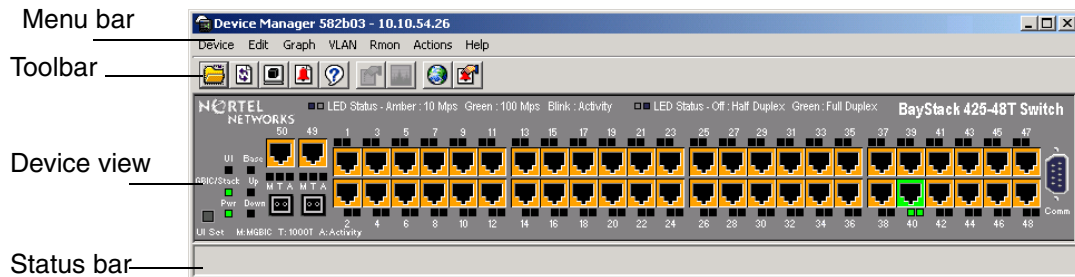
Figure 4 Device view



Device Manager window

The Device Manager window (Figure 5) has the following parts:

- Menu bar
- Toolbar
- Device view
- Status bar

Figure 5 Parts of the Device Manager window

Menu bar

Use the menu bar to set up and operate Device Manager ([Table 4](#)).










Table 4 Menu bar commands

| Command | Description |
|---------|--|
| Device | Opens the Open Device dialog box. It also allows you to <ul style="list-style-type: none"> Set the Properties used during a Device Manager session Refresh the status of the currently viewed device Telnet to a device View SNMP traps or Syslog messages that the device receives. |
| Edit | Opens edit dialog boxes for selected objects in the device view. This command also opens dialog boxes for managing files, running diagnostic tests and configuring data for selected chassis. |
| Graph | Opens statistics and graphing dialog boxes for the selected object. |
| VLAN | Opens dialog boxes for managing VLANs, spanning tree groups (STGs), and Multi-Link Trunks. |
| RMON | Opens RMON configuration and monitoring dialog boxes. |
| Actions | Provides quick access to the Web Management Software Home page. |
| Help | Opens online Help topics for Device Manager and provides a legend for the port colors in the device view. |

Toolbar

The toolbar contains buttons that provide quick access to commonly used commands and some additional actions.([Table 5](#)

Table 5 Toolbar buttons

| Button | Name | Description | Menu bar equivalent |
|---|-----------------------|---|--|
|  | Open Device | Opens the Open Device dialog box. | Device > Open |
|  | Refresh Device Status | Refreshes the device view information. | Device > Refresh Status |
|  | Trap Log | Opens the trap log. | Device > Trap Log |
|  | Help | Opens online Help in a Web browser. | Help > Device |
|  | Edit Selected | Displays configuration data for the selected chassis object. | Edit > Unit Edit > Chassis Edit > Port |
|  | Graph Selected | Opens statistics and graphing dialog boxes for the selected object. | Graph > Chassis Graph > Port |
|  | Home Page | Opens the Web Management Software Home Page. | Actions > Open Home Page |
|  | Telnet | Opens a Telnet session. | Device > Telnet |
|  | Alarm Manager | Opens the Rmon Alarm Manager. | Rmon > Alarm Manager |

Device view

The device view allows you to determine at a glance the operating status of the various units and ports in your hardware configuration. You also use the device view to perform management tasks on specific objects.

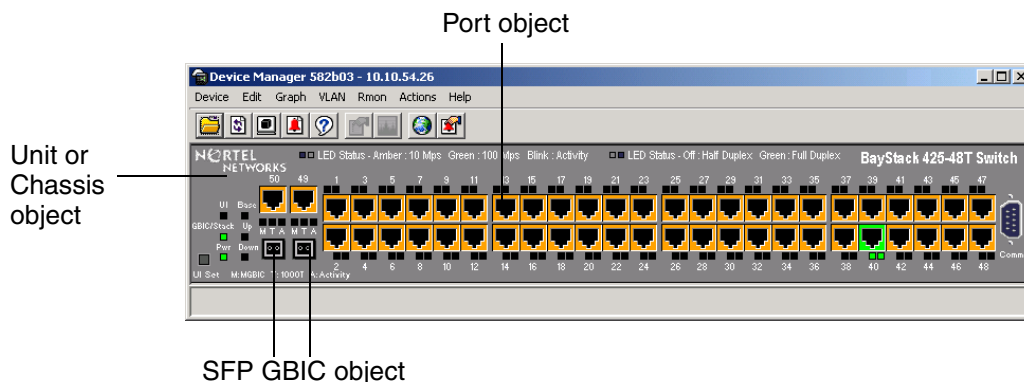
Selecting objects

The types of objects contained in the device view are:

- A standalone switch (called a unit in the menus and dialog boxes)
- A switch stack (called a chassis in the menus and dialog boxes)
- A port (including the SFP GBIC port)

Figure 6 shows the objects in the device view.

Figure 6 Objects in the device view



Selecting a single object

To select a single object:

- ➔ Click the edge of the object.

The object is outlined in yellow, indicating that it is selected. Subsequent activities in Device Manager refer to the selected object.

Selecting multiple objects

To select multiple objects of the same type (such as ports or switches of the same type):

➤ Do one of the following:

- For a block of contiguous ports, drag to select the group of ports.
- For multiple ports, GBICs, or switches in the stack, [Ctrl]-click on the objects.

To select all the ports in a standalone switch or in a switch stack:

➤ Choose Edit > Select > Ports.

To select all the units in the stack:

➤ Choose Edit > Select > Units.

To select an entire stack:

➤ Choose Edit > Select > Chassis.

To view information about a GBIC port:

- 1 Select the GBIC.
- 2 Choose Edit > Port.

The Port dialog box opens with the Interface tab displayed ([Figure 7](#)). The Interface tab describes the GBIC installed in the switch.

Figure 7 Interface tab

10.10.54.26 - Port 1/1

interface | VLAN | STG | EAPOL

Index: 1

Name: This is port number 1

Descr: Nortel Networks BayStack 425_48T Ethernet Switch Module - Port 1

Type: ethernet-csmacd

Mtu: 1514

PhysAddress: 00:0f:6a:7d:c2:a0

AdminStatus: up down

OperStatus: down

LastChange: 39 days, 05h:01m:00s

LinkTrap: enabled disabled

Speed: 100000000

AutoNegotiate

AdminDuplex: half full

OperDuplex: full

AdminSpeed: none mbps10 mbps100 mbps1000

OperSpeed: 100 mbps

AutoNegotiationCapability: 10Half,10Full,100Half,100Full

AutoNegotiationAdvertisements:

| | | |
|---|--|---|
| <input checked="" type="checkbox"/> 10Half | <input checked="" type="checkbox"/> 10Full | <input checked="" type="checkbox"/> 100Half |
| <input checked="" type="checkbox"/> 100Full | <input type="checkbox"/> 1000Half | <input type="checkbox"/> 1000Full |
| <input type="checkbox"/> PauseFrame | <input type="checkbox"/> AsymInPauseFrame | |

MIIid: 0

IsPortShared: portNotShared

PortActiveComponent: fixedPort

Apply Refresh Close Help...

LEDs and ports

The color of LEDs in the device view is the same as the colors of the LEDs on the physical switch. However, the device view does not show blinking activity of the LEDs.

For a full description of the LEDs for the Baystack 420/425, refer to *Using the BayStack 425 Switch*.

The ports on the device view are color coded to show port status.

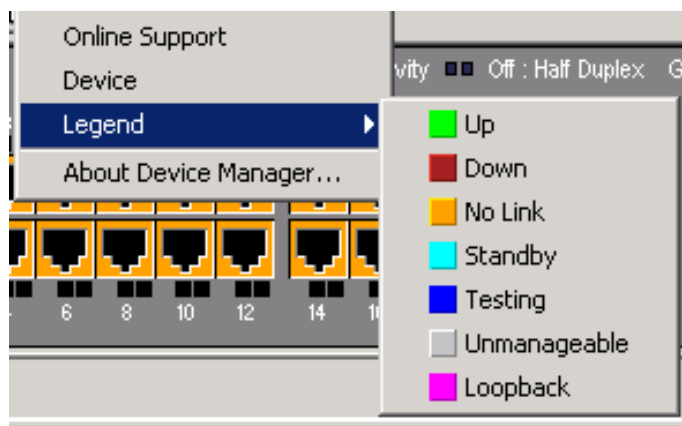
Table 6 shows the status assigned to each color.

Table 6 Port color codes

| Color | Description |
|--------|----------------------------------|
| Green | Port is operating. |
| Red | Port has been manually disabled. |
| Orange | Port has no link. |

In addition, the Help menu provides a legend that identifies the port colors and their meanings (Figure 8).

Figure 8 Color port legend



Shortcut menus

Each object in the device view has a shortcut menu that opens when you right-click a selected object. The switch unit shortcut menu (Figure 9) provides access to basic hardware information about the switch and to the graphing dialog boxes for the switch.

Figure 9 Switch unit shortcut menu

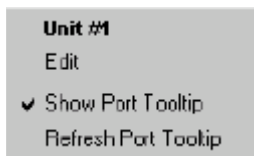


Table 7 describes the Edit command on the switch unit shortcut menu.

Table 7 Switch unit shortcut menu command

| Command | Description |
|----------------------|--|
| Edit | Opens a read-only dialog box that provides basic hardware information about the switch. |
| Show Port Tooltip | Indicates that the tooltip function is active. When unchecked, the tooltip function is disabled. |
| Refresh Port Tooltip | Refreshes the tooltip information. |

The port shortcut menu (Figure 10) provides a faster path for editing and graphing a single port; however, you can access the same options using the menu bar or the toolbar.

Figure 10 Port shortcut menu

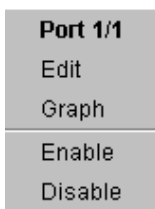


Table 8 describes the commands on the port shortcut menu.

Table 8 Port shortcut menu commands

| Command | Description |
|---------|---|
| Edit | Opens a dialog box that allows you to set operating parameters for the port. |
| Graph | Opens a dialog box that displays statistics for the port and allows you to display the statistics as a graph. |
| Enable | Administratively brings a port up. |
| Disable | Administratively shuts down a port. The color of the port changes to red in the device view. |

Status bar

The status bar displays error and informational messages from the software application. These messages are not related to the device being managed.

Using the buttons in Device Manager dialog boxes

Table 9 describes buttons in Device Manager dialog boxes. Not all buttons appear in all dialog boxes.

Table 9 Device Manager buttons








| Button | Name | Description |
|---|----------------------------|---|
|  | Insert | Opens a dialog box to create a new entry for a table; then from the dialog box, inserts the new entry in the table. |
|  | Copy | Copies selected cells from a table. |
|  | Paste | Pastes copied values to a currently selected table cell. |
|  | Reset Changes | Causes changed (but not applied) fields to revert to their previous values. |
|  | Print Table or Print Graph | Prints the table or graph that is displayed. |

Table 9 Device Manager buttons (continued)

| Button | Name | Description |
|---|--------------|--|
|  | Stop/Refresh | Stops the current action (compiling, saving, and so forth). If you are updating or compiling a large data table, the Refresh button changes to a Stop button while this action is taking place. Clicking the Stop button interrupts the polling process. |
|  | Export Data | Exports information to a file you specify. You can then import this file into a text editor or spreadsheet for further analysis. |

Editing objects

You can edit objects and values in the Device Manager device view in the following ways:

- Select an object and, on the toolbar, click the Edit Selected button.



The edit dialog box opens for that object.

- From a switch or port shortcut menu, choose Edit. The edit dialog box opens for that object.

When you change the value in a box, the changed value is displayed in **bold**. However, changes are not applied to the running configuration until you click Apply.



Note: Many dialog boxes contain a Refresh button. After you apply changes to fields, click Refresh to display the new information in the dialog box.

Working with statistics and graphs

Device Manager tracks a wide range of statistics for the stack (chassis), and each port. You can view and graph statistics for a single object or multiple objects. For information about the statistics tracked for the switch and ports, refer to [“Statistics for single and multiple objects” on page 47](#) and [“Graphing chassis statistics” on page 81](#).

This section describes the types of statistics and graphs available, the graph dialog boxes, and the procedure for creating a graph.

Types of statistics

The data tables in the statistics dialog boxes list the counters, or categories of statistics being gathered, for the specified object. For example, the categories for ports include Interface, Ethernet Errors, Bridge, and Rmon. Each category can be associated with six types of statistics. [Table 10](#) describes the types of statistics that are available.

Table 10 Types of statistics

| Statistic | Description |
|---------------|---|
| AbsoluteValue | The total count since the last time counters were reset. A system reboot resets all counters. |
| Cumulative | The total count since the statistics window was first opened. The elapsed time for the cumulative counter is displayed at the bottom of the graph window. |
| Average | The cumulative count divided by the cumulative elapsed time. |
| Minimum | The minimum average for the counter for a given polling interval over the cumulative elapsed time. |
| Maximum | The maximum average for the counter for a given polling interval over the cumulative elapsed time. |
| LastValue | The average for the counter over the last polling interval. |

Types of graphs

With Device Manager, you can create line, area, bar, and pie graphs. [Figure 11](#), [Figure 12](#), [Figure 13](#), and [Figure 14](#) provide examples of different types of graphs.

Figure 11 Line graph

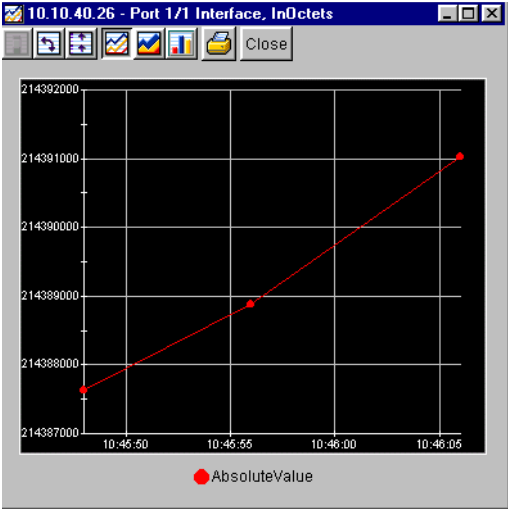


Figure 12 Area graph

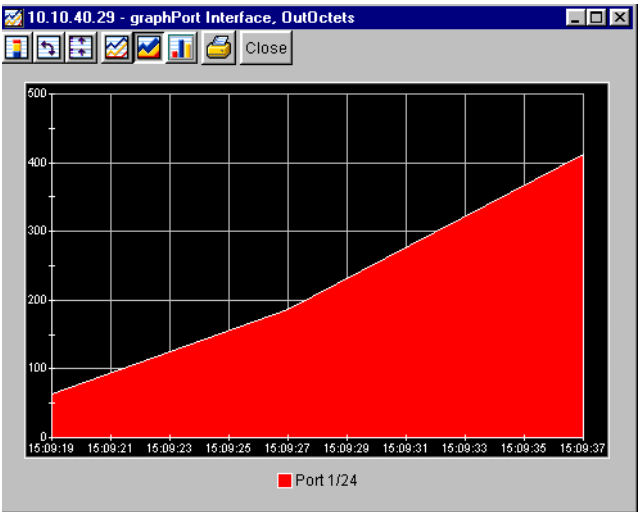


Figure 13 Bar graph

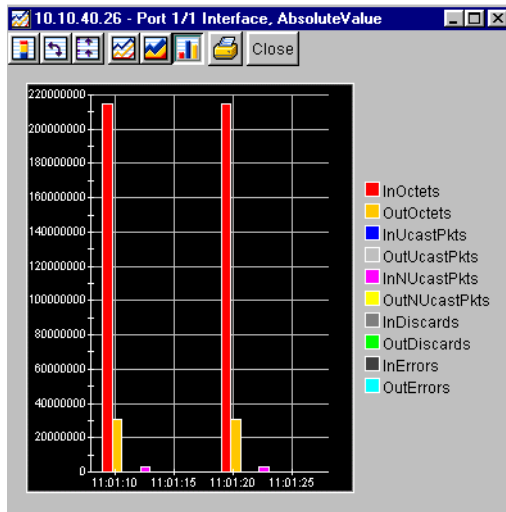


Figure 14 Pie graph

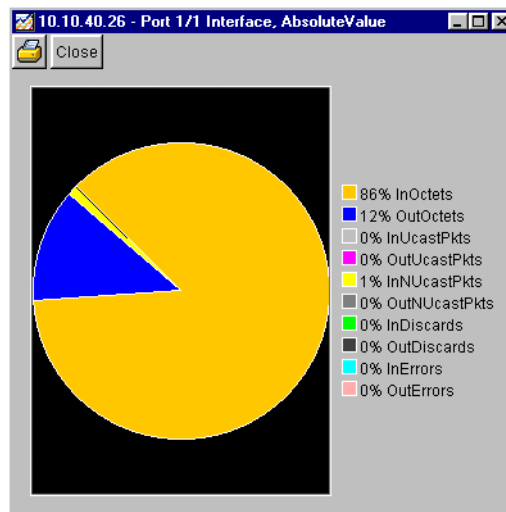
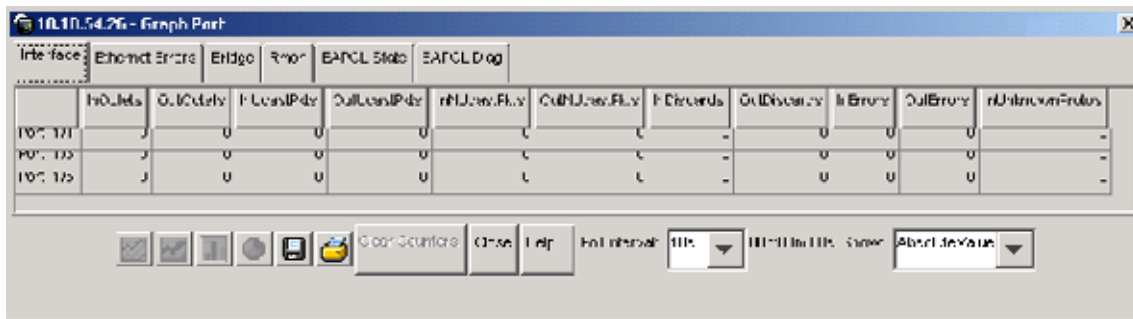


Figure 16 Interface statistics for multiple ports

To change the type of statistics displayed, select a different type from the show list at the bottom of the dialog box.

The statistics are updated based on the poll interval shown at the bottom of the dialog box. You can select a different polling interval.

Buttons for bar, pie, and line graphs are located at the bottom of a statistics dialog box.

See the next section, [“Viewing statistics as graphs,”](#) for instructions to use these buttons.

You can export the statistics to a tab-separated file format and import the file into other applications. To export the information, use the Export Data button below the table.



Viewing statistics as graphs

To create a graph for an object:

- 1 Select the object or objects to be graphed.
See [“Selecting objects” on page 36.](#)
- 2 Do one of the following:

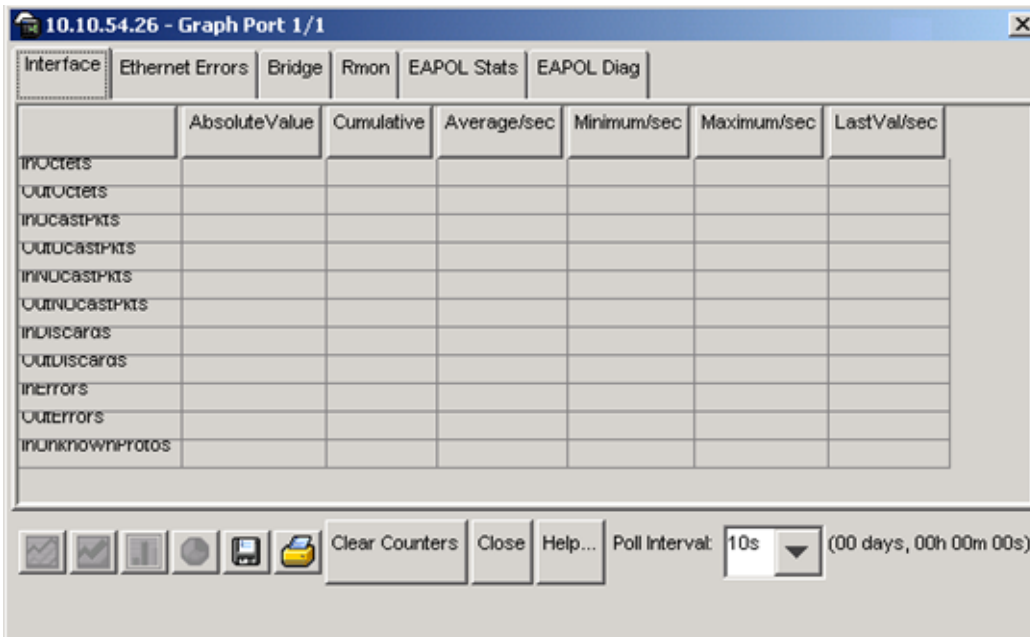
- On the toolbar, click Graph Selected.



- From the shortcut menu for the object, choose Graph.
- From the main menu, choose Graph > Chassis or Graph > Port.

A statistics dialog box opens with tabs for different categories of statistics for the selected object (Figure 17).

Figure 17 Statistics dialog box for a port



- 3 Select a tab for the group of statistics you want to view.
- 4 On the displayed data table, drag to select the cells you want to graph. (They must be in the same row or column.)
- 5 Click one of the graph buttons at the bottom of the dialog box
See “Types of graphs” on page 44.

A graph dialog box opens for the selected graph type.

- 6 To print a copy of the graph, click Print.



Buttons at the top of the graph dialog boxes for line, area, and bar graphs allow you to change the orientation of the graph, change the scale, or change the graph type.

Table 11 describes the buttons in the graph dialog boxes.

Table 11 Graph dialog box buttons

| Button | Name | Description |
|---|------------|--|
| A small icon showing a bar chart with bars stacked on top of each other. | Stacked | “Stacks” data quantities instead of displaying them side-by-side. |
| A small icon showing a bar chart with a curved arrow indicating rotation. | Horizontal | Rotates the graph 90 degrees. |
| A small icon showing a bar chart with a logarithmic scale on the x-axis. | Log Scale | Changes the scale of the x-axis (of an unrotated graph) from numeric to logarithmic. |
| A small icon showing a line graph with a checkmark. | Line Chart | Converts an area graph or bar graph to a line graph. |
| A small icon showing an area graph with a checkmark. | Area Chart | Converts a line graph or bar graph to an area graph. |
| A small icon showing a bar chart with a checkmark. | Bar Chart | Converts a line graph or area graph to a bar graph. |

Telnetting to a switch

From Device Manager, you can initiate a Telnet session to the console interface for the switch or stack you are currently accessing.

To Telnet to a switch:

➤ Do one of the following:

- From the Device Manager main menu, choose Device> Telnet.
- On the toolbar, click the Telnet button.



A Telnet window to the switch opens.

Opening the Web-based management home page

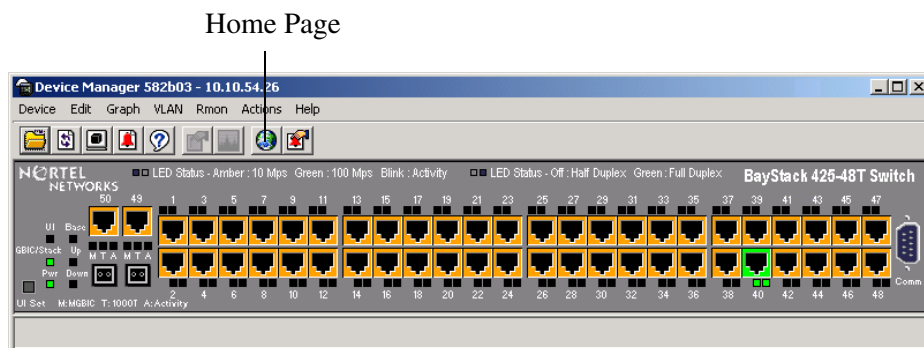
From Device Manager, you can access the Web-based management home page.

To open the Web-based management home page:

➤ Do one of the following:

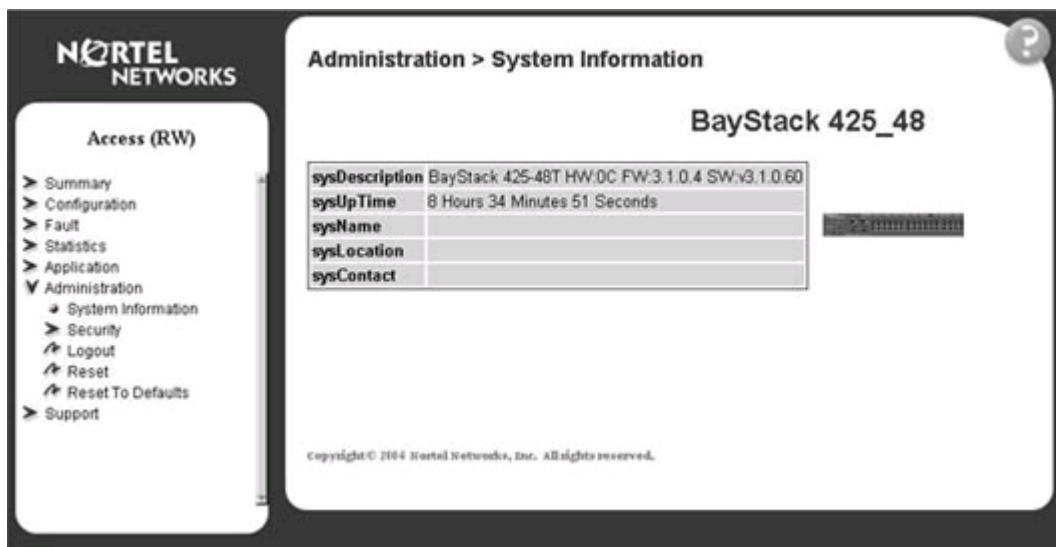
- From the Device Manager main menu, choose Actions > Open home page.
- On the toolbar, click the Open home page button (Figure 18).

Figure 18 Open home page icon



The Web-based management home page opens (Figure 19).

Figure 19 Web-based management home page



Trap log

You can configure a BayStack 420/425 Switch to send SNMP generic traps. When Device Manager is running, any traps received are recorded in the trap log. You set the maximum number of entries in the trap log using the Properties dialog box (Figure 2 on page 29). The default number of trap log entries is 500.

To view the trap log:

➤ Do one of the following:

- On the toolbar, click the Trap Log button.



- From the Device Manager Main Menu, choose Device > Trap Log.



Note: When you operate Device Manager from a UNIX platform, you must be logged in as root in order to receive traps.

Device Manager receives traps on port 162. If this port is being used by another application, you will not be able to view the trap log until the other application is disabled and Device Manager is restarted.

By default, traps are sent in SNMP V2c format. However, if you are using an older network management system (NMS), one that supports only SNMP V1 traps (HP OpenView), you can specify that the traps be sent in V1 format.

For more information about traps and trap receivers, refer to *Using the BayStack 420/425 Switch, Software Release 3.1*.

Online Help

Online Help in Device Manager is context-sensitive. You use a Web browser to display online Help. The Web browser should launch automatically when you click the Help button. If the Help topic you are accessing is not displayed in your browser, exit the existing browser session and click the Help button again.

If, for some reason, the Web browser does not launch, the default locations of the Help files are the directories listed in [Table 12](#).

Table 12 Help file locations

| Platform | Default path |
|--|---|
| Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP | JDM install directory\help\hummingbird\v310\help.html |
| UNIX | JDM install directory\help\hummingbird\v310\help.html |

Chapter 2

Configuring and graphing the switch

The first three sections of this chapter describe how you can use Device Manager to configure your switch. The last section describes how to use Device Manager to graph switch statistics.

Viewing switch IP information

You can view the switch IP information using the IP dialog box.

To open the IP dialog box:

- From the Device Manager main menu, choose Edit > IP.

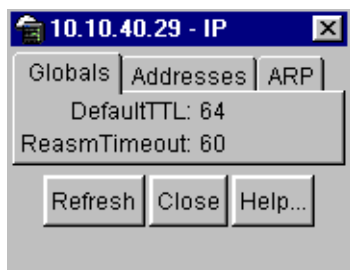
The Edit IP dialog box opens ([Figure 20](#)) with the Globals tab displayed.

Globals tab

To open the Globals tab:

- From the Device Manager main menu, choose Edit > IP.

The IP dialog box opens ([Figure 20](#)) with the Globals tab displayed.

Figure 20 Globals tab

[Table 13](#) describes the Globals tab items.

Table 13 Globals tab items

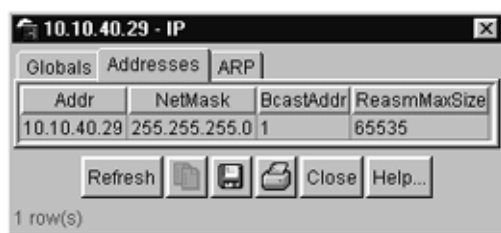
| Item and MIB association | Description |
|--------------------------|--|
| DefaultTTL | Default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol. Default value is 16. |
| ReasmTimeout | Maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity. Default value is 5. |

Addresses tab

The Addresses tab shows the IP address information for the device.

To open the Addresses tab:

- 1 From the Device Manager main menu, choose Edit > IP.
The IP dialog box opens with the Globals tab displayed ([Figure 20 on page 56](#)).
- 2 Click the Addresses tab.
The Addresses tab opens ([Figure 21 on page 57](#)).

Figure 21 Edit IP dialog box — IP Address tab

[Table 14](#) describes the IP Address tab items.

Table 14 IP Addresses tab items

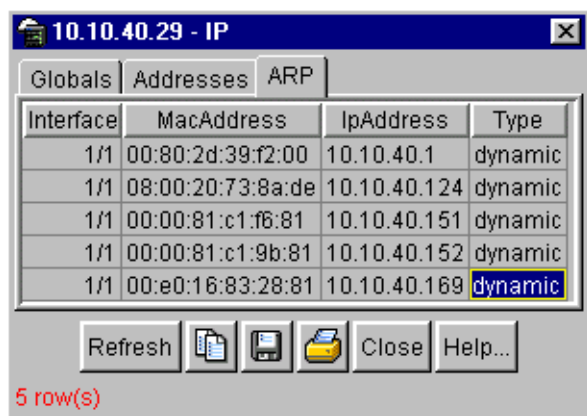
| Item | Description |
|--------------|---|
| Addr | The device IP address. |
| NetMask | The subnet mask address. |
| BcastAddr | The IP broadcast address used. |
| ReasmMaxSize | The size of the largest IP datagram that this entity can reassemble from incoming IP fragmented datagrams received on this interface. |

ARP tab

The Address Resolution Protocol (ARP) tab shows the MAC addresses and the associated IP addresses for the switch.

To open the ARP tab:

- 1 From the Device Manager main menu, choose Edit > IP.
The IP dialog box opens with the Globals tab displayed ([Figure 20 on page 56](#)).
- 2 Click the ARP tab.
The ARP tab opens ([Figure 22 on page 58](#)).

Figure 22 Edit IP dialog box — ARP tab

[Table 15](#) describes the ARP tab items.

Table 15 ARP tab items

| Item | Description |
|------------|---|
| Interface | The device unit number. |
| MacAddress | The unique hardware address of the device. |
| IpAddress | The Internet Protocol address of the device used to represent a point of attachment in a TCP/IP internetwork. |
| Type | The type of mapping. |

Editing the chassis configuration

You can edit a chassis configuration from the Edit Chassis dialog box ([Figure 23 on page 60](#)).

To open the Chassis dialog box:

- 1 Select the chassis.
- 2 Do *one* of the following:
 - From the shortcut menu, choose Edit.
 - From the Device Manager main menu, choose Edit > Chassis.
 - On the toolbar, click Edit.



The following sections provide a description of the tabs in the Edit > Chassis dialog box and details about each item on the tab.

System tab

You can use the System tab to specify, among other things, tracking information for a device and device descriptions.

To open the System tab:

- 1 Select the chassis.
- 2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens with the System tab displayed ([Figure 23](#)).

Figure 23 Edit Chassis dialog box — System tab

10.10.54.26 - Chassis

System | Base Unit Info | Agent | SNMP | Trap Receivers | PowerSupply | Fan | Banner | Custom Banner

sysDescr: BayStack 425-48T HW0C FW:3.1.0.2 SW:v3.1.0.65

sysUpTime: 24 days, 02h:22m:33s

sysContact:

sysName:

sysLocation:

AuthenticationTraps

ReBoot: running reboot

AutoPvid: enabled disabled

NextBootMgmtProtocol: ipOnly

CurrentMgmtProtocol: ipOnly

BootMode: other local net netWhenNeeded netOrLastAddress

ImageLoadMode: net

CurrentImageVersion: v3.1.0.65

LocalStorageImageVersion: v3.1.0.65

NextBootDefaultGateway: 10.10.54.1

CurrentDefaultGateway: 10.10.54.1

NextBootLoadProtocol: ipOnly

LastLoadProtocol: ip

EAPOL Security

SystemAuthControl: enabled disabled

Apply Refresh Close Help...

Table 16 describes the System tab items.

Table 16 System tab items


| Item | Description |
|----------------------|---|
| sysDescr | The assigned system name. |
| sysUpTime | The time since the system was last booted. |
| sysContact | Type the contact information (in this case, an e-mail address) for the system administrator. |
| sysName | Type the name of this device. |
| sysLocation | Type the physical location of this device. |
| AuthenticationTraps | <p>Click enable or disable. When you select enabled, SNMP traps are sent to trap receivers for all SNMP access authentication. When you select disabled, no traps are received.</p> <p>To view traps, click the Trap toolbar button.</p>  |
| AutoPVID | Click enable or disable. When you select enabled, AutoPVID is activated. When you select disabled, AutoPVID is no longer active. |
| NextBootMgmtProtocol | The transport protocol(s) to use after the next boot of the agent. |
| CurrentMgmtProtocol | The current transport protocol(s) that the agent supports. |
| BootMode | <p>This setting determines how the management interface of the switch will be assigned an IP address, the next time the switch boots. The four BootMode options are:</p> <ul style="list-style-type: none"> • local - use the IP address contained in the configuration file. • net- always attempt to get an IP address from the network. • netWhenNeeded - attempt to get an IP address from the network only when one is not contained in the configuration file. • netOrLastAddress - attempt to get an IP address from the network and if that fails use the IP address that was in use on this switch before the last reboot. |
| ImageLoadMode | The source from which to load the agent image at the next boot. |

Table 16 System tab items (continued)

| Item | Description |
|--|---|
| CurrentImageVersion | The version number of the agent image that is currently used on the switch. |
| LocalStorageImageVersion | The version number of the agent image that is stored in flash memory on the switch. |
| NextBootDefaultGateway | The IP address of the default gateway for the agent to use after the next time the switch is booted. |
| CurrentDefaultGateway | The IP address of the default gateway that is currently in use. |
| NextBootLoadProtocol | The transport protocol to be used by the agent to load the configuration information and the image at the next boot. |
| LastLoadProtocol | The transport protocol last used to load the image and configuration information on the switch. |
| Reboot | Action object to reboot the agent. Reboot — initiates a hardware reset. The agent does best efforts to return a response before the action occurs. If any of the combined download actions are requested, neither action occurs until the expiration of s5AgInfoScheduleBootTime, if set. |
| SystemAuthControl (enabled or disabled) | Specifies the administrative enabled or disable state for Port Access Control. |

Base Unit Info tab

The Base Unit Info tab provides read-only information about the operating status of the hardware and whether or not the default factory settings are being used.

To open the Base Unit Info tab:

- 1 Select the chassis.
- 2 From the shortcut menu, choose Edit > Chassis.

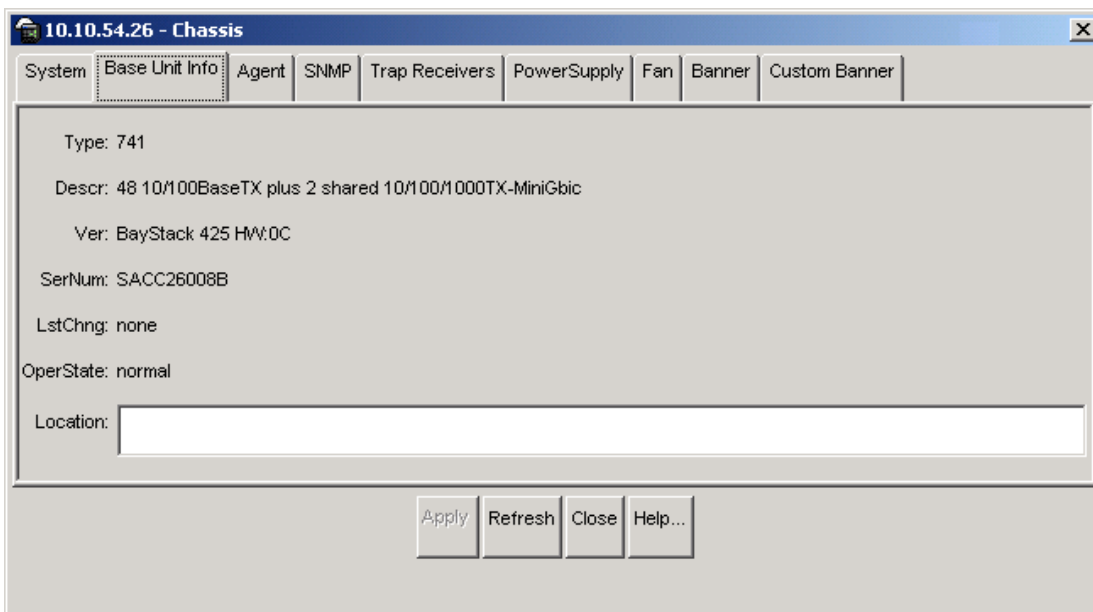
The Chassis dialog box opens with the System tab displayed ([Figure 23 on page 60](#)).

- 3 Click the Base Unit Info tab.

The Base Unit Info tab opens ([Figure 24](#)).

In a stack environment, if the base unit number does not begin with the number one, the information will not be displayed. Use the console interface and the Web-based management interface to change your base unit number. For detailed information, refer to *Using the Baystack 420/425 Switch, Software Release 3.1* and *Using Web-Based Management for the BayStack 420/425 Switch, Software Release 3.1*.

Figure 24 Edit Chassis dialog box — Base Unit Info tab



[Table 17](#) describes the Base Unit Info tab items.

Table 17 Base Unit Info tab items

| Item | Description |
|--------|---|
| Type | The switch type. |
| Descr | A description of the switch hardware, including number of ports and transmission speed. |
| Ver | The switch hardware version number. |
| SerNum | The switch serial number. |

Table 17 Base Unit Info tab items (continued)

| Item | Description |
|-----------|---|
| LstChng | The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero. |
| OperState | The operational state of the switch. |
| Location | Type the physical location of the switch. |

Stack Info tab

Like the Base Unit Info tab, the Stack Info tab provides read-only information about the operating status of the *stacked* switches and whether or not the default factory settings are being used. This tab is enabled for a stack of Baystack 420/425.

To open the Stack Info tab:

- 1 Select the chassis.
- 2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens with the System tab displayed ([Figure 23](#)).

- 3 Click the Stack Info tab.

The Stack Info tab opens ([Figure 25](#)).

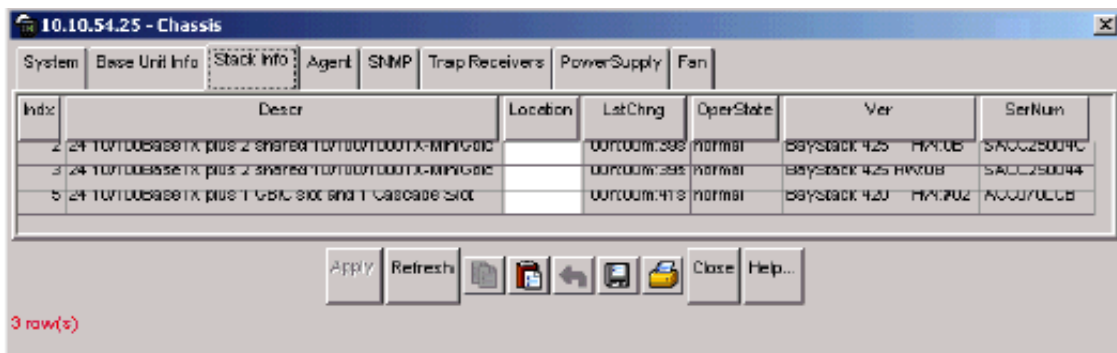
Figure 25 Edit Chassis dialog box — Stack Info tab

Table 18 describes the Stack Info tab fields.

Table 18 Stack Info tab fields

| Field | Description |
|------------|--|
| Descr | A description of the component or subcomponent. If not available, the value is a zero length string. |
| Location | <p>The geographic location of a component in a system modeled as a chassis, but possibly physically implemented with geographically separate devices connected together to exchange management information. Chassis modeled in this manner are sometimes referred to as virtual chassis. An example value is: '4th flr wiring closet in blg A'.</p> <p>Notes: 1. This object is applicable only to components that can be found in either the Board or Unit groups. If the information is unavailable, for example, the chassis is not modeling a virtual chassis or component is not in Board or Unit group, the value is a zero length string.</p> <p>2. If this object is applicable and is not assigned a value through a SNMP SET PDU when the row is created, the value will default to the value of the object s5ChasComSerNum.</p> |
| LstChng | The value of sysUpTime when it was detected that the component/sub-component was added to the chassis. If this has not occurred since the cold/warm start of the agent, then the value is zero. |
| AdminState | <p>The state of the component or subcomponent. The values that are read-only are:</p> <ul style="list-style-type: none"> • other — currently in some other state • notAvail — actual value is not available <p>The possible values that can be read and written are:</p> <ol style="list-style-type: none"> 1.disable—disables operation 2.enable—enables operation 3.reset—resets component 4.test—starts self test of component, with the result to be normal, warning, nonFatalErr, or fatalErr in object s5ChasComOperState <p>The allowable (and meaningful) values are determined by the component type.</p> |

Table 18 Stack Info tab fields (continued)

| Field | Description |
|-----------|--|
| OperState | <p>The current operational state of the component. The possible values are:</p> <ul style="list-style-type: none"> • other—some other state • notAvail—state not available • removed—component removed • disabled—operation disabled • normal—normal operation • resetInProg—reset in progress • testing—doing a self test • warning—operating at warning level • nonFatalErr—operating at error level • fatalErr—error stopped operation <p>The allowable (and meaningful) values are determined by the component type.</p> |
| Ver | The version number of the component or subcomponent. If not available, the value is a zero length string. |
| SerNum | The serial number of the component or subcomponent. If not available, the value is a zero length string. |

Agent tab

The Agent tab provides read-only information about the addresses that the agent software uses to identify the switch.

To open the Agent tab:

- 1 Select the chassis.
- 2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens ([Figure 23 on page 60](#)) with the System tab displayed.

- 3 Click the Agent tab.

The Agent tab opens ([Figure 26](#)).

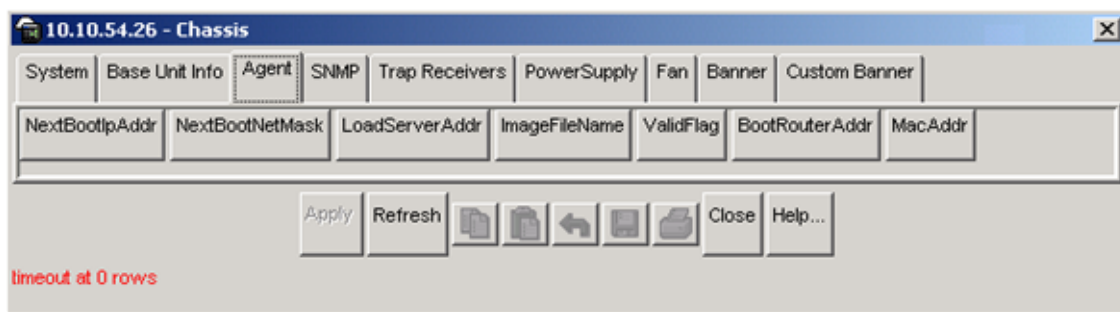
Figure 26 Edit Chassis dialog box — Agent tab

Table 19 describes the Agent tab fields.

Table 19 Agent tab fields

| Item | Description |
|-----------------|--|
| NextBootIpAddr | The IP address of the BootP server to be used the next time the switch is booted. |
| NextBootNetMask | The subnet mask to be used the next time the switch is booted. |
| LoadServerAddr | The IP address of the load server for the configuration file and/or the image file. If not used, then the value is 0.0.0.0. |
| ImageFileName | Name of the image file(s) currently associated with the interface. When the object is not used, the value is a zero length string. |
| ValidFlag | Indicates if the configuration and/or image file(s) were downloaded from this interface and if the file names have not been changed. |
| BootRouterAddr | The IP address of the boot router for the configuration file and/or the image file. |
| MacAddr | The switch's MAC address. |

SNMP tab

The SNMP tab provides read-only information about the addresses that the agent software uses to identify the switch.

To open the SNMP tab:

- 1 Select the chassis.
- 2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens (Figure 23 on page 60) with the System tab displayed.

- 3 Click the SNMP tab.

The SNMP tab opens (Figure 27).

Figure 27 Edit Chassis dialog box — SNMP tab

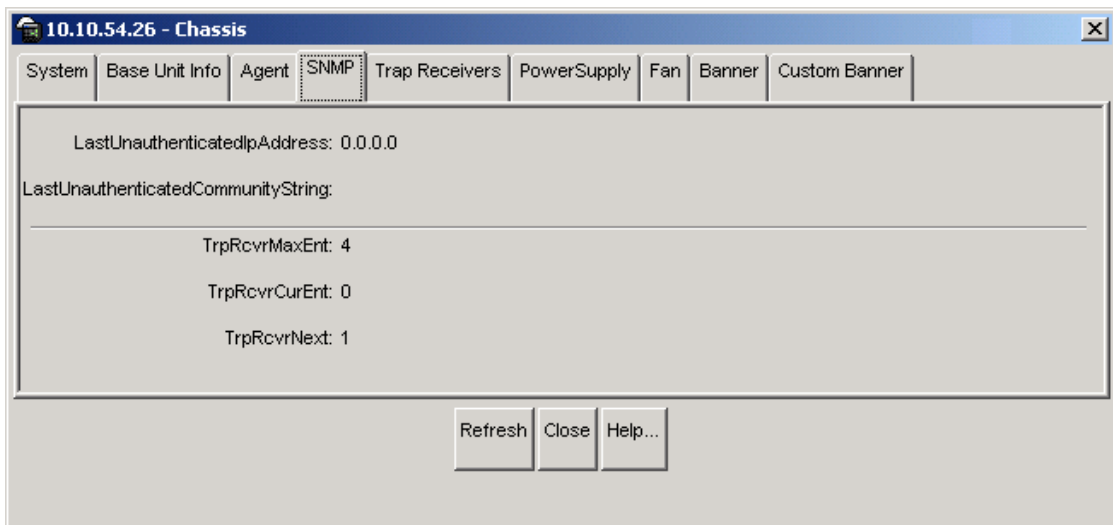


Table 20 describes the SNMP Info tab fields.

Table 20 SNMP tab fields

| Field | Description |
|------------------------------------|---|
| LastUnauthenticatedIpAddress | The last IP address that was not authenticated by the device. |
| LastUnauthenticatedCommunityString | The last community string that was not authenticated by the device. |
| TrpRcvrMaxEnt | The maximum number of trap receiver entries. |
| TrpRcvrCurEnt | The current number of trap receiver entries. |
| TrpRcvrNext | The next trap receiver entry to be created. |

Trap Receivers tab

The Trap Receivers tab lists the devices that will receive SNMP traps from the BayStack 420/425 switch.

To open the Trap Receivers tab:

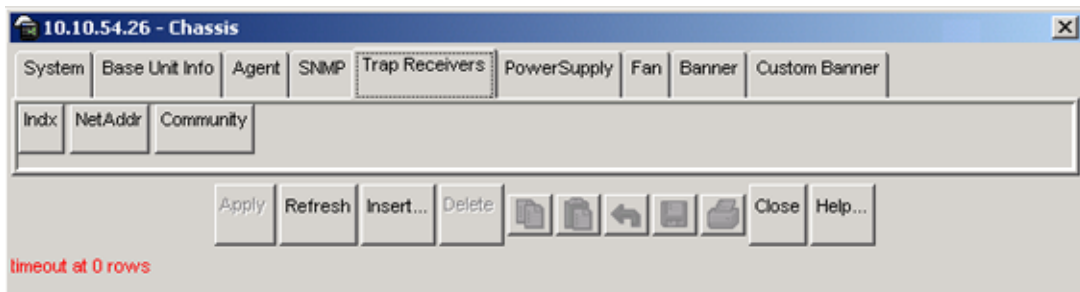
- 1 Select the chassis.
- 2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens (Figure 23 on page 60) with the System tab displayed.

- 3 Click the Trap Receivers tab.

The Trap Receivers tab opens (Figure 28).

Figure 28 Trap Receivers tab



[Table 21](#) describes the Trap Receivers tab items.

Table 21 Edit Chassis dialog box — Trap Receivers tab items

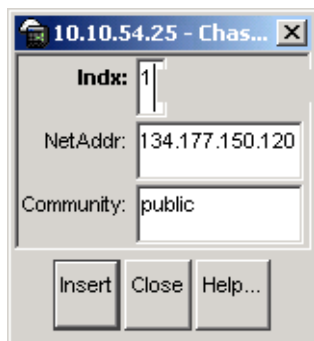
| Item | Description |
|-----------|--|
| NetAddr | The address (or DNS hostname) for the trap receiver. |
| Community | Community string used for trap messages to this trap receiver. |

Adding a Trap Receiver

To edit the network traps table:

- 1 In the Trap Receivers tab ([Figure 28](#)), click Insert.
The Chassis, Insert Trap Receive dialog box opens ([Figure 29](#)).

Figure 29 Chassis, Insert Trap Receive dialog box



- 2 Type the Index, NetAddr, and the Community information.



Note: Refer to [Table 21 on page 70](#) for description of the Chassis, Insert Trap Receivers dialog box items.

- 3 Click Insert.

Power Supply tab

The Power Supply tab provides read-only information about the operating status of the switch power supplies.

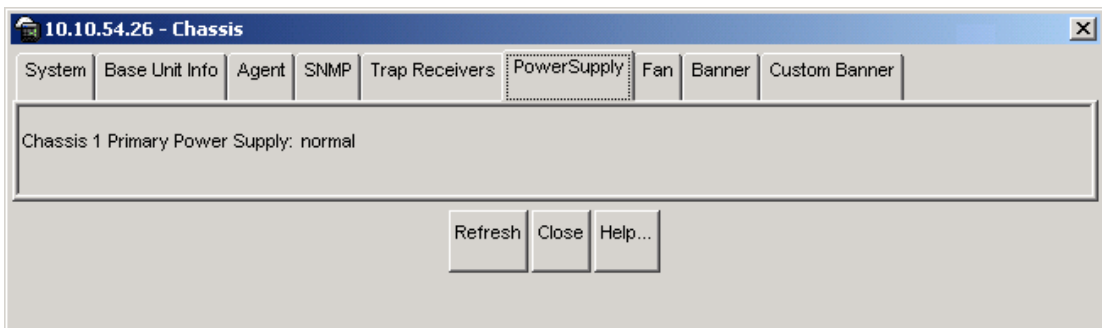
To open the PowerSupply tab:

- 1 Select the chassis.
- 2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens ([Figure 23](#)) with the System tab displayed.

- 3 Click the PowerSupply tab.

The PowerSupply tab opens ([Figure 30](#)).

Figure 30 Edit Chassis dialog box — Power Supply tab

[Table 22](#) describes the Power Supply tab fields.

Table 22 Power Supply tab fields

| Field | Description |
|----------|---|
| Desc | The power supply type. |
| OperStat | <p>The operational state of the power supply. Possible values include:</p> <ul style="list-style-type: none"> • other: Some other state. • notAvail: State not available. • removed: Component was removed. • disabled: Operation disabled. • normal: State is in normal operation. • resetInProg: There is a reset in progress. • testing: System is doing a self test. • warning: System is operating at a warning level. • nonFatalErr: System is operating at error level. • fatalErr: A fatal error stopped operation. • notConfig: A module needs to be configured. The allowable values are determined by the component type. |

Fan tab

The Fan tab provides read-only information about the operating status of the switch fans.

To open the Fan tab:

- 1 Select the chassis.
- 2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens ([Figure 23 on page 60](#)) with the System tab displayed.

- 3 Click the Fan tab.

The Fan tab opens ([Figure 31](#)).

Figure 31 Edit Chassis dialog box — Fan tab

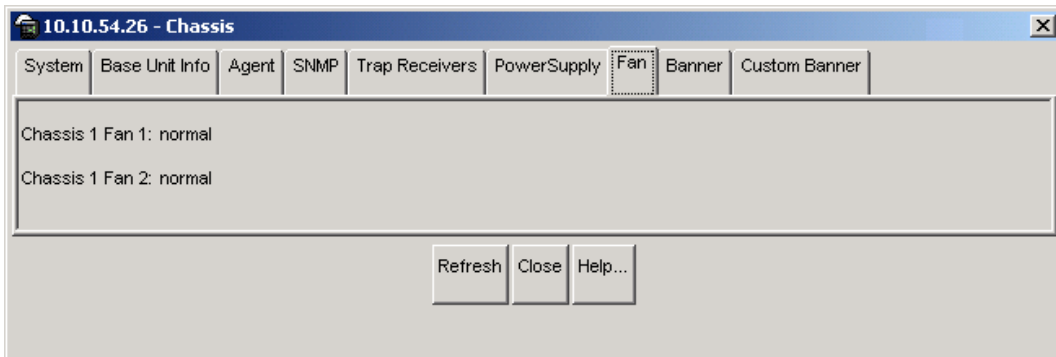


Table 23 describes the Fan tab fields.

Table 23 Fan tab fields

| Field | Description |
|----------|--|
| Desc | The fan type. |
| OperStat | The operational state of the fan. Values include: <ul style="list-style-type: none">• other: Some other state.• notAvail: This state is not available.• removed: Fan was removed.• disabled: Fan is disabled.• normal: Fan is operating in normal operation.• resetInProg: A reset of the fan is in progress.• testing: Fan is doing a self test.• warning: Fan is operating at a warning level.• nonFatalErr: Fan is operating at error level.• fatalErr: An error stopped the fan operation• notConfig: Fan needs to be configured. The allowable values are determined by the component type. |

Banner tab

The banner tab allows you to specify banner display in Telenet. You can specify either the default banner or a custom banner.

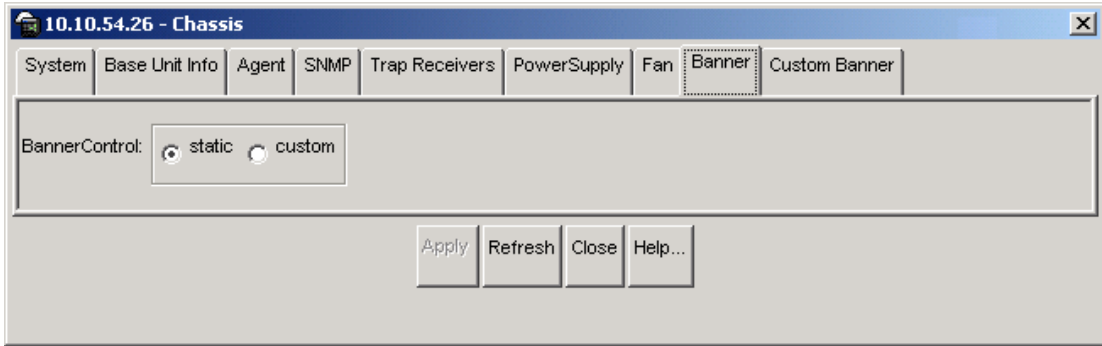
To open the Banner tab:

- 1 Select the chassis.
- 2 From the main menu, choose Edit > Chassis.

The Chassis dialog box opens ([Figure 23 on page 60](#)) with the System tab displayed.

- 3 Click the Banner tab.

The Banner tab opens ([Figure 32](#)).

Figure 32 Edit Chassis dialog box — banner tab

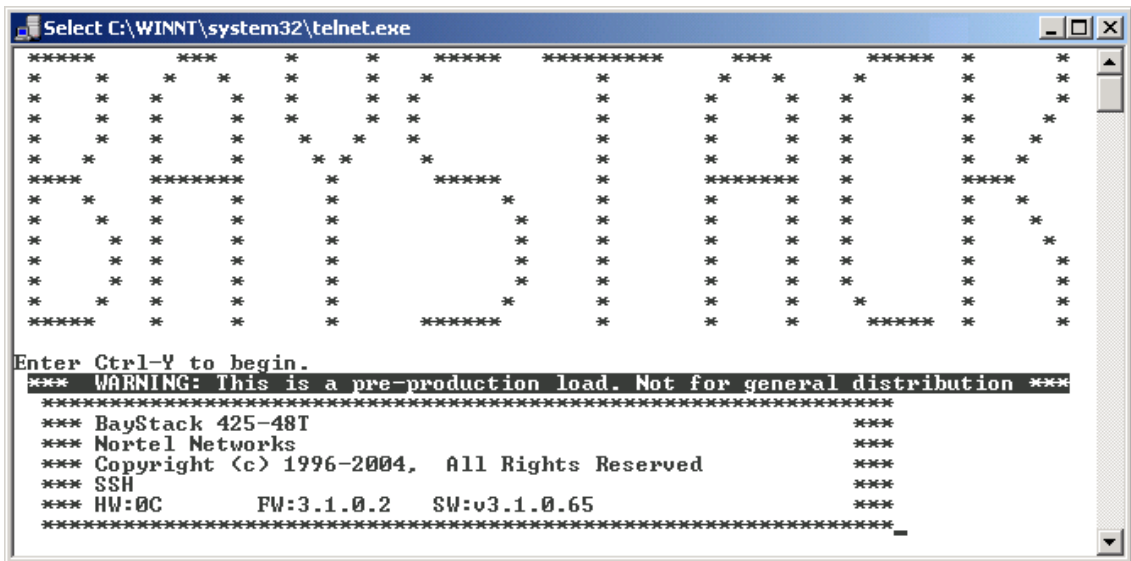
To set the default banner:

- 1 In the Banner tab, click on the Static radio button, and then click the Apply button. This resets the banner in Telnet to the default banner.

To check that the default banner is set in Telnet:

- 2 In the Main Menu, click on Device > Telnet.

The Telnet window opens ((Figure 32)) with the default banner displayed.

Figure 33 Telnet window with default banner

Custom banner tab

The custom banner tab allows you to specify the display for a custom banner in Telnet.

To open the Custom Banner tab:

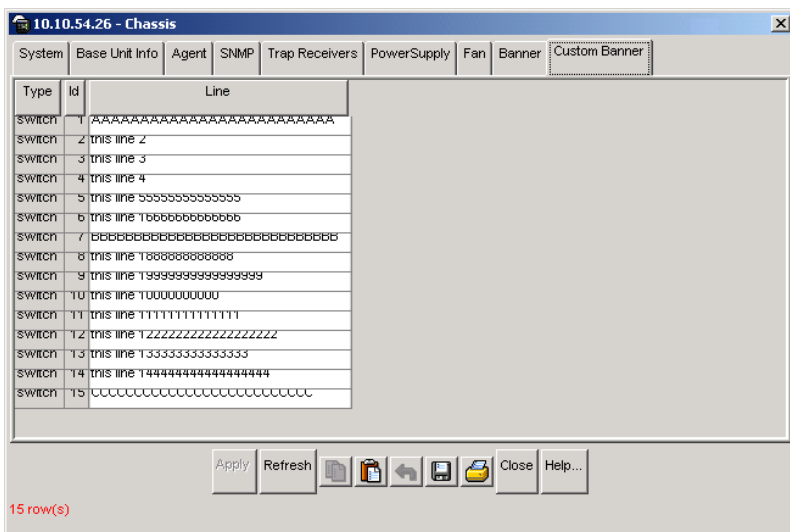
- 1 Select the chassis.
- 2 From the main menu, choose Edit > Chassis.

The Chassis dialog box opens (Figure 23 on page 60) with the System tab displayed.

- 3 Click the Custom Banner tab.

The Custom Banner tab opens (Figure 32).

Figure 34 Edit Chassis dialog box — custom banner tab



To create a custom banner:

- 1 In the Banner tab, click on the Custom radio button, and then click the Apply button.
- 2 Click on the Custom banner tab (Figure 34).

- 3 In the Custom Banner tab, make the changes to the lines of the banner that you want to create, and click on the Apply button. The custom banner is 15 lines high and can be up to 80 characters long.

To check that the custom banner is set in Telnet:

- 4 In the Main menu, click on Device > Telnet

The Telnet window opens (([Figure 34](#))) with the custom banner displayed.

Figure 35 Telnet window with custom banner

```

Select C:\WINNT\system32\telnet.exe
AAAAAAAAAAAAAAAAAAAAAAAAAAAA
this line 2
this line 3
this line 4
this line 5555555555555555
this line 1666666666666666
BBBBBBBBBBBBBBBBBBBBBBBBBBBB
this line 1888888888888888
this line 19999999999999999
this line 100000000000
this line 1111111111111111
this line 122222222222222222
this line 13333333333333333
this line 144444444444444444
CCCCCCCCCCCCCCCCCCCCCCCC
Enter Ctrl-Y to begin.
*** WARNING: This is a pre-production load. Not for general distribution ***
*****
*** BayStack 425-48T ***
*** Nortel Networks ***
*** Copyright (c) 1996-2004. All Rights Reserved ***
*** SSH ***
*** HW:0C FW:3.1.0.2 SW:v3.1.0.65 ***
*****

```

Working with configuration files

You can view information and upload or download the configuration and image files from the Edit FileSystem dialog box.

To open the Edit FileSystem dialog box:

- From the Device Manager main menu, choose Edit > File System.

The FileSystem dialog box opens ([Figure 36](#)) and displays the Config/Image/Diag tab.

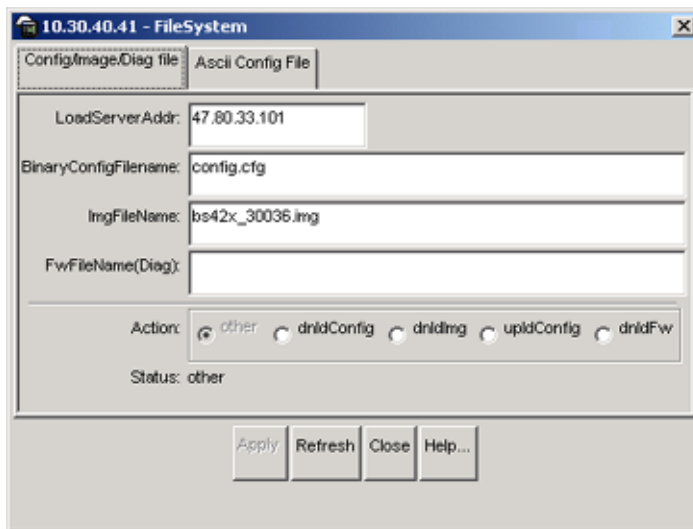
Figure 36 FileSystem - Config/Image/Diag File tab dialog box

Table 24 describes the FileSystem Config/Image/Diag file dialog box items.

Table 24 FileSystem Config/Image/Diag file dialog box items

| Item | Description |
|-------------------|--|
| LoadServerAddr | The IP address of the load server for the configuration file and/or the image file. If not used, then the value is 0.0.0.0. |
| ConfigFileName | Name of the configuration file currently associated with the interface. When not used, the value is a zero length string. |
| ImageFileName | Name of the image file(s) currently associated with the interface. When the object is not used, the value is a zero length string. |
| FwFileName (Diag) | Specifies the FWFileName. |

Table 24 FileSystem Config/Image/Diag file dialog box items (continued)

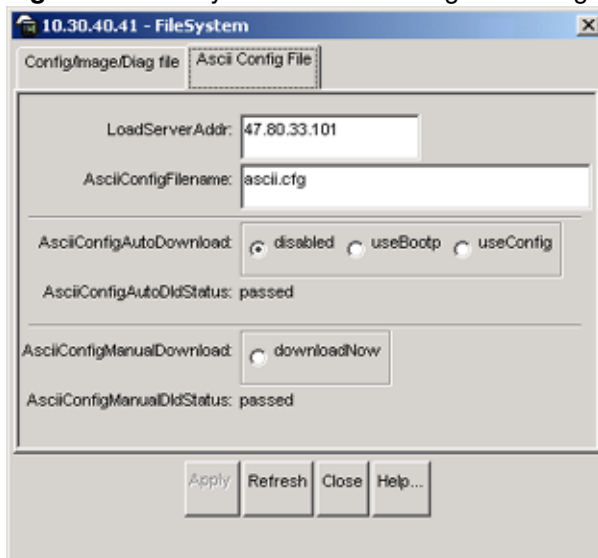
| Item | Description |
|--------|---|
| Action | <ul style="list-style-type: none"> • This object is used to download or upload a config file, an image file or diag firmware file. In read operation, if there is no action taken since the boot up, it will return with a value of other. Otherwise, it will return the latest action such as: dnldConfig dnldImg upldConfig dnldFw • In a write operation, the value that can be written is: dnldConfig - download a config file to a device. • The newly downloaded config, image or diag file will not take effect until the next boot cycle of the device. Possible values are: dnldImg - download an image to a device. dnldConfig - download a config file to device upldConfig - upload a config file to a server from a device. dnldFw - download a diag firmware file to device. |
| Status | <p>This object is used to get the status of the latest action as shown by s5AgInfoFileAction. The values that can be read are:</p> <ul style="list-style-type: none"> • other — if no action taken since the boot up • inProgress — the operation is in progress • success — the operation succeeds. • fail — the operation failed. |

ASCII config file

To see the ASCII Config file dialog box:

- In the Config/Image/Diag File tab, click on the ASCII Config tab..

The FileSystem - ASCII Config File dialog box ([Figure 37](#)) opens.

Figure 37 File system - ASCII Config File dialog box

[Table 25](#) describes the FileSystem - ASCII Config File dialog box items.

Table 25 FileSystem - ASCII Config File dialog box items

| Item | Description |
|----------------------------|---|
| LoadServerAddr | The IP address of the load server for the ASCII configuration file. If not used, then the value is 0.0.0.0. |
| ASCIIConfigFileName | Name of the ASCII configuration file currently associated with the interface. When not used, the value is a zero length string. |
| ASCIIConfigAutoDownload | Specifies automatic ASCII configuration download. |
| ASCIIConfigAutoDldStatus | Specifies the current status of the ASCII configuration file download. |
| ASCIIConfigManualDownload | Specifies manual download of an ASCII configuration file. |
| ASCIIConfigManualDldStatus | Specifies the current status of the manual download of an ASCII configuration file. |

Graphing chassis statistics

To graph chassis statistics:

- 1 Select the chassis.
- 2 Do *one* of the following:
 - From the shortcut menu, choose Graph.
 - From Device Manager main menu, choose Graph > Chassis.



The following sections describe the Graph Chassis dialog box tabs with descriptions of the statistics on each tab.

Six columns provide the statistics for the counters that are listed on the tab.

For descriptions of the chassis IP statistics, refer to [Table 10 on page 44](#).

SNMP tab

The chassis SNMP tab lists chassis statistics.

To open the SNMP tab:

- 1 Select the chassis.
- 2 From the shortcut menu, choose Graph > Chassis.

The Chassis dialog box opens ([Figure 23 on page 60](#)) with the System tab displayed.

- 3 Click the SNMP tab.

The SNMP tab opens ([Figure 38](#)).

Figure 38 Graph Chassis dialog box — Chassis SNMP tab

| SNMP | AbsoluteValue | Cumulative | Average | Minimum | Maximum | LastValue |
|---------------------|---------------|------------|---------|---------|---------|-----------|
| InPkts | 91 | 2 | 0.222 | 0.125 | 1 | 0.125 |
| OutPkts | 90 | 2 | 0.222 | 0.125 | 1 | 0.125 |
| InTotalReqVars | 1,392 | 46 | 5.111 | 2.875 | 23 | 2.875 |
| InTotalSetVars | 0 | 0 | 0 | 0 | 0 | 0 |
| InGetRequests | 68 | 2 | 0.222 | 0.125 | 1 | 0.125 |
| InGetNexts | 18 | 0 | 0 | 0 | 0 | 0 |
| InSetRequests | 0 | 0 | 0 | 0 | 0 | 0 |
| InGetResponses | 0 | 0 | 0 | 0 | 0 | 0 |
| OutTraps | 0 | 0 | 0 | 0 | 0 | 0 |
| OutTooBigs | 0 | 0 | 0 | 0 | 0 | 0 |
| OutNoSuchNames | 1 | 0 | 0 | 0 | 0 | 0 |
| OutBadValues | 0 | 0 | 0 | 0 | 0 | 0 |
| OutGenErrs | 0 | 0 | 0 | 0 | 0 | 0 |
| InBadVersions | 0 | 0 | 0 | 0 | 0 | 0 |
| InBadCommunityNames | 0 | 0 | 0 | 0 | 0 | 0 |
| InBadCommunityUses | 0 | 0 | 0 | 0 | 0 | 0 |
| InASNParseErrs | 0 | 0 | 0 | 0 | 0 | 0 |
| InTooBigs | 0 | 0 | 0 | 0 | 0 | 0 |
| InNoSuchNames | 0 | 0 | 0 | 0 | 0 | 0 |
| InBadValues | 0 | 0 | 0 | 0 | 0 | 0 |
| InReadOnlys | 0 | 0 | 0 | 0 | 0 | 0 |
| InGenErrs | 0 | 0 | 0 | 0 | 0 | 0 |

Table 26 describes the SNMP tab fields.

Table 26 SNMP tab fields

| Field | Description |
|----------------|--|
| InPkts | The total number of messages delivered to the SNMP from the transport service. |
| OutPkts | The total number of SNMP messages passed from the SNMP protocol to the transport service. |
| InTotalReqVars | The total number of MIB objects retrieved successfully by the SNMP protocol as the result of receiving valid SNMP Get-Request and Get-Next PDUs. |
| InTotalSetVars | The total number of MIB objects altered successfully by the SNMP protocol as the result of receiving valid SNMP Set-Request PDUs. |

Table 26 SNMP tab fields (continued)

| Field | Description |
|---------------------|---|
| InGetRequests | The total number of SNMP Get-Request PDUs that have been accepted and processed by the SNMP protocol. |
| InGetNexts | The total number of SNMP Get-Next PDUs accepted and processed by the SNMP protocol. |
| InSetRequests | The total number of SNMP Set-Request PDUs accepted and processed by the SNMP protocol. |
| InGetResponses | The total number of SNMP Get-Response PDUs accepted and processed by the SNMP protocol. |
| OutTraps | The total number of SNMP Trap PDUs generated by the SNMP protocol. |
| OutTooBigs | The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is tooBig. |
| OutNoSuchNames | The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is noSuchName. |
| OutBadValues | The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is badValue. |
| OutGenErrs | The total number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is genErr. |
| InBadVersions | The total number of SNMP messages delivered to the SNMP protocol for an unsupported SNMP version. |
| InBadCommunityNames | The total number of SNMP messages delivered to the SNMP protocol that used an unknown SNMP community name. |
| InBadCommunityUses | The total number of SNMP messages delivered to the SNMP protocol that represented an SNMP operation not allowed by the SNMP community named in the message. |
| InASNParseErrs | The total number of ASN.1 or BER errors encountered by the SNMP protocol when decoding received SNMP messages. |
| InTooBigs | The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is tooBig. |
| InNoSuchNames | The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is noSuchName. |
| InBadValues | The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is badValue. |

Table 26 SNMP tab fields (continued)

| Field | Description |
|-------------|--|
| InReadOnlys | The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is readOnly. It is a protocol error to generate an SNMP PDU containing the value "readOnly" in the error-status field. This object is provided to detect incorrect implementations of the SNMP. |
| InGenErrs | The total number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is genErr. |

IP tab

The IP tab shows IP information for the chassis.

To open the IP tab:

- 1 Select the chassis.
- 2 Do *one* of the following:
 - From Device Manager main menu, choose Graph > Chassis.
 - From the shortcut menu, choose Graph.
 - On the toolbar, click Graph.

The Chassis dialog box opens ([Figure 38 on page 82](#)) with the SNMP tab displayed.

- 3 Click the IP tab.

The IP tab opens ([Figure 39](#)).

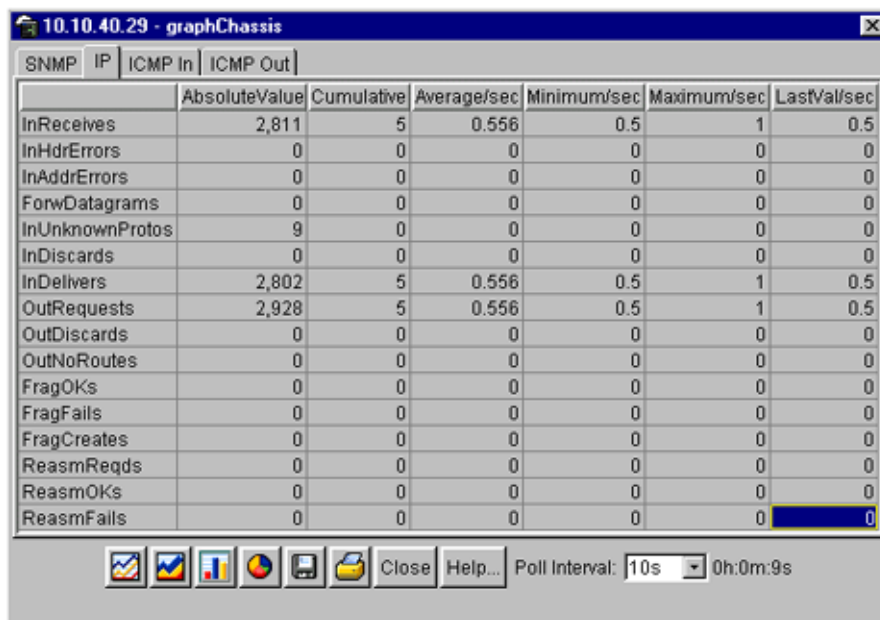
Figure 39 Graph Chassis dialog box — IP tab

Table 27 describes the Chassis IP tab fields

Table 27 Chassis IP tab fields

| Field | Description |
|--------------|--|
| InReceives | The total number of input datagrams received from interfaces, including those received in error. |
| InHdrErrors | The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options. |
| InAddrErrors | The number of input datagrams discarded because the IP address in the IP header destination field was not a valid address. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For addresses that are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address. |

Table 27 Chassis IP tab fields (continued)

| Field | Description |
|-----------------|--|
| ForwDatagrams | The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. For addresses that do not act as IP Gateways, this counter will include only those packets that were Source-Routed by way of this address and had successful Source-Route option processing. |
| InUnknownProtos | The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. |
| InDiscards | The number of input IP datagrams for which no problems were encountered to prevent their continued processing but that were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting reassembly. |
| InDelivers | The total number of input datagrams successfully delivered to IP user-protocols (including ICMP). |
| OutRequests | The total number of IP datagrams that local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams. |
| OutDiscards | The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but that were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion. |
| OutNoRoutes | The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter also includes any packets counted in ipForwDatagrams that have no route. Note that this includes any datagrams a host cannot route because all of its default gateways are down. |
| FragOKs | The number of IP datagrams that have been successfully fragmented at this entity. |
| FragFails | The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, for example, because their Don't Fragment flag was set. |
| FragCreates | The number of IP datagram fragments that have been generated as a result of fragmentation at this entity. |
| ReasmReqds | The number of IP fragments received that needed to be reassembled at this entity. |

Table 27 Chassis IP tab fields (continued)

| Field | Description |
|------------|---|
| ReasmOKs | The number of IP datagrams successfully reassembled. |
| ReasmFails | The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. |

ICMP In tab

The chassis ICMP In tab shows ICMP In statistics.

To open the ICMP In tab:

- 1 Select the chassis.
- 2 Do *one* of the following:
 - From Device Manager main menu, choose Graph > Chassis.
 - From the shortcut menu, choose Graph.
 - On the toolbar, click Graph.

The Chassis dialog box opens ([Figure 38 on page 82](#)) with the SNMP tab displayed.

- 3 Click the ICMP In tab.

The ICMP In tab opens ([Figure 40](#)).

Figure 40 Graph Chassis dialog box — ICMP In tab

| | AbsoluteValue | Cumulative | Average | Minimum | Maximum | LastValue |
|---------------|---------------|------------|---------|---------|---------|-----------|
| SrcQuenches | 0 | 0 | 0 | 0 | 0 | 0 |
| Redirects | 0 | 0 | 0 | 0 | 0 | 0 |
| Echos | 13 | 0 | 0 | 0 | 0 | 0 |
| EchoReps | 0 | 0 | 0 | 0 | 0 | 0 |
| Timestamps | 0 | 0 | 0 | 0 | 0 | 0 |
| TimestampReps | 0 | 0 | 0 | 0 | 0 | 0 |
| AddrMasks | 0 | 0 | 0 | 0 | 0 | 0 |
| AddrMaskReps | 0 | 0 | 0 | 0 | 0 | 0 |
| ParmProbs | 0 | 0 | 0 | 0 | 0 | 0 |
| DestUnreachs | 0 | 0 | 0 | 0 | 0 | 0 |
| TimeExcds | 0 | 0 | 0 | 0 | 0 | 0 |

Table 28 describes the ICMP In tab fields.

Table 28 ICMP In tab fields

| Field | Description |
|---------------|---|
| SrcQuenches | The number of ICMP Source Quench messages received. |
| Redirects | The number of ICMP Redirect messages received. |
| Echos | The number of ICMP Echo (request) messages received. |
| EchoReps | The number of ICMP Echo Reply messages received. |
| Timestamps | The number of ICMP Timestamp (request) messages received. |
| TimestampReps | The number of ICMP Timestamp Reply messages received. |
| AddrMasks | The number of ICMP Address Mask Request messages received. |
| AddrMaskReps | The number of ICMP Address Mask Reply messages received. |
| ParmProbs | The number of ICMP Parameter Problem messages received. |
| DestUnreachs | The number of ICMP Destination Unreachable messages received. |
| TimeExcds | The number of ICMP Time Exceeded messages received. |

ICMP Out tab

The chassis ICMP Out shows ICMP Out statistics.

To open the ICMP Out tab:

- 1 Select the chassis.
- 2 Do *one* of the following:
 - From Device Manager main menu, choose Graph > Chassis.
 - From the shortcut menu, choose Graph.
 - On the toolbar, click Graph.

The Chassis dialog box opens (Figure 38 on page 82) with the SNMP tab displayed.

- 3 Click the ICMP Out tab.

The ICMP Out tab opens (Figure 41).

Figure 41 Graph Chassis dialog box — ICMP Out tab

| | AbsoluteValue | Cumulative | Average | Minimum | Maximum | LastValue |
|---------------|---------------|------------|---------|---------|---------|-----------|
| SrcQuenchs | 0 | 0 | 0 | 0 | 0 | 0 |
| Redirects | 0 | 0 | 0 | 0 | 0 | 0 |
| Echoes | 0 | 0 | 0 | 0 | 0 | 0 |
| EchoReps | 13 | 0 | 0 | 0 | 0 | 0 |
| Timestamps | 0 | 0 | 0 | 0 | 0 | 0 |
| TimestampReps | 0 | 0 | 0 | 0 | 0 | 0 |
| AddrMasks | 0 | 0 | 0 | 0 | 0 | 0 |
| AddrMaskReps | 0 | 0 | 0 | 0 | 0 | 0 |
| ParmProbs | 0 | 0 | 0 | 0 | 0 | 0 |
| DestUnreachs | 3 | 0 | 0 | 0 | 0 | 0 |
| TimeExcds | 0 | 0 | 0 | 0 | 0 | 0 |

Table 29 describes the ICMP Out tab fields.

Table 29 ICMP Out tab fields

| Field | Description |
|---------------|--|
| SrcQuenchs | The number of ICMP Source Quench messages sent. |
| Redirects | The number of ICMP Redirect messages received. For a host, this object will always be zero, because hosts do not send redirects. |
| Echos | The number of ICMP Echo (request) messages sent. |
| EchoReps | The number of ICMP Echo Reply messages sent. |
| Timestamps | The number of ICMP Timestamp (request) messages sent. |
| TimestampReps | The number of ICMP Timestamp Reply messages sent. |
| AddrMasks | The number of ICMP Address Mask Request messages sent. |
| AddrMaskReps | The number of ICMP Address Mask Reply messages sent. |
| ParmProbs | The number of ICMP Parameter Problem messages sent. |
| DestUnreachs | The number of ICMP Destination Unreachable messages sent. |
| TimeExcds | The number of ICMP Time Exceeded messages sent. |

Switch Management

Configuration, monitoring and troubleshooting forms the functionality of Network management.

Baystack 425 supports the following three methods for set-up and management:

- **New Console Interface (CI):** A text-based user interface that is accessible inband (telnet) and out-of-band (serial console). The console features both a menu-driven interface, as well as a command line interface.
- **Web-Based UI:** An embedded HTTP server for inband management.
- **SNMP-Based:** Optivity and JDM applications for inband management.

Ease of use and configuration

Baystack 425 switch does not require VLAN, IP, or Spanning Tree configuration to power up and become operational.

The console/service port will be used as follows:

- Uploadable and downloadable configuration files.
- Persistence of unit configuration across reboots (save & restore)
- Users ability to refer to the desired port (port #) on the unit.
- Ability to configure the switch.

Switch configuration for Management

The switch can be managed and monitored by using SNMP-based network management applications. This function requires configuration of essential parameters such as the switch's IP address, sub-network mask, gateway address and SNMP community strings. This can be done via the local Console or an ASCII configuration file (downloaded through BootP).

TELNET sessions can be used remotely without the SNMP community string. You can configure the IP address, mask and the gateway address via the console/service using the menu-driven serial console interface (CI).

Gateway address is not necessary if a remote host or a Network Management Station (NMS) is on the same sub-network (the same Ethernet segment logically).

Momentary switch operation

Front panel momentary switch helps you to select Stacking or Standalone operational modes, which will be used for setting the base unit and resetting the switch.

As the baystack 425-48 hardware supports only standalone, you can use the push-button to reset the box. The other functionalities of the box will be disabled.

The functionalities of the momentary switch are:

- Set standalone mode: the 26th front panel port is enabled and the stack interface is disabled
- Set stacking mode: the 26th front panel port is disabled and the stack interface is enabled

- Set base unit mode (stacking mode)
- Reset/reboot.

The bicolor LED in the momentary switch will indicate your actions:

- Off - Configuration mode inactive.
- Green blinking – Configuration mode active, wait for user input.
- Green solid – Command accepted
- Amber – Error.

To operate the temporary switch:

- 1** Each command has a assigned code.
 - Standalone – 1.
 - Stacking – 2.
 - Base unit – 3
 - Reset/reboot – 4.
- 2** If you keep the button pressed for three seconds, the software will detect the switch to be in configuration mode. You will notice the LED turning green and blinking.
- 3** The user will press N times the push-button – N is the code assigned to a certain command.
- 4** To confirm, keep the button pressed for 3 seconds. The LED will turn either to solid-green (command accepted) or to solid-amber (error). After a period (5 seconds) the LED will turn Off.
- 5** The software will change to “before config” mode, if you enter an invalid command or fail to confirm.

If the command is accepted, NVRAM will store the result (mode) and when you reboot that particular unit will change to the new mode.

To abort a command, do not confirm the configuration and wait for a timeout period (5 seconds) and your input will be ignored. This action will make the momentary switch change back to either the “pre-config” state.

Chapter 3

Configuring and graphing ports

This chapter describes how you use Device Manager to configure and graph ports on a Baystack 425 Switch.

The windows displayed when you configure a single port differ from the ones displayed when you configure multiple ports. However, the options are similar.

Viewing and editing a single port configuration

To view or edit the configuration of a single or multiple ports:

- 1 Double-click on a single port or select the ports you want to edit.
- 2 Do one of the following:
 - From the shortcut menu, choose Edit.
 - From the Device Manager main menu, choose Edit > Port.
 - Double-click on the selected port.
 - On the toolbar, click Edit.



Note: When you edit a single port, tabs that are not applicable are not available for you to select.

When you edit multiple ports, some tabs are not available, and some tabs are available even though the options are not applicable. When the option does not apply for a given port, NoSuchObject is displayed.

The following sections provide a description of the tabs in the Edit Port dialog box, and details about each field on the tab.

- [“EAPOL tab for multiple ports](#)

Interface tab for a single port

The Interface tab shows the basic configuration and status of a single port.

To view the Interface tab:

- 1 Select the port you want to edit.
- 2 Do one of the following:
 - Double-click on the selected port
 - From the shortcut menu, choose Edit.
 - From the Device Manager main menu, choose Edit > Port.
 - On the toolbar, click Edit button.

The Port dialog box for a single port opens ([Figure 42](#)) with the Interface tab displayed.

Figure 42 Port dialog box — Interface tab

The screenshot shows a window titled "10.10.54.26 - Port 1/1" with tabs for "Interface", "VLAN", "STG", and "EAPOL". The "Interface" tab is active, displaying the following configuration details:

- Index: 1
- Name: This is port number 1
- Descr: Nortel Networks BayStack 425_48T Ethernet Switch Module - Port 1
- Type: ethernet-csmacd
- Mtu: 1514
- PhysAddress: 00:0f:6a:7d:c2:a0
- AdminStatus: up down
- OperStatus: down
- LastChange: 39 days, 05h:01m:00s
- LinkTrap: enabled disabled
- Speed: 100000000

AutoNegotiate:

AdminDuplex: half full

OperDuplex: full

AdminSpeed: none mbps10 mbps100 mbps1000

OperSpeed: 100 mbps

AutoNegotiationCapability: 10Half,10Full,100Half,100Full

AutoNegotiationAdvertisements:

| | | |
|---|--|---|
| <input checked="" type="checkbox"/> 10Half | <input checked="" type="checkbox"/> 10Full | <input checked="" type="checkbox"/> 100Half |
| <input checked="" type="checkbox"/> 100Full | <input type="checkbox"/> 1000Half | <input type="checkbox"/> 1000Full |
| <input type="checkbox"/> PauseFrame | <input type="checkbox"/> AsymPauseFrame | |

Mbit: 0

IsPortShared: portNotShared

PortActiveComponent: fixedPort

Buttons: Apply, Refresh, Close, Help...



Note: 10/100BASE-TX ports may not autonegotiate correctly with older 10/100BASE-TX equipment. In some cases, the older devices can be upgraded with new firmware or driver revisions. If an upgrade does not allow autonegotiation to correctly identify the link speed and duplex settings, you can manually configure the settings for the link in question. Check the Nortel Networks Web site (support.baynetworks.com/software) for the latest compatibility information.

Table 30 describes the Interface tab items for a single port.

Table 30 Interface tab items for a single port

| Field | Description |
|-------------|---|
| Index | A unique value assigned to each interface. The value ranges between 1 and 512. |
| Name | Specifies a name for the port. |
| Descr | The type of switch and number of ports. |
| Type | The media type of this interface. |
| Mtu | The size of the largest packet, in octets, that can be sent or received on the interface. |
| PhysAddress | The MAC address assigned to a particular interface. |
| AdminStatus | <p>The current administrative state of the interface, which can be one of the following:</p> <ul style="list-style-type: none"> • up • down <p>When a managed system is initialized, all interfaces start with AdminStatus in the down state. AdminStatus changes to the up state (or remains in the down state) as a result of either management action or the configuration information available to the managed system.</p> |
| OperStatus | <p>The current operational state of the interface, which can be one of the following:</p> <ul style="list-style-type: none"> • up • down • testing <p>If AdminStatus is up, then OperStatus should be up if the interface is ready to transmit and receive network traffic. If AdminStatus is down, then OperStatus should be down. It should remain in the down state if and only if there is a fault that prevents it from going to the up state. The testing state indicates that no operational packets can be passed.</p> |

Table 30 Interface tab items for a single port (continued)

| Field | Description |
|-------------------------------|---|
| LastChange | The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero. |
| LinkTrap | Specifies whether linkUp/linkDown traps should be generated for this interface |
| Speed | Current speed. |
| AutoNegotiate | Indicates whether this port is enabled for autonegotiation or not. |
| AdminDuplex | The current administrative duplex mode of the port (half or full). |
| AdminSpeed | Set the port's speed. |
| OperSpeed | The current operating speed of the port. |
| MtId | The MultiLink Trunk to which the port is assigned (if any). |
| OperDuplex | The current mode of the port (half duplex or full duplex). |
| IsPortShared | Specifies whether a port is shared. Multiple ports that are logically represented as a single port are shared. Only one shared port may be active at a time. |
| PortActiveComponent | Specifies the physical port components that are active for a shared port. |
| AutoNegotiationCapability | Specifies the port speed and duplex capabilities that a switch can support on a port, and that may be advertised by the port using auto-negotiation |
| AutoNegotiationAdvertisements | Specifies the port speed and duplex abilities to be advertised during link negotiation. |

VLAN tab for a single port

The VLAN tab allows you to view the VLAN membership for a single port.

To view the VLAN tab:

- 1 Select the port you want to edit.
- 2 Do one of the following:
 - Double-click the selected port
 - From the shortcut menu, choose Edit.
 - From the Device Manager main menu, choose Edit > Port.
 - On the toolbar, click Edit.

The Port dialog box for a single port opens (Figure 42 on page 95) with the Interface tab displayed.

3 Click the VLAN tab.

The VLAN tab opens (Figure 43).

Figure 43 Edit Port dialog box — VLAN tab

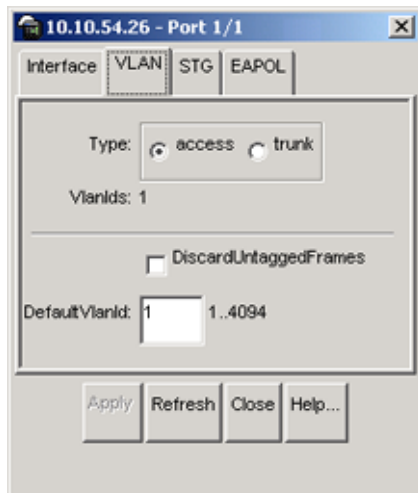


Table 31 describes the VLAN tab items.

Table 31 VLAN tab items for a single port

| Item | Description |
|-----------------------|---|
| Type | Indicates the type of VLAN port (Trunk or Access port). If the port is a trunk port, the port is probably a member of more than one VLAN. If the port is an access port, the port can only be a member of one VLAN if there is no membership conflict. |
| VlanIds | The VLANIDs of which this port is a member. |
| DiscardUntaggedFrames | This field only applies to trunk ports. It acts as a flag used to determine how to process untagged frames received on this port. When the flag is set, the frames are discarded by the forwarding process. When the flag is reset, the frames are assigned to the VLAN specified by rcVlanPortDefaultVlanId. |
| DefaultVlanId | The VLAN ID assigned to untagged frames received on a trunk port. |

STG tab for a single port

In the Spanning Tree Group (STG) tab, you can view the status and modify the configuration of a port's spanning tree parameters.

To view the STG tab:

- 1 Select the port you want to edit.
- 2 Do one of the following:
 - Double-click the selected port.
 - From the shortcut menu, choose Edit.
 - From the Device Manager main menu, choose Edit > Port.
 - On the toolbar, click Edit.

The Port dialog box for a single port opens (Figure 42 on page 95) with the Interface tab displayed.

- 3 Click the STG tab.

The STG tab opens (Figure 44).

Figure 44 Edit Port dialog box — STG tab

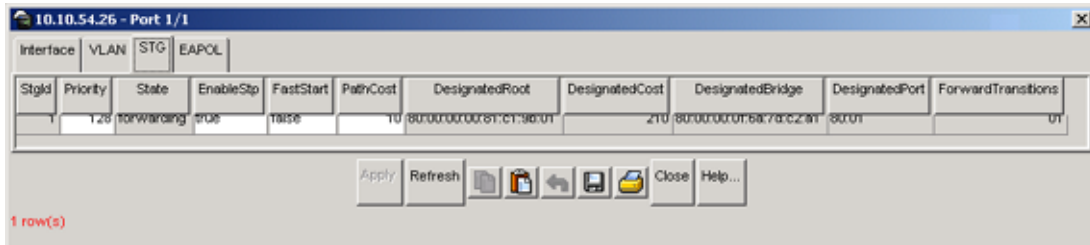


Table 32 describes the STG tab items.

Table 32 STG tab items for a single port

| Item | Description |
|--------------------|---|
| StgId | The number of times this port has transitioned from the Learning state to the Forwarding state. |
| Priority | The value of the priority field that is contained in the first (in network byte order) octet of the (2-octet long) Port ID. The other octet of the Port ID is derived from the value of dot1dStpPort. |
| State | The port's current state as defined by application of the Spanning Tree Protocol. This state controls the action a port takes when it receives a frame. If the bridge detects a port that is malfunctioning, it places that port into the broken state. For ports that are disabled (see EnableStp), this object has a value of disabled. |
| EnableStp | Allows you to select true or false to enable or disable STP. |
| FastStart | Allows you to select true or false to enable or disable FastStart. |
| PathCost | The contribution of this port to the cost of paths toward the spanning tree root, which include this port. The IEEE 802.1D-1990 standard recommends that the default value of this parameter be in inverse proportion to the speed of the attached LAN. |
| DesignatedRoot | The unique Bridge Identifier of the bridge recorded as the Root in the Configuration BPDUs transmitted by the Designated Bridge for the segment to which the port is attached. |
| DesignatedCost | The path cost of the Designated Port of the segment connected to this port. This value is compared to the Root Path Cost field in received bridge PDUs. |
| DesignatedBridge | The Bridge Identifier of the bridge that this port considers to be the Designated Bridge for this port's segment. |
| DesignatedPort | The Port Identifier of the port on the Designated Bridge for this port's segment. |
| ForwardTransitions | The number of times this port has transitioned from the Learning state to the Forwarding state. |

EAPOL tab for a single port

The EAPOL tab allows you to configure EAPOL-based security for a single port.

To view the EAPOL tab:

- 1** Select the port you want to edit.
- 2** Do one of the following:
 - Double-click the selected port
 - From the shortcut menu, choose Edit.
 - From the Device Manager main menu, choose Edit > Port.
 - On the toolbar, click Edit.

The Port dialog box for a single port opens ([Figure 42](#)) with the Interface tab displayed.

- 3** Click the EAPOL tab.

The EAPOL tab opens ([Figure 45](#)).

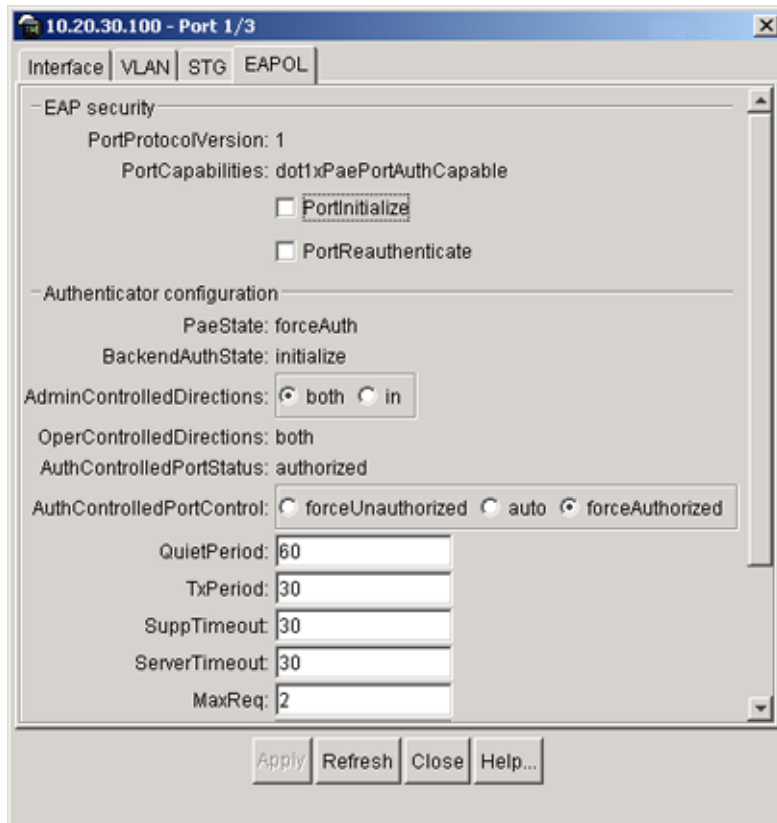
Figure 45 Edit Port dialog box — EAPOL tab

Table 33 describes the EAPOL tab items.

Table 33 EAPOL tab items for a single port

| Item | Description |
|---------------------|--|
| PortProtocolVersion | The EAP Protocol version that is running on this port. |
| PortCapabilities | The PAE functionality that is implemented on this port. Always returns dot1xPaePortAuthCapable(0). |
| PortInitialize | Setting this attribute to True causes this port's EAPOL state to be initialized. |
| PortReauthenticate | Setting this attribute to True causes the reauthentication of the client. |
| PaeState | The current authenticator PAE state machine stat value. |

Table 33 EAPOL tab items for a single port (continued)

| Item | Description |
|---------------------------|--|
| BackendAuthState | The current state of the Backend Authentication state machine. |
| AdminControlledDirections | The current value of the administrative controlled directions parameter for the port. |
| OperControlledDirections | The current value of the operational controlled directions parameter for the port. |
| AuthControlledPortStatus | The current value of the controlled port status parameter for the port. |
| AuthControlledPortControl | The current value of the controlled port control parameter for the port. |
| QuietPeriod | The current value of the time interval between authentication failure and the start of a new authentication. |
| TxPeriod | Time to wait for response from supplicant for EAP requests/ Identity packets. |
| SuppTimeout | Time to wait for response from supplicant for all EAP packets except EAP Request/Identity. |
| ServerTimeout | Time to wait for a response from the RADIUS server |
| MaxReq | Number of times to retry sending packets to the supplicant. |
| ReAuthPeriod | Time interval between successive re-authentications. |
| ReAuthEnabled | Whether to re-authenticate or not. Setting this object to Enabled causes reauthentication of existing supplicant at the time interval specified in the Re-authentication Period field. |
| KeyTxEnabled | The value of the KeyTransmissionEnabled constant currently in use by the Authenticator PAE state machine. This always returns false as key transmission is irrelevant. |
| LastEapolFrameVersion | The protocol version number carried in the most recently received EAPOL frame. |
| LastEapolFrameSource | The source MAC address carried in the most recently received EAPOL frame. |

Viewing and editing multiple port configurations

To view or edit the configurations of multiple ports:

- 1 Select the ports you want to edit.

Press [Ctrl] + left click the ports you want to view or configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- Double-click on the selected port.
- On the toolbar, click Edit.



Note: When you edit multiple ports, some tabs are not available, and some tabs are available even though the options are not applicable. When the option does not apply for a given port, NoSuchObject is displayed.

Graphing multiple ports

You can graph port statistics from the graph port dialog box.

To open the graph port dialog box:

1 Select the port or ports you want to graph.

2 Do one of the following:

- From the shortcut menu, choose Graph.
- From the Device Manager main menu, choose Graph > Port.
- On the toolbar, click Graph.



The following sections discuss the graph port statistics tabs with descriptions of the statistics.



Note: Some statistics are only available when you graph a single port.

Interface tab for multiple ports

The Interface tab shows the basic configuration and status of the selected ports.

To view or edit the Interface tab for multiple ports:

- 1 Select the ports that you want to edit.
[Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the shortcut menu, choose Edit.
- From the Device Manager main menu, choose Edit > Port.
- On the toolbar, click Edit.

The Interface tab ([Figure 46](#)) shows port interface statistics.

Figure 46 Port dialog box — Interface tab

| Index | Port | Name | Descr | Type | Mtu | PhysAddress | AdminStatus | OperStatus | LastChange | Speed | AutoNegotiate | AdminDuplex | OperDuplex | AdminSpeed | OperSpeed | Mbit | bitrate |
|-------|------|------|---------|---------|-------|----------------------|-------------|------------|---------------|---------|---------------|-------------|------------|------------|-----------|------|---------|
| 3 | 113 | | none... | etne... | 15... | 00:00:00:00:00:00... | up | down | 35 days, 1... | 1000... | true | full | full | 1000000 | 100 | 0 | portN |
| 5 | 115 | | none... | etne... | 15... | 00:00:00:00:00:00... | up | down | 35 days, 1... | 1000... | true | full | full | 1000000 | 100 | 0 | portN |
| 7 | 117 | | none... | etne... | 15... | 00:00:00:00:00:00... | up | down | 35 days, 1... | 1000... | true | full | full | 1000000 | 100 | 0 | portN |

[Table 34](#) describes the Interface tab fields.

Table 34 Interface tab fields for multiple ports

| Field | Description |
|-------------|--|
| Index | A unique value assigned to each interface. The value ranges between 1 and 255. |
| Port | Number of Unit and Port Number. |
| Name | Allows you to enter a character string to name the port |
| Descr | Type of switch and number of ports. |
| Type | Media type for this interface. |
| Mtu | Size of the largest packet, in octets, that can be sent or received on the interface. |
| PhysAddress | MAC address assigned to a particular interface. |
| AdminStatus | Current administrative state of the interface, which can be one of the following: <ul style="list-style-type: none"> • up • down When a managed system is initialized, all interfaces start with AdminStatus in the down state. AdminStatus changes to the up state (or remains in the down state) as a result of either management action or the configuration information available to the managed system. |

Table 34 Interface tab fields for multiple ports (continued)

| Field | Description |
|-------------------------------|---|
| OperStatus | <p>Current operational state of the interface, which can be one of the following:</p> <ul style="list-style-type: none"> • up • down • testing <p>If AdminStatus is up, then OperStatus should be up if the interface is ready to transmit and receive network traffic. If AdminStatus is down, then OperStatus should be down. It should remain in the down state if and only if there is a fault that prevents it from going to the up state. The testing state indicates that no operational packets can be passed.</p> |
| LastChange | Value of the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero. |
| LinkTrap | Specifies whether linkUp/linkDown traps should be generated for this interface |
| Speed | The estimate bandwidth of the interface in bits per second (bps). For interfaces that do not vary in bandwidth or have no way to estimate the bandwidth, this object should contain the nominal bandwidth. If the bandwidth of the interface is greater than the maximum value reported by the object, then the object displays its maximum value (4,294,967,295). For a sub-layer that has no concept of bandwidth, the object should be zero. |
| AutoNegotiate | Indicates whether the port is enabled (checked) for autonegotiation or not. |
| AdminDuplex | The current administrative duplex mode of the port (half or full). |
| OperDuplex | Indicate current duplex value of the port. |
| AdminSpeed | Set the speed of a port: none, mbps10, and mbps100 |
| OperSpeed | The current operating speed of the port. |
| MltId | The MultiLink Trunk to which the port is assigned (if any). |
| IsPortShared | Specifies whether a port is shared. Multiple ports that are logically represented as a single port are shared. Only one shared port may be active at a time. |
| PortActiveComponent | Specifies the physical port components that are active for a shared port. |
| AutoNegotiationCapability | Specifies the port speed and duplex capabilities that a switch can support on a port, and that may be advertised by the port using auto-negotiation |
| AutoNegotiationAdvertisements | Specifies the port speed and duplex abilities to be advertised during link negotiation. |

VLAN tab for multiple ports

The VLAN tab shows the VLAN membership for the selected ports.

To view or edit the Interface tab for multiple ports:

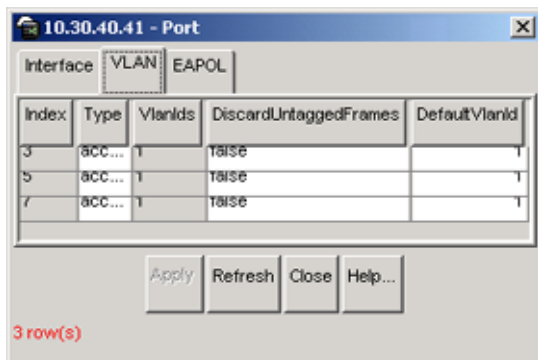
- 1 Select the ports that you want to edit.
[Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.
- 2 Do one of the following:
 - From the shortcut menu, choose Edit.
 - From the Device Manager main menu, choose Edit > Port.
 - On the toolbar, click Edit.

The Port dialog box for a multiple port (Figure 42 on page 95) opens with the Interface tab displayed.

- 3 Click the VLAN tab.

The VLAN tab opens (Figure 47).

Figure 47 VLAN tab for multiple ports



[Table 35](#) describes the VLAN tab fields for multiple ports.

Table 35 VLAN tab fields for multiple ports

| Field | Description |
|-----------------------|---|
| Type | Indicates the type of VLAN port (Trunk or Access port). If the port is a trunk port, the port is probably a member of more than one VLAN. If the port is an access port, the port can only be a member of one VLAN if there is no membership conflict. |
| VlanIds | The VLANIDs of which this port is a member. |
| DiscardUntaggedFrames | This field only applies to trunk ports. It acts as a flag used to determine how to process untagged frames received on this port. When the flag is set, the frames are discarded by the forwarding process. When the flag is reset, the frames are assigned to the VLAN specified by rcVlanPortDefaultVlanId. |
| DefaultVlanId | The VLAN ID assigned to untagged frames received on a trunk port. |

EAPOL tab for multiple ports

The EAPOL tab shows EAPOL statistics for the selected ports.

To view or edit the EAPOL tab for multiple ports:

- 1 Select the ports that you want to edit.
[Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.
- 2 Do one of the following:
 - From the shortcut menu, choose Edit.
 - From the Device Manager main menu, choose Edit > Port.
 - On the toolbar, click Edit.

The Port dialog box for a multiple port ([Figure 42](#)) opens with the Interface tab displayed.

- 3 Click the EAPOL tab.

The EAPOL tab opens ([Figure 48](#)).

Figure 48 EAPOL tab for multiple ports

| Index | PortProtocolVersion | PortCapabilities | PortInitialize | PortReauthenticate | PaeState | BackendAuthState | AdminControlledDirections | OperControlledDirections | AuthControlledPortStatus |
|-------|---------------------|------------------|----------------|--------------------|-----------|------------------|---------------------------|--------------------------|--------------------------|
| 1 | 1 | dot1xPaePortA... | false | false | forceAuth | initialize | both | both | authorize |
| 3 | 1 | dot1xPaePortA... | false | false | forceAuth | initialize | both | both | authorize |
| 5 | 1 | dot1xPaePortA... | false | false | forceAuth | initialize | both | both | authorize |
| 7 | 1 | dot1xPaePortA... | false | false | forceAuth | initialize | both | both | authorize |

[Table 36](#) describes the EAPOL tab fields for multiple ports.

Table 36 EAPOL tab fields for multiple ports

| Field | Description |
|---------------------------|--|
| Index | Displays the unique value assigned to each interface. |
| PortProtocolVersion | The EAP Protocol version that is running on this port. |
| PortCapabilities | The PAE functionality that is implemented on this port. Always returns dot1xPaePortAuthCapable(0). |
| PortInitialize | Setting this attribute to True causes this port's EAPOL state to be initialized. |
| PortReauthenticate | Setting this attribute to True causes the reauthentication of the client. |
| PaeState | The current authenticator PAE state machine stat value. |
| BackendAuthState | The current state of the Backend Authentication state machine. |
| AdminControlledDirections | The current value of the administrative controlled directions parameter for the port. |
| OperControlledDirections | The current value of the operational controlled directions parameter for the port. |
| AuthControlledPortStatus | The current value of the controlled port status parameter for the port. |
| AuthControlledPortControl | The current value of the controlled port control parameter for the port. |
| QuietPeriod | The current value of the time interval between authentication failure and the start of a new authentication. |
| TxPeriod | Time to wait for response from supplicant for EAP requests/Identity packets. |

Table 36 EAPOL tab fields for multiple ports (continued)

| Field | Description |
|-----------------------|--|
| SuppTiemout | Time to wait for response from supplicant for all EAP packets except EAP Request/Identity. |
| ServerTimeout | Time to wait for a response from the RADIUS server |
| MaxReq | Number of times to retry sending packets to the supplicant. |
| ReAuthPeriod | Time interval between successive re-authentications. |
| ReAuthEnabled | Whether to re-authenticate or not. Setting this object to Enabled causes reauthentication of existing supplicant at the time interval specified in the Re-authentication Period field. |
| KeyTxEnabled | The value of the KeyTransmissionEnabled constant currently in use by the Authenticator PAE state machine. This always returns false as key transmission is irrelevant. |
| LastEapolFrameVersion | The protocol version number carried in the most recently received EAPOL frame. |
| LastEapolFrameSource | The source MAC address carried in the most recently received EAPOL frame. |

Graphing port statistics

You can graph statistics for either a single port or multiple ports from the graphPort dialog box. The windows displayed are identical for either single or multiple port configuration.

To open the graphPort dialog box for graphing:

- 1 Select the port or ports you want to graph.

To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

- 2 Do one of the following:

- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The graphPort dialog box for a single port ([Figure 49 on page 112](#)) or for multiple ports opens with the Interface tab displayed.

- “EAPOL Stats tab for graphing ports
- “EAPOL Diag tab for graphing ports

Interface tab for graphing ports

The Interface tab shows interface parameters for graphing a port or ports.

To open the Interface tab for graphing:

- 1 Select the port or ports you want to graph.

To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

- 2 Do one of the following:

- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port ([Figure 49 on page 112](#)) or for multiple ports opens with the Interface tab displayed.

Figure 49 Interface tab for graphing ports

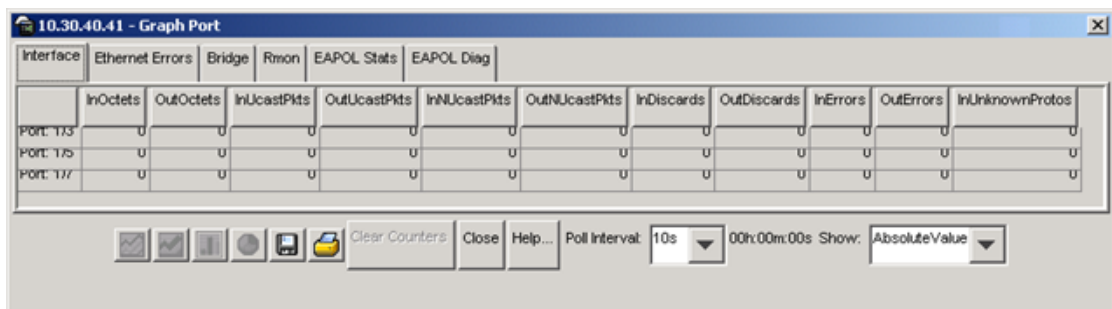


Table 37 describes the Interface tab fields for graphing ports.

Table 37 Port Interface tab fields for multiple ports

| Field | Description |
|-----------------|---|
| ifInOctets | The total number of octets received on the interface, including framing characters. |
| ifOutOctets | The total number of octets transmitted out of the interface, including framing characters. |
| ifInUcastPkts | The number of packets delivered by this sublayer to a higher sublayer that were not addressed to a multicast or broadcast address at this sublayer. |
| ifOutUcastPkts | The number of packets that higher-level protocols requested be transmitted that were not addressed to a multicast address at this sublayer. This total number includes those packets discarded or unsent. |
| ifInNUcastPkts | The number of packets delivered by this sublayer to a higher (sub)layer, which were addressed to a multicast or broadcast address at this sublayer. |
| ifOutNUcastPkts | The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast or broadcast address at this sublayer, including those that were discarded or not sent. |
| InDiscards | The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space. |
| OutDiscards | The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space. |
| InErrors | For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol. |

Table 37 Port Interface tab fields for multiple ports (continued)

| Field | Description |
|-----------------|--|
| OutErrors | For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors. |
| InUnknownProtos | For packet-oriented interfaces, the number of packets received via the interface that were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of transmission units received via the interface that were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter will always be 0. |

Ethernet Errors tab for graphing ports

The port Ethernet Errors tab shows port Ethernet Errors statistics.

To open the Ethernet Errors tab for graphing:

- 1 Select the port or ports you want to graph.

To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port (Figure 42 on page 95) or for multiple ports opens with the Interface tab displayed.

3 Click the Ethernet Errors tab.

The Ethernet Errors tab opens (Figure 50).

Figure 50 Graph Port dialog box — Ethernet Errors tab

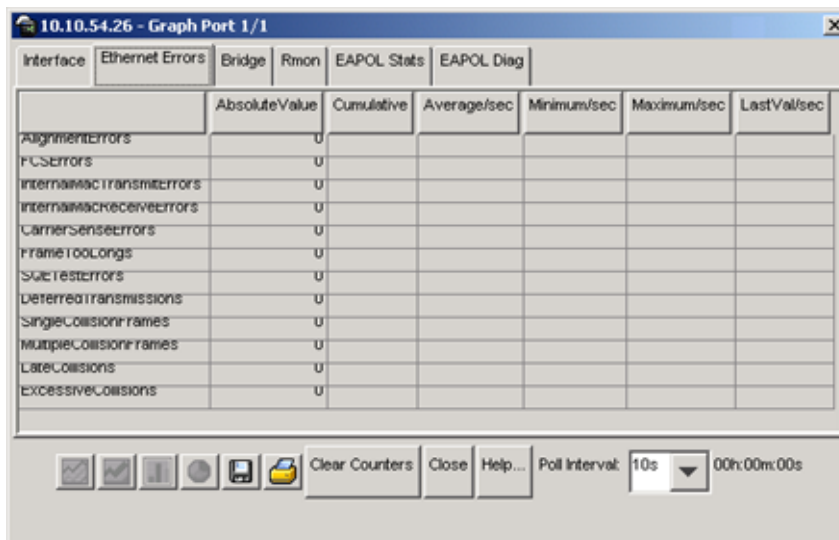


Table 38 describes the Ethernet Errors tab fields.

Table 38 Ethernet Errors tab fields

| Field | Description |
|---------------------------|--|
| AlignmentErrors | A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. |
| FCSErrors | A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. |
| InternalMacTransmitErrors | A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions object, the ExcessiveCollisions object, or the CarrierSenseErrors object. |
| InternalMacReceiveErrors | A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLongs object, the AlignmentErrors object, or the FCSErrors object. The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted. |
| CarrierSenseErrors | The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt. |

Table 38 Ethernet Errors tab fields (continued)

| Field | Description |
|-------------------------|---|
| FrameTooLongs | A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. |
| SQETestErrors | A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message 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. |
| DeferredTransmissions | A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions. |
| SingleCollisionFrames | A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the MultipleCollisionFrames object. |
| MultipleCollisionFrames | A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object. |
| LateCollisions | The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics. |
| ExcessiveCollisions | A count of frames for which transmission on a particular interface fails due to excessive collisions. |

Bridge tab for graphing ports

The Bridge tab displays port frame statistics.

To open the Bridge tab for graphing:

- 1 Select the port or ports you want to graph.

To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

- 2 Do one of the following:

- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port (Figure 42 on page 95) or for multiple ports opens with the Interface tab displayed.

- 3 Click the Bridge tab.

The Bridge tab for graphing ports opens (Figure 51).

Figure 51 Graph Port dialog box — Bridge tab

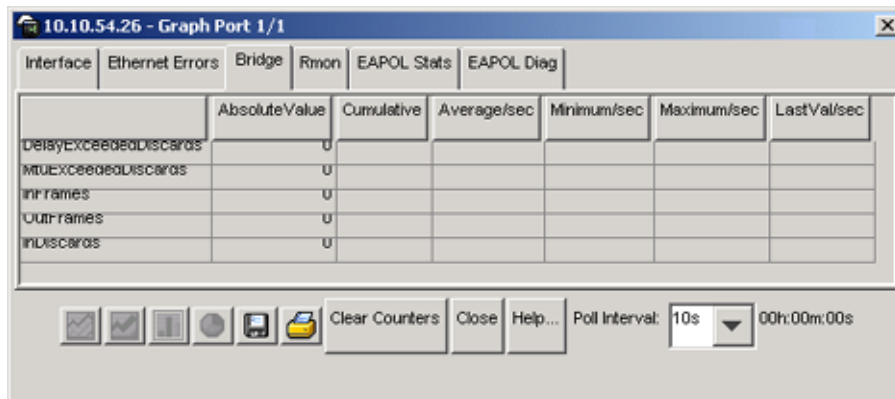


Table 39 describes the Bridge tab fields.

Table 39 Bridge tab fields

| Field | Description |
|-----------------------|--|
| DelayExceededDiscards | Number of frames discarded by the port due to excessive transit delays through the bridge. It is incremented by both transparent and source route bridges. |
| MtuExceededDiscards | Number of frames discarded by the port due to an excessive size. It is incremented by both transparent and source route bridges. |
| InFrames | The number of frames that have been received by this port from its segment. |
| OutFrames | The number of frames that have been received by this port from its segment. |
| InDiscards | Count of valid frames received which were discarded (filtered) by the Forwarding Process. |

RMON tab

The RMON tab displays Ethernet statistics for graphing a port or ports.

To open the RMON tab for graphing:

- 1 Select the port or ports you want to graph.

To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

2 Do one of the following:

- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The Port dialog box for a single port (Figure 42 on page 95) or for multiple ports opens with the Interface tab displayed.

3 Click the RMON tab.

The RMON tab for graphing ports opens (Figure 52).

Figure 52 Graph Port dialog box — RMON tab

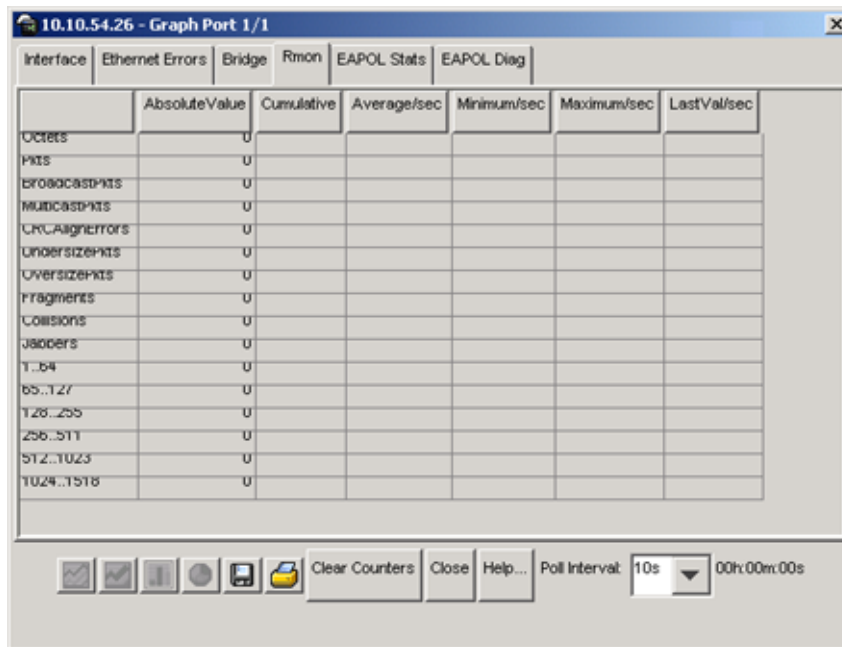


Table 40 describes the RMON tab fields.

Table 40 RMON tab fields

| Field | Description |
|-----------------|---|
| Octets | The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). You can use this object as a reasonable estimate of Ethernet utilization. For greater precision, sample the etherStatsPkts and etherStatsOctets objects before and after a common interval. |
| Pkts | The total number of packets (including bad packets, broadcast packets, and multicast packets) received. |
| BroadcastPkts | The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets. |
| MulticastPkts | The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address. |
| CRCAAlignErrors | The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). |
| UndersizePkts | The total number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed. |
| OversizePkts | The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed. |
| Fragments | The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). It is entirely normal for etherStatsFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits. |
| Collisions | The best estimate of the total number of collisions on this Ethernet segment. |
| Jabbers | The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. |

Table 40 RMON tab fields (continued)

| Field | Description |
|------------|---|
| <=64 | The total number of packets (including bad packets) received that were less than or equal to 64 octets in length (excluding framing bits but including FCS octets). |
| 65 - 127 | The total number of packets (including bad packets) received that were greater than 64 octets in length (excluding framing bits but including FCS octets). |
| 128 - 255 | The total number of packets (including bad packets) received that were greater than 127 octets in length (excluding framing bits but including FCS octets). |
| 256 - 511 | The total number of packets (including bad packets) received that were greater than 255 octets in length (excluding framing bits but including FCS octets). |
| 512 - 1023 | The total number of packets (including bad packets) received that were greater than 511 octets in length (excluding framing bits but including FCS octets). |
| 1024-1518 | The total number of packets (including bad packets) received that were greater than 1023 octets in length (excluding framing bits but including FCS octets). |
| >1518 | The total number of packets (including bad packets) received that were greater than 1518 octets in length (excluding framing bits but including FCS octets). |

EAPOL Stats tab for graphing ports

The EAPOL Stats tab displays EAPOL statistics.

To open the EAPOL Stats tab for graphing:

- 1 Select the port or ports you want to graph.
To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.
- 2 Do one of the following:
 - From the Device Manager main menu, choose Graph > Port.
 - From the shortcut menu, choose Graph.
 - On the toolbar, click Graph.

The Port dialog box for a single port or for multiple ports opens with the Interface tab displayed.

3 Click the EAPOL Stats tab.

The EAPOL Stats tab for graphing multiple ports opens (Figure 53).

Figure 53 Graph Port dialog box — EAPOL Stats tab

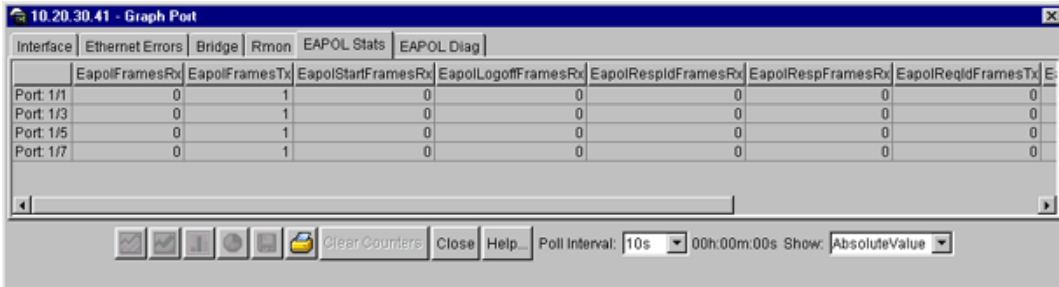


Table 41 describes the EAPOL stats tab fields.

Table 41 EAPOL tab stats fields

| Field | Description |
|---------------------|--|
| EapolFramesRx | The number of valid EAPOL frames of any type that have been received by this authenticator. |
| EapolFramesTx | The number of EAPOL frame types of any type that have been transmitted by this authenticator. |
| EapolStartFramesRx | The number of EAPOL start frames that have been received by this authenticator. |
| EapolLogoffFramesRx | The number of EAPOL Logoff frames that have been received by this authenticator. |
| EapolRespIdFramesRx | The number of EAPOL Resp/Id frames that have been received by this authenticator. |
| EapolRespFramesRx | The number of valid EAP Response frames (Other than Resp/Id frames) that have been received by this authenticator. |
| EapolReqIdFramesTx | The number of EAPOL Req/Id frames that have been transmitted by this authenticator. |
| EapolReqFramesTx | The number of EAP Req/Id frames (Other than Rq/Id frames) that have been transmitted by this authenticator. |

Table 41 EAPOL tab stats fields (continued)

| Field | Description |
|------------------------|--|
| InvalidEapolFramesRx | The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized. |
| EapLengthErrorFramesRx | The number of EAPOL frames that have been received by this authenticator in which the packet body length field is not valid. |

EAPOL Diag tab for graphing ports

The EAPOL Diag tab displays EAPOL diagnostics statistics.

To open the EAPOL Diag tab for graphing:

- 1 Select the port or ports you want to graph.
To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.
- 2 Do one of the following:
 - From the Device Manager main menu, choose Graph > Port.
 - From the shortcut menu, choose Graph.
 - On the toolbar, click Graph.

The Port dialog box for a single port or for multiple ports opens with the Interface tab displayed.

- 3 Click the EAPOL Diag tab.
The EAPOL Diag tab for graphing multiple ports opens ([Figure 54](#)).

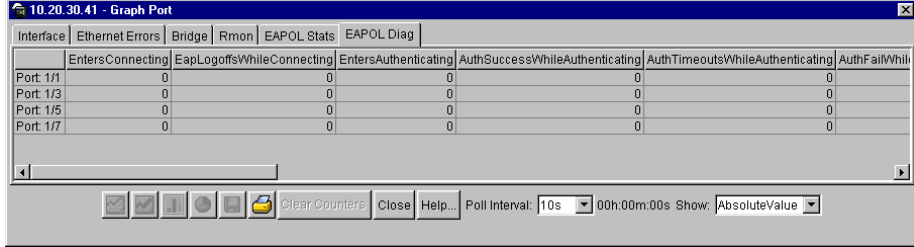
Figure 54 Graph Port dialog box — EAPOL Diag tab

Table 42 describes the EAPOL Diag tab fields.

Table 42 EAPOL Diag tab fields

| Field | Description |
|----------------------------------|---|
| EntersConnecting | Counts the number of times that the state machine transitions to the connecting state from any other state. |
| EapLogoffsWhileConnecting | Counts the number of times that the state machine transitions from connecting to disconnecting as a result of receiving an EAPOL-Logoff message. |
| EntersAuthenticating | Counts the number of times that the state machine transitions from connecting to authenticating, as a result of an EAP-Response or Identity message being received from the Supplicant. |
| AuthSuccessWhileAuthenticating | Counts the number of times that the state machine transitions from authenticating to authenticated, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant. |
| AuthTimeoutsWhileAuthenticating | Counts the number of times that the state machine transitions from authenticating to aborting, as a result of the Backend Authentication state machine indicating authentication timeout. |
| AuthFailWhileAuthenticating | Counts the number of times that the state machine transitions from authenticating to held, as a result of the Backend Authentication state machine indicating authentication failure. |
| AuthReauthsWhileAuthenticating | Counts the number of times that the state machine transitions from authenticating to aborting, as a result of a reauthentication request. |
| AuthEapStartsWhileAuthenticating | Counts the number of times that the state machine transitions from authenticating to aborting, as a result of an EAPOL-Start message being received from the Supplicant. |

Table 42 EAPOL Diag tab feilds

| Field | Description |
|--------------------------------------|--|
| AuthEapLogoffWhileAuthenticating | Counts the number of times that the state machine transitions from authenticating to aborting, as a result of an EAPOL-Logoff message being received from the Supplicant. |
| AuthReauthsWhileAuthenticated | Counts the number of times that the state machine transitions from authenticated to connecting, as a result of a reauthentication request. |
| AuthEapStartsWhileAuthenticated | Counts the number of times that the state machine transitions from authenticated to connecting, as a result of an EAPOL-Start message being received from the Supplicant. |
| AuthEapLogoffWhileAuthenticated | Counts the number of times that the state machine transitions from authenticated to disconnected, as a result of an EAPOL-Logoff message being received from the Supplicant. |
| BackendResponses | Counts the number of times that the state machine sends an initial Access-Request packet to the Authentication server. Indicates that the Authenticator attempted communication with the Authentication Server. |
| BackendAccessChallenges | Counts the number of times that the state machine receives an initial Access-Challenge packet from the Authentication server. Indicates that the Authentication Server has communication with the Authenticator. |
| BackendOtherRequestsToSupplicant | Counts the number of times that the state machine sends an EAP-Request packet, other than an Identity, Notification, Failure or Success message, to the Supplicant. Indicates that the Authenticator chose an EAP-method. |
| BackendNonNakResponsesFromSupplicant | Counts the number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK. Indicates that the Supplicant can respond to the Authenticator's chosen EAP-method. |
| BackendAuthSuccesses | Counts the number of times that the state machine receives an EAP-Success message from the Authentication Server. Indicates that the Supplicant has successfully authenticated to the Authentication Server. |
| BackendAuthFails | Counts the number of times that the state machine receives an EAP-Failure message from the Authentication Server. Indicates that the Supplicant has not authenticated to the Authentication Server. |

Chapter 4

Setting up MultiLink Trunk ports

MultiLink Trunking (MLT) is a point-to-point connection that aggregates multiple ports so that they logically act like a single port with the aggregated bandwidth. Grouping multiple ports into a logical link allows you to achieve higher aggregate throughput on a switch-to-switch or switch-to-server application. MultiLink Trunking provides media and module redundancy.

MultiLink Trunk (MLT) features

A number of Nortel Networks products implement MultiLink Trunking and have different features and requirements based on the architecture of the device. For the BayStack 420/425, MultiLink Trunking has the following general features and requirements:

- A unit can have up to six MultiLink Trunks (MLTs).
- Up to four ports can belong to an MLT.
- The ports must be in the same unit in the stack.
- MultiLink Trunking is supported on 10BASE-T and 100BASE-TX ports.
- MultiLink Trunking is compatible with the Spanning Tree Protocol.
- IEEE 802.1Q tagging is supported on an MLT.
- For bridge traffic, the algorithm that distributes traffic across an MLT is based on the source and destination MAC addresses.

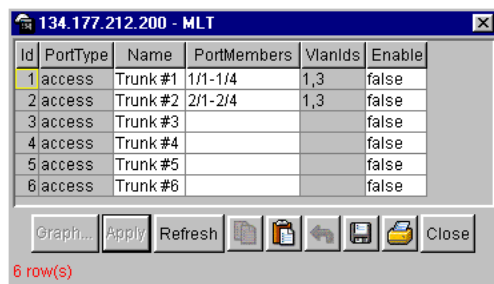
Setting up MLTs

To set up MLTs:

- From the Device Manager menu bar, choose VLAN > MLT.

The MLT dialog box opens (Figure 55).

Figure 55 MLT dialog box



The active MultiLink Trunks are displayed with the fields described in Table 43.

Table 43 MLT dialog box fields

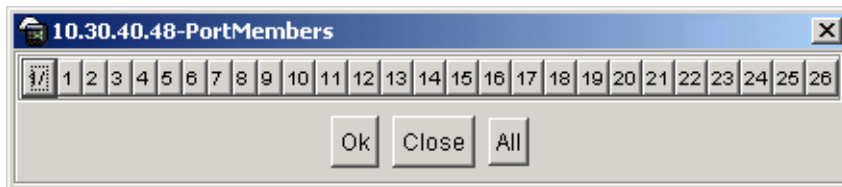
| Field | Description |
|-------------|---|
| ID | The number of the MLT (assigned consecutively). |
| Name | The name given to the MLT. |
| PortType | Access or trunk port. |
| PortMembers | The ports that are assigned to the MLT. |
| VLANIDS | The VLANs assigned to the MLT |
| Enable | Specifies enabling of the MLT. |

Adding ports to a MultiLink Trunk

To add ports to an existing MLT:

- 1 From the Device Manager menu bar, choose VLAN > MLT.
The MLT dialog box opens (Figure 55 on page 128).
- 2 Double-click the PortMembers field.
The PortMembers dialog box opens (Figure 56).

Figure 56 PortMembers dialog box



- 3 Click the port numbers you want to add.
- 4 Click OK.
- 5 In the Enable column, select True to enable your selection.

MultiLink Trunk statistics

To view MLT interface statistics:

- 1 From the Device Manager menu bar, choose VLAN > MLT.
The MLT dialog box opens (Figure 55 on page 128).
- 2 Select an MLT row and then click Graph.
The Statistics, MLT window (Figure 57) opens with the Interface tab displayed.

Figure 57 MLT Statistics — Interface tab

| | AbsoluteValue | Cumulative | Average/sec | Minimum/sec | Maximum/sec | LastVal/sec |
|------------------|---------------|------------|-------------|-------------|-------------|-------------|
| InMulticastPkts | 0 | 0 | 0 | 0 | 0 | 0 |
| OutMulticastPkts | 0 | 0 | 0 | 0 | 0 | 0 |
| InBroadcastPkts | 0 | 0 | 0 | 0 | 0 | 0 |
| OutBroadcastPkts | 0 | 0 | 0 | 0 | 0 | 0 |
| HCInOctets | 0 | 0 | 0 | 0 | 0 | 0 |
| HCOutOctets | 0 | 0 | 0 | 0 | 0 | 0 |
| HCInUcastPkts | 0 | 0 | 0 | 0 | 0 | 0 |
| HCOutUcastPkts | 0 | 0 | 0 | 0 | 0 | 0 |
| HCInMulticastPkt | 0 | 0 | 0 | 0 | 0 | 0 |
| HCOutMulticast | 0 | 0 | 0 | 0 | 0 | 0 |
| HCInBroadcastPkt | 0 | 0 | 0 | 0 | 0 | 0 |
| HCOutBroadcast | 0 | 0 | 0 | 0 | 0 | 0 |

Table 44 describes the fields in the Interface tab.

Table 44 Interface tab fields

| Field | Description |
|----------------|--|
| InMulticastPkt | The number of packets delivered to this MLT that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses. |
| OutMulticast | The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a multicast address at this MLT, including those that were discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses. |
| InBroadcastPkt | The number of packets delivered to this MLT that were addressed to a broadcast address at this sublayer. |
| OutBroadcast | The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this MLT, including those that were discarded or not sent. |
| HCInOctets | The total number of octets received on the MLT interface, including framing characters. |
| HCInUcastPkts | The number of packets delivered by this MLT to a higher MLT that were not addressed to a nulticast or broadcast address at this sublayer. |

Table 44 Interface tab fields (continued)

| Field | Description |
|------------------|--|
| HcInMulticastPkt | The number of packets delivered to this MLT that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses. |
| HcInBroadcastPkt | The number of packets delivered to this MLT that were addressed to a broadcast address at this sublayer. |
| HcOutOctets | The total number of octets transmitted out of the MLT interface, including framing characters. |
| HcOutUcastPkts | The number of packets that high-level protocols requested be transmitted that were not addressed to a multicast address at this MLT. This total number includes those packets discarded or unsent. |
| HcOutMulticast | The total number of packets that high-level protocols requested be transmitted, and that were addressed to a multicast address at this MLT, including those that were discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses. |
| HcOutBroadcast | The total number of packets that high-level protocols requested be transmitted, and that were addressed to a broadcast address at this MLT, including those that were discarded or not sent. |

MultiLink Trunk Ethernet error statistics

To view MultiLink Trunk Ethernet error statistics:

- 1 From the Device Manager menu bar, choose VLAN > MLT.
The MLT dialog box opens ([Figure 55 on page 128](#)).
- 2 Select an MLT by clicking anywhere within a field in the row.
- 3 Click Graph.
The Statistics, MLT dialog box opens ([Figure 57 on page 130](#)) with the Interface tab displayed.
- 4 Click the Ethernet Errors tab.
The Ethernet Errors tab opens ([Figure 58](#)).

Figure 58 MLT Statics dialog box — Ethernet Errors tab

| Interface | AbsoluteValue | Cumulative | Average | Minimum | Maximum | LastValue |
|--------------------|---------------|------------|---------|---------|---------|-----------|
| AlignmentErrors | 0 | 0 | 0 | 0 | 0 | 0 |
| FCSErrors | 0 | 0 | 0 | 0 | 0 | 0 |
| IMacTransmitError | 0 | 0 | 0 | 0 | 0 | 0 |
| IMacReceiveError | 0 | 0 | 0 | 0 | 0 | 0 |
| CarrierSenseError | 0 | 0 | 0 | 0 | 0 | 0 |
| FrameTooLong | 0 | 0 | 0 | 0 | 0 | 0 |
| SQETestError | 0 | 0 | 0 | 0 | 0 | 0 |
| DeferredTransmiss | 0 | 0 | 0 | 0 | 0 | 0 |
| SingleCollFrames | 0 | 0 | 0 | 0 | 0 | 0 |
| MultipleCollFrames | 0 | 0 | 0 | 0 | 0 | 0 |
| LateCollisions | 0 | 0 | 0 | 0 | 0 | 0 |
| ExcessiveCollis | 0 | 0 | 0 | 0 | 0 | 0 |

Table 45 describes the fields in the Ethernet Errors tab.

Table 45 Ethernet Errors tab fields

| Field | Description |
|-------------------|--|
| AlignmentErrors | A count of frames received on a particular MLT that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. |
| FCSErrors | A count of frames received on an MLT that are an integral number of octets in length but do not pass the FCS check. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. |
| IMacTransmitError | A count of frames for which transmission on a particular MLT fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions object, the ExcessiveCollisions object, or the CarrierSenseErrors object. |

Table 45 Ethernet Errors tab fields (continued)

| Field | Description |
|--------------------|---|
| IMacReceiveError | <p>A count of frames for which reception on a particular MLT fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLongs object, the AlignmentErrors object, or the FCSErrors object.</p> <p>The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted.</p> |
| CarrierSenseErrors | <p>The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular MLT. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt.</p> |
| FrameTooLong | <p>A count of frames received on a particular MLT that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.</p> |
| SQETestError | <p>A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular MLT. The SQE TEST ERROR message 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.</p> |
| DeferredTransmiss | <p>A count of frames for which the first transmission attempt on a particular MLT is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.</p> |
| SingleCollFrames | <p>A count of successfully transmitted frames on a particular MLT for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the MultipleCollisionFrames object.</p> |

Table 45 Ethernet Errors tab fields (continued)

| Field | Description |
|--------------------|---|
| MultipleCollFrames | A count of successfully transmitted frames on a particular MLT for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object. |
| LateCollisions | The number of times that a collision is detected on a particular MLT later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics. |
| ExcessiveColls | A count of frames for which transmission on a particular MLT fails due to excessive collisions. |

Chapter 5

Creating and managing VLANs

This chapter describes using Device Manager to manage VLANs on your BayStack 425 Switch. The chapter covers creating, editing, and deleting VLANs. It includes the following sections:

- VLANs (next)
- [VLAN Information \(page 135\)](#)
- [Modifying and managing existing VLANs \(page 140\)](#)

VLANs

A VLAN is a collection of ports on one or more switches that define a broadcast domain. The Baystack 420/425 switch supports port-based VLANs.

For a further description of VLANs, refer to *Using the BayStack 420/425 Switch, Software Release 3.1*.

When you create VLANs using Device Manager, observe the following rules:

- The ports in a VLAN or MLT must be a subset of a single spanning tree group.
- VLANs must have unique VLAN IDs and names.

VLAN Information

The VLAN information is described in the Basic and Snoop tabs of the VLAN dialog box.

To open the VLAN dialog box:

- From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens (Figure 59) with the Basic tab displayed.

Figure 59 VLAN - dialog box with the Basic tab displayed

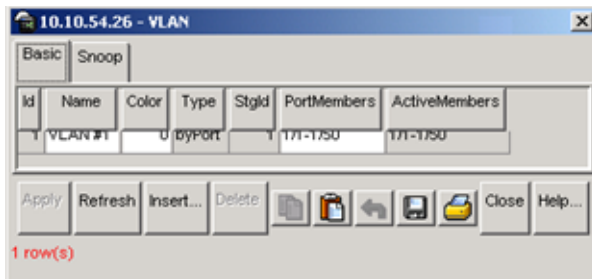


Table 46 describes the VLAN - Basic tab fields.

Table 46 VLAN Basic tab fields

| Field | Description |
|--------------|--|
| Id | The VLAN ID for the VLAN (unlabeled farthest left column). |
| Name | Name of the VLAN. |
| Color | An administratively-assigned color code for the VLAN. The value of this object is used by the VLAN Manager GUI tool to select a color when it draws this VLAN on the screen. |
| Type | Indicates the type of VLAN: byPort or byProtocolId. |
| Stgld | Spanning tree group ID to which the VLAN belongs. |
| PortMembers | Ports that are members of the VLAN. |
| ActiveMember | Set of ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. |

To open the VLAN - Snoop tab:

- In the VLAN - Basic tab, click on the Snoop tab.

The VLAN - Snoop tab (Figure 60) opens.

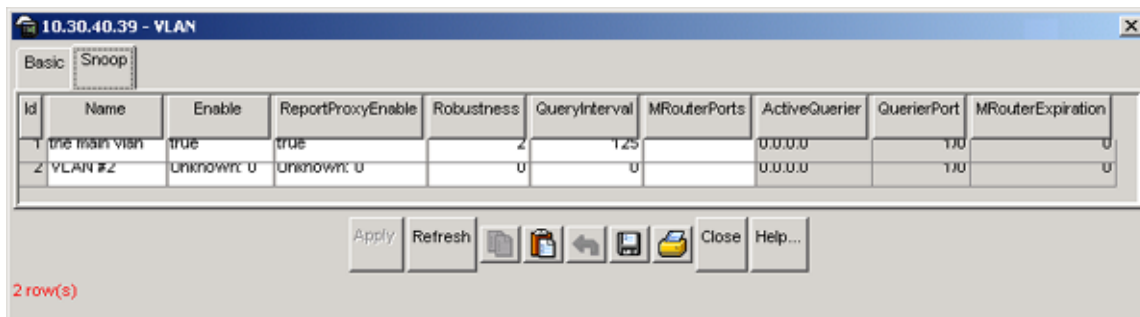
Figure 60 VLAN dialog box- Snoop tab

Table 47 describes the VLAN - Snoop tab fields.

Table 47 VLAN - Snoop tab fields

| Field | Description |
|-------------------|---|
| Name | Name of the VLAN. |
| Enable | Sets whether IGMP snooping is enabled or disabled. |
| ReportProxyEnable | Sets whether IGMP report proxy is enabled or disabled. |
| Robustness | Allows tuning for the expected packet loss on a subnet. If a subnet is expected to be bad, the Robustness variable can be increased. IGMP is robust to packet losses. |
| QueryInterval | Sets the intervals (in seconds) between IGMP host and query packets transmitted on an interface. |
| MRouterPorts | Specifies the set of ports in the VLAN that provide connectivity to an IP multicast router. |
| ActiveQuerier | This is the IP address of a multicast querier router. |
| QuerierPort | The port that the multicast querier router was heard. |
| MRouterExpiration | The multicast querier router aging that will be timed out. |

Creating VLANs

Device Manager enables you to create a port-based VLAN.

Creating a port-based VLAN

To create a port-based VLAN:

- 1 From the Device Manager menu bar, choose VLAN > VLANs.

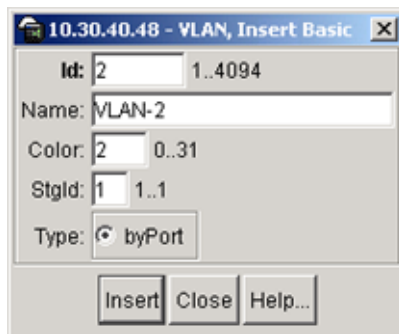
The VLAN dialog box opens ([Figure 59 on page 136](#)).

- 2 Click Insert.

The VLAN Insert Basic dialog box for creating VLANs opens ([Figure 61](#)).

This dialog box opens with the Type field set to byPort.

Figure 61 VLAN, Insert Basic dialog box for a port-based VLANs



- 3 Type the VLAN ID.

The value can be from 1 to 4094, as long as it is not already in use. (The default VLAN has a VID=1.)

- 4 Type the VLAN name (optional).

If no name is entered, a default name is created.

- 5 In the Type field, click byPort if not already selected.

- 6 Specify the port membership by clicking the PortMembers buttons.

- 7 Click Insert.

Accepting untagged frames

In the BayStack 420/425, you configure whether or not untagged frames are sent or received on the port level. Refer to [“VLAN tab for a single port” on page 97](#) for VLAN tab field descriptions. You can select whether or not to discard untagged frames received on a port:

The default is not to discard the untagged frames. You can also designate the port-based VLAN to which these frames are assigned by setting the untagged port's default VID (the default is 1).

To set a port to discard untagged frames it receives:

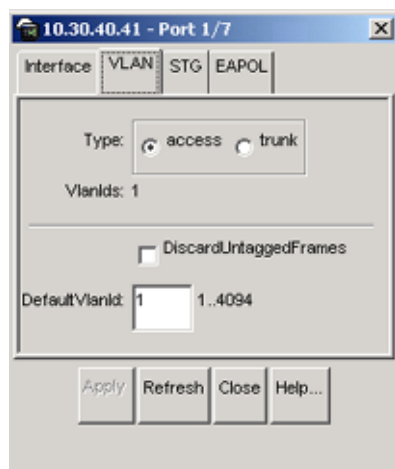
- 1 In the Device Manager main window, select a port.
- 2 From the Device Manager menu bar, choose Edit > Port.

The Port dialog box opens with the Interface tab displayed ([Figure 42 on page 95](#)).

- 3 Click the VLAN tab.

The VLAN tab opens ([Figure 62](#)).

Figure 62 VLAN tab



Select the DiscardTaggedFrames and the DiscardUntaggFrames check boxes.

- 4 Click Apply.

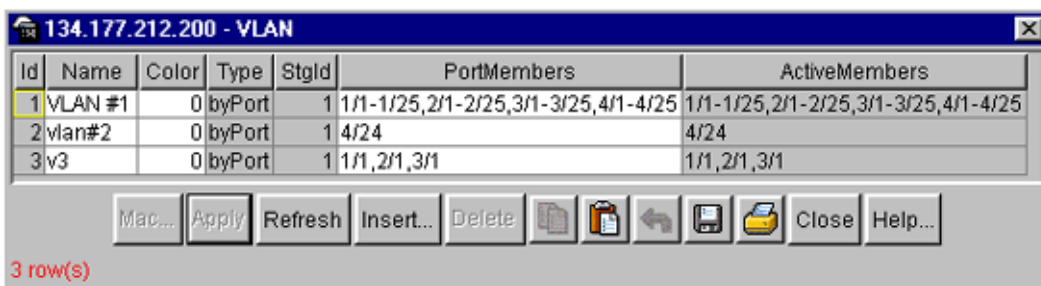
Modifying and managing existing VLANs

The main dialog box for managing VLANs in Device Manager is the VLAN dialog box. To open the VLAN dialog box:

- From the Device Manager main menu, choose VLAN > VLANs.

The VLAN dialog box opens (Figure 63). The VLAN dialog box displays all defined VLANs, their configurations, and their current status.

Figure 63 VLAN dialog box



Note: After a VLAN is created, you cannot change the VLAN type. The VLAN must be deleted and a new VLAN of the chosen type created.

Table 48 describes the fields in the VLAN dialog box.

Table 48 VLAN dialog box fields

| Field | Description |
|-------|---|
| Id | The VLAN ID for the VLAN (unlabeled farthest left column). |
| Name | The name of the VLAN. |
| Color | The color used, for visual purposes only, by VLAN Manager to associate a color with a VLAN. The assigned color does not affect the behavior of a frame, only the attributes assigned to the VLAN. |
| Type | Indicates the type of VLAN: byPort. |

Table 48 VLAN dialog box fields (continued)

| Field | Description |
|---------------|--|
| Stgld | The spanning tree group ID to which the VLAN belongs. |
| PortMembers | The ports that are members of the VLAN. |
| ActiveMembers | Set of ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met. |

Chapter 6

Setting up bridging

The Bridge parameters allow you to configure the global Spanning Tree and to view MAC address table for a Baystack 420/425. Bridge information also includes Spanning Tree Group (STG) information.

This chapter describes the bridge information available in Device Manager on the following tabs:

- Base tab (next)
- [Spanning Tree tab \(page 144\)](#)
- [Transparent tab \(page 147\)](#)
- [Forwarding tab \(page 148\)](#)
- [Spanning tree group \(STG\) \(page 150\)](#)
- [Configuration tab \(page 151\)](#)
- [Status tab \(page 152\)](#)
- [Ports tab \(page 154\)](#)

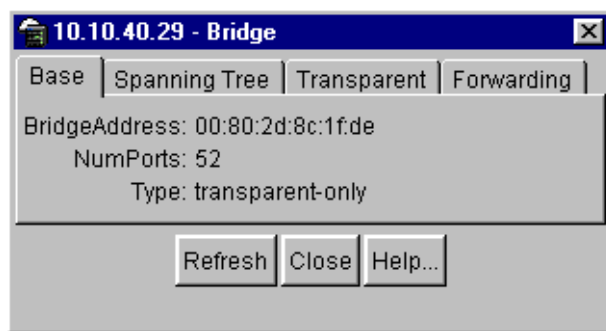
Base tab

The MAC address used by the bridge must be referred to in a unique fashion; moreover, it should be the smallest MAC address (numerically) of all ports that belong to the bridge. However it is only required to be unique when integrated with dot1dStpPriority. A unique BridgeIdentifier is formed that is used in the Spanning Tree Protocol.

To view the Base tab:

- From the menu bar, select Edit > Bridge.

The Bridge dialog box opens with the Base tab displayed ([Figure 64](#)).

Figure 64 Base tab

[Table 49](#) describes the Base tab fields.

Table 49 Base tab fields

| Field | Description |
|---------------|---|
| BridgeAddress | MAC address of the bridge when it is referred to in a unique fashion. This address should be the smallest MAC address of all ports that belong to the bridge. However, it is has to be unique. When concatenated with dot1dStpPriority, a unique bridge ID is formed that is then used in the Spanning Tree Protocol. |
| NumPorts | Number of ports controlled by the bridging entity. |
| Type | Indicates the type of bridging this bridge can perform. If the bridge is actually performing a certain type of bridging, this will be indicated by entries in the port table for the given type. |

Spanning Tree tab

The Spanning Tree tab displays the version of the spanning tree protocol currently running. If future versions of the IEEE spanning tree protocol are released that are incompatible with the current version, a new value will be defined.

To view the Spanning Tree tab:

- 1 From the Device Manager menu bar, choose Edit > Bridge.
The Bridge dialog box opens, with the Base tab displayed ([Figure 65](#)).
- 2 Click the Spanning Tree tab.
The Spanning Tree tab opens.

Figure 65 Spanning Tree tab

[Table 50](#) describes the Spanning Tree tab fields.

Table 50 Spanning Tree tab fields

| Field | Description |
|-------------------------|--|
| ProtocolSpecification | Version of the Spanning Tree Protocol being run. Values include: <ul style="list-style-type: none"> • decLb100: Indicates the DEC LANbridge 100 Spanning Tree Protocol. • ieee8021d: IEEE 802.1d implementations will return this entry. When future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version, a new value will be defined. |
| Priority | Value of the writable portion of the bridge ID. That is, the first two octets of the (8-octet long) bridge ID. The last six octets of the bridge ID are given by the value of BridgeAddress. |
| TimeSinceTopologyChange | Time (in hundredths of a second) since the last time a topology change was detected by the bridge entity. |
| TopChanges | Number of topology changes detected by this bridge since the management entity was reset or initialized. |
| DesignatedRoot | Bridge ID of the root of the spanning tree as determined by the Spanning Tree Protocol. This is executed by the node. This value is used as the Root ID parameter in all configuration bridge PDUs originated by the node. |

Table 50 Spanning Tree tab fields (continued)

| Field | Description |
|--------------|---|
| RootCost | Cost of the path to the root as seen from this bridge. |
| RootPort | Port number of the port that offers the lowest cost path from this bridge to the root bridge. |
| MaxAge | Maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in units of hundredths of a second. This is the actual value that this bridge is currently using. |
| HelloTime | Time between the transmission of Configuration bridge PDUs by the node on any port when it is the root of the spanning tree (in units of hundredths of a second). This is the actual value that the bridge is currently using. |
| ForwardDelay | <p>Value (in hundredths of a second) that controls how fast a port changes its spanning state when moving towards the Forwarding state. The value determines how long the port stays in each of the Listening and Learning states, that precede the Forwarding state. The value is also used when a topology change has been detected and is underway. This ages all dynamic entries in the Forwarding database.</p> <p>Note: This value is the one that this bridge is currently using, in contrast to dot1dStpBridge ForwardDelay which is the value that this bridge and all others would start using if/when this bridge were to become the root.]</p> |
| BridgeMaxAge | <p>Value that all bridges use for the maximum age of a bridge when it is acting as the root.</p> <p>Note: 802.1D-1990 specifies that the range is related to the value of BridgeHelloTime. The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error may be returned if the value set is not a whole number.</p> |

Table 50 Spanning Tree tab fields (continued)

| Field | Description |
|-------------------------|--|
| BridgeHelloTime | Value that the bridge uses for HelloTime when the bridge is acting as the root. The granularity of this timer is specified by 802.1D-1990 to be one second. An agent may return a badValue error if a set is attempted to a value that is not a whole number of seconds. |
| TimeSinceTopologyChange | Value that all bridges use for ForwardDelay when this bridge is acting as the root. Note: 802.1D-1990 specifies that the range for this parameter is related to the value of dot1dStpBridgeMaxAge. The granularity of this timer is specified by 802.1D-1990 to be one second. An agent may return a badValue error if a set is attempted to a value that is not a whole number of seconds. |

Transparent tab

The Transparent tab contains information about a specific unicast MAC address that has forwarding information for the bridge.

To view the Transparent tab:

- 1 From the Device Manager menu bar, choose Edit > Bridge.
The Bridge dialog box opens, with the Base tab displayed.
- 2 Click the Transparent tab.
The Transparent tab opens ([Figure 66](#)).

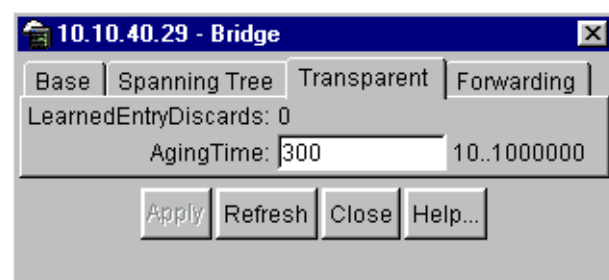
Figure 66 Transparent tab

Table 51 describes the Transparent tab items.

Table 51 Transparent tab items

| Item | Description |
|---------------------|--|
| LearnedEntryDiscard | Number of Forwarding database entries learned that have been discarded due to a lack of space in the Forwarding database. If this counter is increasing, it indicates that the Forwarding database is becoming full regularly. This condition will effect the performance of the subnetwork. If the counter has a significant value and is not presently increasing, it indicates that the problem has been occurring but is not persistent. |
| AgingTime | Time-out period in seconds for aging out dynamically learned forwarding information. Note: The 802.1D-1990 specification recommends a default of 300 seconds. |

Forwarding tab

The Forwarding tab displays the current state of the port, as defined by application of the Spanning Tree Protocol. This state controls what action a port takes when a frame is received. If the bridge detects a port that is malfunctioning, it places the port into the “broken” state. For ports that are disabled, the value is “disabled.”

To view the Forwarding tab:

- 1 From the Device Manager menu bar, choose Edit > Bridge.
The Bridge dialog box opens, with the Base tab displayed.
- 2 Click the Forwarding tab.
The Forwarding tab opens (Figure 67).

Figure 67 Forwarding tab

| Status | Address | Port |
|---------|-------------------|------|
| learned | 00:00:5e:00:01:01 | 2/1 |
| learned | 00:00:5e:00:01:20 | 2/1 |
| learned | 00:00:81:bc:ea:81 | 2/1 |
| learned | 00:00:81:c1:9b:81 | 2/1 |
| learned | 00:00:81:c1:f6:81 | 2/1 |
| learned | 00:60:5c:83:2f:08 | 2/1 |
| learned | 00:60:fd:9e:2b:6a | 2/1 |
| learned | 00:60:fd:9e:2b:6b | 2/1 |
| learned | 00:60:fd:ee:19:b2 | 2/1 |
| learned | 00:80:2d:22:0e:00 | 2/1 |
| learned | 00:80:2d:22:b7:f6 | 2/1 |
| learned | 00:80:2d:39:f2:00 | 2/1 |
| mgmt | 00:80:2d:8c:1f:df | 0 |
| learned | 00:80:5f:e7:e4:39 | 2/1 |
| learned | 00:e0:16:57:7e:81 | 2/1 |
| learned | 00:e0:16:83:26:81 | 2/1 |
| learned | 00:e0:7b:ab:7a:00 | 2/1 |

Refresh Save Print Close Help...

17 row(s)

Table 52 describes the Forwarding tab fields.

Table 52 Forwarding tab fields

| Field | Description |
|---------|--|
| Status | <p>The values of this fields include:</p> <ul style="list-style-type: none"> • invalid: Entry is no longer valid, but has not been removed from the table. • learned: Value of the corresponding instance of dot1dTpFdbPort was learned and is being used. • self: Value of the corresponding instance of dot1dTpFdbAddress represents an address of the bridge. The corresponding instance of dot1dTpFdbPort indicates that a specific port on the bridge has this address. • mgmt(5): Value of the corresponding instance of dot1dTpFdbAddress is also the value of an existing instance of dot1dStaticAddress. • other: none of the preceding. This would include where some other MIB object (not the corresponding instance of dot1dTpFdbPort or an entry in the dot1dStaticTable) is being used to determine if a frames addressed to the value of dot1dTpFdbAddress are being forwarded. |
| Address | A unicast MAC address for which the bridge has forwarding or filtering information. |
| Port | <p>Either the value "0" or the port number on a frame has been seen. The source address must be equal to the value of the corresponding instance of dot1dTpFdbAddress</p> <p>A value of "0" indicates that the port number has not been learned, so the bridge does have the forwarding/filtering information for this address (located in the dot1dStaticTable). You should assign the port value to this object whenever it is learned even for addresses for which the corresponding value of dot1dTpFdbStatus is not learned(3).</p> |

Spanning tree group (STG)

The spanning tree group (STG) information is stored in the STG dialog box. Each row in each tab specifies a different STG in the device.

Configuration tab

The Configuration tab in the STG dialog box has general information for the STG.

To view the Configuration tab:

➔ From the Device Manager menu bar, choose VLANs > STG.

The STG dialog box opens, with the Configuration tab displayed (Figure 68).

Figure 68 Configuration tab

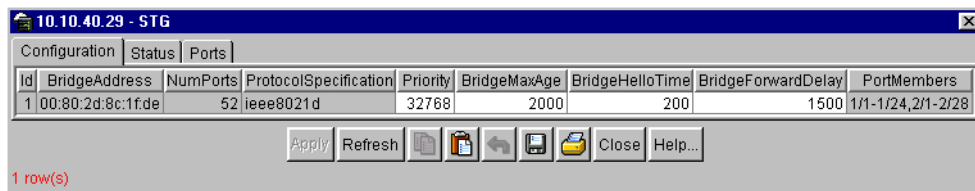


Table 53 describes the Configuration tab fields.

Table 53 Configuration tab fields

| Item | Description |
|-----------------------|--|
| ID | An identifier used to identify a STG in the device. |
| BridgeAddress | MAC address used by a bridge when it is referred to in a unique fashion. Nortel Network recommends that the number be the smallest MAC address of all ports belonging to the bridge. However, it is only required to be unique. When concatenated with Priority, a unique bridge identifier is formed that is used in the Spanning Tree Protocol. |
| NumPorts | Number of ports controlled by this bridging entity. |
| ProtocolSpecification | Version of the spanning tree protocol being run. Values include: <ul style="list-style-type: none"> • decLb100: Indicates the DEC LANbridge 100 Spanning Tree Protocol. • ieee8021d: IEEE 802.1d implementations will return this entry. When future versions of the IEEE Spanning Tree Protocol are released that are incompatible with the current version, a new value will be defined. |
| Priority | Value of the writable portion of the bridge ID. That is, the first two octets of the (8-octet long) bridge ID. The last six octets of the bridge ID are given by the value of BridgeAddress. |

Table 53 Configuration tab fields (continued)

| Item | Description |
|--------------------|---|
| BridgeMaxAge | Value that all bridges use for the maximum age of a bridge when it is acting as the root. Note: 802.1D-1990 specifies that the range is related to the value of BridgeHelloTime. The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error may be returned if the value set is not a whole number. |
| BridgeHelloTime | Value that all bridges use for HelloTime when a bridge is acting as the root. Note: The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error may be returned if the value set is not a whole number. |
| BridgeForwardDelay | Value that all bridges use for ForwardDelay when this bridge is acting as the root. Note: 802.1D-1990 specifies that the range is related to the value of BridgeHelloTime. The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error may be returned if the value set is not a whole number. |
| PortMembers | Bit-field used to identify the ports in the system that are members this STG. The bit-field is 32 octets long representing ports 0 to 255 (inclusive). |

Status tab

The Status tab in the STG dialog box has status information for the STG.

To view the Status tab:

- 1** From the Device Manager menu bar, choose VLANs > STG.
The STG dialog box opens, with the Configuration tab displayed.
- 2** Click the Status tab.
The Status tab opens ([Figure 69](#)).

Figure 69 Status tab

| Id | BridgeAddress | NumPorts | ProtocolSpecif... | TimeSinceTopol... | TopCha... | DesignatedRoot | RootCost | RootPort | MaxAge | HelloTime | Hold... | ForwardDelay |
|----|------------------|----------|-------------------|--------------------|-----------|------------------|----------|----------|--------|-----------|---------|--------------|
| 1 | 00:80:2d:8c:1... | 52 | ieee8021d | 8 days, 19h:27m... | 7 | 80:00:00:00:0... | 210 | 2/1 | 2000 | 200 | 100 | 1500 |

Table 54 describes the Status tab fields.

Table 54 Status tab fields

| Field | Description |
|-------------------------|--|
| ID | An identifier used to identify a STG in the device. |
| BridgeAddress | MAC address used by a bridge when it is referred to in a unique fashion. Nortel Networks recommends that the number be the smallest MAC address of all ports belonging to the bridge. However, it is only required to be unique. When concatenated with Priority, a unique bridge identifier is formed that is used in the Spanning Tree Protocol. |
| NumPorts | Number of ports controlled by this bridging entity. |
| ProtocolSpecification | Version of the Spanning Tree Protocol being run. Values include: <ul style="list-style-type: none"> • decLb100: Indicates the DEC LANbridge 100 spanning tree protocol. • ieee8021d: IEEE 802.1d implementations will return this entry. When future versions of the IEEE spanning tree protocol are released that are incompatible with the current version, a new value will be defined. |
| TimeSinceTopologyChange | Time (in hundredths of seconds) since the last topology change was detected by the bridge entity. |
| TopChange | Number of topology changes detected by the bridge since the management entity was last reset or initialized. |
| DesignatedRoot | Bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol. The value is used as the root identifier parameter in all configuration bridge PDUs originated by this node. |
| RootCost | Cost of the path to the root as seen from the bridge. |
| RootPort | Port that has the lowest cost path from the bridge to the root bridge. |

Table 54 Status tab fields (continued)

| Field | Description |
|--------------|---|
| MaxAge | Maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in units of hundredths of a second. This is the actual value that this bridge is currently using. |
| HelloTime | Amount of time between the transmission of configuration bridge PDUs by this node on any port when it is the root of the spanning tree (in hundredths of a seconds). This is the actual value that this bridge is currently using. |
| HoldTime | Value of the interval length during which no more than two configuration bridge PDUs shall be transmitted by this node (in hundredths of a second). |
| ForwardDelay | This time value (in hundredths of a seconds) that controls how fast a port changes its spanning state when moving towards the forwarding state. Value determines how long the port stays in each of the listening and learning states, which precede the forwarding state. This is also used when a topology change has been detected and is underway, to age all dynamic entries in the forwarding database. Note: This value is the one that this bridge is currently using, in contrast to BridgeForwardDelay which is the value that this bridge and all others would start using if/when this bridge were to become the root. |

Ports tab

The Ports tab in the STG dialog box has port information for the STG.

To view the Ports tab:

- 1 From the Device Manager menu bar, choose VLANs > STG.
The STG dialog box opens, with the Configuration tab displayed.
- 2 Click the Ports tab.
The Ports tab opens ([Figure 70](#)).

Figure 70 Ports tab

| | StgId | Priority | State | EnableStp | FastStart | PathCost | DesignatedRoot | DesignatedCost | DesignatedBridge | DesignatedPort | ForwardTransitions |
|------|-------|----------|-------------|-----------|-----------|----------|-------------------|----------------|---------------------|----------------|--------------------|
| 1/1 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:01 | 6 |
| 1/2 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:02 | 3 |
| 1/3 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:03 | 4 |
| 1/4 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:04 | 1 |
| 1/5 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:05 | 1 |
| 1/6 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:06 | 1 |
| 1/7 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:07 | 1 |
| 1/8 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:08 | 1 |
| 1/9 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:09 | 1 |
| 1/10 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:0a | 1 |
| 1/11 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:0b | 1 |
| 1/12 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:0c | 1 |
| 1/13 | 1 | 128 | forwardi... | true | true | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:0d | 1 |
| 1/14 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:0e | 1 |
| 1/15 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:0f | 1 |
| 1/16 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:10 | 1 |
| 1/17 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:11 | 1 |
| 1/18 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:12 | 1 |
| 1/19 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:13 | 1 |
| 1/20 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:14 | 1 |
| 1/21 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:15 | 1 |
| 1/22 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:16 | 1 |
| 1/23 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:17 | 1 |
| 1/24 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:18 | 1 |
| 2/1 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 200 | 80:00:00:60:fd:9... | 80:2c | 1 |
| 2/2 | 1 | 128 | forwardi... | true | false | 10 | 80:00:00:00:00... | 210 | 80:00:00:80:2d:8... | 80:22 | 1 |

52 row(s)

Table 55 describes the Ports tab fields.

Table 55 Ports tab fields

| Field | Description |
|-----------|---|
| StgId | STG identifier assigned to this port. |
| Priority | Value of the priority field contained in the first octet of the port ID. The other octet is given by the value of the "rcStgPort." |
| State | The current state of the port as defined by application of the Spanning Tree Protocol. These are the instructions the port takes on a frame when it is received. If the bridge detects a port is malfunctioning, it will list it as "broken(6)." For ports that are disabled, the value is "disabled(1)." |
| EnableStp | Enables (True) or disables (False) the spanning tree of the port. |
| FastStart | When this is enabled (True), the port is move to forwarding or blocking state in 4 seconds. |

Table 55 Ports tab fields (continued)

| Field | Description |
|--------------------|---|
| PathCost | Contribution of the port to the pathcost of paths towards the spanning tree root, including the current port. 802.1D-1990 specifications recommends that the default of this parameter be in inverse proportion to the speed of the attached LAN. |
| DesignatedRoot | The unique "Bridge Identifier." This is recorded as Root in the configuration bridge PDUs transmitted by the Designated Bridge for the segment to that the port is attached. |
| DesignatedCost | Path cost of the Designated Port of the segment connected to the port. The value is compared to the Root Path Cost field in received bridge PDUs. |
| DesignatedBridge | Bridge identifier of the bridge that this port considers to be the Designated Bridge for this port's segment. |
| DesignatedPort | Port identifier of the port on the Designated Bridge for this port's segment. |
| ForwardTransitions | Number of times this port has transitioned from the learning state to the forwarding state. |

Chapter 7

Troubleshooting Device Manager

This chapter describes diagnostic information available in Device Manager on the following tabs:

- [Topology tab](#) (next)
- [Topology Table tab](#) (page 158)

Topology tab

To view topology information:

- From the Device Manager menu bar, select Edit > Diagnostics.

The Diagnostics dialog box opens with the Topology tab displayed ([Figure 71](#)).

Figure 71 Diagnostics dialog box — Topology tab

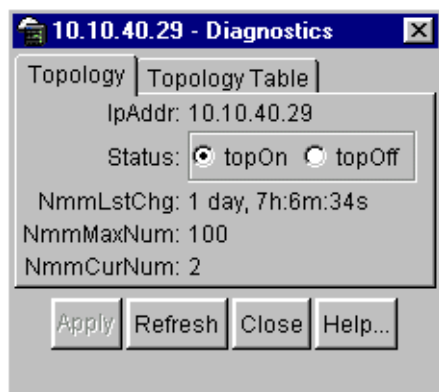


Table 56 describes the Topology tab items.

Table 56 Topology tab items

| Items | Description |
|-----------|--|
| IpAddr | The IP address of the device. |
| Status | Whether Nortel Networks topology is on (topOn) or off (topOff) for the device. The default value is topOn. |
| NmmLstChg | The value of sysUpTime the last time an entry in the network management MIB (NMM) topology table was added, deleted, or modified. If the table has not changed since the last cold or warm start of the agent. |
| NmmMaxNum | The maximum number of entries in the NMM topology table. |
| NmmCurNum | The current number of entries in the NMM topology table. |

Topology Table tab

To view more topology information:

- 1 From the Device Manager menu bar, choose Edit > Diagnostics.

The Diagnostics dialog box opens with the Topology tab displayed (Figure 71 on page 157).

- 2 Click the Topology Table tab.

The Topology Table tab opens (Figure 72).

Figure 72 Diagnostics dialog box — Topology Table tab

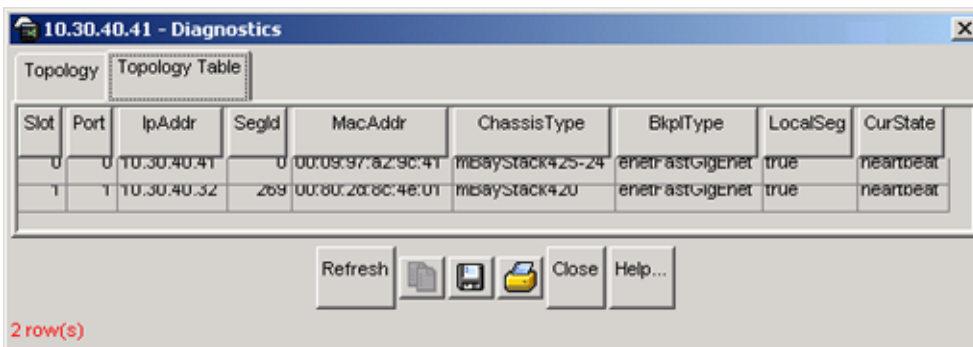


Table 57 describes the Topology Table tab fields.

Table 57 Topology Table tab fields

| Field | Description |
|-------------|---|
| Slot | The slot number in the chassis in which the topology message was received. |
| Port | The port on which the topology message was received. |
| IpAddr | The IP address of the sender of the topology message. |
| SegId | The segment identifier of the segment from which the remote agent sent the topology message. This value is extracted from the message. |
| MacAddr | The MAC address of the sender of the topology message. |
| ChassisType | The chassis type of the device that sent the topology message. |
| BkplType | The backplane type of the device that sent the topology message. |
| LocalSeg | Indicates if the sender of the topology message is on the same Ethernet segment as the reporting agent. |
| CurState | The current state of the sender of the topology message. The choices are: <ul style="list-style-type: none"> topChanged —Topology information has recently changed. heartbeat —Topology information is unchanged. new — The sending agent is in a new state. |

Chapter 8

RMON

The Remote Network Monitoring (RMON) MIB is an interface between the RMON agent on a Baystack 425 Switch and an RMON management application, such as the Device Manager. It defines objects that are suitable for the management of any type of network, but some groups are targeted for Ethernet networks in particular. The RMON agent continuously collects statistics and proactively monitors switch performance. You can view this data through the Device Manager.

RMON has three major functions:

- Creating and displaying alarms for user-defined events
- Gathering cumulative statistics for Ethernet interfaces
- Tracking a history of statistics for Ethernet interfaces

Working with RMON information

You can view RMON information by looking at the Graph information associated with the port or chassis.

Viewing statistics

Device Manager gathers Ethernet statistics that you can have graphed in a variety of formats, or you can save them to a file and export the statistics to an outside presentation or graphing application.

To view RMON Ethernet statistics:

- 1 Select an object (port).

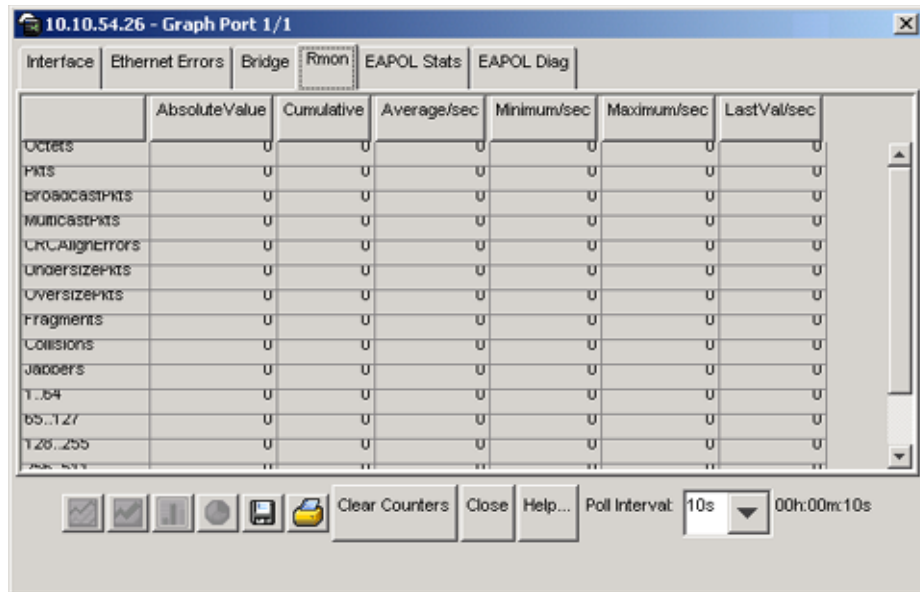
2 Do one of the following:

- Double-click on the selected port
- From the shortcut menu, choose Graph.
- From the Device Manager main menu, choose Graph.

The Graph Port dialog box opens with the Interface tab displayed ([Figure 42 on page 95](#)).

3 Click the RMON tab.

The RMON tab opens ([Figure 73](#)).

Figure 73 Port dialog box — RMON tab

For descriptions of the RMON tab fields, refer to [Table 40 on page 121](#). For descriptions of the statistics columns, refer to [Table 10 on page 44](#).

Table 58 Port dialog box — RMON tab fields

| Field | Description |
|---------------|--|
| Octets | The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). You can use this object as a reasonable estimate of Ethernet utilization. For greater precision, sample the etherStatsPkts and etherStatsOctets objects before and after a common interval. |
| Pkts | The total number of packets (including bad packets, broadcast packets, and multicast packets) received. |
| BroadcastPkts | The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets. |
| MulticastPkts | The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address. |

Table 58 Port dialog box — RMON tab fields (continued)

| Field | Description |
|-----------------|---|
| CRCAAlignErrors | The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). |
| UndersizePkts | The total number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed. |
| OversizePkts | The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed. |
| Fragments | The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). It is entirely normal for etherStatsFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits. |
| Collisions | The best estimate of the total number of collisions on this Ethernet segment. |
| Jabbers | The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. |
| 1..64 | The total number of packets (including bad packets) received that were less than or equal to 64 octets in length (excluding framing bits but including FCS octets). |
| 65..127 | The total number of packets (including bad packets) received that were greater than 64 octets in length (excluding framing bits but including FCS octets). |
| 128..255 | The total number of packets (including bad packets) received that were greater than 127 octets in length (excluding framing bits but including FCS octets). |
| 256..511 | The total number of packets (including bad packets) received that were greater than 255 octets in length (excluding framing bits but including FCS octets). |

Table 58 Port dialog box — RMON tab fields (continued)

| Field | Description |
|------------|--|
| 512..1023 | The total number of packets (including bad packets) received that were greater than 511 octets in length (excluding framing bits but including FCS octets). |
| 1024..1518 | The total number of packets (including bad packets) received that were greater than 1023 octets in length (excluding framing bits but including FCS octets). |

Table 59 Types of statistics

| Statistic | Description |
|-------------|--|
| Absolute | The total count since the last time counters were reset. A system reboot resets all counters. |
| Cumulative | The total count since the statistics tab was first opened. The elapsed time for the cumulative counter is displayed at the bottom of the graph window. |
| Average/sec | The cumulative count divided by the cumulative elapsed time. |
| Min/sec | The minimum average for the counter for a given polling interval over the cumulative elapsed time. |
| Max/sec | The maximum average for the counter for a given polling interval over the cumulative elapsed time. |
| Last/sec | The average for the counter over the last polling interval. |

Viewing history

Ethernet history records periodic statistical samples from a network. A sample is called a history and is gathered in time intervals referred to as “buckets.” Histories establish a time-dependent method for gathering RMON statistics on a port. The default values for history are:

- Buckets are gathered at 30-minute intervals.
- Number of buckets gathered is 50.

Both the time interval and the number of buckets is configurable. However, when the last bucket is reached, bucket 1 is dumped and “recycled” to hold a new bucket of statistics. Then bucket 2 is dumped, and so forth.

To view RMON history:

- 1 Select an object (port or chassis).
- 2 On the toolbar, click Graph.

The graph Port dialog box opens with the Interface tab displayed (Figure 49 on page 112).

- 3 Click the RMON tab.

The RMON tab opens (Figure 74).

Figure 74 Port dialog box — RMON tab

| | Absolute value | Cumulative | Averaged/sec | Min/minute | Max/minute | Last/minute |
|--------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Bytes | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Pkts | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Encapsulated | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Multicast | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Broadcast | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Control | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Discards | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Errors | <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"/> |

Creating a history

You can use RMON to collect statistics at intervals. For example, if you want RMON statistics to be gathered over the weekend, you will want enough buckets to cover two days. To do this, set the history to gather one bucket each hour, thus covering a 48-hour period. After you set history characteristics, you cannot modify them; you must delete the history and create another one.

To establish a history for a port and set the bucket interval:

- 1 From the Device Manager main menu, choose RMON > Control.

The RMONControl dialog box opens with the History tab displayed (Figure 75).

Figure 75 History tab

| Index | Port | BucketsRequested | BucketsGranted | Interval | Owner |
|-------|------|------------------|----------------|----------|---------|
| 1 | 1/1 | 3 | 3 | 30 | monitor |
| 2 | 1/2 | 3 | 3 | 30 | monitor |
| 3 | 1/3 | 3 | 3 | 30 | monitor |
| 4 | 1/4 | 3 | 3 | 30 | monitor |
| 5 | 1/5 | 3 | 3 | 30 | monitor |
| 6 | 1/6 | 3 | 3 | 30 | monitor |
| 7 | 1/7 | 3 | 3 | 30 | monitor |
| 8 | 1/8 | 3 | 3 | 30 | monitor |
| 9 | 1/9 | 3 | 3 | 30 | monitor |
| 10 | 1/10 | 3 | 3 | 30 | monitor |
| 11 | 1/11 | 3 | 3 | 30 | monitor |
| 12 | 1/12 | 3 | 3 | 30 | monitor |
| 13 | 1/13 | 3 | 3 | 30 | monitor |
| 14 | 1/14 | 3 | 3 | 30 | monitor |

56 row(s)

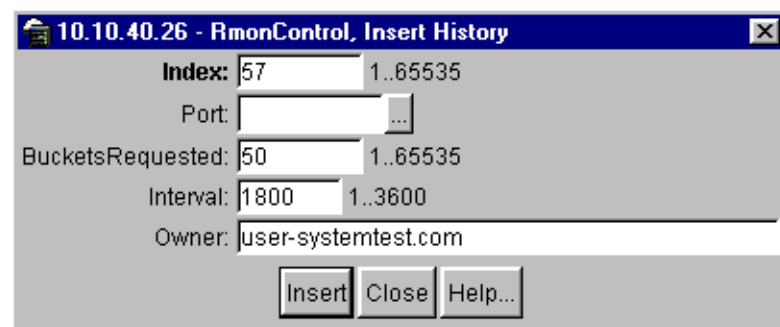
Table 60 describes the History fields.

Table 60 History tab fields

| Field | Description |
|------------------|--|
| Index | A unique value assigned to each interface. An index identifies an entry in a table. |
| Port | Any Ethernet interface on the device. |
| BucketsRequested | The requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this entry. |
| BucketsGranted | The number of discrete sampling intervals over which data is saved in the part of the media-specific table associated with this entry. There are instances when the actual number of buckets associated with this entry is less than the value of this object. In this case, at the end of each sampling interval, a new bucket is added to the media-specific table. |
| Interval | The interval in seconds over which the data is sampled for each bucket in the part of the media-specific table associated with this entry. You can set this interval to any number of seconds between 1 and 3600 (1 hour). Because the counters in a bucket may overflow at their maximum value with no indication, note the possibility of overflow in any of the associated counters. It is important to consider the minimum time in which any counter could overflow on a particular media type and set the historyControlInterval object to a value less than this interval. This is typically most important for the 'octets' counter in any media-specific table. For example, on an Ethernet network, the etherHistoryOctets counter could overflow in about one hour at the Ethernet's maximum utilization. |
| Owner | The network management system that created this entry. |

- 2 Select an index and then click Insert.

The RMONControl, Insert History dialog box opens ([Figure 76](#)).

Figure 76 RMONControl, Insert History dialog box

- 3 Select the port from the port list or type the port number.
- 4 Set the number of buckets.
The default is 50.
- 5 Set the interval.
The default is 1800 seconds.
- 6 Type the owner, the network management system that created this entry.
- 7 Click Insert.
RMON collects statistics using the index, port, bucket, and interval that you specified.

[Table 61](#) describes the RMON History items

Table 61 RMON History items

| Item | Description |
|---------------|--|
| SampleIndex | An index that uniquely identifies the particular sample this entry represents among all the samples associated with the same entry. This index starts at 1 and increases by one as each new sample is taken. |
| Utilization | The best estimate of the mean physical layer network utilization on this interface during the sampling interval (in hundredths of a percent). |
| Octets | The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). You can use this object as a reasonable estimate of Ethernet utilization. For greater precision, sample the etherStatsPkts and etherStatsOctets objects before and after a common interval. |
| Pkts | The total number of packets (including bad packets, broadcast packets, and multicast packets) received. |
| BroadcastPkts | The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets. |
| MulticastPkts | The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address. |

Table 61 RMON History items

| Item | Description |
|-----------------|---|
| DropEvents | The total number of events in which packets were dropped by the probe due to lack of resources during this sampling. This number is not necessarily the number of packets dropped. It is the number of times this condition has been detected. |
| CRCAAlignErrors | The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). |
| UndersizePkts | The total number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed. |
| OversizePkts | The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed. |

Disabling history

To disable RMON history on a port:

- 1 From the Device Manager main menu, choose RMON > Control.
The RMONControl dialog box opens with the History tab displayed ([Figure 75 on page 167](#)).
- 2 Highlight the row that contains the port ID you want to delete.
- 3 Click Delete.
The entry is removed from the table.

Enabling Ethernet statistics gathering

You can use RMON to gather Ethernet statistics.

To gather Ethernet statistics:

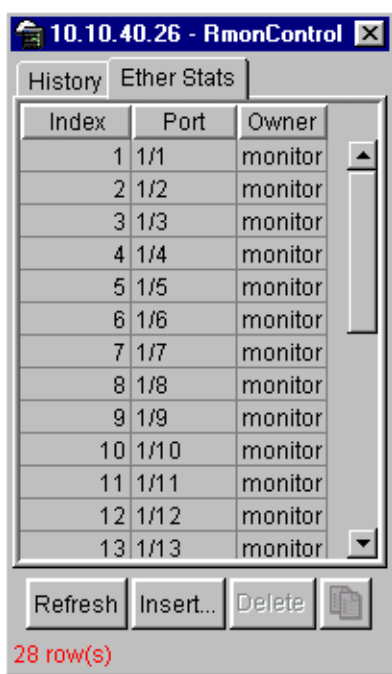
- 1 From the Device Manager main menu, choose RMON > Control.

The RMONControl dialog box opens with the History tab displayed (Figure 75 on page 167).

- 2 Click the Ether Stats tab.

The Ether Stats tab opens (Figure 77).

Figure 77 RMONControl dialog box — Ether Stats tab



[Table 62](#) describes the Ether Stats tab fields.

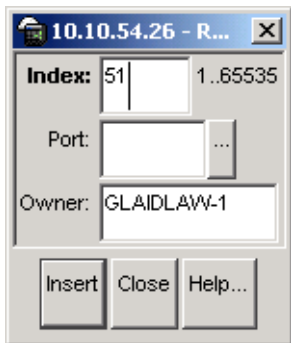
Table 62 Ether Stats tab fields

| Field | Description |
|--------------|---|
| Index | A unique value assigned to each interface. An index identifies an entry in a table. |
| Port | Any Ethernet interface on the device. |
| Owner | The network management system which created this entry. |

- 3 Click Insert.

The RMONControl, Insert Ether Stats dialog box opens (Figure 78).

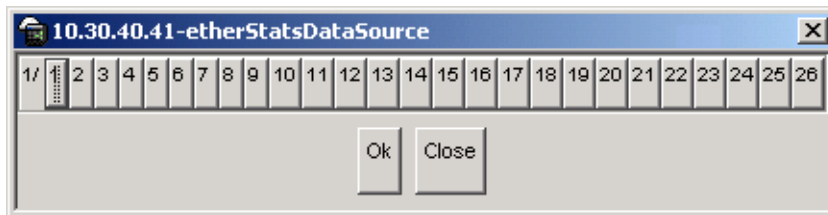
Figure 78 RMONControl, Insert Ether Stats dialog box



- 4 Select the port(s).

Enter the port number you want or select the port from the list menu (Figure 79).

Figure 79 RMONControl, Insert Ether Stats dialog box port list



Device Manager assigns the index.

- 5 Click Insert.

The new Ethernet Statistics entry is displayed in the Ether Stats tab.

Disabling Ethernet statistics gathering

To disable Ethernet statistics that you have set:

- 1 From the Device Manager main menu, choose RMON > Control.

The RMONControl dialog box opens with the History tab displayed (Figure 75 on page 167).

- 2 Click the Ether Stats tab.

The Ether Stats tab opens (Figure 78 on page 174).

- 3 Highlight the row that contains the port ID you want to delete.

- 4 Click Delete.

The Ether Stats entry is removed from the table.

Alarms

Alarms are useful when you need to know when the values of a variable go out of range. You can define an RMON alarm for any MIB variable that resolves to an integer value. You cannot use string variables (such as system description) as alarm variables.

All alarms share the following characteristics:

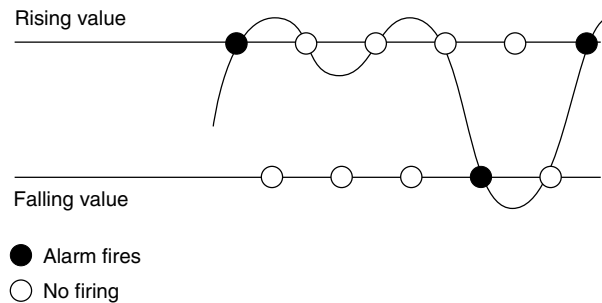
- An upper and lower threshold value is defined.
- A corresponding rising and falling event occurs.
- An alarm interval or polling period is reached.

When alarms are activated, you can view the activity in a log or a trap log, or you can create a script to notify you by beeping a console, sending e-mail, or calling a pager.

How RMON alarms work

The alarm variable is polled and the result is compared against upper and lower limit values you select when you create the alarm. If either limit is reached or crossed during the polling period, then the alarm fires and generates an event that you can view in the event log or the trap log.

The alarm's upper limit is called the *rising value*, and its lower limit is called the *falling value*. RMON periodically samples the data based upon the alarm interval. During the *first* interval that the data passes above the rising value, the alarm fires as a rising event. During the first interval that the data drops below the falling value, the alarm fires as a falling event (Figure 80).

Figure 80 How alarms fire

It is important to note that the alarm fires during the first interval that the sample goes out of range. No additional events are generated for that threshold until the opposite threshold is crossed. Therefore, it is important to carefully define the rising and falling threshold values for alarms to work as expected. Otherwise, incorrect thresholds causes an alarm to fire at every alarm interval.

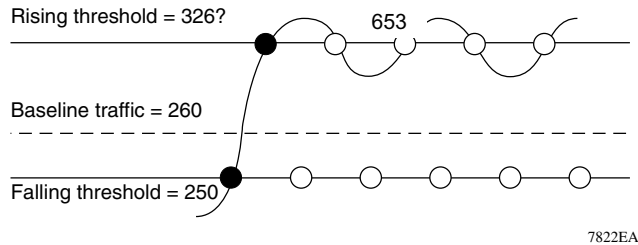
A general guideline is to define one of the threshold values to an expected, baseline value, and then define the opposite threshold as the out-of-bounds limit. Because of sample averaging, the value may be equal to ± 1 of the baseline units. For example, assume an alarm is defined on octets going out of a port as the variable. The intent of the alarm is to provide notification to the system administrator when excessive traffic occurs on that port. If spanning tree is enabled, then 52 octets are transmitted out of the port every 2 seconds, which is equivalent to baseline traffic of 260 octets every 10 seconds. This alarm should provide the notification the system administrator needs if the lower limit of octets going out is defined at 260 and the upper limit is defined at 320 (or at any value greater than $260 + 52 = 312$).

The first time outbound traffic other than spanning tree Bridge Protocol Data Units (BPDUs) occurs, the rising alarm fires. When outbound traffic other than spanning tree ceases, the falling alarm fires. This process provides the system administrator with time intervals of any nonbaseline outbound traffic.

If the alarm is defined with a falling threshold less than 260 (assuming the alarm polling interval is 10 seconds), say 250, then the rising alarm can fire only once ([Figure 81](#)). The reason is that for the rising alarm to fire a second time, the falling alarm (the opposite threshold) must fire. Unless the port becomes inactive or

spanning tree is disabled (which would cause the value for outbound octets to drop to zero), the falling alarm cannot fire because the baseline traffic is always greater than the value of the falling threshold. By definition, the failure of the falling alarm to fire prevents the rising alarm from firing a second time.

Figure 81 Alarm example — threshold less than 260



Creating alarms

When you create an alarm, you select a variable from the variable list and a port, or other switch component, to which it is connected. Some variables require port IDs, card IDs, or other indices (for example, spanning tree group IDs). You then select a rising and a falling threshold value. The rising and falling values are compared against the actual value of the variable that you choose. If the variable falls outside of the rising or falling value range, an alarm is triggered and an event is logged or trapped.

When you create an alarm, you also select a sample type, which can be either absolute or delta. *Absolute* alarms are defined on the cumulative 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.

Most alarm variables related to Ethernet traffic are set to *delta* 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. If you track the current values of a given delta-valued alarm and add them together, therefore, the result is twice the actual value. (This result is not an error in the software.)

Alarm Manager example



Note: The example alarm described in the following procedure generates at least one alarm every five minutes. The example is intended only to demonstrate how alarms fire; it is not a useful alarm. Because of the high frequency, you may want to delete this alarm and replace it with a practical setting.

To create an alarm to receive statistics and history using default values:

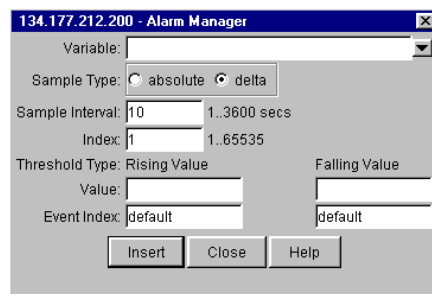
1 Do one of the following:

- From the Device Manager main menu, choose RMON >Alarm Manager.
- On the toolbar, click the Alarm Manager button.



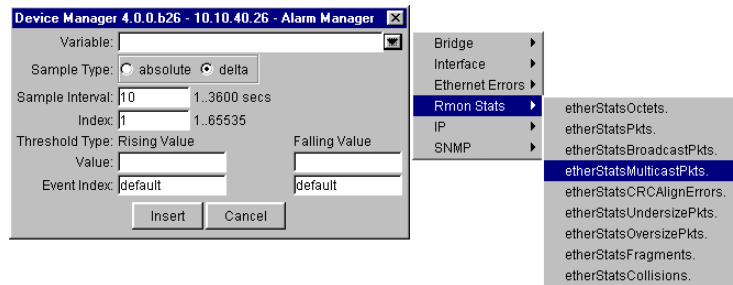
The Alarm Manager dialog box opens ([Figure 82](#)).

Figure 82 Alarm Manager dialog box



- In the variable field, select a variable for the alarm from the list and a port (or other ID) on which you want to set an alarm (Figure 83).

Figure 83 Alarm variable list



Alarm variables are in three formats, depending on the type:

- A chassis alarm ends in .x where the x index is hard-coded. No further information is required.
- A card, spanning tree group (STG) or EtherStat alarm ends with a dot (.). You must enter a card number, STG ID, IP address, or EtherStat information.
- A port alarm ends with no dot or index and requires using the port shortcut menu. An example of a port alarm would be ifInOctets (interface incoming octet count).

For this example, select Bridge > dot1dStpTopChanges.0 from the variable list. This example is a chassis alarm, indicated by the “.0” in the variable.

- For this example, select a rising value of 4 and a falling value of 0.
- Leave the remaining fields at their default values, including a sample type of Delta. Click Insert.

If you want to make field changes, see the field descriptions shown in [Table 63](#).

Table 63 RMON Insert Alarm dialog box fields

| Field | Description | |
|-----------------|---|---|
| Variable | Name and type of alarm—indicated by the format: <i>alarmname.x</i> where x=0 indicates a chassis alarm. <i>alarmname</i> . where the user must specify the index. This will be a card number for module-related alarms, an STG ID for spanning tree group alarms (the default STG is 1, other STG IDs are user-configured), or the Ether Statistics Control Index for RMON Stats alarms <i>alarmname</i> with no dot or index is a port-related alarm and results in display of the port selection tool. | |
| Sample Type | Can be either absolute or delta. For more information about sample types, refer to “Creating alarms” on page 178 . | |
| Sample Interval | Time period (in seconds) over which the data is sampled and compared with the rising and falling thresholds. | |
| Index | Uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device. | |
| Threshold Type | Rising Value | Falling Value |
| Value | 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, generates a single event. | When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, generates a single event. |
| Event Index | Index of the event entry that is used when a rising threshold is crossed. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. (Generally, accept the default that is already filled in.) | Index of the event entry that is used when a falling threshold is crossed. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. (Generally, accept the default that is already filled in.) |

To view the RMON statistics and history for the port for which you have created an alarm:

- 1 Select the port on which you have created an alarm.
- 2 From the Device Manager main menu, choose RMON > Control.

The RMONControl dialog box opens with the History tab displayed ([Figure 75 on page 167](#)).

- 3 Click the Ether Stats tab to view statistics (Figure 79 on page 174).
The RMONAlarms dialog box opens with the Alarms tab (Figure 84) displayed.

Figure 84 RMONAlarms dialog box — Alarms tab



Table 64 describes the fields on the Alarms tab.

Table 64 Describes the fields on the Alarms tab

| Field | Description |
|-------------|---|
| Index | Uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device |
| Interval | The interval in seconds over which data is sampled and compared with the rising and falling thresholds. When setting this variable, note that in the case of deltaValue sampling, you should set the interval short enough so that the sampled variable is very unlikely to increase or decrease by more than $2^{31} - 1$ during a single sampling interval. |
| Variable | The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Counter, Gauge, or TimeTicks) may be sampled. |
| Sample Type | The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue(1), the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue(2), the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds. |
| Value | The value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value is the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value is the sampled value at the end of the period. This is the value that is compared with the rising and falling thresholds. The value during the current sampling period is not made available until the period is completed and remains available until the next period completes. |

Table 64 Describes the fields on the Alarms tab (continued)

| Field | Description |
|-------------------|--|
| StartupAlarm | The alarm that may be sent when this entry is first set to valid. If the first sample after this entry becomes valid is greater than or equal to the risingThreshold and alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3), then a single rising alarm is generated. If the first sample after this entry becomes valid is less than or equal to the fallingThreshold and alarmStartupAlarm is equal to fallingAlarm(2) or risingOrFallingAlarm(3), then a single falling alarm is generated. |
| RisingThreshold | A threshold for the sampled statistic. 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 is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal to this threshold and the associated alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3). After a rising event is generated, another such event is not generated until the sampled value falls below this threshold and reaches the alarmFallingThreshold. |
| RisingEventIndex | The index of the eventEntry that is used when a rising threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If there is no corresponding entry in the eventTable, then no association exists. In particular, if this value is zero, no associated event is generated, because zero is not a valid event index. |
| FallingThreshold | A threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is less than or equal to this threshold and the associated alarmStartupAlarm is equal to fallingAlarm(2) or risingOrFallingAlarm(3). After a falling event is generated, another such event is not generated until the sampled value rises above this threshold and reaches the alarmRisingThreshold. |
| FallingEventIndex | The index of the eventEntry that is used when a falling threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If there is no corresponding entry in the eventTable, then no association exists. In particular, if this value is zero, no associated event is generated, because zero is not a valid event index. |
| Owner | The network management system which created this entry. |
| Status | The status of this alarm entry. |

To delete an alarm:

- 1 From the Device Manager main menu, choose RMON >Alarms.
The RMONAlarms dialog box opens with the Alarms tab (Figure 84) displayed.
- 2 Click any field for the alarm that you want to delete to highlight it.
- 3 Click Delete.

Events

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

How events work

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

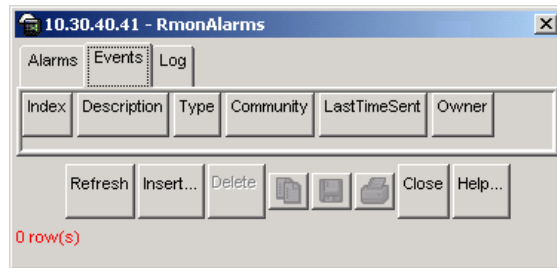
- RisingEvent
- FallingEvent

The default events specify that when an alarm goes out of range, the “firing” of the alarm will be 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. Likewise, when an alarm passes the falling threshold, the falling event specifies that this information be sent to a trap and a log.

Viewing an event

To view a table of events:

- 1 From the Device Manager main menu, choose RMON > Alarms.
The RMONAlarms dialog box opens displaying the Alarms tab ([Figure 84 on page 182](#)).
- 2 Click the Events tab.
The Events tab opens ([Figure 85](#)).

Figure 85 RMONAlarms dialog box — Events tab

[Table 65](#) describes the RMONAlarms Events tab fields.

Table 65 Events tab fields

| Field | Description |
|--------------|--|
| Index | This index uniquely identifies an entry in the event table. Each entry defines one event that is to be generated when the appropriate conditions occur. |
| Description | Specifies whether the event is a rising or falling event. |
| Type | The type of notification that the Device Manager provides about this event. In the case of log, an entry is made in the log table for each event. In the case of trap, an SNMP trap is sent to one or more management stations. Possible notifications follow: <ul style="list-style-type: none"> • none • log • trap • log-and-trap |
| Community | The SNMP community string acts as a password. Only those management applications with this community string can view the alarms. |
| LastTimeSent | The value of sysUpTime at the time this event entry last generated an event. If this entry has not generated any events, this value is zero. |
| Owner | If traps are specified to be sent to the owner, then this is the name of the machine that will receive alarm traps. |

Creating an event

To create an event:

- 1 In the RMONAlarms dialog box Events tab, click Insert.

The RMONAlarms, Insert Events dialog box opens (Figure 86).

Figure 86 Insert Events dialog box

- 2 In the Description field, type a name for the event.

- 3 Select the type of event you want.

You can set the event type to log to save memory or to snmp-trap to reduce traffic from the switch or for better CPU utilization.

If you select snmp-trap or log-and-trap, you must set trap receivers.

- 4 Click Insert.

The new event is displayed in the Events tab (Figure 87).

Figure 87 New event in the Events tab

| Index | Description | Type | Community | LastTimeSent | Owner | Status |
|-------|---------------|--------------|-----------|--------------|-------------------------------------|--------|
| 60534 | Rising Event | log-and-trap | public | none | jritter-lt.corpwest.baynetworks.com | valid |
| 60535 | Falling Event | log-and-trap | public | 0h:22m:7s | jritter-lt.corpwest.baynetworks.com | valid |
| 60536 | Test123 | log-and-trap | public | none | | valid |

Deleting an event

To delete an event:

- 1 In the Events tab, highlight an event Description.
- 2 Click Delete.

The event is removed from the table.

Log information

The Log tab chronicles and describes the alarm activity, which is then generated to viewed.

To view the Log tab:

- 1 From the Device Manager main menu, choose RMON > Alarms.
The RMONAlarm dialog box opens with the Alarms tab displayed ([Figure 84 on page 182](#)).
- 2 Click the Log tab.
The Log tab opens ([Figure 88](#)).

Figure 88 Log tab

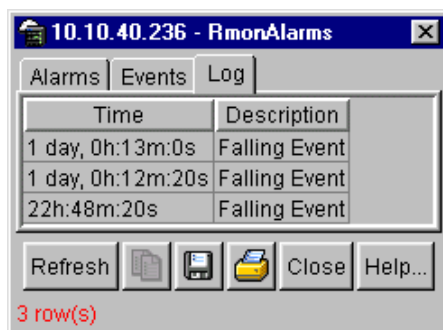


Table 66 describes the Log tab fields.

Table 66 Log tab fields

| Item | Description |
|-------------|--|
| Time | An implementation-dependent description of the event that activated the log entry. |
| Description | Specifies whether the event is a rising or falling event. |

Chapter 9

Security parameters

You can set the security features for a switch so that the actions are performed by the software when a violation occurs. The security actions you specify are applied to all ports of the switch.

This chapter describes the Security information available in Device Manager on the following tabs:

- [General tab](#) (next)
- [SecurityList tab](#) (page 192)
- [AuthConfig tab](#) (page 194)
- [AuthStatus tab](#) (page 197)
- [AuthViolation tab](#) (page 199)
- [SSH tab](#) (page 201)
- [SSH Sessions tab](#) (page 202)

General tab

The General tab allows you to set and view general security information for the switch.

To view the General tab:

- From the Device Manager menu bar, select Edit > Security.

The Security dialog box opens with the General tab displayed ([Figure 89](#)).

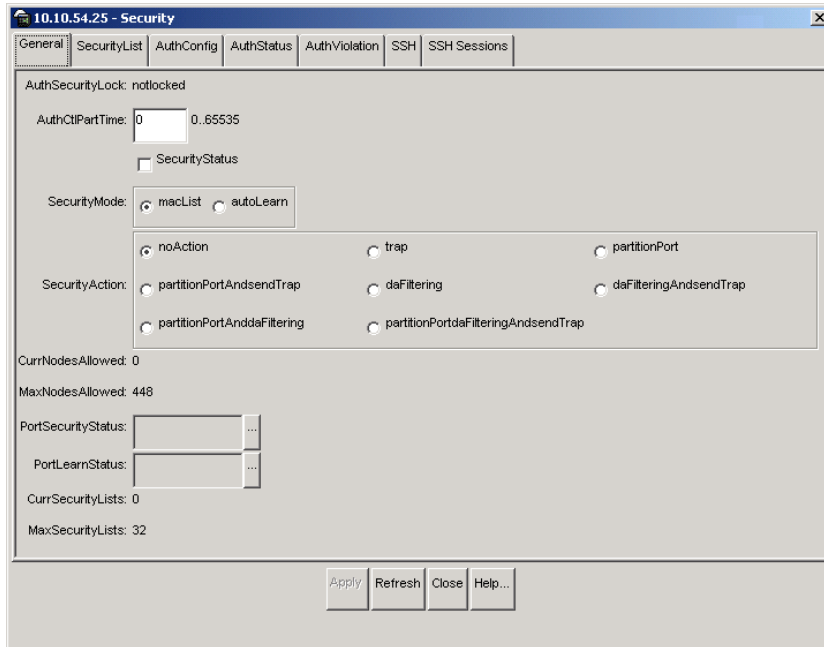
Figure 89 General tab

Table 67 describes the General tab items.

Table 67 General tab items

| Items | Description |
|------------------|--|
| AuthSecurityLock | If this parameter is listed as “locked,” the agent refuses all requests to modify the security configuration. Entries also include: <ul style="list-style-type: none"> • other • notlocked |
| AuthCtlPartTime | This value indicates the duration of the time for port partitioning in seconds. Default: 0 (zero). When the value is zero, port remains partitioned until it is manually re-enabled. |
| SecurityStatus | Indicates whether or not the switch security feature is enabled. |

Table 67 General tab items (continued)

| Items | Description |
|--------------------|---|
| SecurityMode | Mode of switch security. Entries include: <ul style="list-style-type: none"> • macList: Indicates that the switch is in the MAC-list mode. You can configure more than one MAC address per port. • autoLearn: Indicates that the switch learns the first MAC address on each port as an allowed address of that port. |
| SecurityAction | Actions performed by the software when a violation occurs (when SecurityStatus is enabled). The security action specified here applies to all ports of the switch. A blocked address causes the port to be partitioned when unauthorized access is attempted. Selections include: <ul style="list-style-type: none"> • noAction: Port does not have any security assigned to it, or the security feature is turned off. • trap: Listed trap. • partitionPort: Port is partitioned. • partitionPortAndsendTrap: Port is partitioned and traps are sent to the trap receiver. • daFiltering: Port filters out the frames where the destination address field is the MAC address of unauthorized Station. • daFilteringAndsendTrap: Port filters out the frames where the destination address field is the MAC address of unauthorized station. Traps are sent to trap receiver(s). • partitionPortAnddaFiltering: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. • partitionPortdaFilteringAndsendTrap: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. Traps are sent to trap receiver(s). <p>Note: “da” means destination address.</p> |
| CurrNodesAllowed | Current number of entries of the nodes allowed in the AuthConfig tab. |
| MaxNodesAllowed | Maximum number of entries of the nodes allowed in the AuthConfig tab. |
| PortSecurityStatus | Set of ports for which security is enabled. |
| PortLearnStatus | Set of ports where auto-learning is enabled. |
| CurrSecurityLists | Current number of entries of the Security listed in the SecurityList tab |
| MaxSecurityLists | Maximum entries of the Security listed in the SecurityList tab. |

SecurityList tab

The SecurityList tab contains a list of Security port items.

To view the SecurityList tab:

- 1 From the Device Manager menu bar, select Edit > Security.

The Security window opens with the General tab displayed (Figure 89 on page 190).

- 2 Click the SecurityList tab.

The SecurityList tab opens (Figure 90).

Figure 90 SecurityList tab

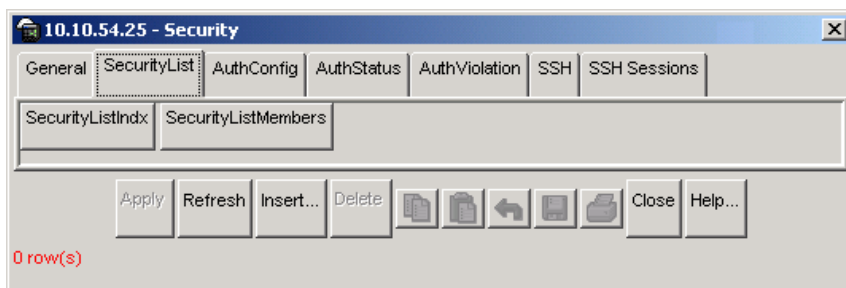


Table 68 describes the SecurityList tab fields.

Table 68 SecurityList tab fields

| Field | Description |
|---------------------|---|
| SecurityListIdx | An index of the security list. This corresponds to the Security port list that can be used as an index into AuthConfig tab. |
| SecurityListMembers | The set of ports that are currently members in the Port list. |

Security, Insert SecurityList dialog box

Security, Insert SecurityList dialog box has editable fields for the SecurityList tab. Each row in this dialog box has information that can be updated or changed.

To view the Security, Insert AuthConfig dialog box:

- 1 From the Device Manager menu bar, select Edit > Security.

The Security window opens with the General tab displayed ([Figure 89 on page 190](#)).

- 2 Click the SecurityList tab.

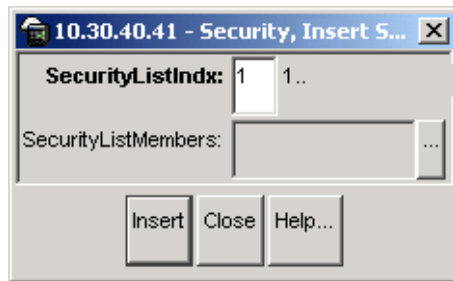
The SecurityList tab opens ([Figure 90 on page 192](#)).

- 3 Click inside a row.

- 4 Click Insert.

The Security, Insert SecurityList dialog box opens ([Figure 91](#)).

Figure 91 Security, Insert SecurityList dialog box



[Table 69](#) describes the Security, Insert AuthConfig dialog box items.

Table 69 Security, Insert AuthConfig dialog box fields

| Field | Description |
|---------------------|---|
| SecurityListIdx | An index of the security list. This corresponds to the Security port list that can be used as an index into AuthConfig tab. |
| SecurityListMembers | The set of ports that are currently members in the Port list. |

AuthConfig tab

The AuthConfig tab contains a list of boards, ports and MAC addresses that have the security configuration. An SNMP SET PDU for a row in the tab requires the entire sequence of the MIB objects in each entry to be stored in one PDU. Otherwise, GENERR return-value is returned.

To view the AuthConfig tab:

- 1 From the Device Manager menu bar, select Edit > Security.

The Security window opens with the General tab displayed (Figure 89 on page 190).

- 2 Click the AuthConfig tab.

The AuthConfig tab opens (Figure 96).

Figure 92 AuthConfig tab

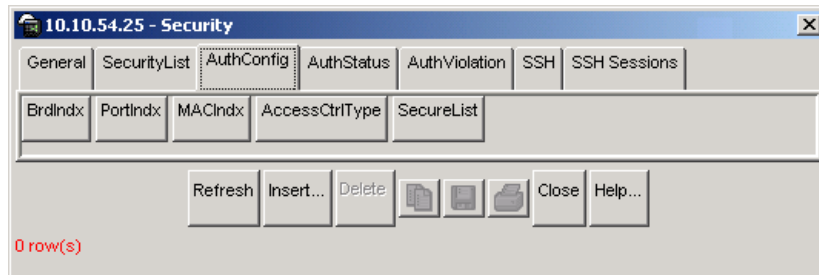


Table 70 describes the AuthConfig tab fields.

Table 70 AuthConfig tab fields

| Field | Description |
|---------|---|
| BrdIdx | Index of the slot containing the board on where the port is located. If you specify SecureList, this field must be 0. |
| PortIdx | Index of the port on the board. If you specify SecureList, this field must be 0. |
| MACIdx | An index of MAC addresses that are designated as allowed (station). |

Table 70 AuthConfig tab fields (continued)

| Field | Description |
|----------------|---|
| AccessCtrlType | Displays the node entry as <code>node allowed</code> . A MAC address may be allowed on multiple ports. |
| SecureList | The index of the security list. This value is meaningful only if BrdIndx and PortIndx values are set to zero. For other board and port index values, it should also have the value of zero. The corresponding MAC Address of this entry is allowed or blocked on all ports of that this port list. |

Security, Insert AuthConfig dialog box

Security, Insert AuthConfig dialog box has editable fields for the AuthConfig tab. Each row in this dialog box has information that can be updated or changed.

To view the Security, Insert AuthConfig dialog box:

- 1 From the Device Manager menu bar, select Edit > Security.

The Security window opens with the General tab displayed ([Figure 89 on page 190](#)).

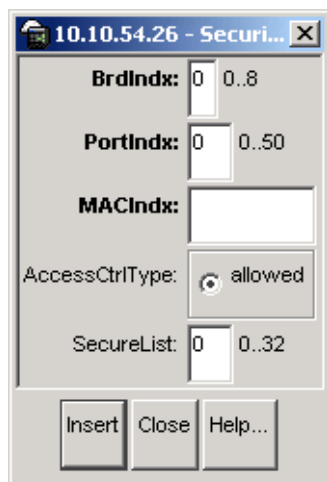
- 2 Click the AuthConfig tab.

The AuthConfig tab opens ([Figure 96 on page 201](#)).

- 3 Click inside a row.

- 4 Click Insert.

The Security, Insert AuthConfig dialog box opens ([Figure 93](#)).

Figure 93 Security, Insert AuthConfig dialog box

[Table 71](#) describes the Security, Insert AuthConfig dialog box fields.

Table 71 Security, Insert AuthConfig dialog box fields

| Item | Description |
|----------------|---|
| BrdIndx | Index of the board. This corresponds to the index of the unit containing the board, but only if the index is greater than zero. A zero index is a wild card. |
| PortIndx | Index of the port on the board. This corresponds to the index of the last manageable port on the board, but only if the index is greater than zero. A zero index is a wild card. |
| MACIndx | An index of MAC addresses that are either designated as allowed (station) or not-allowed (station). |
| AccessCtrlType | Displays whether the node entry is node allowed or node blocked. A MAC address may be allowed on multiple ports. |
| SecureList | The index of the security list. This value is meaningful only if BrdIndx and PortIndx values are set to zero. For other board and port index values, it should also have the value of zero. The corresponding MAC Address of this entry is allowed or blocked on all ports of that this port list. |

AuthStatus tab

The AuthStatus tab displays information of the authorized boards and port status data collection. Information includes actions to be performed when an unauthorized station is detected and the current security status of a port. An entries in this tab may include:

- A single MAC address
- All MAC addresses on a single port
- A single port
- All the ports on a single board
- A particular port on all the boards
- All the ports on all the boards.

To view the AuthStatus tab:

- 1** From the Device Manager menu bar, select Edit > Security.

The Security window opens with the General tab displayed ([Figure 89 on page 190](#)).

- 2** Click the AuthStatus tab.

The AuthStatus tab opens ([Figure 94](#)).

Figure 94 AuthStatus tab

| AuthStatusBrdIdx | AuthStatusPortIdx | AuthStatusMACIdx | CurrentAccessCtrlType | CurrentActionMode | CurrentPortSecurStatus |
|------------------|-------------------|-------------------|-----------------------|-------------------|------------------------|
| 2 | 1 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 2 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 3 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 4 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 5 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 6 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 7 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 8 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 9 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 10 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 11 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 12 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 13 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 14 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 15 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 16 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 17 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 18 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 19 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 20 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 21 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 22 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 23 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 24 | 00:00:00:00:00:00 | allow | noAction | notApplicable |
| 2 | 25 | 00:00:00:00:00:00 | allow | noAction | notApplicable |

Table 72 describes the AuthStatus tab fields.

Table 72 AuthStatus tab fields

| Item | Description |
|-----------------------|---|
| AuthStatusBrdIdx | The index of the board. This corresponds to the index of the slot containing the board if the index is greater than zero. |
| AuthStatusPortIdx | The index of the port on the board. This corresponds to the index of the last manageable port on the board if the index is greater than zero. |
| AuthStatusMACIdx | The index of MAC address on the port. This corresponds to the index of the MAC address on the port if the index is greater than zero. |
| CurrentAccessCtrlType | Displays whether the node entry is node allowed or node blocked type. |

Table 72 AuthStatus tab fields (continued)

| Item | Description |
|------------------------|--|
| CurrentActionMode | <p>A value representing the type of information contained, including:</p> <p>noAction: Port does not have any security assigned to it, or the security feature is turned off.</p> <p>partitionPort: Port is partitioned.</p> <p>partitionPortAndsendTrap: Port is partitioned and traps are sent to the trap receiver.</p> <p>Filtering: Port filters out the frames, where the destination address field is the MAC address of unauthorized station.</p> <p>FilteringAndsendTrap: Port filters out the frames, where the destination address field is the MAC address of unauthorized station. Trap are sent to trap receiver.</p> <p>sendTrap: A trap is sent to trap receiver(s).</p> <p>partitionPortAnddaFiltering: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station.</p> <p>partitionPortdaFilteringAndsendTrap: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. Traps are sent to trap receiver(s).</p> |
| CurrentPortSecurStatus | <p>Displays the security status of the current port, including:</p> <ul style="list-style-type: none"> • If the port is disabled, notApplicable is returned. • If the port is in a normal state, portSecure is returned. • If the port is partitioned, portPartition is returned. |

AuthViolation tab

The AuthViolation tab contains a list of boards and ports where network access violations have occurred, and also the identity of the offending MAC addresses.

To view the AuthViolation tab:

- 1 From the Device Manager menu bar, select Edit > Security.

The Security window opens with the General tab displayed ([Figure 89 on page 190](#)).

2 Click the AuthViolation tab.

The AuthViolation tab opens (Figure 95).

Figure 95 AuthViolation tab

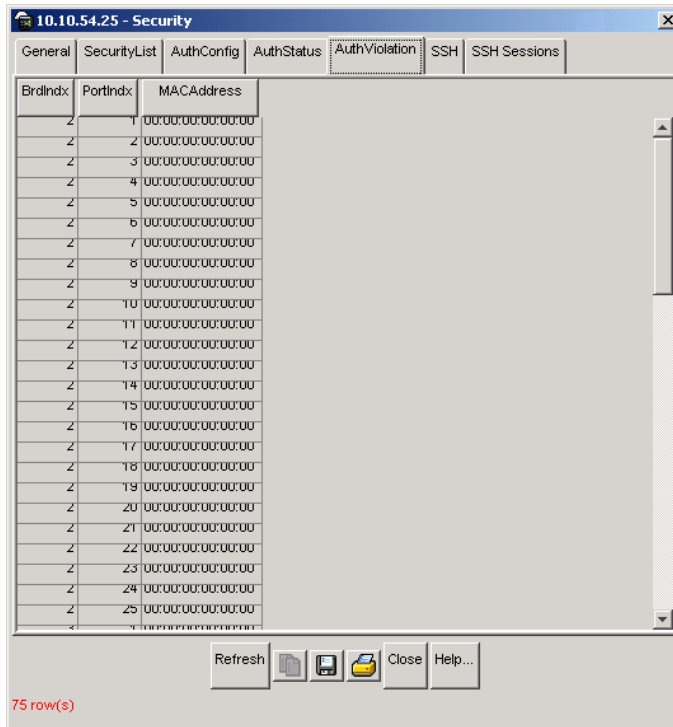


Table 73 describes fields for the AuthViolation tab fields.

Table 73 AuthViolation tab fields

| Field | Description |
|------------|--|
| BrdIdx | The index of the board. This corresponds to the unit containing the board. The index will be 1 where it is not applicable. |
| PortIdx | The index of the port on the board. This corresponds to the port on that a security violation was seen. |
| MACAddress | The MAC address of the device attempting unauthorized network access (MAC address-based security). |

SSH tab

The SSH tab displays the parameters available for SSH.

To view the SSH tab:

- 1 From the Device Manager menu bar, select Edit > Security.

The Security window opens with the General tab displayed ([Figure 89 on page 190](#)).

- 2 Click the SSH tab.

The SSH tab opens ([Figure 96](#)).

Figure 96 SSH tab

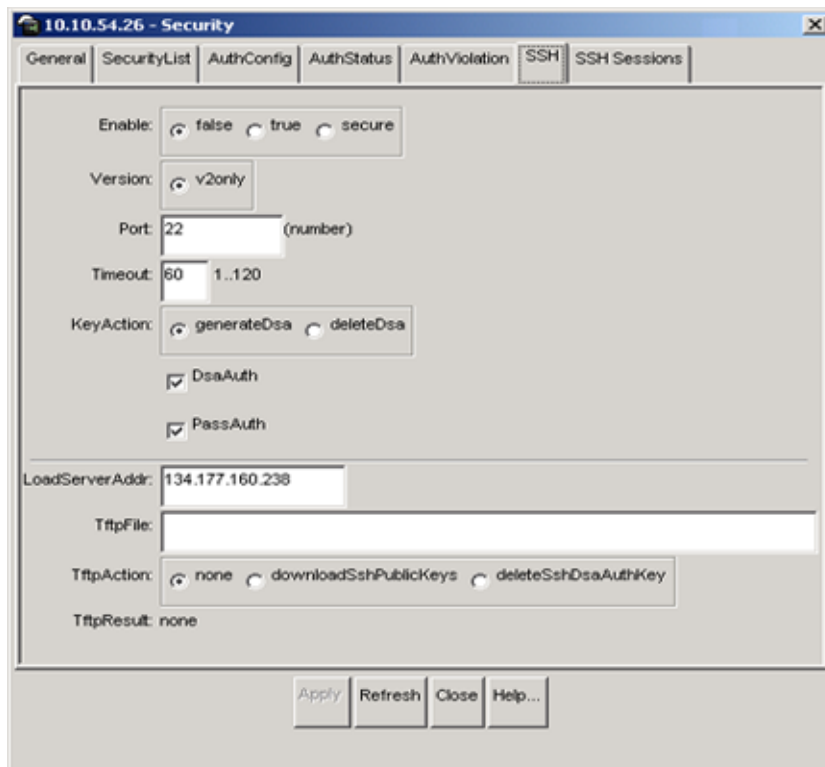


Table 74 describes the SSH tab fields.

Table 74 SSH tab fields

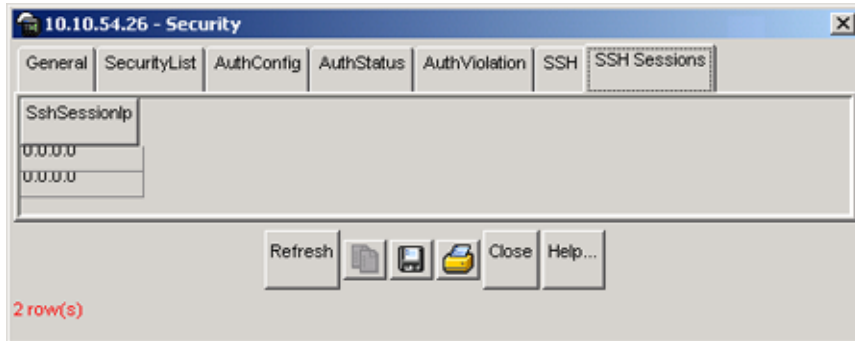
| Field | Description |
|----------------|--|
| Enable | Enables, disables or securely enables SSH. Securely enable turns off other daemon flag, and it takes effect after reboot |
| Version | Indicates the SSH version |
| Port | Indicates the SSH connection port. |
| Timeout | Indicates the SSH connection timeout in seconds. |
| KeyAction | Indicates the SSH key action |
| DsaKeySize | Indicates the SSH Dsa key size. |
| DsaAuth | Enables or disables the SSH DSA authentication |
| PathAuth | Enables or disables the SSH RSA authentication |
| LoadServerAddr | Indicates the current server IP address |
| TftpFile | Indicates the name of file for the TFTP transfer |
| TftpAction | Indicates the SSH public keys that is set to initiate a TFTP download. |
| TftpResult | Indicates the retrieved value of the TFTP transfer. |

SSH Sessions tab

The SSH Sessions tab displays the currently active SSH sessions.

To view the SSH Sessions tab:

- 1 From the Device Manager menu bar, select Edit > Security.
The Security window opens with the General tab displayed ([Figure 89 on page 190](#)).
- 2 Click the SSH Sessions tab.
The SSH Sessions tab opens ([Figure 97](#)).

Figure 97 SSH Sessions tab

[Table 74](#) describes the SSH Sessions tab fields.

Table 75 SSH Sessions tab fields

| Field | Description |
|-------------|--|
| SSHSessions | Lists the currently active SSH sessions. |

Chapter 10

Working with SNMPv3

SNMPv3 Overview

Simple Network Management Protocol (SNMP) provides a mechanism to remotely configure and manage a network device. An SNMP agent is a software process that listens on UDP port 161 for SNMP messages, and sends "trap" messages using destination UDP port 162.

SNMPv3 is based on the architecture of SNMPv1 and SNMPv2c. It supports better authentication and data encryption than SNMPv1 and SNMPv2c.

SNMPv3 provides protection against the following security threats:

- Modification of SNMP messages by a third party.
- Impersonation of an authorized SNMP user by an unauthorized person.
- Disclosure of network management information to unauthorized parties.
- Delayed SNMP message replays or message redirection attacks.

The new configuration parameters introduced in SNMPv3 makes it more secure and flexible than the previous versions of SNMP.

For more information on the SNMPv3 architecture, see RFC 3411.

This chapter describes the following concepts associated with SNMPv3:

- [“Initial Login with an SNMPv3 User”](#), next
- [“User-based Security Model” on page 206](#)
- [“View-based Access Control Model” on page 211](#)
- [“Management Targets” on page 219](#)

- [“The Notify Table” on page 224](#)

Initial Login with an SNMPv3 User

In order to configure SNMPv3 with Device Manager, you must first login and create an SNMPv3 user through the NNCLI or web interface. If you specify only read and write community strings at the time of logging in, you will not have sufficient rights to view or change the SNMPv3 settings of the switch.



Caution: By default, the NNCLI and web interface are not password protected. Nortel Networks strongly recommends that once you have setup an SNMPv3 user, you should change or delete all factory default settings that might allow an unauthorized person to login to your device.

For more information on how to configure an initial SNMPv3 user, see *Using Web-Based Management for the BayStack 420/425 Switch, Software Release 3.1 (215660-B)* or *Reference for the BayStack 425 Command Line Interface, Software Release 3.1 (215659-B)*.

To log in to the BayStack 420/425 Device Manager as an SNMPv3 user:

- 1 On the Device Manager menu bar select Device > Open.
- 2 In the Device Name field enter the DNS name or the IP address of the switch.
- 3 Select the V3 enable checkbox (notice that the default Read and Write community strings are grayed out when SNMPv3 is enabled).
- 4 Enter the login name of the SNMPv3 user.
- 5 From the Authentication Protocol pull-down list, select: MD5, SHA or None.
- 6 If the user is configured to use an authentication protocol, enter the authentication password in the Authentication Password field.

User-based Security Model

The User-based Security Model (USM) provides a mechanisms to authenticate and encrypt SNMPv3 messages.

A message, if configured, is authenticated with the help of a one-way hash function that is associated with an individual user ID. In the BayStack 425, a user can be configured to use the HMAC-MD5-96 or the HMAC-SHA-96 algorithm, for the authentication of SNMPv3 messages.

An SNMPv3 message, if configured, is encrypted with the help of the Cipher Block Chaining - Data Encryption Standard (CBC-DEC).

An SNMPv3 user can be configured in three ways.

[Table 76 on page 207](#), describes the ways in which an SNMPv3 user can be configured.

Table 76 SNMPv3 user configuration method

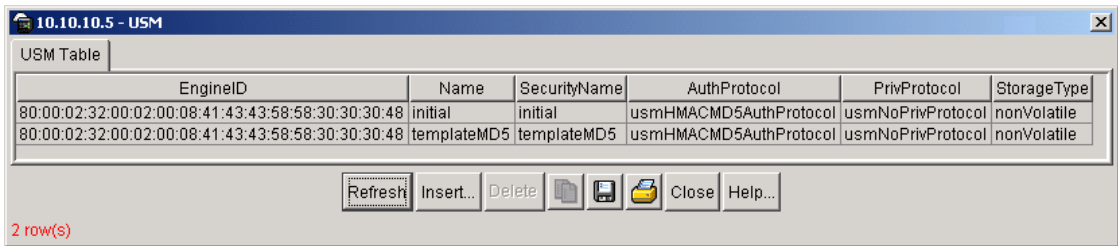
| SNMPv3 Configuration Method | Description |
|------------------------------------|--|
| NoAuthNoPriv | The user cannot use an authentication or an encryption mechanism. |
| AuthNoPriv | The user may use an authentication but not an encryption mechanisms. |
| AuthPriv | The user may use an authentication and as well as an encryption mechanism. |

For more information on USM, see RFC 3414.

Configuring the User-based Security Model

To create a user in the USM table:

- 1 From the Device Manager menu bar, click Edit > SnmpV3 > USM Table.
The USM dialog box opens ([Figure 98](#)).

Figure 98 USM dialog box

[Table 77](#) describes the USM tab fields.

Table 77 USM dialog box fields

| Field | Description |
|--------------|--|
| EngineID | Indicates the SNMP engine's administratively-unique Identifier |
| Name | Indicates the qdp h# i##h#vhu#q#vp Xvhu! |
| SecurityName | Creates the name that is used as an index to the table. The range is 1 to 32 characters. |
| AuthProtocol | Identifies the authentication protocol used. |
| PrivProtocol | Identifies the privacy protocol used. |
| StorageType | Specifies whether the table entry (row) should be stored in volatile or non-volatile memory. If the entry is stored in volatile memory, it will not persist if the switch loses power. |

2 Click Insert.

The USM, Insert USM Table dialog box opens ([Figure 99](#)).

Figure 99 USM, Insert USM Table dialog box

- 3 Enter a name.
- 4 In the Clone From User list, select a security name from which the new entry should copy authentication data and privacy data. For example, Authentication Protocol, Authentication password, Privacy Protocol, and Privacy password.



Note: The Clone From User you select will define the maximum authentication and privacy settings for a new user. For example, if the Clone From User does not use an authentication or encryption protocol, users created from this clone will not be able to use the authentication or the encryption protocol. For this reason, it is recommended that you assign both an authentication and encryption protocol to the first user you create through the NNCLI or web interface.

- 5 From the Auth Protocol pull-down list, select an authentication protocol for this user. If you select an authentication protocol, you must enter an old and new authentication password in the next two fields.
- 6 In the Cloned User's Auth Password field, enter the authentication password of the Cloned From User.

- 7 In the New User's Auth Password field, enter a new authentication password for this user.
- 8 Select a privacy protocol. If you choose to specify a privacy protocol, you must enter an old and new privacy password in the next two fields. This is optional but recommended.
- 9 Enter the Cloned User's Priv Password.
- 10 Enter a new privacy password for this user.
- 11 Click Insert.

The new entry is shown.

Table 78 describes the USM, Insert USM Table dialog box fields.

Table 78 USM, Insert USM Table dialog box fields

| Field | Description |
|--------------------------------|---|
| New User Name | Creates the new entry with this security name. The name is used as an index to the table. The range is 1 to 32 characters. |
| CloneFrom | Specifies the security name from which the new entry must copy privacy and authentication parameters. The range is 1 to 32 characters. |
| AuthProtocol (Optional) | Assigns an authentication protocol (or no authentication) from a pulldown menu. If you select this, you must enter an old AuthPass and a new AuthPass. |
| Cloned User's Auth Password | Specifies the current authentication password. |
| New User's Auth Password | Specifies the new authentication password to use for this user. |
| Priv Protocol (Optional) | Assigns a privacy protocol (or no privacy) from a pulldown menu. |
| F σ qhg#Kvhú# Súy#Sdvz r úg | Specifies the current privacy password |
| New User's Priv Password | Specifies the new privacy password to use for this user entry. |
| StorageType | Specifies whether this table entry (row) should be stored in volatile or non-volatile memory. If the entry is stored in volatile memory, it will not persist if the switch loses power. |

View-based Access Control Model

The View-based Access Control Model (VACM) is used to map a user to a set of access rights and MIB views. This mapping is done with the help of three tables.

[Table 79 on page 211](#), describes the tables with the help of which a user is mapped to access rights and MIB views.

Table 79 View-based access control mapping tables

| Table Name | Description |
|--------------------------|---|
| Group Membership table | Defines a set of users that can be referenced by a single group name. |
| Group Access Right table | Associates a group with Read, Write, and Notify views. |
| MIB View table | Defines a set of MIB subtrees or objects. |

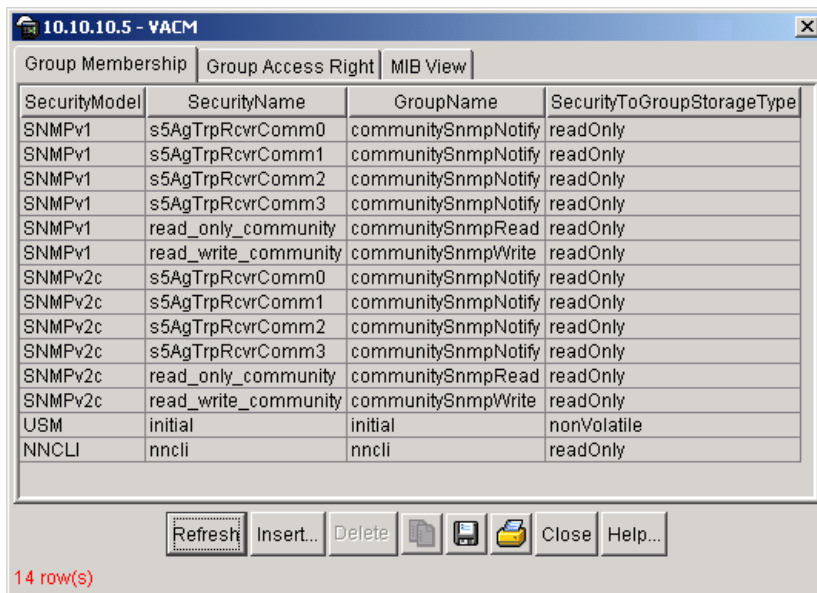
For more detailed information on VACM, see RFC 3415.

Defining Group Membership with VACM

To add members to a group in the View-based Access Control Model (VACM) table:

- 1 From the Device Manager menu bar, click Edit > SnmpV3 > VACM table.

The VACM dialog box with the Group Membership tab options visible opens ([Figure 100](#)).

Figure 100 VACM dialog, Group Membership tab

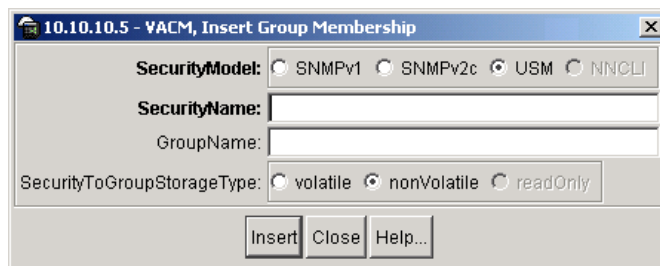
[Table 80](#) describes the Group Membership tab fields.

Table 80 Group Membership tab fields

| Field | Description |
|----------------------------|---|
| SecurityModel | The security model for the entry. |
| SecurityName | The name of an entry in the USM table or the Community Table. |
| GroupName | The name of the group to which this entry belongs. When multiple entries in this table have the same GroupName, they all belong to the same group. |
| SecurityToGroupStorageType | Specifies whether this table entry (row) should be stored in volatile or non-volatile memory. If the entry is stored in volatile memory, it will not persist if the switch loses power. |

2 Click Insert.

The VACM, Insert Group Membership dialog box opens ([Figure 101](#)).

Figure 101 VACM, Insert Group Membership dialog box

- 3 Select a SecurityModel.
- 4 Enter a SecurityName.
- 5 Enter a GroupName.
- 6 Click Insert.

The new group membership is shown in the list.

Assigning Group Access Rights with VACM

To assign new access rights to a group:

To create new access for a group:

- 1 From the Device Manager menu bar, click Edit > SnmpV3 > VACM table.
The VACM dialog box opens (Figure 100).
- 2 Click the Group Access Right tab.
The Group Access Right tab displays (Figure 102).

Figure 102 Group Access Right tab

| vacmGroupName | ContextPrefix | SecurityModel | SecurityLevel | ContextMatch | ReadViewName | WriteViewName | NotifyViewName | StorageType |
|---------------------|---------------|---------------|---------------|--------------|--------------|---------------|----------------|-------------|
| nncli | | NNCLI | noAuthNoPriv | exact | nncli | nncli | | readOnly |
| initial | | USM | noAuthNoPriv | exact | restricted | | restricted | nonVolatile |
| initial | | USM | authNoPriv | exact | internet | internet | internet | nonVolatile |
| communitySnmpRead | | SNMPv1 | noAuthNoPriv | exact | snmpv1Objs | | | readOnly |
| communitySnmpRead | | SNMPv2c | noAuthNoPriv | exact | snmpv1Objs | | | readOnly |
| communitySnmpWrite | | SNMPv1 | noAuthNoPriv | exact | snmpv1Objs | snmpv1Objs | | readOnly |
| communitySnmpWrite | | SNMPv2c | noAuthNoPriv | exact | snmpv1Objs | snmpv1Objs | | readOnly |
| communitySnmpNotify | | SNMPv1 | noAuthNoPriv | exact | | | snmpv1Objs | readOnly |
| communitySnmpNotify | | SNMPv2c | noAuthNoPriv | exact | | | snmpv1Objs | readOnly |

9 row(s)

Table 81 on page 214 describes the Group Access Right tab fields.

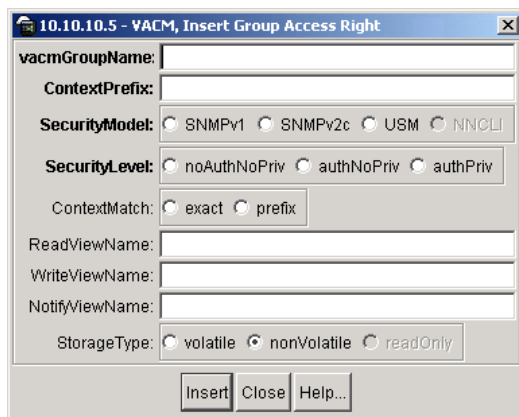
Table 81 VACM dialog box—Group Access Right tab fields

| Field | Description |
|----------------|---|
| vacmGroupName | A GroupName from the Group Membership table |
| ContextPrefix | The Context Prefix for this entry. By default, the field is empty. This is an optional field. |
| SecurityModel | The security model assigned to users in the Group Membership table. Options are, SNMPv1, SNMPv2c, or USM |
| SecurityLevel | The security level assigned to users in the Group Membership table. Options are noAuthNoPriv, authNoPriv, or authPriv |
| ContextMatch | Specifies whether to use an exact match or the context prefix for assigning the rights defined in this row to a user. The default is exact. This is an optional field. |
| ReadViewName | The name of the MIB View to which the user is assigned read access. |
| WriteViewName | The name of the MIB View to which the user is assigned write access. |
| NotifyViewName | The name of the MIB View from which the user will receive notifications. |
| StorageType | Specifies whether this table entry (row) should be stored in volatile or non-volatile memory. If the entry is stored in volatile memory, it will not persist if the switch loses power. |

3 Click Insert.

The VACM, Insert Group Access Right dialog box opens (Figure 103).

Figure 103 VACM, Insert Group Access Right dialog box



- 4 Enter the name of a group.
- 5 Enter the context prefix.
- 6 Select the security model.
- 7 Select the security level.
- 8 Enter the name of a MIB View that will enable a user to read the MIB subtrees and objects.
- 9 Enter the name of a MIB View that will enable the user to write to the MIB subtrees and objects.
- 10 Enter the name of a MIB View from which the user can receive traps or inform messages.
- 11 Click Insert.

The new Group Access Right entry is shown in the table.

Defining a MIB view

To assign MIB view access for an object:

- 1 From the Device Manager menu bar, click Edit > SnmpV3 > VACM table.

The VACM dialog box opens (Figure 100).

2 Select the MIB View tab.

The MIB View tab opens (Figure 104).

Figure 104 MIB View tab

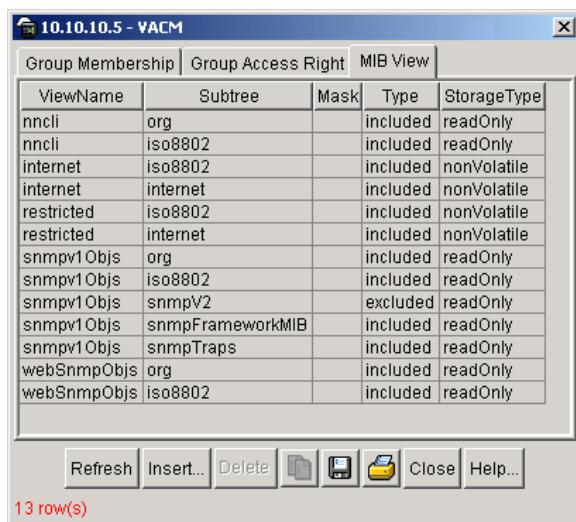


Table 82 describes the MIB View tab fields.

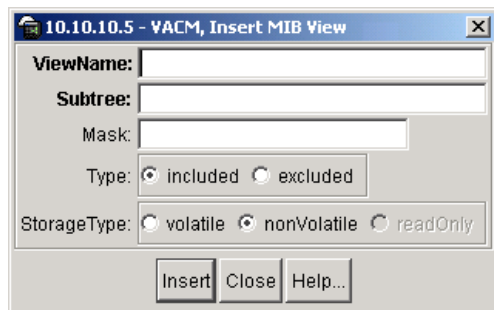
Table 82 VACM dialog box—MIB View tab fields

| Field | Description |
|--------------------|---|
| ViewName | Creates a new entry with this group name. The range is 1 to 32 characters. |
| Subtree | Refers to any valid object identifier that defines the set of MIB objects accessible by this SNMP entity, for example, org, iso8802, or 1.3.6.1.1.5 OID string. |
| Mask (Optional) | Specifies that a bit mask be used with vacmViewTreeFamilySubtree to determine whether an OID falls under a view subtree. |
| Type | Determines whether access to a mib object is granted (Included) or denied (Excluded). By default., it is Included. |
| StorageType | Specifies whether this table entry (row) should be stored in volatile or non-volatile memory. If the entry is stored in volatile memory, it will not persist if the switch loses power. |

- 3 Click Insert.

The VACM, Insert MIB View dialog box opens (Figure 105).

Figure 105 VACM, Insert MIB View dialog box



- 4 Enter a ViewName.
- 5 Enter a MIB Subtree name, for example, org, iso8802 etc, or a dotted-decimal OID string.
- 6 Enter a Mask to specify wild cards in the OID string. The default is to leave this field blank which is the same as specifying a mask of all ones (exact match).
- 7 Select whether to include or exclude this MIB subtree from the collection of all MIB objects with this same ViewName.
- 8 Click Insert.

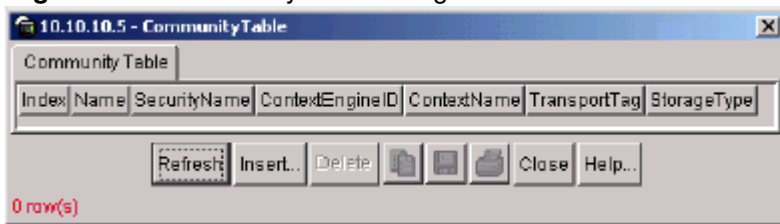
The assigned MIB view appears in the list.

Creating a community

A community table contains objects for mapping between community strings and the security name created in VACM Group Member. To create a community:

- 1 From the Device Manager menu bar, click Edit > SnmpV3 > Community Table.

The Community Table dialog box opens Figure 106.

Figure 106 Community Table dialog box

- 2 Click Insert.

The Community Table, Insert Community Table dialog box opens [Figure 107](#).

Figure 107 Community Table, Insert Community Table dialog box

- 3 Enter an Index.
- 4 Enter name that is a community string.
- 5 Enter a SecurityName.
- 6 Click Insert.

The new community is shown in the list.

[Table 83](#) describes the Community Table dialog box fields.

Table 83 Community Table dialog box fields

| Field | Description |
|--------------|---|
| Index | The unique index value of a row in this table. SnmpAdminString 1-32 characters. |
| Name | The community string for which a row in this table represents a configuration |
| SecurityName | The security name assigned to this entry in the Community table. The range is 1 to 32 characters. |

Table 83 Community Table dialog box fields

| Field | Description |
|-----------------|--|
| ContextEngineID | The contextEngineID indicating the location of the context in which management information is accessed when using the community string specified by the corresponding instance of snmpCommunityName. The default value is the snmpEngineID of the entity in which this object is instantiated. |
| ContextName | The context in which management information is accessed when using the community string specified by the corresponding instance of snmpCommunityName. |
| TransportTag | This object specifies a set of transport endpoints which are associated a community string. The community string is only valid when found in an SNMPv1 or SNMPv2c message received from one of these transport endpoints, or when used in an SNMPv1 or SNMPv2c message to be sent to one of these transport endpoints. |
| StorageType | The storage type for this conceptual row in the snmpCommunityTable. Conceptual rows having the value 'permanent' need not allow write-access to any columnar object in the row. |

Management Targets

The concept of SNMPv3 management target is similar to trap receivers in SNMPv1 and SNMPv2c. Management targets are defined with the help of three tables.

[Table 84](#), describes the tables that helps to define the management targets.

Table 84 Management target tables

| Table Name | Description |
|-------------------------|---|
| Target Address table | Lists the IP address and destination UDP port number of stations that receives trap or inform messages. |
| Target Parameters table | Specifies how to format and process an outgoing message that is sent to an associated target address. |
| Notify table | Specifies the type of message to send to a management target; 'trap' or 'inform'. |

Creating a Management Target Address

To create an entry in the Management Target Address table:

- 1 From the Device Manager menu bar, click Edit > SnmpV3 > Target Table.

The Target Table dialog box opens, with Target Address Table tab displayed (Figure 108).

Figure 108 Target Table dialog box, Target Address Table tab.

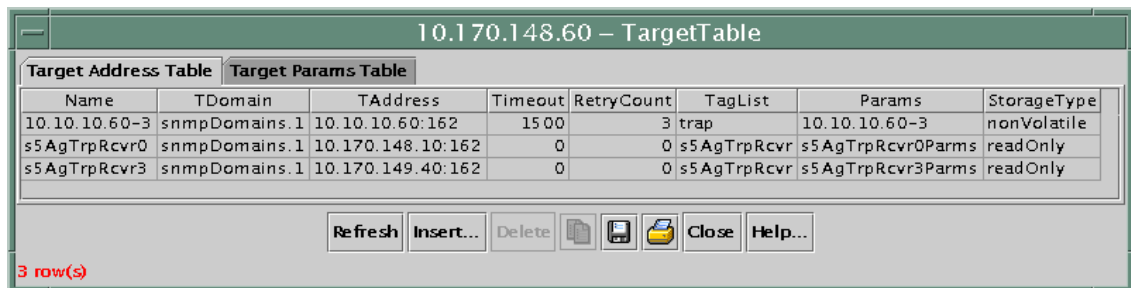


Table 85 describes the Target Address Table fields.

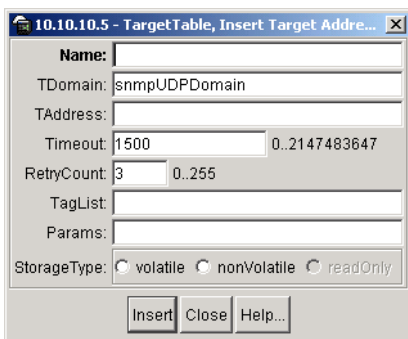
Table 85 Target Address Table fields

| Field | Description |
|-------------|---|
| Name | Specifies the name for this target table entry. |
| TDomain | Specifies the domain of the management target. The default is 'snmpUDPDomain' |
| TAddress | Specifies the IP address and destination UDP port for this management target. For example, 10.0.4.27:162 |
| Timeout | Specifies the length of the time to wait in 1/100 th of a second, for an acknowledgement from this management target before declaring message as timed-out. The default is 1500 milliseconds. |
| RetryCount | Specifies the number of times this device should resend messages to this management target if initial messages are not acknowledged. The default is 3. |
| Taglist | Refers to zero or more Notify tags that are used to link this entry with entries in the Notify table. By default, you can enter either 'trap' or 'inform' without having to create new entries in the Notification table. |
| Params | Specifies the entry in the Target Parameter table which is associated with this Management Target Address. |
| StorageType | Specifies whether this table entry (row) should be stored in volatile or non-volatile memory. If the entry is stored in volatile memory, it will not persist if the switch loses power. |

2 Click Insert.

The Target Table, Insert Target Address Table dialog box opens (Figure 109).

Figure 109 Target Table, Insert Target Address Table dialog box



- 3 Enter a Name.
- 4 Enter a TDomain Name.
- 5 Enter the IP address and UDP port number for this management target. For example, 10.0.4.27:162.
- 6 Accept or modify the default values in the TimeOut and RetryCount fields.
- 7 In the Taglist field, enter the name of the tags ('trap' or 'inform'), separated by comma if more than one tag is entered. Refer [Notify Table dialog box fields](#) for more details.
- 8 In the Params field, enter the name of an entry in the Target Param table.
- 9 Click Insert.

The new Target address is shown in the list.

Creating Target Parameters

To create a target parameter:

- 1 From the Device Manager menu bar, click Edit > SnmpV3 > Target Table.
The Target Table dialog box opens, with Target Address Table displayed ([Figure 110](#)).

Figure 110 Target Params Table tab

| Name | MPModel | SecurityModel | SecurityName | SecurityLevel | StorageType |
|-------------------|------------|---------------|------------------|---------------|-------------|
| 10.10.10.60-3 | SNMPv3/USM | USM | initial | authNoPriv | nonVolatile |
| s5AgTrpRcvr0Parms | SNMPv1 | SNMPv1 | s5AgTrpRcvrComm0 | noAuthNoPriv | readOnly |
| s5AgTrpRcvr3Parms | SNMPv1 | SNMPv1 | s5AgTrpRcvrComm3 | noAuthNoPriv | readOnly |

- 2 Select the Target Params Table tab.
- 3 Click Insert.

The Target Table, Insert Target Params Table dialog box opens ([Figure 111](#)).

Figure 111 Target Table, Insert Target Params Table dialog box

- 4 Enter a Name for this set of parameters.
- 5 Select the MPModel.
- 6 Select the SecurityModel.
- 7 Enter a SecurityName.
- 8 Specify a SecurityLevel value.
- 9 Enter the storage type.
- 10 Click Insert.

The new target parameter is shown in the list.

[Table 86](#) describes the Target Params Table dialog box fields.

Table 86 Target Params Table dialog box fields

| Field | Description |
|---------------|---|
| Name | Specifies the name of the target parameters table. |
| MPModel | Specifies the Message Processing model, SNMPv1, SNMPv2c, or SNMPv3/USM. |
| SecurityModel | Specifies the security model, SNMPv1, SNMPv2c, or SNMPv3/USM. |
| SecurityName | Specifies the security name for generating SNMP messages. |
| SecurityLevel | Specifies the security level for SNMP messages: noAuthnoPriv, authnoPriv, or authPriv. |
| Storage Type | Specifies whether this table entry (row) should be stored in volatile or non-volatile memory. If the entry is stored in volatile memory, it will not persist if the switch loses power. |

The Notify Table

The Notify table contains default entries for a trap notification type and inform notification type.

To create a Notify table entry:

- 1 From the Device Manager menu bar, click Edit > SnmpV3 > Notify.

The Notify Table dialog box opens (Figure 112).

Figure 112 NotifyTable dialog box



Table 87 describes the Notify Table dialog box fields.

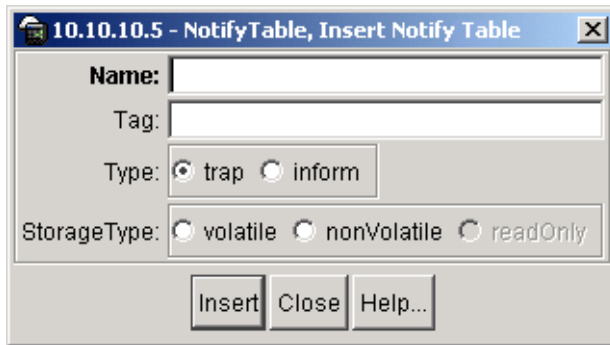
Table 87 Notify Table dialog box fields

| Field | Description |
|-------------|---|
| Name | A name or index value for this row in the table. |
| Tag name | A single tag value used to associate this entry with an entry in the Target Address Table. |
| Type | This selection specifies the type of notification sent to a management target address. If the value is 'trap', sent messages will contain SNMPv2-Trap PDUs. If the value is 'inform', messages will contain Inform PDUs. Note: If an SNMP entity only supports trap (and not inform) messages, then this object may be read-only. |
| StorageType | Specifies whether this table entry (row) should be stored in volatile or non-volatile memory. If the entry is stored in volatile memory, it will not persist if the switch loses power. |

- 2 Click Insert.

The Notify Table, Insert Notify Table dialog box opens (Figure 113).

Figure 113 Notify Table, Insert Notify Table dialog box



- 3 Enter a Name for this table row.
- 4 Enter a Tag name which will connect this entry to one or more Target Address table entries.
- 5 Specify the Type of message Protocol Data Units (PDUs) to send to an associated Management Target Address; 'trap' or 'inform'
- 6 Specify the StorageType
- 7 Click Insert.

The new notify entry shown in the list.

Index

Symbols

[<=64 field](#) 122, 164
[>1023 field](#) 122, 165
[>127 field](#) 122, 164
[>1518 field](#) 122
[>255 field](#) 122, 164
[>511 field](#) 122, 165
[>64 field](#) 122, 164

A

[Absolute statistic](#) 165
[AbsoluteValue statistics](#) 44
[access levels](#) 31
[Action field](#) 79
[Actions menu](#) 34
[ActiveMember field](#) 136
[ActiveMembers field](#) 141
[ActiveQuerier field](#) 137
[Addr field](#) 57
[AddrMaskReps field](#) 88, 90
[AddrMasks field](#) 88, 90
[AdminControlledDirections field](#) 103, 110
[AdminDuplex field](#) 97, 107
[AdminSpeed field](#) 97, 107
[AdminState field](#) 65
[AdminStatus field](#) 96, 106
[Agent Info tab](#) 67
[Alarm Manager button](#) 35
[alarms tab](#) 182, 183
[alarms, RMON](#)
 [characteristics of](#) 176
 [creating](#) 178
[AlignmentErrors field](#) 116, 132
[Area Chart button](#) 50
[area graph example](#) 45
[ARP tab](#) 58
[AuthConfig tab](#)
 [AccessCtrlType field](#) 195
 [BrdIndx field](#) 194
 [MACIndx field](#) 194
 [PortIndx field](#) 194
 [SecureList field](#) 195
[AuthControlledPortControl field](#) 103, 110
[AuthControlledPortStatus field](#) 103, 110
[AuthEapLogoffWhileAuthenticated feild](#) 126
[AuthEapLogoffWhileAuthenticating feild](#) 126
[AuthEapStartsWhileAuthenticated feild](#) 126
[AuthEapStartsWhileAuthenticating feild](#) 125
[AuthenticationTraps field](#) 61
[AuthFailWhileAuthenticating feild](#) 125
[AuthReauthsWhileAuthenticated feild](#) 126
[AuthReauthsWhileAuthenticating feild](#) 125
[AuthStatus tab](#)
 [AuthStatusBrdIndx field](#) 198
 [AuthStatusMACIndx field](#) 198
 [AuthStatusPortIndx field](#) 198
 [CurrentAccessCtrlType field](#) 198
 [CurrentActionMode field](#) 199
 [CurrentPortSecurStatus field](#) 199
[AuthSuccessWhileAuthenticating feild](#) 125
[AuthTimeoutsWhileAuthenticating feild](#) 125

AuthViolation tab
 BrdIndx field 200
 MACIndx field 200
 PortIndx field 200
AutoNegotiate field 97, 107
Average statistics 44
Average/sec statistic 165

B

BackendAccessChallenges feild 126
BackendAuthFails feild 126
BackendAuthState field 103, 110
BackendAuthSuccesses feild 126
BackendNonNakResponsesFromSupplicant feild 126
BackendOtherRequestsToSupplicant feild 126
BackendResponses feild 126
Bar Chart button 50
Base tab 143
BcastAddr field 57
blinking LEDs 39
BootMode field 61
BootRouterAddr tab 67
Bridge dialog box 143
Bridge parameter
 Base tab
 BridgeAddress field 144
 NumPorts field 144
 Type 144
 Forwarding tab
 Address field 150
 Port field 150
 Status field 150
 Spanning Tree tab
 BridgeHelloTime field 147
 BridgeMaxAge field 146
 DesignatedRoot field 145
 ForwardDelay field 146
 HelloTime field 146
 MaxAge field 146

- Priority field 145
- ProtocolSpecification field 145
- RootCost field 146
- RootPort field 146
- TimeSinceTopologyChange field 147
- TimeSinceTopologyChange field 145
- TopChanges field 145
- Transparent tab
 - AgingTime field 148
 - LearnedEntryDiscard field 148
- BroadcastPkts field 121, 163
- buckets 165
- BucketsGranted field 169
- BucketsRequested field 169
- buttons
 - dialog boxes 41
 - toolbar 35

C

- CarrierSenseErrors field 116, 133
- chassis
 - configuration, editing 59
 - graphing 81
- Chassis ICMP In statistics window 87
- Chassis ICMP Out statistics tab 89
- Chassis SNMP tab 82
- Collisions field 121, 164
- Color field 136
- color-coded ports 39
- communication parameters, setting for Device Manager 28
- Community field 70, 185
- community strings
 - default 31
 - entering 32
- ConfigFileName field 78, 80
- configuration
 - downloading 77
 - Multi-Link Trunks 128
 - port-based VLAN 135, 136, 138

- ports 157
- Confirm row deletion field 30
- Control tab 167
- conventions, text 23
- Copy button 41
- Copy File tab 77
- CRAAlignErrors field 121, 164
- Cumulative statistic 165
- Cumulative statistics 44
- CurrentDefaultGateway field 62
- CurrentImageVersion field 62
- CurrentMgmtProtocol field 61
- customer support 25

D

- data, exporting 48
- default access community strings 31
- Default TTL field 56
- DefaultVLANId field 98, 109
- DeferredTransmissions field 117, 133
- Descr field 63, 65, 72, 74, 96, 106
- Description field 185
- DestUnreachs field 88, 90
- Device Manager
 - setting properties 28
- Device Manager window 27, 28
- Device menu 34
- Device Name field 32
- device view, summary 35
- device, opening 31
- Disable command 41
- disabled port, color 39
- DiscardUntaggedFrames field 98, 109

E

EapLengthErrorFramesRx field 124
EapLogoffsWhileConnecting feild 125
EAPOL 101, 122, 124
EAPOL Diag tab 124
EAPOL Stats tab 122
EAPOL tab for multiple ports 109
EapolFramesRx field 123
EapolFramesTx Field 123
EapolLogoffFramesRx field 123
EapolReqFramesTx field 123
EapolReqIdFramesTx field 123
EapolRespFramesRx field 123
EapolRespIdFramesRx 123
EapolStartFramesRx field 123
EchoReps field 88, 90
Echos field 88, 90
Edit command 40, 41
Edit menu 34
Edit Selected button 35
Enable 137
Enable command 41
Enable field 30
EntersAuthenticating feild 125
EntersConnecting feild 125
Ether Stats Control tab 172
Ethernet Errors tab 115
Ethernet statistics, disabling 174
Event Index field 181
events, RMON 184
ExcessiveCollisions field 117, 134
Export Data button 42, 48

F

falling event 184

falling value, RMON alarms 176
FallingEventIndex field 183
FallingThreshold field 183
Fan tab 73
FCSErrors field 116, 132
File System window 77
Forwarding tab 148
ForwDatagrams field 86
FragCreates field 86
FragFails field 86
FragOKs field 86
frames, discarding tagged frames on 139
FrameTooLongs field 117, 133

G

Globals tab 56
graph
 creating 48
 modifying 50
Graph command 41
graph dialog box 49
Graph menu 34
Graph Selected button 35, 49
graph types 44
graphPort, Interface tab 112

H

HCInBroadcastPkt feild 131
HCInMulticastPkt feild 131
HCInOctets feild 130
HCInUcastPkts feild 130
HCOutBroadcast feild 131
HCOutMulticast feild 131
HCOutOctets feild 131
HCOutUcastPkts feild 131
Help button 35

Help menu 34
Help, Device Manager 53
Horizontal button 50

I

ICMP In tab 88
ICMP Out statistics 89
ICMP Out tab 89
ifInNUcastPkts field 113
ifInOctets field 113
ifInUcastPkts field 113
ifOutNUcastPkts field 113
ifOutOctets field 113
ifOutUcastPkts field 113
image file 77
ImageFileName field 67, 78, 80
ImageLoadMode field 61
InAddrErrors field 85
InASNParseErrs field 83
InBadCommunityNames field 83
InBadCommunityUses field 83
InBadValues field 83
InBadVersions field 83
InBroadcastPkt field 130
InDelivers field 86
Index field 96, 106, 110, 181
InDiscards field 86, 113
InErrors field 113
InGenErrs field 84
InGetNexts field 83
InGetRequests field 83
InGetResponses field 83
InHdrErrors field 85
InMulticastPkts field 130
InNoSuchNames field 83

Inpkts field 82
InReadOnlys field 84
InReceives field 85
Insert Alarm dialog box 179
Insert AuthConfig dialog box
 BrdIndx field 196
Insert button 41
Insert Control dialog box 169
Insert Ether Stats dialog box 174
Insert Event dialog box 186
InSetRequests field 83
Interface item, ARP 58
Interface tab 94
Interface tab for a multiple port 105
Interface window 130
InternalMacReceiveErrors field 116, 133
InternalMacTransmitErrors field 116, 132
Interval field 169, 182
InTooBigs field 83
InTotalReqVars field 82
InTotalSetVars field 82
InUnknownProtos field 86, 114
InvalidEapolFramesRx field 124
IP Address tab 57
IP dialog box 55
IP Globals tab
 fields 208, 210, 212
IP tab 85
IPAddress field 58

J

Jabbers field 121, 164

K

KeyTxEnabled field 103, 111

L

Last/sec statistic 165
LastChange field 97, 107
LastEapolFrameSource 103
LastEapolFrameSource field 111
LastEapolFrameVersion field 103, 111
LastLoadProtocol field 62
LastTimeSent field 185
LastUnauthenticatedCommunityString field 69
LastUnauthenticatedIpAddress field 69
LastValue statistics 44
LateCollisions field 117, 134
LEDs in device view 39
legend, port color 34, 39
Line Chart button 50
link, lacking, color 39
LoadServerAddr field 67, 78, 80
LocalStorageImageVersion field 62
Location field 64, 65
Log Scale button 50
Log tab 187
logs 187
LstChng field 64, 65

M

MacAddr field 67
MacAddress field 58
Max Traps in Log field 30
Max/sec statistic 165
Maximum statistics 44
MaxReq field 103, 111
MDA
 viewing 37
menu bar, Device Manager 34
menus. *See* individual menu names

Min/sec statistic 165
Minimum statistics 44
MLT requirements 127
MltId field 97, 107
MRouterExpiration field 137
MRouterPorts field 137
Mtu field 96, 106
MulticastPkts field 121, 163
Multi-Link Trunk window 129
Multi-Link Trunking. *See* MLT
Multi-Link Trunks window 128
multiple objects, selecting 37
MultipleCollisionFrames field 117, 134

N

Name field 128, 136, 137
NetMask field 57
new table entry, creating 41
NextBootDefaultGateway field 62
NextBootLoadProtocol field 62
NextBootMgmtProtocol field 61
NextBootNetMask field 67
NextBootpAddr field 67
NmmCurNum field 158
NmmLstChg field 158
NmmMaxNum field 158
NoSuchObject error message 93, 104

O

object types 36
objects
 editing 43
 selecting 36
Octets field 121, 163
online Help 34, 53
Open Device button 31, 35

Open Device dialog box 31, 32
operating port, color 39
OperControlledDirections field 103, 110
OperSpeed field 97, 107
OperState field 66, 72, 74
OperStatus field 96, 107
OutBadValues field 83
OutBroadcast field 130
OutDiscards field 86, 113
OutErrors field 114
OutGenErrs field 83
OutMulticast field 130
OutNoRoutes field 86
OutNoSuchNames field 83
Outpkts field 82
OutRequests field 86
OutTooBigs field 83
OutTraps field 83
OversizePkts field 121, 164
Owner field 169, 173, 183, 185

P

PaeState 102
PaeState field 110
ParmProbs field 88, 90
Paste button 41
PhysAddress field 96, 106
Pkts field 121, 163
polling interval 48
Port Capabilities field 102
port color legend 39
Port dialog box 112
port Ethernet Error Statistics tab 114
Port field 173
Port Interface tab 95, 106

- port shortcut menu 40
- Port Spanning Tree window 99
- PortCapabilities field 110
- PortInitialize field 102, 110
- PortMembers field 128, 136, 141
- PortProtocolVersion field 102, 110
- PortReauthenticate field 102, 110
- ports
 - color-coded 39
 - configuring 93, 157
 - controlling 93
 - disabled 39
 - editing 93, 103
 - graphing 94, 104, 111, 112
 - selecting 37
 - viewing 93, 103
- PortType field 128
- Power Supply tab 72
- Print button 41
- product support 25
- Properties dialog box 28, 29
 - Hotswap Poll Interval field 30
 - If Traps, Status Interval) field 30
 - Status Poll Interval field 30
- publications
 - related 24

Q

- QuerierPort field 137
- QueryInterval field 137
- QuietPeriod field 103, 110

R

- Read Community field 32
- Read Community, SNMP 33
- Read Community, SNMP field 32
- Read-Write-All access 33

ReasmFails field 87
ReasmMaxSize field 57
ReasmOKs field 87
ReasmReqds field 86
ReasmTimeout field 56
ReAuthEnabled field 103, 111
ReAuthPeriod field 103, 111
Reboot field 62
Rebustness field 137
Redirects field 88, 90
Refresh Device Status button 35
Remote Monitoring. *See* RMON
Reset Changes button 41
Result field 79
Retry Count field 30
rising event 184
rising value, RMON alarms 176
RisingEventIndex field 183
RisingThreshold field 183
RMON
 alarms
 characteristics 176
 creating 178
 deleting 182
 inserting 180
 events
 definition 184
 history
 creating 166
 definition 165
 disabling 171
 statistics 161, 166
RMON EtherStat tab 120, 163
RMON Event tab 185
Rmon menu 34

S

Sample Interval field 181

Sample Type field 181, 182

security 101

Security parameters

General tab

- AuthCtlPartTime field 190
- AuthSecurityLock field 190
- CurrNodesAllowed field 191
- CurrSecurityLists field 191
- MaxNodesAllowed field 191
- MaxSecurityLists field 191
- PortLearnStatus field 191
- PortSecurityStatus field 191
- SecurityAction field 191
- SecurityMode field 191
- SecurityStatus field 190

Security, Insert AuthConfig dialog box

- AccessCtrlType field 196
- MACIndx field 196
- PortIndx field 196
- SecureList field 196

SerNum field 63, 66

ServerTimeout 111

ServerTimeout field 103

shortcut menus

- port 40
- switch unit 40

single object, selecting 36

SingleCollisionFrames field 117, 133

SNMP Info tab 68

SNMP tab 68

SNMP traps 52

Spanning Tree tab 144, 145

Spanning Tree window 99

Speed field 107

SQETestErrors field 117, 133

SrcQuenchs field 88, 90

Stack Info tab 64

Stacked button 50

Standalone Unit Info Tab 63

StartupAlarm field 183

statistics

- Ethernet statistics, enabling 172
- for a single object 47
- for multiple objects 48
- graphing 43
- ICMP Out 89
- MLT 129
- RMON 161, 166
- single port 47
- types 44

statistics dialog box

- multiple objects 48

statistics dialog boxes 34

Status field 158, 183

STG 99

STG dialog box

- Ports tab
 - DesignatedBridge field 156
 - DesignatedCost field 156
 - DesignatedPort field 156
 - DesignatedRoot field 156
 - EnableStp field 155
 - FastStart field 155
 - ForwardTransitions field 156
 - PathCost field 156
 - Priority field 155
 - State field 155
 - StgId field 155

StgId field 136, 141

Stop button 42

support, Nortel Networks 25

SuppTiemout field 111

SuppTimeout field 103

switch stack, selecting 37

switch unit shortcut menu 40

switch, selecting 36

sysContact field 61

sysDescr field 61

sysLocation field 61

sysName field 61
System tab 60
sysUpTime field 61

T

tagged frame, discarding 139
technical support 25
Telnet button 35, 51
Telnet session 35, 50
text conventions 23
Threshold Type field 181
TimeExcds field 88, 90
Timeout field 30
TimestampReps field 88, 90
Timestamps field 88, 90
toolbar, Device Manager 35
topology 157
Trace field 30
Transparent Bridging tab 118, 123, 125
Transparent tab 147
trap log 52
Trap Log button 35
Trap Port field 30
Trap Receivers
 NetAddr field 70
Trap Receivers tab 69
troubleshooting
 locations of Help files 53
 receiving traps 52
TrpRcvrCurEnt field 69
TrpRcvrMaxEnt field 69
TrpRcvrNext field 69
TxPeriod field 103, 110
Type 136
Type field 58, 63, 96, 98, 106, 109, 185
types of objects 36

U

UndersizePkts field 121, 164

UNIX

receiving traps 52

V

ValidFlag tab 67

Value field 181, 182

value, changed 43

Variable field 181, 182

Ver field 63, 66

Viewing 93

VLAN 97

VLAN Basic tab 136, 137

VLAN dialog box 136, 137

VLAN menu 34

VLAN tab 98, 102

VLAN tab for multiple ports 108

VlanIds field 98, 109

VLANs

limitations 135

managing 140

W

Web-based management interface

home page, graphic 52

window, Device Manager 33

Write Community field 32

Write Community, SNMP 32, 33