

Part No. 209322-A
August 2000

4401 Great America Parkway
Santa Clara, CA 95054

Reference for the Business Policy Switch 2000 Management Software

NORTEL
NETWORKS™

Copyright © 2000 Nortel Networks

All rights reserved. August 2000.

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

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

NORTEL NETWORKS is a trademark of Nortel Networks.

Optivity is a registered trademark and BayStack is a trademark of Nortel Networks.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

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 NA Inc. reserves the right to make changes to the products described in this document without notice.

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

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).

Nortel Networks NA Inc. software license agreement

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

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

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

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee’s intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee’s requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor’s product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED,

INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

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

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

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

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

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

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

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

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS

AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface	17
Before you begin	17
Text conventions	17
Related publications	18
How to get help	19
 Chapter 1	
Device Manager basics	21
Starting Device Manager	21
Setting the Device Manager properties	22
Opening a device	24
Device Manager window	27
Menu bar	27
Toolbar	28
Graphical representation of the switch	28
Device view	30
Selecting objects	30
Selecting a single object	30
Selecting multiple objects	31
Viewing information about an MDA	31
LEDs and ports	33
Shortcut menus	34
Status bar	36
Using the buttons in Device Manager dialog boxes	36
Editing objects	37
Working with statistics and graphs	38
Types of statistics	38
Types of graphs	39

Statistics for single and multiple objects	41
Viewing statistics as graphs	43
Telneting to a switch	45
Trap log	45
Online Help	46

Chapter 2

Configuring and graphing the switch 47

Viewing switch IP information	47
Globals tab	47
Addresses tab	48
ARP tab	49
Editing the chassis configuration	50
System tab	51
Base Unit Info tab	54
Stack Info tab	55
Agent tab	57
SNMP tab	58
Trap Receivers tab	59
Editing network traps	60
Power Supply tab	61
Fan tab	62
Working with configuration files	64
Graphing chassis statistics	65
SNMP tab	66
IP tab	69
ICMP In tab	72
ICMP Out tab	74

Chapter 3

Configuring and graphing ports 77

Viewing and editing a single port configuration	77
Interface tab for a single port	78
VLAN tab for a single port	80
STG tab for a single port	82

Graphing multiple ports	84
Interface tab for multiple ports	84
VLAN tab for multiple ports	86
Graphing port statistics	88
Interface tab for graphing ports	89
Ethernet Errors tab for graphing ports	91
Bridge tab for graphing ports	94
RMON tab	96
 Chapter 4	
Setting up MultiLink Trunk ports	99
MultiLink Trunk (MLT) features	99
Setting up MLTs	100
Adding ports to a MultiLink Trunk	100
MultiLink Trunk statistics	101
MultiLink Trunk Ethernet error statistics	103
 Chapter 5	
Creating and managing VLANs	107
VLANs	107
Creating VLANs	108
VLAN Information	108
Creating a port-based VLAN	109
Creating a protocol-based VLAN	110
Creating a source address MAC-based VLAN	112
Accepting tagged and untagged frames	114
Snoop tab	115
Modifying and managing existing VLANs	116
 Chapter 6	
Troubleshooting Device Manager	119
Topology tab	119
Topology Table tab	120

Chapter 7	
RMON	123
Working with RMON information	123
Viewing statistics	123
Viewing history	124
Creating a history	126
Disabling history	128
Enabling Ethernet statistics gathering	129
Disabling Ethernet statistics gathering	130
Alarms	131
How RMON alarms work	131
Creating alarms	133
Alarm Manager example	134
Events	139
How events work	139
Viewing an event	139
Creating an event	141
Deleting an event	142
Log information	142
HP OpenView	143
Log only event bug	145
 Chapter 8	
Security parameters.	147
General tab	147
SecurityList tab	150
Security, Insert SecurityList dialog box	150
AuthConfig tab	151
Security, Insert AuthConfig dialog box	153
AuthStatus tab	155
AuthViolation tab	157
 Index	159

Figures

Figure 1	Device Manager window	22
Figure 2	Device Manager Properties dialog box	23
Figure 3	Open Device dialog box	25
Figure 4	Device view	26
Figure 5	Parts of the Device Manager window	27
Figure 6	Objects in the device view	30
Figure 7	MDA dialog box	32
Figure 8	Color port legend	34
Figure 9	Switch unit shortcut menu	34
Figure 10	Port shortcut menu	35
Figure 11	MDA shortcut menu	36
Figure 12	Line graph	39
Figure 13	Area graph	39
Figure 14	Bar graph	40
Figure 15	Pie graph	40
Figure 16	Interface statistics for a single port	41
Figure 17	Interface statistics for multiple ports	42
Figure 18	Statistics dialog box for a port	43
Figure 19	Globals tab	48
Figure 20	Edit IP dialog box — IP Address tab	49
Figure 21	Edit IP dialog box — ARP tab	50
Figure 22	Edit Chassis dialog box — System tab	52
Figure 23	Edit Chassis dialog box — Base Unit Info tab	54
Figure 24	Edit Chassis dialog box — Stack Info tab	56
Figure 25	Edit Chassis dialog box — Agent tab	58
Figure 26	Edit Chassis dialog box — SNMP tab	59
Figure 27	Edit Chassis dialog box — Trap Receivers tab	60
Figure 28	Chassis, Insert Trap Receive dialog box	61
Figure 29	Edit Chassis dialog box — Power Supply tab	62

Figure 30	Edit Chassis dialog box — Fan tab	63
Figure 31	Edit FileSystem dialog box	64
Figure 32	Graph Chassis dialog box — Chassis SNMP tab	67
Figure 33	Graph Chassis dialog box — IP tab	70
Figure 34	Graph Chassis dialog box — ICMP In tab	73
Figure 35	Graph Chassis dialog box — ICMP Out tab	74
Figure 36	Edit Port dialog box — Interface tab	78
Figure 37	Edit Port dialog box — VLAN tab	81
Figure 38	Edit Port dialog box — STG tab	82
Figure 39	Graph Port dialog box — Port Interface tab	85
Figure 40	VLAN tab for multiple ports	87
Figure 41	Interface tab for graphing ports	89
Figure 42	Graph Port dialog box — Port Ethernet Errors tab	92
Figure 43	Graph Port dialog box — Bridge tab	95
Figure 44	Graph Port dialog box — RMON tab	96
Figure 45	MLT dialog box	100
Figure 46	PortMembers dialog box	101
Figure 47	MLT Statistics — Interface tab	102
Figure 48	MLT Statics dialog box — Ethernet Errors tab	104
Figure 49	VLAN Basic tab	108
Figure 50	VLAN, Insert Basic dialog box for a port-based VLANs	110
Figure 51	VLAN, Insert Basic dialog box for a protocol-based VLAN	111
Figure 52	VLAN, Insert Basic dialog box for a source MAC-based VLAN	112
Figure 53	VLAN dialog box	113
Figure 54	MAC, VLAN dialog box	113
Figure 55	Insert VLAN MAC dialog box	113
Figure 56	VLAN tab	115
Figure 57	Snoop tab	116
Figure 58	VLAN dialog box	117
Figure 59	Diagnostics dialog box — Topology tab	119
Figure 60	Diagnostics dialog box — Topology Table tab	120
Figure 61	Port dialog box — RMON tab	124
Figure 62	Port dialog box — RMON tab	125
Figure 63	History tab	126
Figure 64	RMONControl, Insert History dialog box	127

Figure 65	RMONControl dialog box — Ether Stats tab	129
Figure 66	RMONControl, Insert Ether Stats dialog box	129
Figure 67	RMONControl, Insert Ether Stats dialog box port list	130
Figure 68	How alarms fire	132
Figure 69	Alarm example — threshold less than 260	133
Figure 70	Alarm Manager dialog box	134
Figure 71	Alarm variable list	135
Figure 72	RMONAlarms dialog box — Alarms tab	137
Figure 73	RMONAlarms dialog box — Events tab	140
Figure 74	Insert Events dialog box	141
Figure 75	New event in the Events tab	141
Figure 76	Log tab	142
Figure 77	General tab	148
Figure 78	SecurityList tab	150
Figure 79	Security, Insert SecurityList dialog box	151
Figure 80	AuthConfig tab	152
Figure 81	Security, Insert AuthConfig dialog box	154
Figure 82	AuthStatus tab	156
Figure 83	AuthViolation tab	158

Tables

Table 1	Properties dialog box items	23
Table 2	SNMP community string default values	24
Table 3	Open Device dialog box fields	25
Table 4	Menu bar commands	27
Table 5	Toolbar buttons	28
Table 6	MDA dialog box fields	32
Table 7	MDA and MDA port colors	32
Table 8	Port color codes	33
Table 9	Switch unit shortcut menu commands	35
Table 10	Port shortcut menu commands	35
Table 11	Device Manager buttons	36
Table 12	Types of statistics	38
Table 13	Graph dialog box buttons	44
Table 14	Help file locations	46
Table 15	Globals tab items	48
Table 16	IP Addresses tab items	49
Table 17	ARP tab items	50
Table 18	System tab items	52
Table 19	Base Unit Info tab items	55
Table 20	Stack Info tab fields	56
Table 21	Agent tab fields	58
Table 22	SNMP tab fields	59
Table 23	Edit Chassis dialog box — Trap Receivers tab items	60
Table 24	Power Supply tab fields	62
Table 25	Fan tab fields	63
Table 26	FileSystem dialog box items	64
Table 27	SNMP tab fields	67
Table 28	Chassis IP tab fields	70
Table 29	ICMP In tab fields	73

Table 30	ICMP Out tab fields	75
Table 31	Interface tab items for a single port	79
Table 32	VLAN tab items for a single port	81
Table 33	STG tab items for a single port	83
Table 34	Interface tab fields for multiple ports	85
Table 35	VLAN tab fields for multiple ports	87
Table 36	Port Interface tab fields for multiple ports	90
Table 37	Ethernet Errors tab fields	92
Table 38	Bridge tab fields	95
Table 39	RMON tab fields	97
Table 40	MLT dialog box fields	100
Table 41	Interface tab fields	102
Table 42	Ethernet Errors tab fields	105
Table 43	Basic tab fields	109
Table 44	Snoop tab fields	116
Table 45	VLAN dialog box fields	117
Table 46	Topology tab items	120
Table 47	Topology Table tab fields	121
Table 48	History tab fields	127
Table 49	Ether Stats tab fields	130
Table 50	RMON Insert Alarm dialog box fields	136
Table 51	Alarms tab fields	137
Table 52	Events tab fields	140
Table 53	Log tab fields	143
Table 54	General tab items	148
Table 55	SecurityList tab fields	150
Table 56	Security, Insert AuthConfig dialog box fields	151
Table 57	AuthConfig tab fields	153
Table 58	Security, Insert AuthConfig dialog box fields	154
Table 59	AuthStatus tab fields	156
Table 60	AuthViolation tab fields	158

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 Business Policy Switch 2000™. 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.



Note: This version of Device Manager supports Business Policy Switch software version 1.0.

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:

italic text

Indicates book titles.

separator (>)

Shows menu paths.

Example: Protocols > IP identifies the IP option on the Protocols menu.

Related publications

Refer to the following publications for information to help you develop your documentation:

- *Using the Business Policy Switch 2000* (part number 208700-A)
- *Business Policy Switch 2000 Installation Instructions* (part number 209319-A)
- *Getting Started with the Business Policy Switch 2000 Management Software* (part number 209321-A)

These documents provide information about the Business Policy Switch including installation instructions and configuration settings.

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

You can purchase selected documentation sets, CDs, and technical publications though the Internet at the www1.fatbrain.com/documentation/nortel/ URL.

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
EMEA	(33) (4) 92-966-968
North America	(800) 2LANWAN or (800) 252-6926
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

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

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 27](#))
- Instructions to view statistics and display graphs ([page 38](#))
- Instructions to use Device Manager to Telnet to a switch ([page 45](#))
- Information about the trap log ([page 45](#))
- Information about online Help ([page 46](#))



Note: This version of Device Manager supports Business Policy Switch 2000 software version 1.0.

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 Frame Switch Management Software > Device Manager.
- 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 Using the Business Policy Switch 2000 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 may want to 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 Device Manager Properties dialog box

Device Manager 4.0.0.b30 - Properties

Polling

Status Interval: 20 secs

(If Traps, Status Interval: 60 secs)

Hotswap Detect every: 1 intervals

☒ Enable

SNMP

Retry Count: 0 0..5

Timeout: 5 3..30 secs

☐ Trace

☒ Register for Traps

Max Traps in Log: 500 1..10000

Trap Port: 162

☐ Confirm row deletion

Ok Close

- 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
Polling	Status Interval	Interval at which status information is gathered (default is 300 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 300.
	Hotswap Poll Interval	The interval at which Device Manager polls for module information. The default is 60 seconds.
	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.

Table 1 Properties dialog box items (continued)

Area	Item	Description
SNMP	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.
	Register for Traps	When selected (enabled), automatically registers to received traps when Device Manager is launched against a device.
	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 on to receive SNMP traps.
	Confirm row deletion	A dialog box displays when checked, before deleting a row.

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
Read-write-all	secret

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

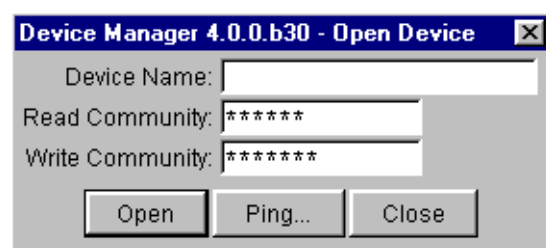


Table 3 describes the Open Device dialog box fields.

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.

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.



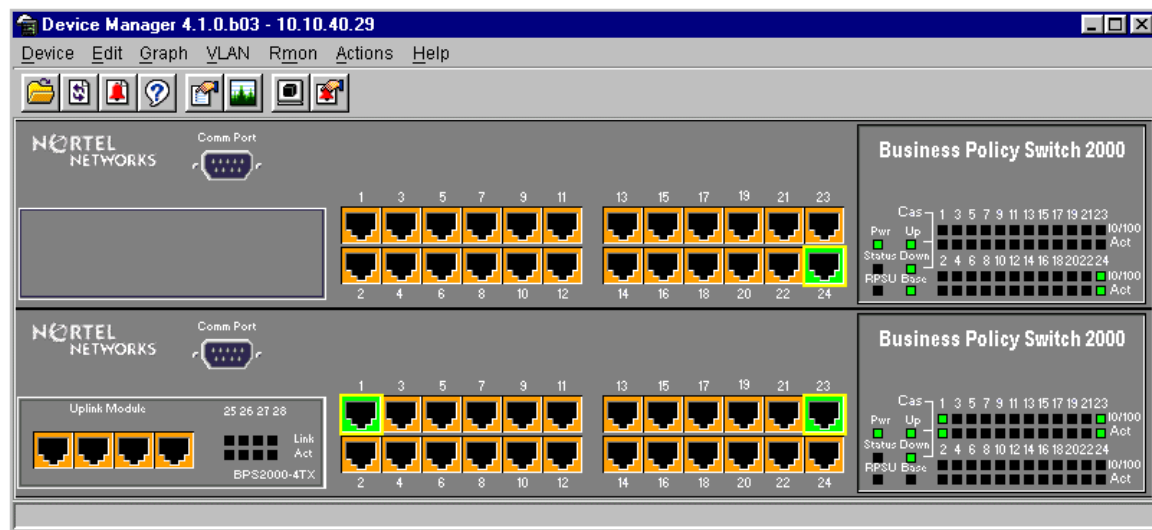
Note: To gain Read-Write-All access to a device in Device Manager, you must enter the Read-Write-All community string for both the Read Community and Write Community strings.

- 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

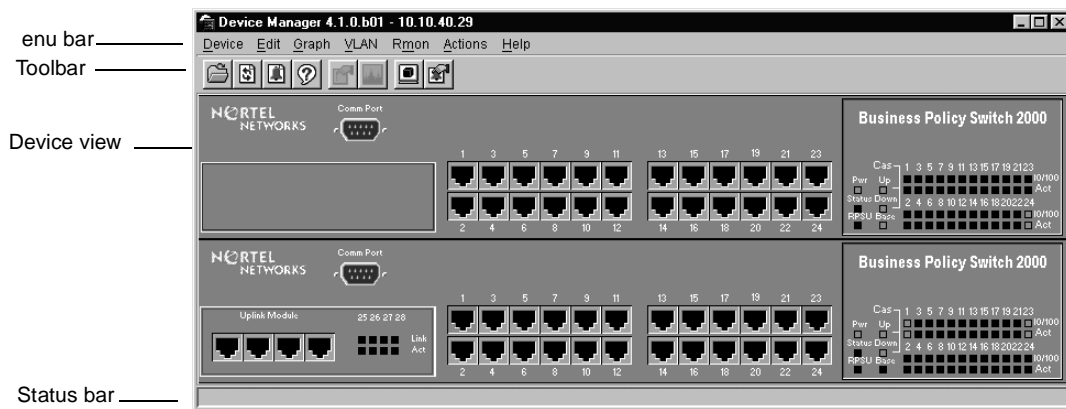


Device Manager window

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.
Edit	Opens edit dialog boxes for selected objects in the device view. This command also opens dialog boxes for managing files and running diagnostic tests.
Graph	Opens statistics dialog boxes for the selected object.
VLAN	Opens dialog boxes for managing VLANs, spanning tree groups (STGs), and Multi-Link Trunks.

Table 4 Menu bar commands (continued)

Command	Description
Rmon	Opens RMON configuration and monitoring dialog boxes.
Actions	Provides quick opening of a Telnet session without going through other dialog boxes.
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.

Graphical representation of the switch

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

Table 5 Toolbar buttons (continued)

Button	Name	Description	Menu bar equivalent
	Telnet	Opens a Telnet session.	Actions > Telnet
	Alarm Manager	Opens the Rmon Alarm Manager.	Rmon > Alarm Manager

Device view

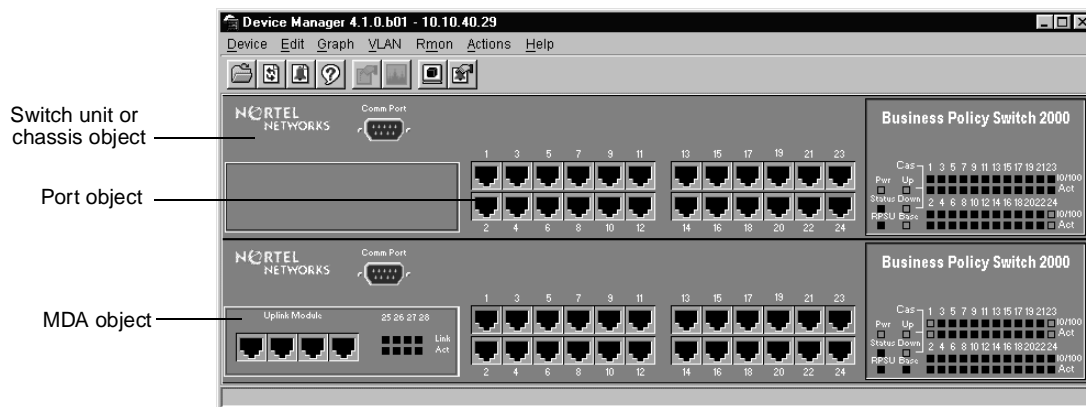
The device view allows you to determine at a glance the operating status of the various units and ports in your hardware configuration. You also use the device view to perform management tasks on specific objects.

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 media dependent adapter (MDA) (called a unit in the menus and dialog boxes)
- A port

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, MDAs, or switches in the stack, [Ctrl]-click on the objects.



Note: In a switch stack that contains Business Policy Switches and BayStack switches, you can select only one type of switch at a time.

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

➡ Choose Edit > Select > Ports.

To select all the “units” (switches and MDAs, but not ports):

➡ Choose Edit > Select > Units.

To select an entire stack:

➡ Choose Edit > Select > Chassis.

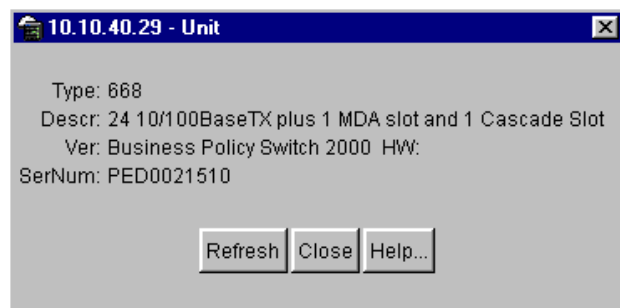
Viewing information about an MDA

To view information about an MDA:

- 1 Select the MDA.
- 2 Choose Edit > Unit.

The Edit > Unit dialog box opens for the MDA.

The Edit > Unit dialog box describes the MDA installed in the switch ([Figure 7](#)).

Figure 7 MDA dialog box

[Table 7](#) describes the MDA dialog box fields.

MDA dialog box

Table 6 MDA dialog box fields

Field	Description
Type	Type of component or subcomponent installed in the Business Policy Switch 2000.
Descr	Description of the component or subcomponent installed in the Business Policy Switch 2000. If not available, the value is a zero length string

Media dependent adapters and port conventions

The conventions on the graphical representation of the switch are different from the actual switch. This section explains these conventions and how information is visually displayed on the MDAs and ports.

[Table 7](#) describes the colors in the graphical representation of the MDA and its ports. The ports on the chassis representation are color-coded to provide port status.

Table 7 MDA and MDA port colors

Color	Description
Green	The module/port is operating.
Red	The module/port is present, but not operating.

Table 7 MDA and MDA port colors (continued)

Color	Description
Dark blue	Port is being tested.
Dark red	Port has been manually disabled.
Orange	Port has no link.

A blinking LED on an MDA is not indicated in the graphical representation of the switch.

For a full description of switch LEDs, refer to the respective switch user manuals.

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 Business Policy Switch, refer to *Using the Business Policy Switch 2000*.

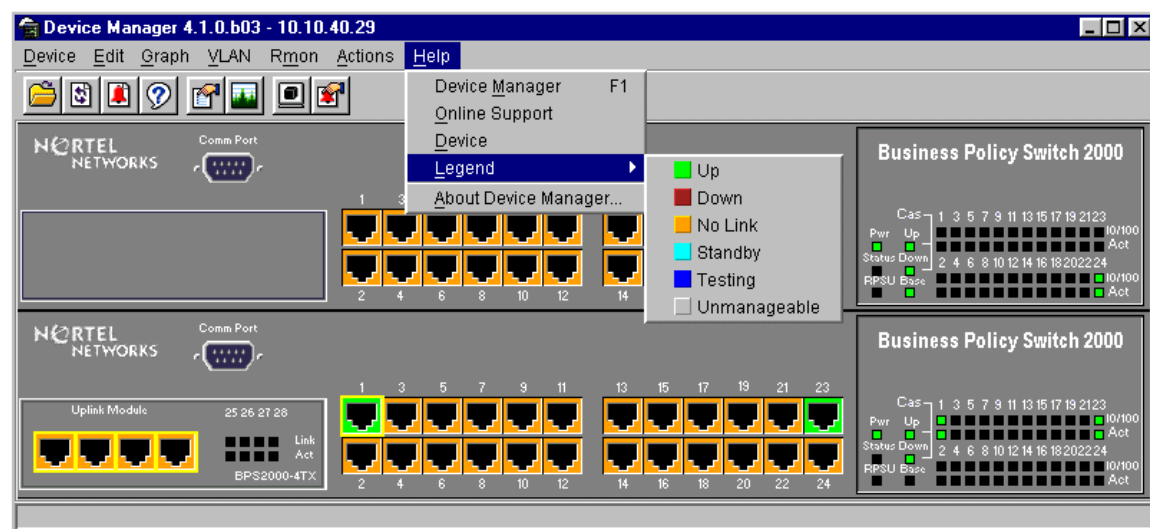
The ports on the device view are color coded to show port status.

[Table 8](#) shows the status assigned to each color.

Table 8 Port color codes

Color	Description
Green	Port is operating.
Red	Port has been manually disabled.
Orange	Port has no link.
Light Blue	Port is in standby mode.
Dark Blue	Port is being tested.
Gray	Port is unmanageable.

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

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 shortcut menu provides access to basic hardware information about the switch and to the graphing dialog boxes for the switch.

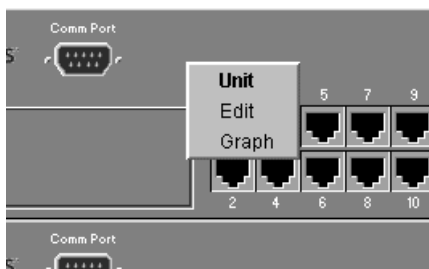
Figure 9 Switch unit shortcut menu

Table 9 describes the commands on the switch unit shortcut menu.

Table 9 Switch unit shortcut menu commands

Command	Description
Edit	Opens a read-only dialog box that provides basic hardware information about the switch.
Graph	Opens a dialog box that displays statistics for the switch and allows you to display the statistics as a graph.

The port shortcut menu 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

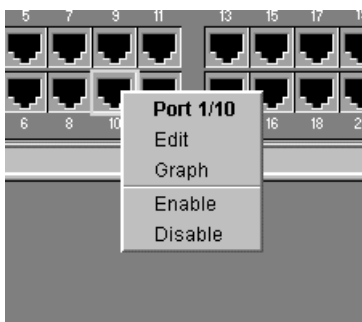


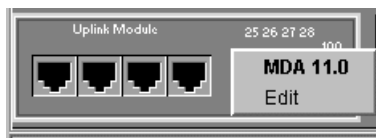
Table 10 describes the commands on the port shortcut menu.

Table 10 Port shortcut menu commands

Command	Descriptions
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.

The MDA shortcut menu contains a single command, Edit, that opens a read-only dialog box with basic hardware information about the MDA.

Figure 11 MDA shortcut menu



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 11](#) describes buttons in Device Manager dialog boxes. Not all buttons appear in all dialog boxes.

Table 11 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 11 Device Manager buttons (continued)

Button	Name	Description
	Stop	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 each switch, 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 41](#) and [“Graphing chassis statistics” on page 65](#).

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 12 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 12](#), [Figure 13](#), [Figure 14](#), and [Figure 15](#) illustrate the different graph styles, respectively.

Figure 12 Line graph

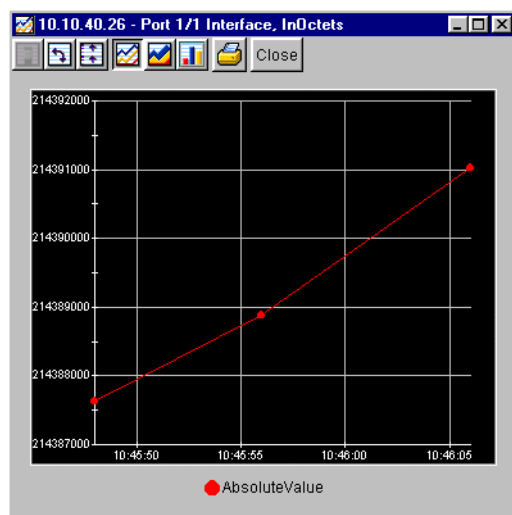


Figure 13 Area graph

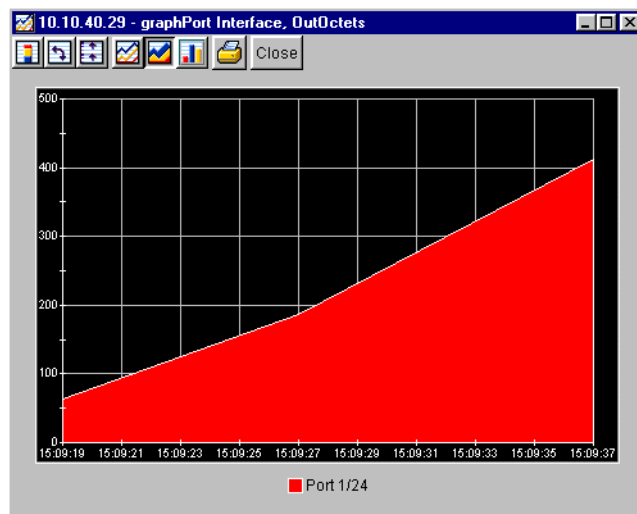


Figure 14 Bar graph

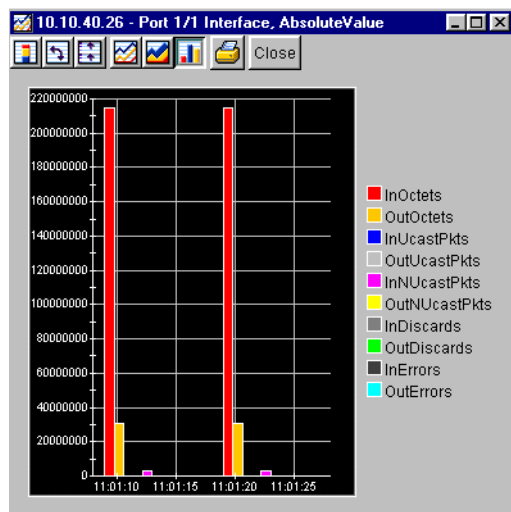
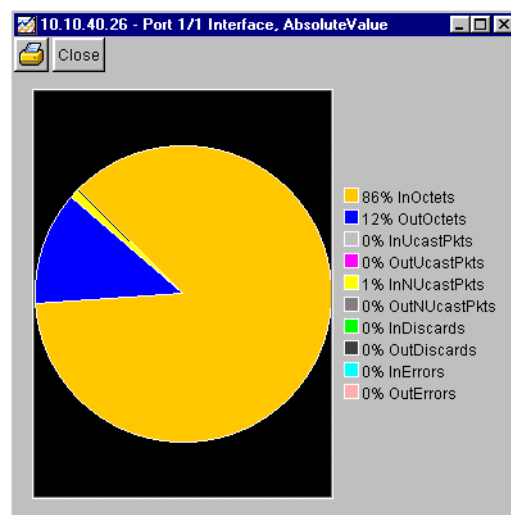


Figure 15 Pie graph

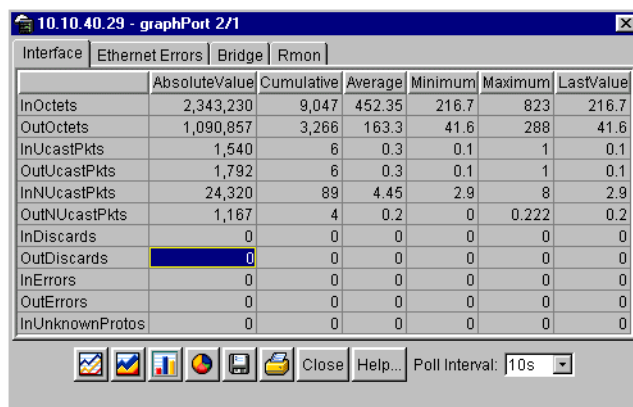


Statistics for single and multiple objects

Statistics for a selected object or objects are displayed in the statistics dialog box.

The dialog box for a single object shows all six types of statistics for each counter (Figure 16).

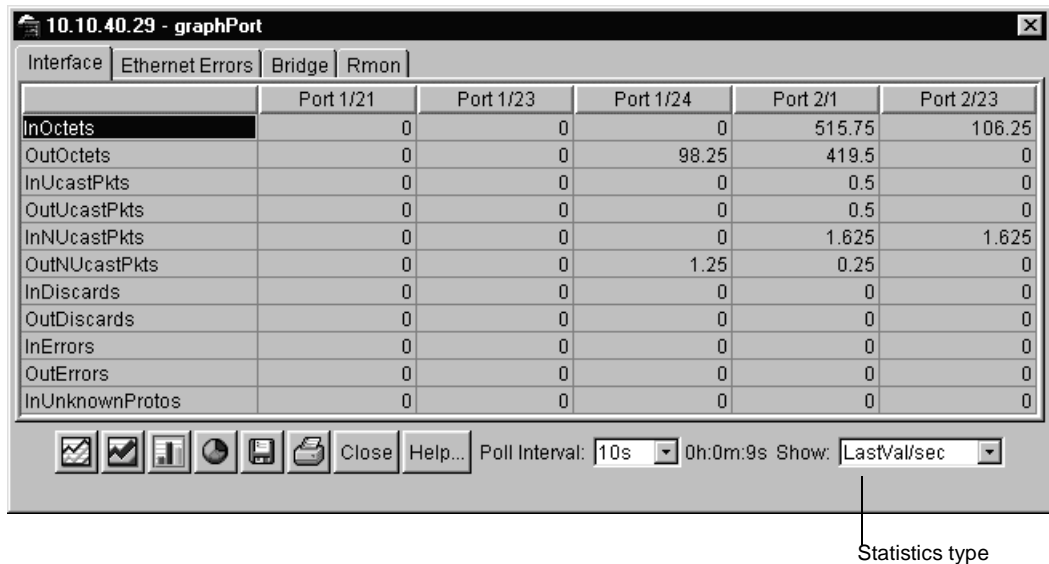
Figure 16 Interface statistics for a single port



	AbsoluteValue	Cumulative	Average	Minimum	Maximum	LastValue
InOctets	2,343,230	9,047	452.35	216.7	823	216.7
OutOctets	1,090,857	3,266	163.3	41.6	288	41.6
InUcastPkts	1,540	6	0.3	0.1	1	0.1
OutUcastPkts	1,792	6	0.3	0.1	1	0.1
InNUcastPkts	24,320	89	4.45	2.9	8	2.9
OutNUcastPkts	1,167	4	0.2	0	0.222	0.2
InDiscards	0	0	0	0	0	0
OutDiscards	0	0	0	0	0	0
InErrors	0	0	0	0	0	0
OutErrors	0	0	0	0	0	0
InUnknownProtos	0	0	0	0	0	0

At the bottom of the dialog box, there are icons for various functions and a 'Poll Interval' dropdown menu set to '10s'.

The statistics dialog box for multiple objects shows a single type of statistics (Table 12) for the selected objects. For example, Figure 17 shows LastValue statistics for the selected ports.

Figure 17 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:

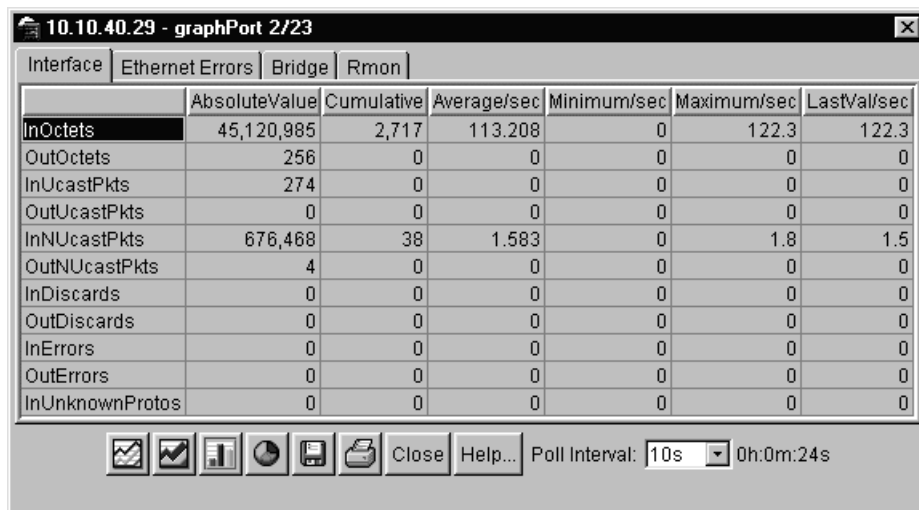
- 1 Select the object or objects to be graphed
See [“Selecting objects” on page 30](#).
- 2 Do one of the following:
 - On the toolbar, click Graph Selected.



- 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 18](#)).

Figure 18 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 39](#).

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 13](#) describes the buttons in the graph dialog boxes.

Table 13 Graph dialog box buttons

Button	Name	Description
	Stacked	“Stacks” data quantities instead of displaying them side-by-side.
	Horizontal	Rotates the graph 90 degrees.
	Log Scale	Changes the scale of the x-axis (of an unrotated graph) from numeric to logarithmic.
	Line Chart	Converts an area graph or bar graph to a line graph.
	Area Chart	Converts a line graph or bar graph to an area graph.
	Bar Chart	Converts a line graph or area graph to a bar graph.

Telneting 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 Actions > Telnet.
- On the toolbar, click the Telnet button.



A Telnet window to the switch opens.

Trap log

You can configure a Business Policy 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 window (Figure 2). 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.

Management stations operating with Device Manager are automatically added to trap receivers.

For more information about traps and trap receivers, refer to *Using the Business Policy Switch 2000*.

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 14](#).

Table 14 Help file locations

Platform	Default path
Windows 95, Windows 98, or Windows NT	c:\DM\help\dm\dm.html
UNIX	DM-UNIX/DM/help

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.

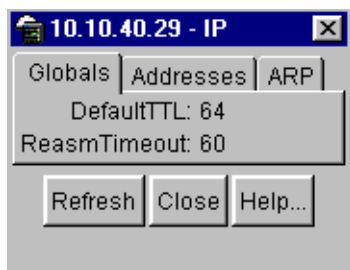
The Edit IP dialog box opens ([Figure 19](#)) with the Globals tab displayed.

Globals tab

To open the Globals tab:

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

The IP dialog box opens ([Figure 19](#)) with the Globals tab displayed.

Figure 19 Globals tab

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

Table 15 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 19](#)).

- 2 Click the Addresses tab.

The Addresses tab opens ([Figure 20](#)).

Figure 20 Edit IP dialog box — IP Address tab

[Table 16](#) describes the IP Address tab items.

Table 16 IP Addresses tab items

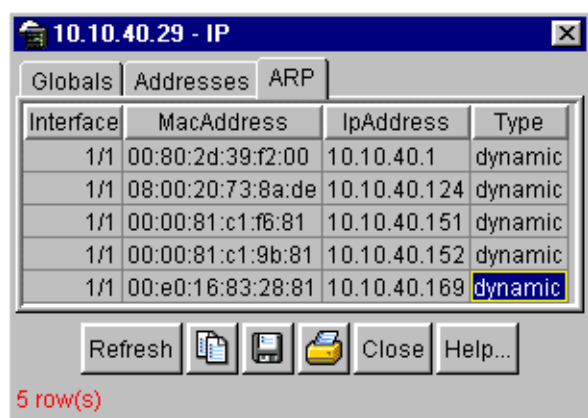
Item	Description
Addr	The device IP address.
NetMask	The subnet mask address.
BcastAddr	The IP broadcast address used.
ReasmMaxSize	The size of the largest IP datagram that this entity can reassemble from incoming IP fragmented datagrams received on this interface.

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 19](#)).
- 2 Click the ARP tab.
The ARP tab opens ([Figure 21](#)).

Figure 21 Edit IP dialog box — ARP tab

[Table 17](#) describes the ARP tab items.

Table 17 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 22](#)).

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 22](#)).

Figure 22 Edit Chassis dialog box — System tab

10.10.40.29 - Chassis

System | Base Unit Info | Stack Info | Agent | SNMP | Trap Receivers | PowerSupply | Fan

sysDescr: Business Policy Switch 2000 HW:AB3 FW:V0.9E SW:v1.0.0.68

sysUpTime: 2 days, 5h:13m:52s

sysContact:

sysName:

sysLocation:

☒ AuthenticationTraps

ReBoot: ☒ running ☐ reboot

NextBootMgmtProtocol: ipOnly

CurrentMgmtProtocol: ipOnly

BootMode: local

ImageLoadMode: net

CurrentImageVersion: v1.0.0.68

LocalStorageImageVersion: v1.0.0.68

NextBootDefaultGateway: 10.10.40.1

CurrentDefaultGateway: 10.10.40.1

NextBootLoadProtocol: ipOnly

LastLoadProtocol: ip

Apply Refresh Close Help...




Note: The chassis keeps track of the elapsed time and calculates the time and date using the system clock of the Device Manager machine as a reference.

Table 18 describes the System tab items.

Table 18 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.

Table 18 System tab items (continued)

Item	Description
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> 
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	The source from which to load the initial protocol configuration information to boot the switch the next time, local (from the switch), or net (over the network), or none.
ImageLoadMode	The source from which to load the agent image at the next boot.
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	<p>Action object to reboot the agent.</p> <p>Reset — initiates a hardware reset.</p> <p>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.</p>

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 22](#)).

- 3 Click the Base Unit Info tab.

The Base Unit Info tab opens ([Figure 23](#)).

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 Business Policy Switch 2000* and *Using Web-based Management for the Business Policy Switch 2000*.

Figure 23 Edit Chassis dialog box — Base Unit Info tab

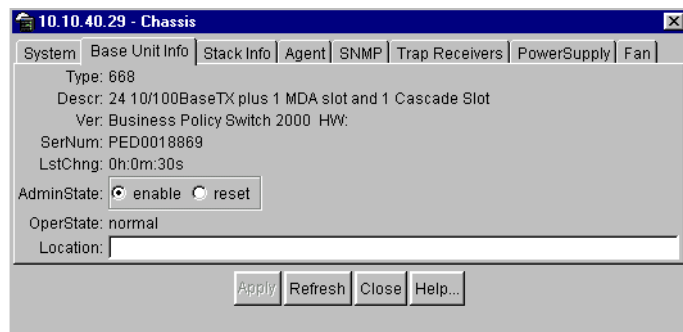


Table 19 describes the Base Unit Info tab items.

Table 19 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.
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.
AdminState	Administrative state of the switch. Select either <code>enable</code> or <code>reset</code> . Note: In a stack configuration, <code>Reset</code> only resets the base unit.
OperState	The operational state of the switch.
Location	Type the physical location of the switch.

Stack 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 Business Policy Switches or a mixed stack of BayStack 450, and BayStack 410 *and* Business Policy switches.

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 22).

- 3 Click the Stack Info tab.

The Stack Info tab opens (Figure 24).

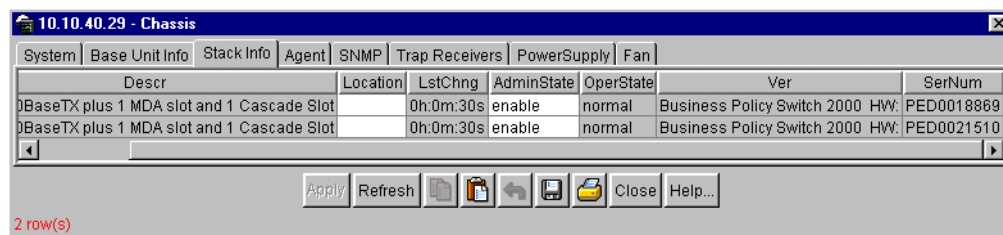
Figure 24 Edit Chassis dialog box — Stack Info tab

Table 20 describes the Stack Info tab fields.

Table 20 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"> disable—disables operation enable—enables operation reset—resets component 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 20 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 • resetInProgress—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.

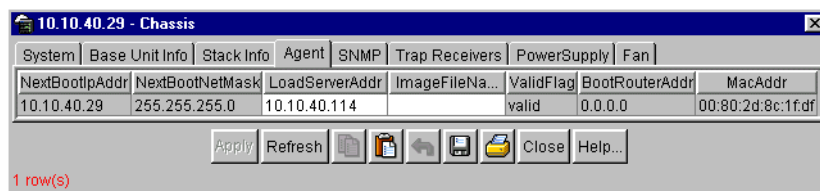
To open the Agent tab:

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

The Chassis dialog box opens ([Figure 22](#)) with the System tab displayed.

- 3 Click the Agent tab.

The Agent tab opens ([Figure 25](#)).

Figure 25 Edit Chassis dialog box — Agent tab

[Table 21](#) describes the Agent tab fields.

Table 21 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.
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.

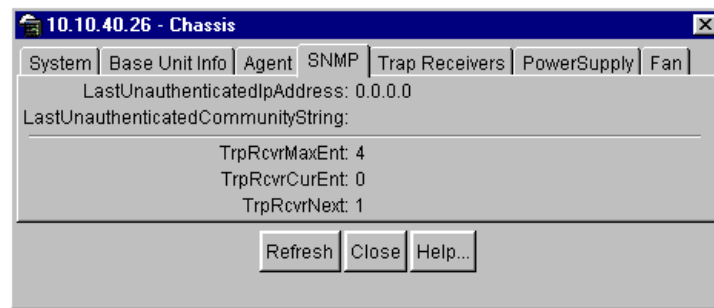
To open the SNMP tab:

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

The Chassis dialog box opens ([Figure 22](#)) with the System tab displayed.

- 3 Click the SNMP tab.

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

Figure 26 Edit Chassis dialog box — SNMP tab

[Table 22](#) describes the SNMP Info tab fields.

Table 22 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 Business Policy Switch 2000 switch.

When Device Manager opens a device, it automatically adds the device to the Trap Receivers list.

To open the Trap Receivers tab:

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

The Chassis dialog box opens ([Figure 22](#)) with the System tab displayed.

- 3 Click the Trap Receivers tab.

The Trap Receivers tab opens (Figure 27).

Figure 27 Edit Chassis dialog box — Trap Receivers tab



Table 23 describes the Trap Receivers tab items.

Table 23 Edit Chassis dialog box — Trap Receivers tab items

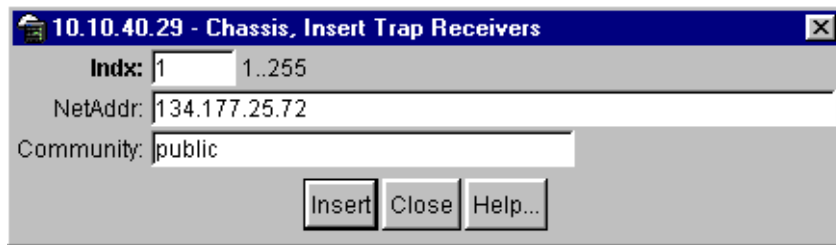
Item	Description
NetAddr	The address (or DNS hostname) for the trap receiver.
Community	Community string used for trap messages to this trap receiver.
Status	<p>This object is used to create and delete rows in the table and control them if they are used. The values that can be written are:</p> <ul style="list-style-type: none"> valid — makes an existing row valid - can only be written to change the value from the ignore values ignore —Note: do not use this entry to send traps to at this time delete—deletes the row create—creates a new row. This is the only value that can be used to create a row in the table. If the row exists, then a SET with value of create shows error 'badValue'. Deleted rows are removed immediately. The following values can be returned on reads: other — some other case; valid—the row exists and is valid; ignore — Note: do not use this entry to send traps to at this time.

Editing network traps

To edit the network traps table:

- 1 In the Trap Receivers tab (Figure 27), click Insert.

The Chassis, Insert Trap Receive dialog box opens (Figure 28).

Figure 28 Chassis, Insert Trap Receive dialog box

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



Note: Refer to [Table 23](#) 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.

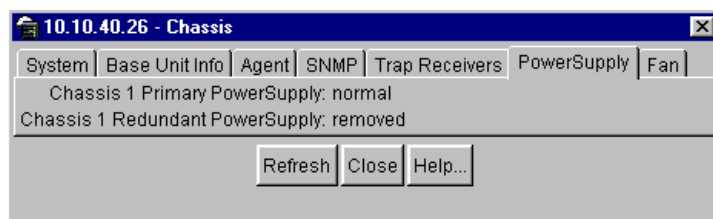
To open the PowerSupply tab:

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

The Chassis dialog box opens ([Figure 22](#)) with the System tab displayed.

- 3 Click the PowerSupply tab.

The PowerSupply tab opens ([Figure 29](#)).

Figure 29 Edit Chassis dialog box — Power Supply tab

[Table 24](#) describes the Power Supply tab fields.

Table 24 Power Supply tab fields

Field	Description
Desc	The power supply type.
OperStat	The operational state of the power supply. Possible values include: <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 22) with the System tab displayed.

- 3 Click the Fan tab.

The Fan tab opens (Figure 30).

Figure 30 Edit Chassis dialog box — Fan tab

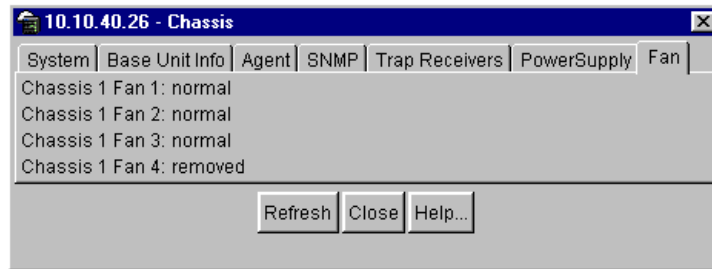


Table 25 describes the Fan tab fields.

Table 25 Fan tab fields

Field	Description
Desc	The fan type.
OperStat	<p>The operational state of the fan. Values include:</p> <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.

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 31).

Update only one item at a time. Click Apply after each change.

Figure 31 Edit FileSystem dialog box

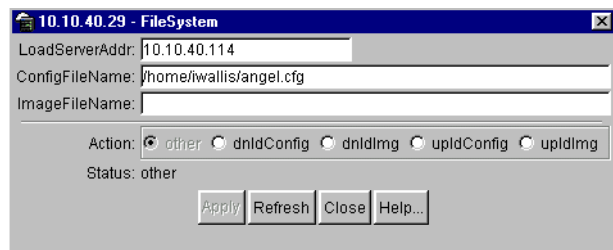


Table 26 describes the FileSystem dialog box items.

Table 26 FileSystem 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.

Table 26 FileSystem dialog box items (continued)

Item	Description
Action	<ul style="list-style-type: none"> This object is used to download or upload a config file or an image 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 upldImg In a write operation, the value that can be written is: dnldConfig - download a config file to a device. The new config file will not take effect until the next boot cycle of the device. Possible values are: dnldImg - download an image to a device. upldConfig - upload a config file to a server from a device. The config file contains the current MIB object values of the device. upldImg - upload an image from a device to a server.
Result	<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.

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.
 - On the toolbar, click Graph.



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 12 on page 38](#).

SNMP tab

The chassis SNMP tab lists chassis statistics. For descriptions of the type of statistics shown in each column, refer to [Table 27](#).

To open the SNMP tab:

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

The Chassis dialog box opens ([Figure 22](#)) with the System tab displayed.

- 3 Click the SNMP tab.

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

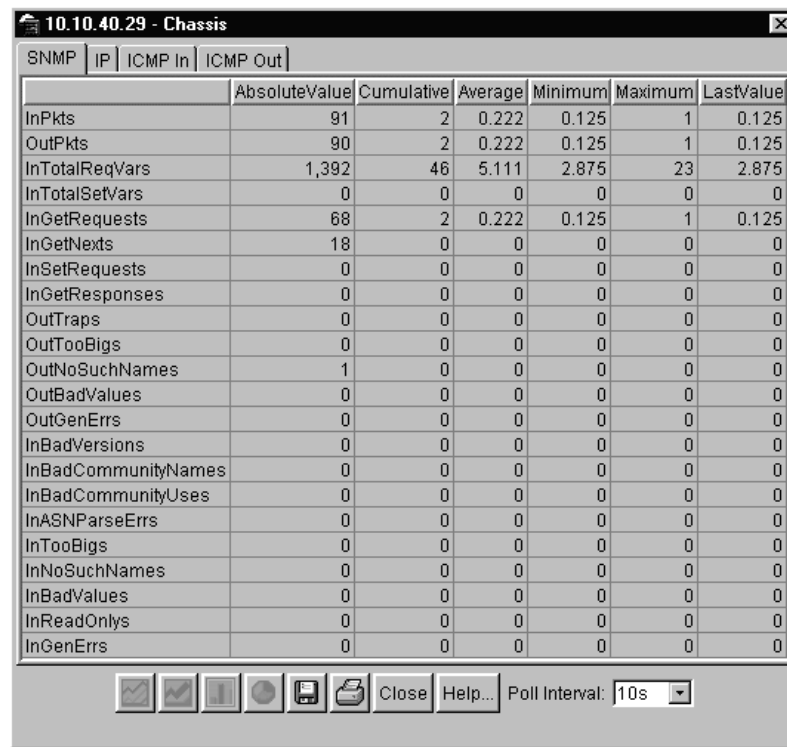
Figure 32 Graph Chassis dialog box — Chassis SNMP tab

Table 27 describes the SNMP tab fields.

Table 27 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 27 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 27 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 32) with the SNMP tab displayed.

- 3 Click the IP tab.

The IP tab opens (Figure 33).

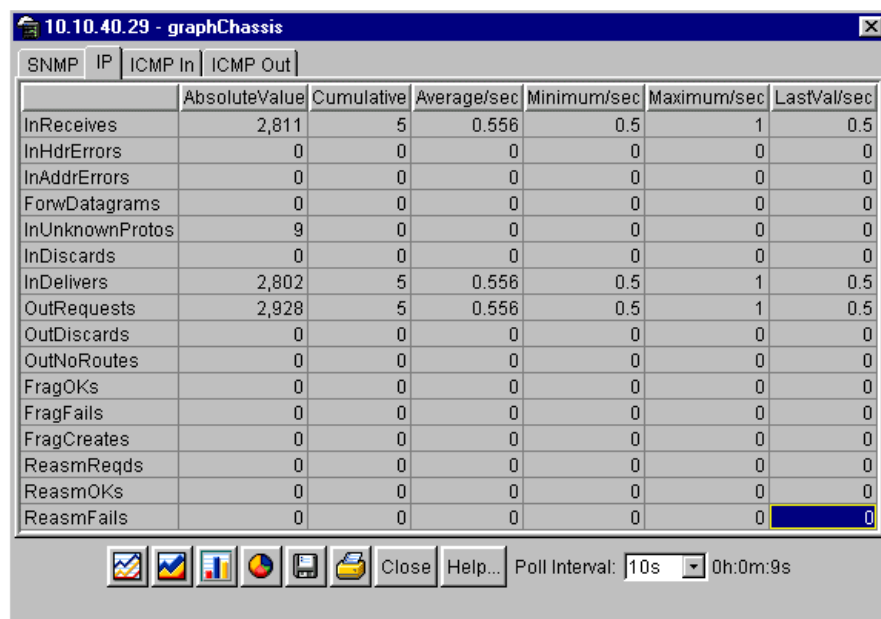
Figure 33 Graph Chassis dialog box — IP tab

Table 28 describes the Chassis IP tab fields.

Table 28 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 28 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 includes any packets counted in ipForwDatagrams that meet this no-route criterion. 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 28 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 [\(Figure 32\)](#) with the SNMP tab displayed.

- 3 Click the ICMP In tab.

The ICMP In tab opens [\(Figure 34\)](#).

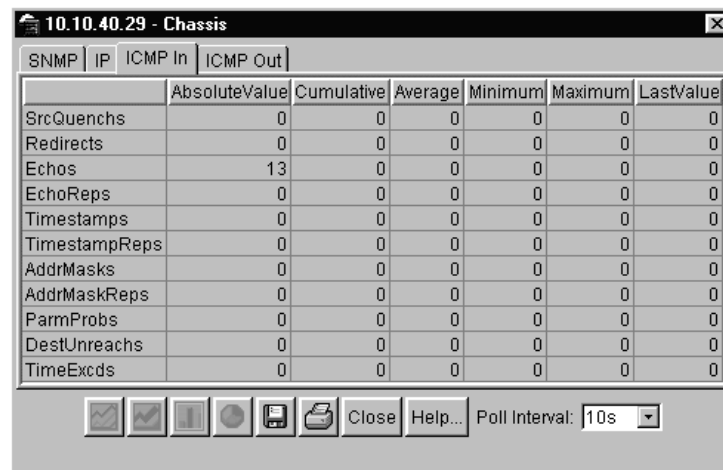
Figure 34 Graph Chassis dialog box — ICMP In tab

Table 29 describes the ICMP In tab fields.

Table 29 ICMP In tab fields

Field	Description
SrcQuenchs	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 32) with the SNMP tab displayed.

- 3 Click the ICMP Out tab.

The ICMP Out tab opens (Figure 35).

Figure 35 Graph Chassis dialog box — ICMP Out tab

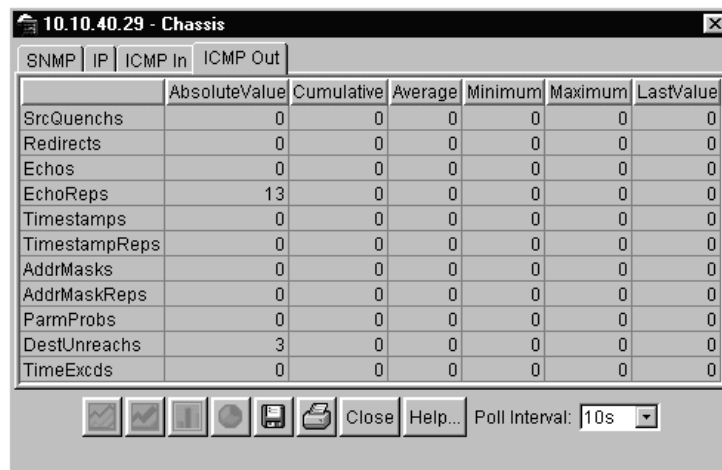


Table 30 describes the ICMP Out tab fields.

Table 30 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.

Chapter 3

Configuring and graphing ports

This chapter describes how you use Device Manager to configure and graph ports on a Business Policy Switch 2000.

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 port, double-click on the port.

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

- 1 Select the port or 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.

Interface tab for a single port

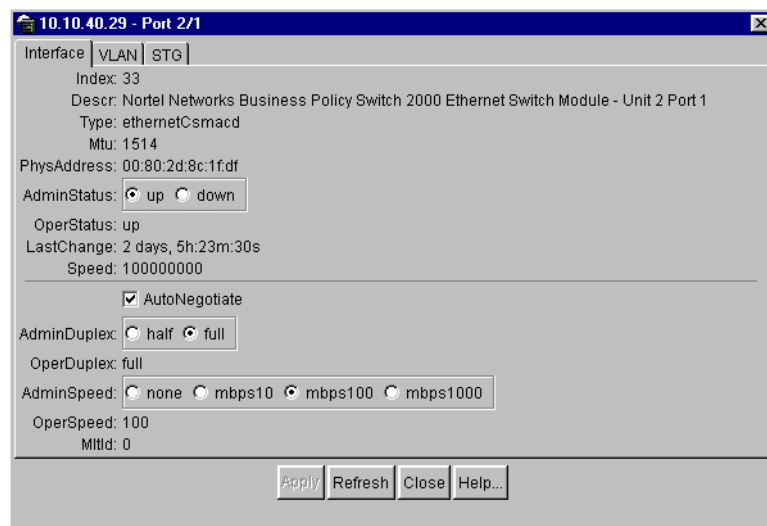
The Interface tab shows the basic configuration and status of a single port.

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 36) with the Interface tab displayed.

Figure 36 Edit Port dialog box — Interface tab





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 31 describes the Interface tab items for a single port.

Table 31 Interface tab items for a single port

Field	Description
Index	A unique value assigned to each interface. The value ranges between 12 and 255.
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 31 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.
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.
MltId	The Multi-Link Trunk to which the port is assigned (if any).

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 36](#)) with the Interface tab displayed.

- 3 Click the VLAN tab.

The VLAN tab opens ([Figure 37](#)).

Figure 37 Edit Port dialog box — VLAN tab

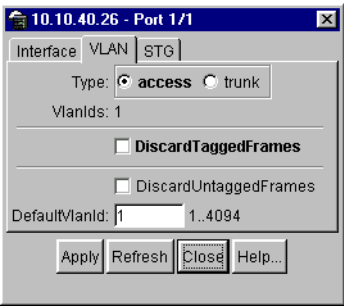


Table 32 describes the VLAN tab items.

Table 32 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.
DiscardTagged Frames	This field only applies to access ports. It acts as a flag used to determine how to process tagged 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 processed normally.
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.
Port	Allows you to change the switch port being viewed.

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 36](#)) with the Interface tab displayed.

- 3 Click the STG tab.

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

Figure 38 Edit Port dialog box — STG tab

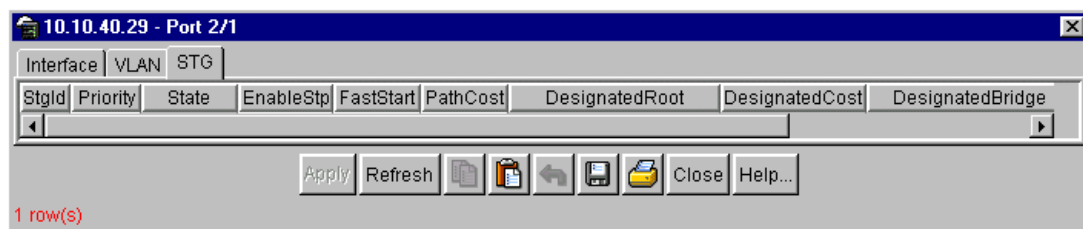


Table 33 describes the STG tab items.

Table 33 STG tab items for a single port

Item	Description
Stgld	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.

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 Graph Port Interface tab (Figure 39) shows port interface statistics.

Figure 39 Graph Port dialog box — Port Interface tab

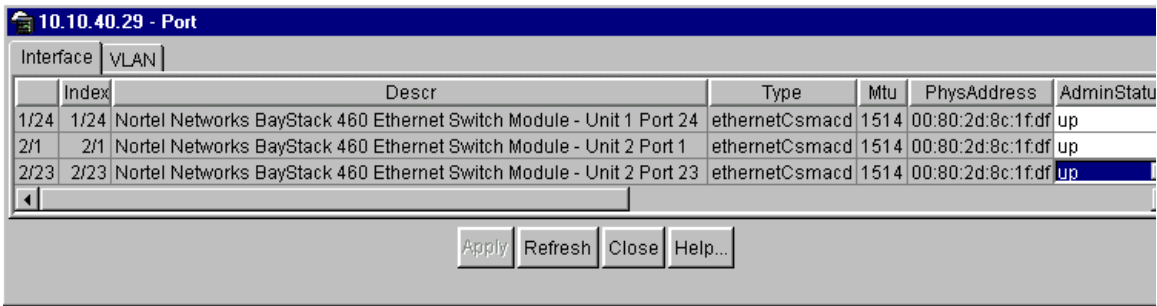


Table 34 describes the Port Interface tab fields.

Table 34 Interface tab fields for multiple ports

Field	Description
Index	A unique value assigned to each interface. The value ranges between 12 and 255.
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	<p>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>

Table 34 Interface tab fields for multiple ports (continued)

Field	Description
OperStatus	Current operational state of the interface, which can be one of the following: <ul style="list-style-type: none"> • up • down • testing 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.
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.
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.
MtId	The MultiLink Trunk to which the port is assigned (if any).

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 36) opens with the Interface tab displayed.

- 3 Click the VLAN tab.
- The VLAN tab opens (Figure 40).

Figure 40 VLAN tab for multiple ports

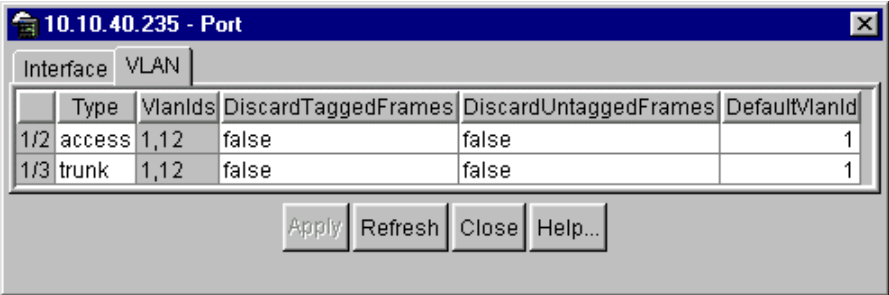


Table 35 describes the VLAN tab fields for multiple ports.

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.
DiscardTaggedFrames	This field only applies to access ports. It acts as a flag used to determine how to process tagged 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 processed normally.

Table 35 VLAN tab fields for multiple ports (continued)

Field	Description
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.

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 36](#)) or for multiple ports opens with the Interface tab displayed.

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.

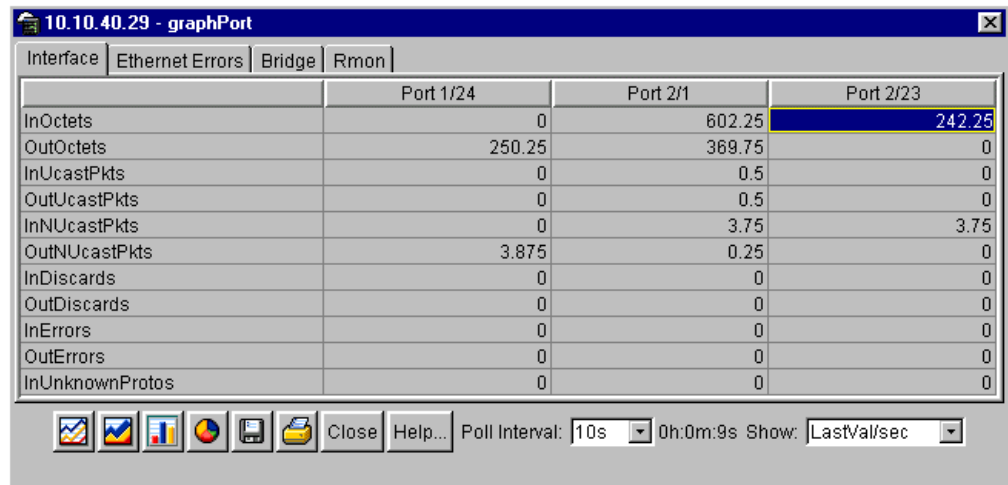
To select multiple ports, [Ctrl] + left-click the ports that you want to configure. A yellow outline appears around the selected ports.

- 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 41) or for multiple ports opens with the Interface tab displayed.

Figure 41 Interface tab for graphing ports



[Table 36](#) describes the Interface tab fields for graphing ports.

Table 36 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 36 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 36) or for multiple ports opens with the Interface tab displayed.

- 3 Click the Ethernet Errors tab.

The Port Ethernet Errors tab opens (Figure 42).

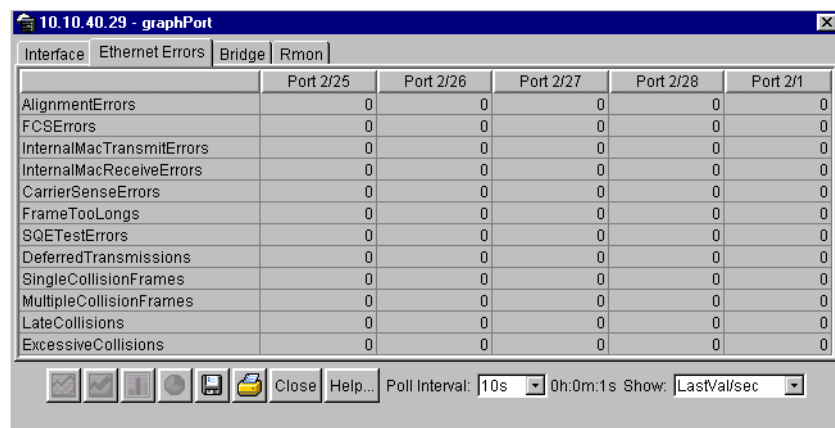
Figure 42 Graph Port dialog box — Port Ethernet Errors tab

Table 37 describes the Port Ethernet Errors tab fields.

Table 37 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.

Table 37 Ethernet Errors tab fields (continued)

Field	Description
InternalMacReceiveErrors	<p>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.</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 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.</p>
FrameTooLongs	<p>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.</p>
SQETestErrors	<p>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.</p>
DeferredTransmissions	<p>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.</p>
SingleCollisionFrames	<p>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.</p>

Table 37 Ethernet Errors tab fields (continued)

Field	Description
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.
Poll Interval	Statistics are updated based on the poll interval.
	Default: 10s
	Range: None, 2s, 5s, 10s, 30s, 1m, 5m, 30m 1h

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 36) or for multiple ports opens with the Interface tab displayed.

- 3 Click the Bridge tab.
- The Bridge tab for graphing ports opens (Figure 43).

Figure 43 Graph Port dialog box — Bridge tab

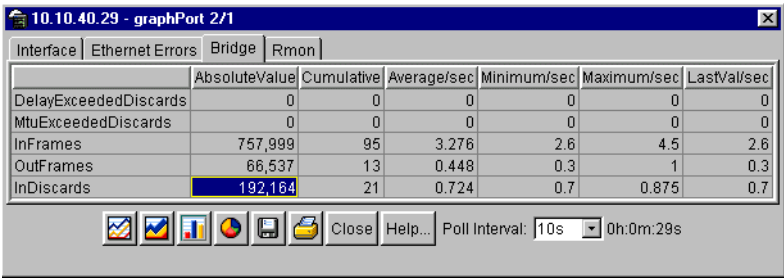


Table 38 describes the Bridge tab fields.

Table 38 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 36) or for multiple ports opens with the Interface tab displayed.

- 3 Click the RMON tab.

The RMON tab for graphing ports opens (Figure 44).

Figure 44 Graph Port dialog box — RMON tab

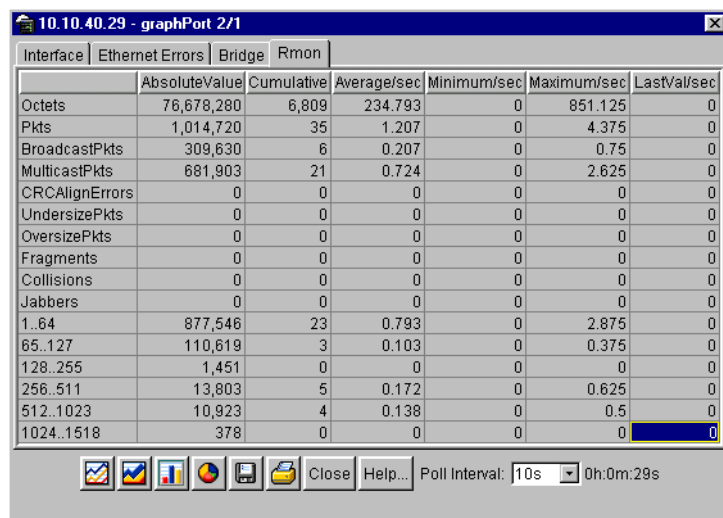


Table 39 describes the RMON tab fields.

Table 39 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 39 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).
>64	The total number of packets (including bad packets) received that were greater than 64 octets in length (excluding framing bits but including FCS octets).
>127	The total number of packets (including bad packets) received that were greater than 127 octets in length (excluding framing bits but including FCS octets).
>255	The total number of packets (including bad packets) received that were greater than 255 octets in length (excluding framing bits but including FCS octets).
>511	The total number of packets (including bad packets) received that were greater than 511 octets in length (excluding framing bits but including FCS octets).
>1023	The total number of packets (including bad packets) received that were greater than 1023 octets in length (excluding framing bits but including FCS octets).

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 Business Policy Switch 2000, 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 in an MLT can be on different unit in the stack.
- MultiLink Trunking is supported on 10BASE-T, 100BASE-TX, 100BASE-FX, and Gigabit Ethernet 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.

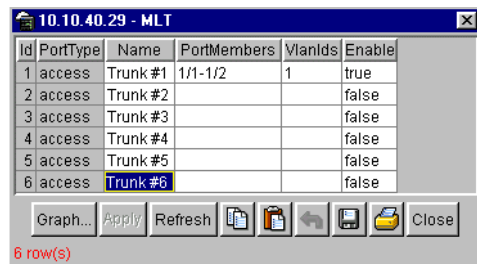
Setting up MLTs

To set up MLTs:

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

The MLT dialog box opens ([Figure 45](#)).

Figure 45 MLT dialog box



The active MultiLink Trunks are displayed with the fields described in [Table 40](#).

Table 40 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.

Adding ports to a MultiLink Trunk

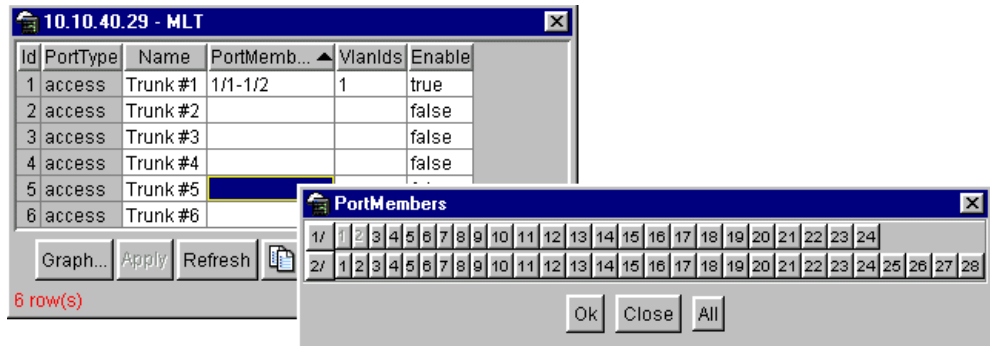
To add ports to an existing MLT:

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

The MLT dialog box opens.

- 2 Double-click the PortMembers field.

The PortMembers dialog box opens ([Figure 46](#)).

Figure 46 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.



Note: The first enabled distributed MLT causes the stack to reset. Please refer to the switch manuals for more details on MLT rules.

MultiLink Trunk statistics

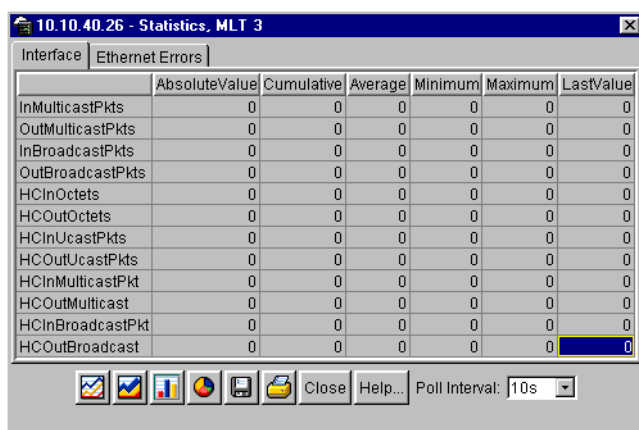
To view MLT interface statistics:

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

The MLT window opens ([Figure 47](#)).

- 2 Select an MLT row and then click Graph.

The Statistics, MLT window ([Figure 47](#)) opens with the Interface tab displayed.

Figure 47 MLT Statistics — Interface tab


	AbsoluteValue	Cumulative	Average	Minimum	Maximum	LastValue
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
HCOctets	0	0	0	0	0	0
HCInUcastPkts	0	0	0	0	0	0
HCOctets	0	0	0	0	0	0
HCInMulticastPkt	0	0	0	0	0	0
HCOctets	0	0	0	0	0	0
HCInBroadcastPkt	0	0	0	0	0	0
HCOctets	0	0	0	0	0	0

Table 41 describes the fields in the Interface tab.

Table 41 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.
HCOctets	The total number of octets transmitted out of the MLT interface, including framing characters.
HCInUcastPkts	The number of packets delivered by this MLT to higher level protocols that were not addressed to a multicast or broadcast address at this sublayer.

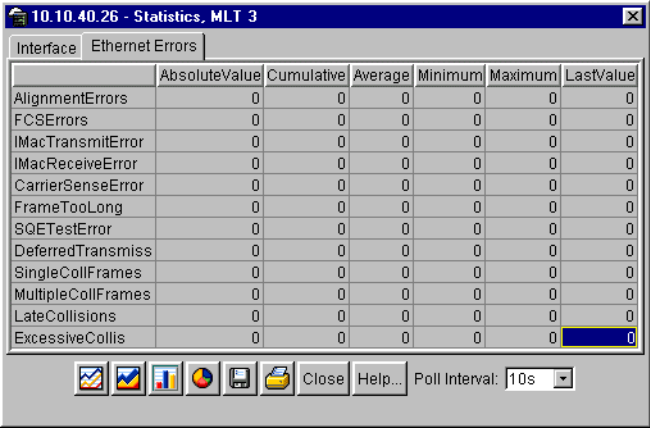
Table 41 Interface tab fields (continued)

Field	Description
HCOUcastPkts	The number of packets that higher-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.
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.
HCOUmulticast	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.
HcInBroadcastPkt	The number of packets delivered to this MLT that were addressed to a broadcast address at this sublayer.
HcOutBroadcast	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.

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 45](#)).
- 2 Select an MLT by clicking anywhere within a field in the row.
- 3 Click Graph.
The Statistics, MLT dialog box opens ([Figure 47](#)) with the Interface tab displayed.
- 4 Click the Ethernet Errors tab.
The Ethernet Errors tab opens ([Figure 48](#)).

Figure 48 MLT Statics dialog box — Ethernet Errors tab

10.10.40.26 - Statistics, MLT 3

Interface EthernetErrors

	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

Close Help... Poll Interval: 10s

Table 42 describes the fields in the Ethernet Errors tab.

Table 42 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.
IMacReceiveError	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. 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 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.

Table 42 Ethernet Errors tab fields (continued)

Field	Description
FrameTooLong	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.
SQETestError	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.
DeferredTransmiss	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.
SingleCollFrames	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.
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 Business Policy Switch 2000. The chapter covers creating, editing, and deleting VLANs. It includes the following sections:

- VLANs (this page)
- [Creating VLANs \(page 108\)](#)
- [Modifying and managing existing VLANs \(page 116\)](#)

VLANs

A VLAN is a collection of ports on one or more switches that define a broadcast domain. The Business Policy Switch supports three types of VLANs:

- Port-based VLANs
- Protocol-based VLANs
- Source MAC-based VLANs

For a further description of VLANs, refer to *Using the Business Policy Switch 2000*.

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.
- An access port can belong to one and only one protocol-based VLAN for a given protocol.

- The default VLAN (VLAN ID 1) cannot be renamed or deleted, and it cannot have its type changed from port-based VLAN.

Creating VLANs

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

Device Manager enables you to create a port-based, protocol-based, and source address MAC-based VLAN.



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.

VLAN Information

To open the port-based VLAN dialog box:

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

The VLAN dialog box opens with the Basic tab displayed ([Figure 49](#)).

Figure 49 VLAN Basic tab

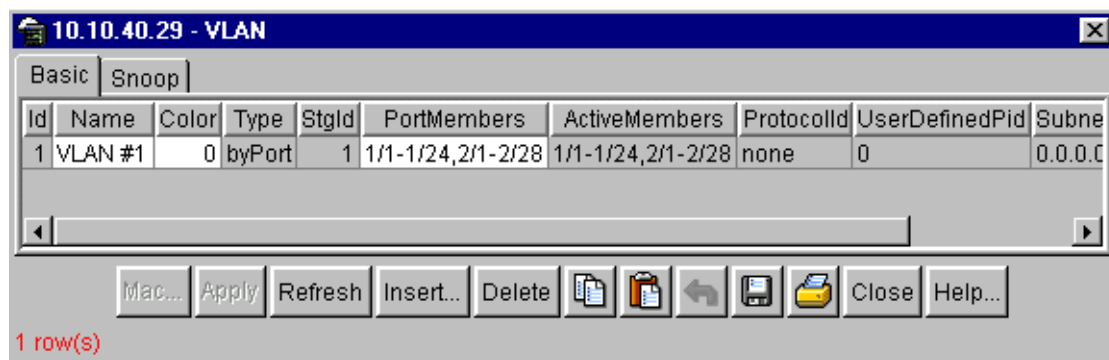


Table 43 describes the Basic tab fields.

Table 43 Basic tab fields

Field	Description
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.
StgId	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.
ProtocolId	Protocol for protocol-based VLANs. This value is taken from the Assigned Numbers RFC. For port-based VLANs, none is the displayed value.
UserDefinedPid	When rcVlanProtocolId is set to usrDefined(15) in a protocol-based VLAN, this field represents the 16-bit user defined protocol identifier.
SubnetAddr	IP subnet address of the VLAN. This is important only if rcVlanType is equal to byIpSubnet(2). For other VLANs, set this value to 0 . 0 . 0 . 0.
SubnetMask	IP subnet mask of the VLAN. This is important only if rcVlanType is equal to byIpSubnet(2). For other VLANs, set this value to 0 . 0 . 0 . 0.

Creating a port-based VLAN

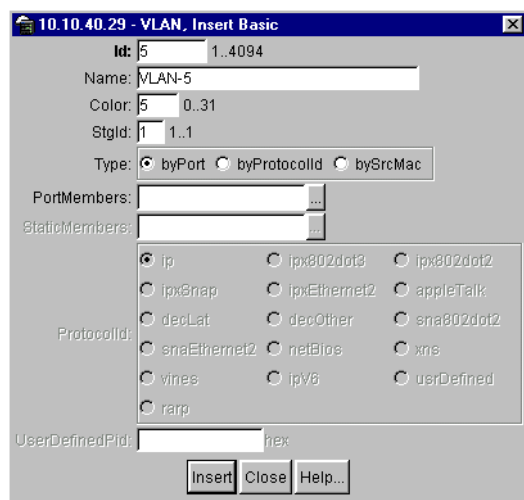
To create a port-based VLAN:

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

The VLAN dialog box opens (Figure 49).

- 2 Click Insert.

The Insert Basic dialog box for creating VLANs opens (Figure 50). This dialog box opens with the Type field set to byPort.

Figure 50 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.

Creating a protocol-based VLAN

To create a protocol-based VLAN:

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

The VLAN dialog box opens (Figure 49).

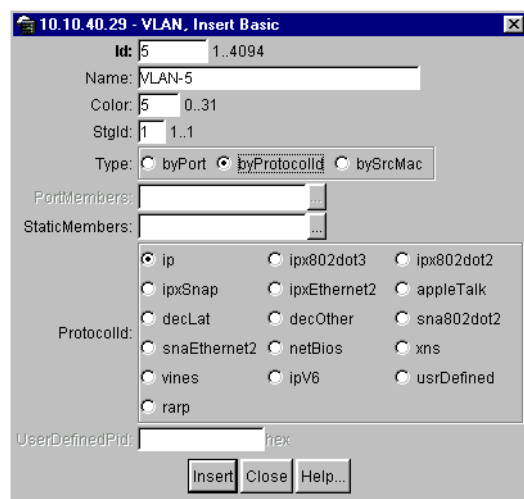
2 Click Insert.

The Insert Basic dialog box for creating VLANs opens (Figure 50).

3 Change the Type field to byProtocolID.

The dialog box changes to display additional fields needed to set up protocol-based VLANs (Figure 51).

Figure 51 VLAN, Insert Basic dialog box for a protocol-based VLAN



4 Type the unique VLAN ID.

5 Type the VLAN name (optional).

If no name is entered, the protocol name becomes the default VLAN name.

6 In the Color text box, type in the color.

7 In the StgID text box, type in spanning tree group ID (stgid).

8 In the Type field, click byProtocolID if not already selected.

9 Specify the port membership by clicking the ellipsis (...) field.

10 Specify Static Members by clicking the ellipsis (...) field.

11 Specify by NotAllowToJoin by clicking the ellipsis (...) field.

12 In the ProtocolID field select one protocol radio button.

13 Click Insert.

Creating a source address MAC-based VLAN

To create a source address MAC-based VLAN:

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

The VLAN dialog box opens ([Figure 49](#)).

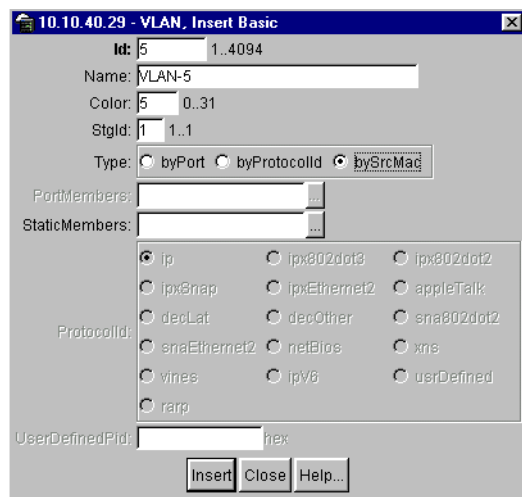
- 2 Click Insert.

The VLAN, Insert Basic dialog box opens ([Figure 52](#)). This dialog box opens with the Type field set to byPort.

- 3 Change the Type field to bySrcMac.

The dialog box changes to display additional fields needed to set up source MAC-based VLANs ([Figure 52](#)).

Figure 52 VLAN, Insert Basic dialog box for a source MAC-based VLAN



- 4 Enter the unique VLAN ID.
- 5 Enter the VLAN name (optional).

If no name is entered, the protocol name becomes the default VLAN name.

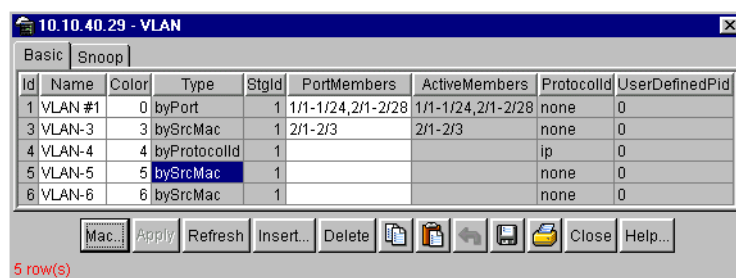
- 6 Enter a color (optional).

Device Manager will suggest a color, but it can be changed.

- 7 Type in the spanning tree group ID of the VLAN.
- 8 In the Type field, click bySrcMac if not already selected.
- 9 Specify the static membership by clicking the ellipsis (...) field.
- 10 Click Insert.

The VLAN dialog box opens (Figure 53).

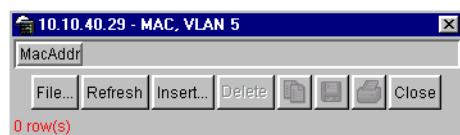
Figure 53 VLAN dialog box



- 11 Highlight the BySrcMac field.
- 12 Click MAC.

The MAC, VLAN dialog box opens (Figure 54).

Figure 54 MAC, VLAN dialog box



- 13 Click Insert

The Insert VLAN MAC dialog box opens (Figure 55).

Figure 55 Insert VLAN MAC dialog box



- 14 Type the source MAC address for the VLAN.

15 Click Insert.

Note: In a source MAC-based VLAN, a potential member becomes an active member of the VLAN when a frame with the specified source MAC address is received. Source MAC-based VLANs are not supported in a mixed stack environment.

Accepting tagged and untagged frames

In the Business Policy Switch 2000, you configure whether or not tagged frames are sent or received on the port level. Refer to [“VLAN tab for a single port” on page 80](#) for VLAN tab field descriptions. Tagging is set as true or false for the port and applied to all VLANs on that port. You can select whether or not to discard:

- Tagged frames received on a port where tagging is disabled
- Untagged frames received on a port where tagging is enabled

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

A Business Policy Switch 2000 switch port with tagging enabled is a port from which all frames sent are tagged. A tagged port can be configured to discard untagged frames or to associate them with a VLAN set by the PVID. In the latter case, when an untagged frame is received on a tagged port, it is sent to the user-specified PVID.

A port with tagging disabled is a port that does not send tagged frames. If a tagged frame is forwarded out a port with tagging set to false, the switch removes the tag from the frame before sending it out the port. When a port with tagging set to false receives a frame, it can be configured to discard tagged frames or to associate them with the VLAN specified in the tag.



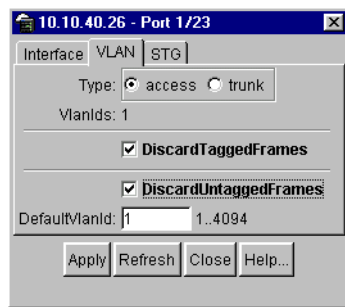
Note: To optimize performance, on untagged ports in configurations where you do not expect to see tagged frames, set DiscardTaggedFrames to true. However, on untagged ports for interconnecting switches, it is probably better to set DiscardTaggedFrames to false. Then, if you convert an interswitch port from an untagged port to a tagged port, connectivity is not lost.

To set a port to discard tagged 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 displaying the Interface tab.
- 3 Click the VLAN tab.
The VLAN tab opens ([Figure 56](#)).

Select the DiscardTaggedFrames and the DiscardUntaggFrames check boxes.

Figure 56 VLAN tab



- 4 Click Apply.

Snoop tab

You can use the Snoop tab to enable or disable the VLAN snooping on a switch.

To open the port-based VLAN:

- 1 From the Device Manager menu bar, choose VLAN > VLANs.
The VLAN dialog box opens ([Figure 49](#)) with the Basic tab displayed.
- 2 Click the Snoop tab.
The Snoop tab opens ([Figure 57](#)).

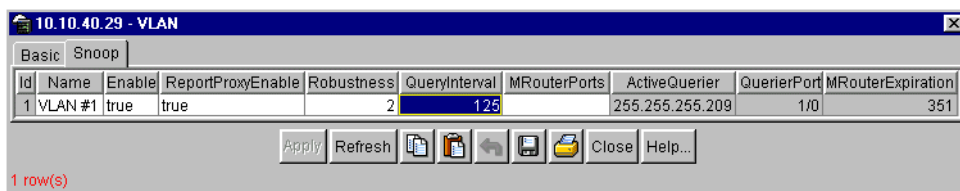
Figure 57 Snoop tab

Table 44 describes the Snoop tab fields.

Table 44 Snoop tab fields

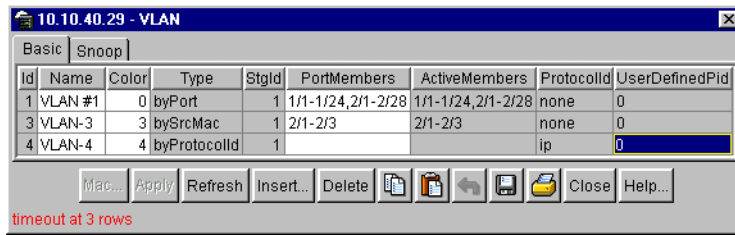
Field	Description
Name	Name of the VLAN.
Enable	Sets whether IGMP snooping is enabled or disabled.
ReportProxyEnable	Sets whether IGMP report proxy is enabled or disabled.
Robustness	Allows tuning for the expected packet loss on a subnet. If a subnet is expected to be bad, the Robustness variable can be increased. IGMP is robust to packet losses.
QueryInterval	Intervals (in seconds) between IGMP host and query packets transmitted on an interface.
MRouterPorts	A 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.

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 58). The VLAN dialog box displays all defined VLANs, their configurations, and their current status.

Figure 58 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 45 describes the fields in the VLAN dialog box.

Table 45 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 or byProtocolId.
Stgid	The spanning tree group ID to which the VLAN belongs.
PortMembers	The ports that are members of the VLAN.w
ActiveMembers	The ports that are members of the VLAN.
ProtocolId	The protocol for protocol-based VLANs. This value is taken from the Assigned Numbers RFC. For port-based VLANs, none is the displayed value.
UserDefined	When rcVlanProtocolId is set to usrDefined(15) in a protocol-based VLAN, this field represents the 16-bit user defined protocol identifier.

Chapter 6

Troubleshooting Device Manager

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

- [Topology tab](#) (this page)
- Topology Table tab ([page 120](#))

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 59](#)).

Figure 59 Diagnostics dialog box — Topology tab

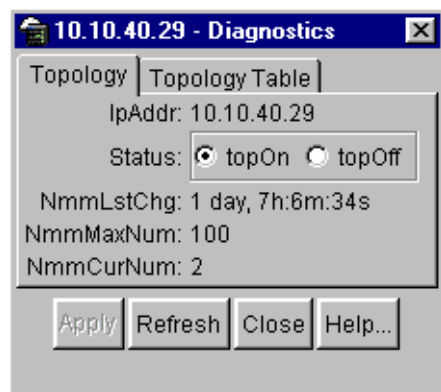


Table 46 describes the Topology tab items.

Table 46 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:

- From the Device Manager menu bar, choose Edit > Diagnostics.
The Diagnostics dialog box opens with the Topology tab displayed (Figure 59).
- Click the Topology Table tab.
The Topology Table tab opens (Figure 60).

Figure 60 Diagnostics dialog box — Topology Table tab

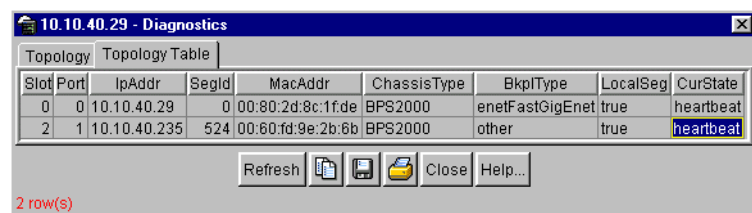


Table 47 describes the Topology Table tab fields.

Table 47 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 7

RMON

The Remote Network Monitoring (RMON) MIB is an interface between the RMON agent on a Business Policy Switch 2000 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 or chassis).

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 or Edit > Chassis.
- On the toolbar, click Graph button.

The Port dialog box opens displaying the Interface tab ([Figure 61](#)).

3 Click the RMON tab.

The RMON tab opens and displays the Ethernet statistics ([Figure 61](#)).

Figure 61 Port dialog box — RMON tab

	AbsoluteValue	Cumulative	Average	Minimum	Maximum	LastValue
Octets	465,700,347	1,248	1,248	1,248	1,248	1,248
Pkts	6,390,928	9	9	9	9	9
BroadcastPkts	4,688,974	6	6	6	6	6
MulticastPkts	6,902,090	8	8	8	8	8
CRCAlignErrors	0	0	0	0	0	0
UndersizePkts	0	0	0	0	0	0
OversizePkts	0	0	0	0	0	0
Fragments	0	0	0	0	0	0
Collisions	0	0	0	0	0	0
Jabbers	0	0	0	0	0	0
1..64	5,856,264	7	7	7	7	7
65..127	371,742	0	0	0	0	0
128..255	27,552	0	0	0	0	0
256..511	110,201	2	2	2	2	2
512..1023	24,814	0	0	0	0	0
1024..1518	355	0	0	0	0	0

For descriptions of the RMON tab fields, refer to [Table 39 on page 97](#). For descriptions of the statistics columns, refer to [Table 12 on page 38](#).

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:

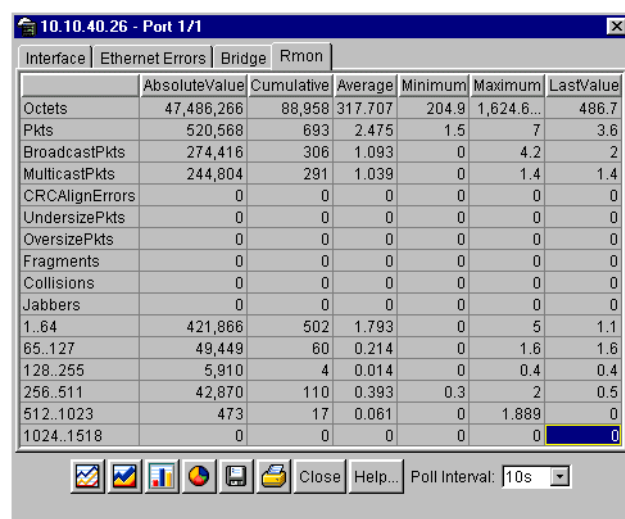
- 1 Select an object (port or chassis).
- 2 On the toolbar, click Graph.

The graph Port dialog box opens displaying the Interface tab.

- 3 Click the RMON tab.

The RMON tab opens (Figure 62).

Figure 62 Port dialog box — RMON tab



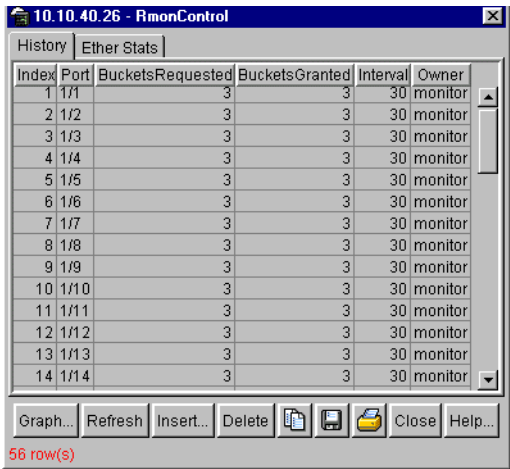
Creating a history

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 63).

Figure 63 History tab



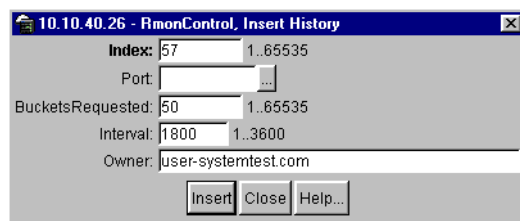
Index	Port	BucketsRequested	BucketsGranted	Interval	Owner
1	1/1	3	3	30	monitor
2	1/2	3	3	30	monitor
3	1/3	3	3	30	monitor
4	1/4	3	3	30	monitor
5	1/5	3	3	30	monitor
6	1/6	3	3	30	monitor
7	1/7	3	3	30	monitor
8	1/8	3	3	30	monitor
9	1/9	3	3	30	monitor
10	1/10	3	3	30	monitor
11	1/11	3	3	30	monitor
12	1/12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

56 row(s)

Table 48 describes the History fields.

- 2 Select an index and then click Insert.
The RMONControl, Insert History dialog box opens (Figure 64).

Figure 64 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.

Table 48 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.

Table 48 History tab fields (continued)

Field	Description
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.

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 63](#)).
- 2 Highlight the row that contains the port ID you want to delete.
- 3 Click **Delete**.
The entry is removed from the table.

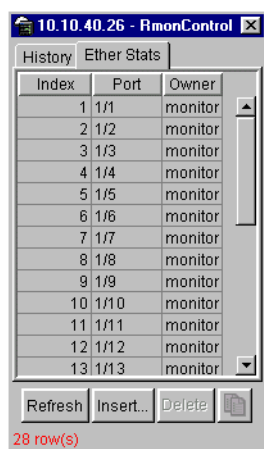
Enabling Ethernet statistics gathering

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.
- 2 Click the Ether Stats tab.
The Ether Stats tab opens ([Figure 65](#)).

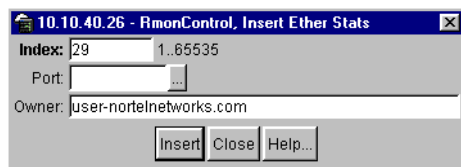
Figure 65 RMONControl dialog box — Ether Stats tab



- 3 Click Insert.

The RMONControl, Insert Ether Stats dialog box opens ([Figure 66](#)).

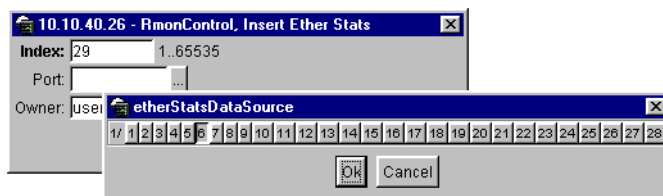
Figure 66 RMONControl, Insert Ether Stats dialog box



4 Select the port(s).

Enter the port number you want or select the port from the list menu (Figure 67).

Figure 67 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. [Table 49](#) describes the Ether Stats tab fields.

Table 49 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.

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 displaying the History tab.

2 Click the Ether Stats tab.

The Ether Stats tab opens ([Figure 65](#)).

- 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:

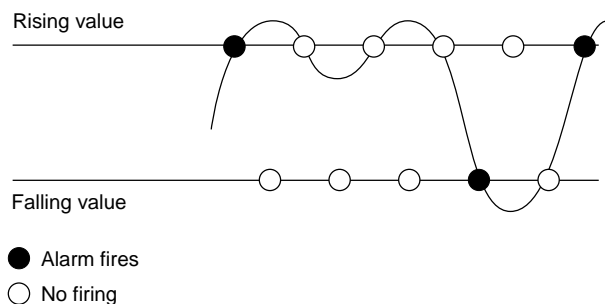
- An upper and lower threshold value is defined.
- A corresponding rising and falling event occurs.
- An alarm interval or polling period is reached.

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 68](#)).

Figure 68 How alarms fire

7821EA

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.

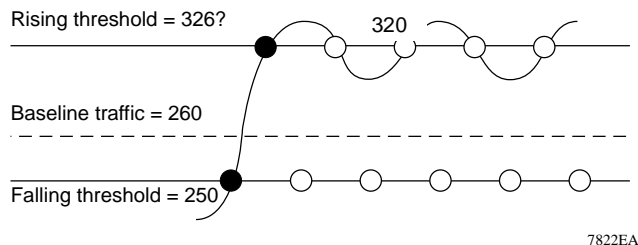
A general guideline is to define one of the threshold values to an expected, baseline value, and then define the opposite threshold as the out-of-bounds limit. Because of sample averaging, the value may be equal to ± 1 of the baseline units. For example, assume an alarm is defined on octets going out 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 69](#)). 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 69 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.

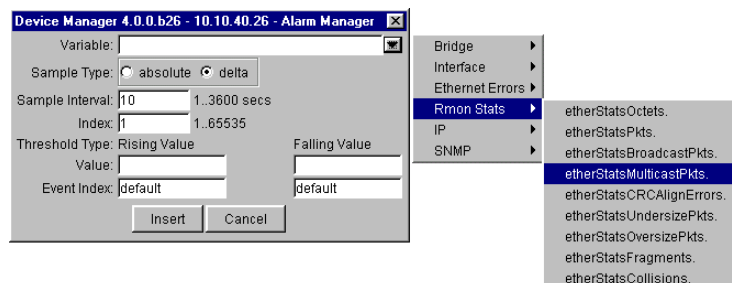


The Alarm Manager dialog box opens (Figure 70).

Figure 70 Alarm Manager dialog box

- 2 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 71).

Figure 71 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. (A list of variable definitions is located in [Appendix B, “RMON alarm variables.”](#)) This example is a chassis alarm, indicated by the “.0” in the variable.

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

5 Click Insert.

If you want to make field changes, see the field descriptions shown in [Table 50](#).

Table 50 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 133 .	
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 displaying the History tab ([Figure 63](#)).

- 3 Click the Ether Stats tab to view statistics (Figure 61 on page 124).
The RMONAlarms dialog box opens with the Alarms tab (Figure 72) displayed.

To delete an alarm:

- 1 From the Device Manager main menu, choose RMON > Alarms.
The RMONAlarms dialog box opens with the Alarms tab (Figure 72) displayed.

Figure 72 RMONAlarms dialog box — Alarms tab



- 2 Click any field for the alarm that you want to delete to highlight it.
- 3 Click Delete.

Table 51 describes the fields on the Alarms tab.

Table 51 Alarms tab fields

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.

Table 51 Alarms tab fields (continued)

Field	Description
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 <code>absoluteValue(1)</code> , 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 <code>deltaValue(2)</code> , 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 <code>deltaValue</code> , this value is the difference between the samples at the beginning and end of the period. If the sample type is <code>absoluteValue</code> , 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.
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 <code>risingThreshold</code> and <code>alarmStartupAlarm</code> is equal to <code>risingAlarm(1)</code> or <code>risingOrFallingAlarm(3)</code> , then a single rising alarm is generated. If the first sample after this entry becomes valid is less than or equal to the <code>fallingThreshold</code> and <code>alarmStartupAlarm</code> is equal to <code>fallingAlarm(2)</code> or <code>risingOrFallingAlarm(3)</code> , 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 <code>alarmStartupAlarm</code> is equal to <code>risingAlarm(1)</code> or <code>risingOrFallingAlarm(3)</code> . After a rising event is generated, another such event is not generated until the sampled value falls below this threshold and reaches the <code>alarmFallingThreshold</code> .
RisingEventIndex	The index of the <code>eventEntry</code> that is used when a rising threshold is crossed. The <code>eventEntry</code> identified by a particular value of this index is the same as identified by the same value of the <code>eventIndex</code> object. If there is no corresponding entry in the <code>eventTable</code> , 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 <code>alarmStartupAlarm</code> is equal to <code>fallingAlarm(2)</code> or <code>risingOrFallingAlarm(3)</code> . After a falling event is generated, another such event is not generated until the sampled value rises above this threshold and reaches the <code>alarmRisingThreshold</code> .
FallingEventIndex	The index of the <code>eventEntry</code> that is used when a falling threshold is crossed. The <code>eventEntry</code> identified by a particular value of this index is the same as identified by the same value of the <code>eventIndex</code> object. If there is no corresponding entry in the <code>eventTable</code> , then no association exists. In particular, if this value is zero, no associated event is generated, because zero is not a valid event index.

Table 51 Alarms tab fields (continued)

Field	Description
Owner	The network management system which created this entry.
Status	The status of this alarm entry.

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:

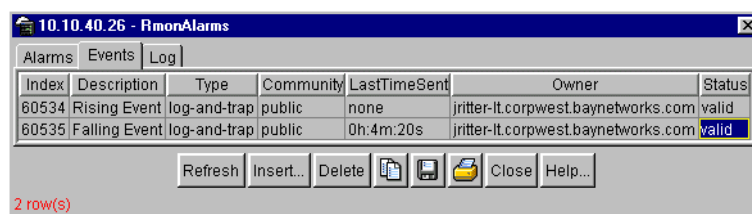
- RisingEvent
- FallingEvent

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 72 on page 137](#)).
- 2 Click the Events tab.
The Events tab opens ([Figure 73](#)).

Figure 73 RMONAlarms dialog box — Events tab

[Table 52](#) describes the RMONAlarms Events tab fields.

Table 52 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.
Status	Normally valid. A not-valid field indicates that an SNMP agent other than the Device Manager has tried to modify an RMON parameter or that network conditions have corrupted an SNMP packet sent by the Device Manager. The status would temporarily appear as “under creation” and then the status would become either “valid” or the field would be deleted.

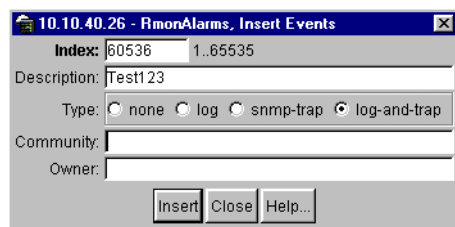
Creating an event

To create an event:

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

The RMONAlarms, Insert Events dialog box opens (Figure 74).

Figure 74 Insert Events dialog box



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

- 3 Select the type of event you want.


The default setting is log-and-trap. 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 75).

Figure 75 New event in the Events tab



Index	Description	Type	Community	LastTimeSent	Owner	Status
60534	Rising Event	log-and-trap	public	none	jritter-it.corpwest.baynetworks.com	valid
60535	Falling Event	log-and-trap	public	0h:22m:7s	jritter-it.corpwest.baynetworks.com	valid
60536	Test123	log-and-trap		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 72 on page 137](#)).

- 2 Click the Log tab.

The Log tab opens ([Figure 76](#)).

Figure 76 Log tab

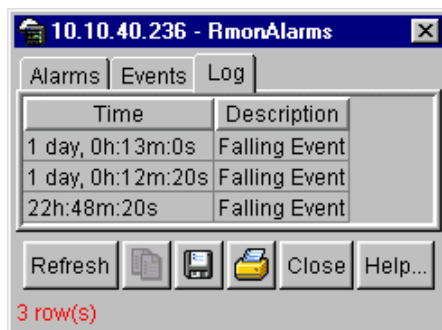


Table 53 describes the Log tab fields.

Table 53 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.

HP OpenView

You can integrate RMON into HP OpenView. To do so, you must set the HP OpenView path to include the UNIX environment variable. The path is set in the .cshrc file.

To see the path;

1 Enter:

```
setenv | grep PATH
```

A path is displayed similar to this:

```
PATH=/usr/local/
```

```
xemacs/bin/sparc-sun-solaris2.4:
```

```
bin:/sbin:/usr/sbin:/usr/ccs/bin:/usr/dt/bin:/usr/
openwin/bin:/
```

```
usr/etc:/usr/ucb:/usr/local/bin:/usr/local/share/lib:/
usr/
local/
```

```
share/bin:/opt/OV/bin:/home/jblogs/bin:.
```

- 2** Ensure that the HP OpenView directory is in path /opt/OV/bin.

MIB files are shipped with the Device Manager and are located in the following directory:

`dm/hpov/baystack_mibs`

- 3** Load each of the MIB files in the following order:

- bayAgent.mib
- bayChas.mib
- bayChasTraps.mib
- bayEMTmib
- baylfex.mib
- bayS5Reg.mib
- bayS5Rt.mib
- bayS5Tcs.mib
- baySRoot.mib
- rc_vlan.mib
- rfc1213.mib
- rfc1215.mib
- rfc1447.mib
- rfc1450.mib
- rfc1493.mib
- rfc1573_bs.mib
- rfc1573_rcc.mib
- rfc1643.mib
- rfc1757.mib
- rfc1757_rcc.mib
- rfc1907.mib

Now you can start HP OpenView.

Log only event bug

HP OpenView versions 4.0 and 5.0 contain bugs that do not affect the integrity of the product when it stands alone. However, when combined with Device Manager, unexpected results occur.

The “Log only” event categorization bug in HP OpenView 4.0 causes traps to be written to the ASCII trap log file and to be displayed in the event browser.

The default category for SNMP traps, such as “link up” and “link down,” happens to be “Log only.” The correct procedure for an event (trap) with a “Log only” categorization is that it should only be written to the ASCII trap log file.

In version 4.0, standard SNMP traps are displayed in the event browser when the default category of “Log only” is selected. However, SNMP traps are not displayed in the event browser version 5.0, because this bug is fixed. If you were not aware that version 4.0 had a problem, then you may have erroneously assumed that the switch was not sending these traps. In this case, you can view the ASCII trap log file. Enter:

```
/var/opt/OV/share/log/trapd.log
```

When you view the log, you can verify that the switch is sending the traps. In fact, when both HP OpenView and Device Manager are running on a machine, and that machine is configured on the switch as a trap receiver, HP OpenView receives the trap. HP OpenView then passes the trap to Device Manager. If Device Manager displays a trap, HP OpenView has also received the trap.

To have standard SNMP traps displayed in the event browser for HP OpenView 5.0:

- 1** From the Options menu, choose Event Configuration.
- 2** Select enterprise name snmpTraps.
- 3** Double-click the event (trap) name you want.
- 4** Change the category from Log Only to any event type.

Your choices are Error Events, Threshold Events (normally used for RMON alarms), Status Events, Configuration Events, or Application Alert Events.

- 5** Click OK.
- 6** Choose File > Save.

Chapter 8

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)
- AuthConfig tab ([page 151](#))
- SecurityList tab ([page 155](#))
- AuthStatus tab ([page 155](#))
- AuthViolation ([page 157](#))

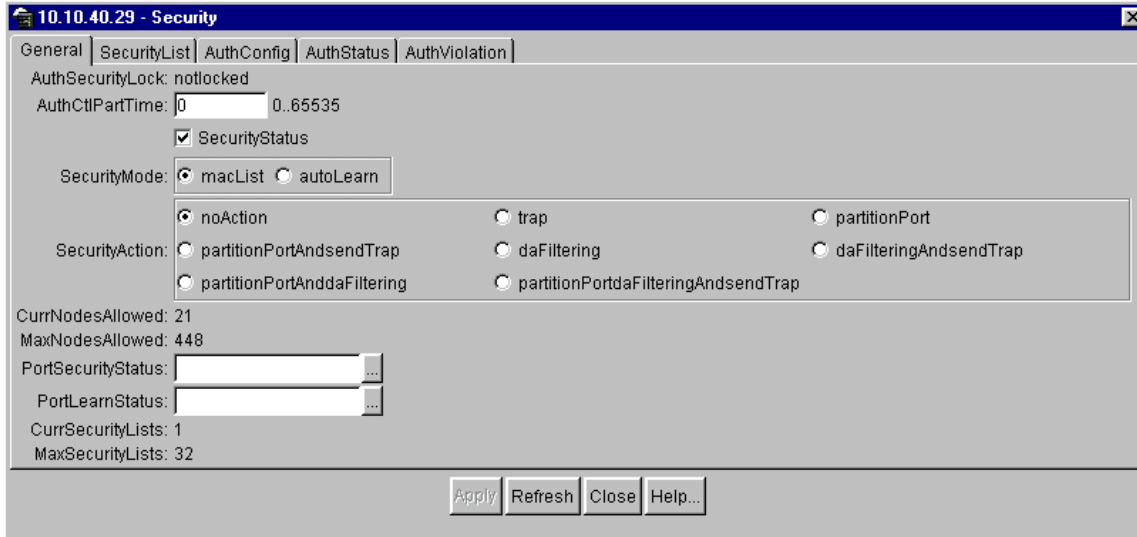
General tab

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 77](#)).

Figure 77 General tab


10.10.40.29 - Security

General | SecurityList | AuthConfig | AuthStatus | AuthViolation

AuthSecurityLock: notlocked

AuthCtlPartTime: 0 0..65535

☒ SecurityStatus

SecurityMode: ☒ macList ☐ autoLearn

SecurityAction: ☒ noAction ☐ trap ☐ partitionPort

☐ partitionPortAndsendTrap ☐ daFiltering ☐ daFilteringAndsendTrap

☐ partitionPortAnddaFiltering ☐ partitionPortdaFilteringAndsendTrap

CurrNodesAllowed: 21

MaxNodesAllowed: 448

PortSecurityStatus: ...

PortLearnStatus: ...

CurrSecurityLists: 1

MaxSecurityLists: 32

Apply Refresh Close Help...

Table 54 describes the General tab items.

Table 54 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.
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.

Table 54 General tab items (continued)

Items	Description
SecurityAction	<p>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.</p> <p>A blocked address causes the port to be partitioned when unauthorized access is attempted. Selections include:</p> <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 receive station. • 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 desitnation address field is the MAC address of unauthorized station. Traps are sent to trap receive station(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 receive station(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.
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 77).

- 2 Click the SecurityList tab.

The SecurityList tab opens (Figure 78).

Figure 78 SecurityList tab

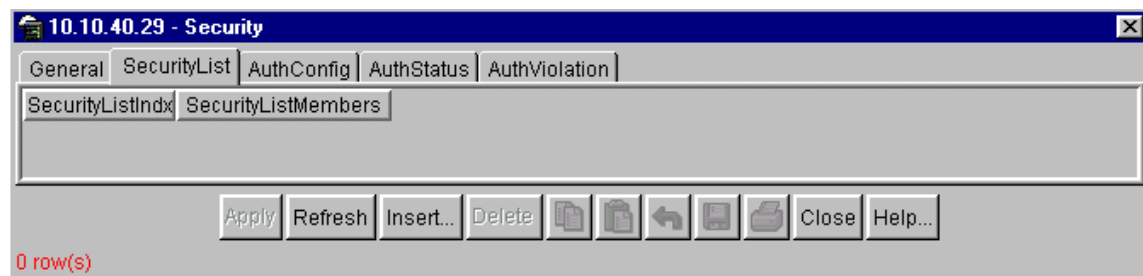


Table 55 describes the SecurityList tab fields.

Table 55 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.

- 2 Click the SecurityList tab.

The SecurityList tab opens (Figure 78).

- 3 Click inside a row.

- 4 Click Insert.

The Security, Insert SecurityList dialog box opens (Figure 79).

Figure 79 Security, Insert SecurityList dialog box

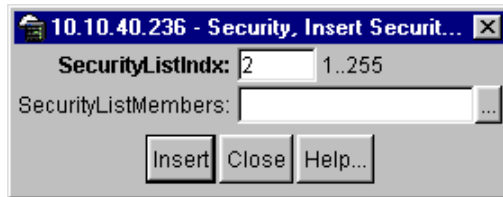


Table 56 describes the Security, Insert AuthConfig dialog box items.

Table 56 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 77).

- 2 Click the AuthConfig tab.

The AuthConfig tab opens (Figure 80).

Figure 80 AuthConfig tab

BrdIndx	PortIndx	MACIndx	AccessCtrlType	SecureList
1	1	00:00:00:00:00:11	allowed	0
2	5	00:00:5e:00:01:03	allowed	0
2	5	00:00:81:bc:ea:81	allowed	0
2	5	00:00:81:c1:9b:81	allowed	0
2	5	00:00:81:c1:f6:81	allowed	0
2	5	00:08:c7:02:c4:c0	allowed	0
2	5	00:60:5c:83:2f:08	allowed	0
2	5	00:60:fd:9e:2b:6a	allowed	0
2	5	00:80:2d:22:0e:00	allowed	0
2	5	00:80:2d:22:86:00	allowed	0
2	5	00:80:2d:39:f2:00	allowed	0
2	5	00:80:5f:e7:e4:39	allowed	0
2	5	00:e0:16:00:00:00	allowed	0
2	5	00:e0:16:83:26:81	allowed	0
2	5	08:00:20:22:1b:ea	allowed	0
2	5	08:00:20:73:94:2e	allowed	0
2	5	08:00:20:73:a3:f9	allowed	0
2	5	08:00:20:78:33:37	allowed	0
2	5	08:00:20:81:bf:bc	allowed	0
2	5	08:00:20:8f:6a:bb	allowed	0

20 row(s)

Table 57 describes the AuthConfig tab fields.

Table 57 AuthConfig tab fields

Field	Description
BrdIdx	Index of the slot containing the board on where the port is located. This value is meaningful only if SecureList value is zero. For other SecureList values, this parameter should have the value of zero.
PortIdx	Index of the port on the board. This value is meaningful only if SecureList value is zero. For other SecureList values, this parameter should have the value of zero.
MACIdx	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 BrdIdx and PortIdx 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.

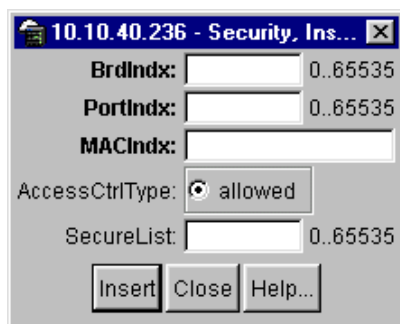
- 2 Click the AuthConfig tab.

The AuthConfig tab opens (Figure 80).

- 3 Click inside a row.

- 4 Click Insert.

The Security, Insert AuthConfig dialog box opens (Figure 81).

Figure 81 Security, Insert AuthConfig dialog box

[Table 58](#) describes the Security, Insert AuthConfig dialog box fields.

Table 58 Security, Insert AuthConfig dialog box fields

Item	Description
BrdIdx	Index of the board. This corresponds to the index of the slot containing the board, but only if the index is greater than zero. A zero index is a wild card.
PortIdx	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.
MACIdx	An index of MAC addresses that are either designated as <code>allowed</code> (station) or <code>not-allowed</code> (station).
AccessCtrlType	Displays whether the node entry is <code>node allowed</code> or <code>node blocked</code> . A MAC address may be allowed on multiple ports.
SecureList	The index of the security list. This value is meaningful only if BrdIdx and PortIdx 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 77](#)).

- 2 Click the AuthStatus tab.

The AuthStatus tab opens ([Figure 82](#)).

Figure 82 AuthStatus tab

AuthStatusBrdIndx	AuthStatusPortIndx	AuthStatusMACIndx	CurrentAccessCtrlType	CurrentActionMode	CurrentPortSecurStat
1	1	00:00:00:00:00:00	allow	noAction	notApplicable
1	2	00:00:00:00:00:00	allow	noAction	notApplicable
1	3	00:00:00:00:00:00	allow	noAction	notApplicable
1	4	00:00:00:00:00:00	allow	noAction	notApplicable
1	5	00:00:00:00:00:00	allow	noAction	notApplicable
1	6	00:00:00:00:00:00	allow	noAction	notApplicable
1	7	00:00:00:00:00:00	allow	noAction	notApplicable
1	8	00:00:00:00:00:00	allow	noAction	notApplicable
1	9	00:00:00:00:00:00	allow	noAction	notApplicable
1	10	00:00:00:00:00:00	allow	noAction	notApplicable
1	11	00:00:00:00:00:00	allow	noAction	notApplicable
1	12	00:00:00:00:00:00	allow	noAction	notApplicable
1	13	00:00:00:00:00:00	allow	noAction	notApplicable
1	14	00:00:00:00:00:00	allow	noAction	notApplicable
1	15	00:00:00:00:00:00	allow	noAction	notApplicable
1	16	00:00:00:00:00:00	allow	noAction	notApplicable

Table 59 describes the AuthStatus tab fields.

Table 59 AuthStatus tab fields

Item	Description
AuthStatusBrdIndx	The index of the board. This corresponds to the index of the slot containing the board if the index is greater than zero.
AuthStatusPortIndx	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.
AuthStatusMACIndx	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 59 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 receive station.</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 receive station.</p> <p>sendTrap: A trap is sent to trap receive station(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 receive station(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 77).

- 2 Click the AuthViolation tab.

The AuthViolation tab opens (Figure 83).

Figure 83 AuthViolation tab

BrdIdx	PortIdx	MACAddress
1	16	00:00:00:00
1	17	00:00:00:00
1	18	00:00:00:00
1	19	00:00:00:00
1	20	00:00:00:00
1	21	00:00:00:00
1	22	00:00:00:00
1	23	00:00:00:00
1	24	00:00:00:00
2	1	00:00:00:00
2	2	00:00:00:00
2	3	00:00:00:00
2	4	00:00:00:00
2	5	00:00:00:00
2	6	00:00:00:00
2	7	00:00:00:00
2	8	00:00:00:00
2	9	00:00:00:00
2	10	00:00:00:00

[Table 60](#) describes fields for the AuthViolation tab fields.

Table 60 AuthViolation tab fields

Field	Description
BrdIdx	The index of the board. This corresponds to the slot 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).

Index

Symbols

<=64 field 98
>1023 field 98
>127 field 98
>255 field 98
>511 field 98
>64 field 98

A

AbsoluteValue statistics 38
access levels 24
Action field 65
Actions menu 28
ActiveMember field 109
ActiveMembers field 117
ActiveQuerier field 116
Addr field 49
AddrMaskReps field 73, 75
AddrMasks field 73, 75
Admin field 55
AdminDuplex field 80, 86
AdminSpeed field 80, 86
AdminState field 56
AdminStatus field 79, 85
Agent Info tab 58
Alarm Manager button 29
alarms tab 137

alarms, RMON
 characteristics of 131
 creating 133
AlignmentErrors field 92, 105
Area Chart button 44
area graph example 39
ARP tab 50
AuthConfig tab
 AccessCtrlType field 153
 BrdIndx field 153
 MACIndx field 153
 PortIndx field 153
 SecureList field 153
AuthenticationTraps field 53
AuthStatus tab
 AuthStatusBrdIndx field 156
 AuthStatusMACIndx field 156
 AuthStatusPortIndx field 156
 CurrentAccessCtrlType field 156
 CurrentActionMode field 157
 CurrentPortSecurStatus field 157
AuthViolation tab
 BrdIndx field 158
 MACIndx field 158
 PortIndx field 158
AutoNegotiate field 80, 86
Average statistics 38

B

Bar Chart button 44
BcastAddr field 49
blinking LEDs 33

BootMode field 53
BootRouterAddr tab 58
Bridge tab 94
BroadcastPkts field 97
buckets 124
BucketsGranted field 127
BucketsRequested field 127
buttons
 dialog boxes 36
 toolbar 28

C

CarrierSenseErrors field 93, 105
chassis
 configuration, editing 50
 graphing 65
Chassis ICMP In statistics window 72
Chassis ICMP Out statistics tab 74
Chassis SNMP tab 67
Collisions field 97
Color field 109
color-coded ports 32, 33
communication parameters, setting for Device Manager 22
Community field 60, 140
community strings
 default 24
 entering 25
ConfigFileName field 64
configuration
 downloading 64
 MAC-SA-based VLAN 112
 Multi-Link Trunks 100
 port-based VLAN 108, 109, 115
 ports 119
 protocol-based VLAN 110
Confirm row deletion field 24
Control tab 126

conventions
 text 17
Copy button 36
Copy File tab 64
CRAAlignErrors field 97
Cumulative statistics 38
CurrentDefaultGateway field 53
CurrentImageVersion field 53
CurrentMgmtProtocol field 53
customer support 19

D

data, exporting 42
default access community strings 24
Default TTL field 48
DefaultVLANId field 81, 88
DeferredTransmissions field 93, 106
Descr field 55, 56, 62, 63, 79, 85
Description field 140
DestUnreachs field 73, 75
Device Manager
 setting properties 22
Device Manager window 21, 22
Device menu 27
Device Name field 25
device view
 summary 30
device, opening 25
Disable command 35
disabled port, color 33
DiscardTagged Frames field 81, 87
DiscardUntaggedFrames field 81, 88

E

EchoReps field 73, 75
Echos field 73, 75

Edit command 35
Edit menu 27
Edit Selected button 28
Enable 116
Enable command 35
Enable field 23
Ether Stats Control tab 129
Ethernet Errors tab 92
Ethernet statistics, disabling 130
Event Index field 136
events, RMON 139
ExcessiveCollisions field 94, 106
Export Data button 37, 42

F

falling event 139
falling value, RMON alarms 131
FallingEventIndex field 138
FallingThreshold field 138
Fan tab 63
FCSErrors field 92, 105
File System window 64
ForwDatagrams field 71
FragCreates field 71
FragFails field 71
FragOKs field 71
frames, discarding tagged frames on 114
FrameTooLongs field 93, 106

G

Globals tab 48
graph
 creating 43
 modifying 44
Graph command 35
graph dialog box 44

Graph menu 27
Graph Selected button 28, 43
graph types 39
graphPort, Interface tab 89

H

Help button 28
Help menu 28
Help, Device Manager 46
Horizontal button 44
HP OpenView, using with RMON 143

I

ICMP In tab 73
ICMP Out statistics 74
ICMP Out tab 74
ID field (VLAN) 112
ifInNUcastPkts field 90
ifInOctets field 90
ifInUcastPkts field 90
ifOutNUcastPkts field 90
ifOutOctets field 90
ifOutUcastPkts field 90
image file 64
ImageFileName field 64
ImageLoadMode field 53
InAddrErrors field 70
InASNParseErrs field 68
InBadCommunityNames field 68
InBadCommunityUses field 68
InBadValues field 68
InBadVersions field 68
InBroadcastPkt field 102
InDelivers field 71
Index field 79, 85, 136

InDiscards field 71, 90
InErrors field 90
InGenErrs field 69
InGetNexts field 68
InGetRequests field 68
InGetResponses field 68
InHdrErrors field 70
InMulticastPkts field 102
InNoSuchNames field 68
Inpkts field 67
InReadOnlys field 69
InReceives field 70
Insert Alarm dialog box 134
Insert AuthConfig dialog box
 BrdIndx field 154
Insert button 36
Insert Control dialog box 127
Insert Ether Stats dialog box 129
Insert Event dialog box 141
InSetRequests field 68
Interface item
 ARP 50
Interface tab 78
Interface tab for a multiple port 84
Interface window 102
InternalMacReceiveErrors field 93, 105
InternalMacTransmitErrors field 92, 105
Interval field 128, 137
InTooBigs field 68
InTotalReqVars field 67
InTotalSetVars field 67
InUnknownProtos field 71, 91
IP Address tab 49
IP dialog box 47
IP tab 70
IPAddress field 50

J

Jabbers field 97

L

LastChange field 80, 86
LastLoadProtocol field 53
LastTimeSent field 140
LastUnauthenticatedCommunityString field 59
LastUnauthenticatedIpAddress field 59
LastValue statistics 38
LateCollisions field 94, 106
LEDs 33
LEDs in device view 33
legend, port color 28, 33
Line Chart button 44
link, lacking, color 33
LoadServerAddr field 64
LocalStorageImageVersion field 53
Location field 55, 56
Log Scale button 44
Log tab 142
logs 142
LstChng field 55, 56

M

MacAddr field 58
MacAddress field 50
MAC-SA-based VLAN 112
Max Traps in Log field 24
Maximum statistics 38
MDA
 shortcut menu 36
 viewing 31
media dependent adapter. *See* MDA
menu bar, Device Manager 27

menus. *See* individual menu names

Minimum statistics 38

MLT

 requirements 99

MltId field 80, 86

MRouterExpiration field 116

MRouterPorts field 116

Mtu field 79, 85

MulticastPkts field 97

Multi-Link Trunk window 101

Multi-Link Trunking. *See* MLT

Multi-Link Trunks window 100

multiple objects, selecting 31

MultipleCollisionFrames field 94, 106

N

Name field 100, 109, 116

NetMask field 49

new table entry, creating 36

NextBootDefaultGateway field 53

NextBootLoadProtocol field 53

NextBootMgmtProtocol field 53

NextBootNetMask field 58

NextBootpAddr field 58

NmmCurNum field 120

NmmLstChg field 120

NmmMaxNum field 120

NoSuchObject error message 77

O

object types 30

objects

 editing 37

 selecting 30

Octets field 97

online Help 28, 46

Open Device button 25, 28

Open Device dialog box 25, 27

operating port, color 33

OperSpeed field 80, 86

OperState field 55, 57, 62, 63

OperStatus field 79, 86

OutBadValues field 68

OutBroadcast field 102

OutDiscards field 71, 90

OutErrors field 91

OutGenErrs field 68

OutMulticast field 102

OutNoRoutes field 71

OutNoSuchNames field 68

Outpkts field 67

OutRequests field 71

OutTooBigs field 68

OutTraps field 68

OversizePkts field 97

Owner field 128, 130, 139, 140

P

ParmProbs field 73, 75

Paste button 36

PhysAddress field 79, 85

Pkts field 97

Poll 94

polling interval 42

port color legend 33

Port dialog box 88

port Ethernet Error Statistics tab 91

Port field 81, 130

Port Interface tab 78, 85

port shortcut menu 35

Port Spanning Tree window 82

- port-based VLANs 108
- PortMembers field 100, 109, 117
- ports
 - color-coded 32, 33
 - configuring 77, 119
 - controlling 77
 - disabled 33
 - editing 77
 - graphing 78, 84, 88, 89
 - selecting 31
 - viewing 77
- PortType field 100
- Power Supply tab 62
- Print button 36
- product support 19
- Properties dialog box 22, 23
 - Hotswap Poll Interval field 23
 - If Traps, Status Interval) field 23
 - Status Poll Interval field 23
- protocol-based VLAN 110
- Protocol-based VLAN window 111
- ProtocolId field 109, 117
- publications
 - hard copy 18
- publications, related 18

Q

- QuerierPort field 116
- QueryInterval field 116

R

- Read Community field 25
- Read Community, SNMP 26
- Read Community, SNMP field 25
- Read-Write-All access 26
- ReasmFails field 72
- ReasmMaxSize field 49

- ReasmOKs field 72
- ReasmReqds field 71
- ReasmTimeout field 48
- Reboot field 53
- Rebustness field 116
- Redirects field 73, 75
- Refresh Device Status button 28
- Register for Traps field 24
- related publications 18
- Remote Monitoring. *See* RMON
- Reset Changes button 36
- Result field 65
- Retry Count field 24
- rising event 139
- rising value, RMON alarms 131
- RisingEventIndex field 138
- RisingThreshold field 138

RMON

- alarms
 - characteristics 131
 - creating 133
 - deleting 137
 - inserting 135
- events
 - definition 139
- history
 - creating 126
 - definition 124
 - disabling 128
- statistics 123, 126
 - using HP OpenView with 143

- RMON EtherStat tab 96, 124

- RMON Event tab 140

- Rmon menu 28

S

- Sample Interval field 136
- Sample Type field 136, 138

- Security parameters
 - General tab
 - AuthCtlPartTime field 148
 - AuthSecurityLock field 148
 - CurrNodesAllowed field 149
 - CurrSecurityLists field 149
 - MaxNodesAllowed field 149
 - MaxSecurityLists field 149
 - PortLearnStatus field 149
 - SecurityAction field 149
 - SecurityMode field 148
 - SecurityStatus field 148
 - Security, Insert AuthConfig dialog box
 - AccessCtrlType field 154
 - MACIndx field 154
 - PortIndx field 154
 - SecureList field 154
 - SerNum field 55, 57
 - shortcut menus
 - MDA 36
 - port 35
 - switch unit 34
 - single object, selecting 30
 - SingleCollisionFrames field 93, 106
 - SNMP Info tab 59
 - SNMP tab 58
 - SNMP traps 45
 - Snoop tab 115
 - spanning tree group ID field 113
 - Spanning Tree window 82
 - Speed field 86
 - SQETestErrors field 93, 106
 - SrcQuenchs field 73, 75
 - Stack Info tab 56
 - Stacked button 44
 - Standalone Unit Info Tab 54
 - standby port, color 33
 - StartupAlarm field 138
 - statistics
 - Ethernet statistics, enabling 129
 - for a single object 41
 - for multiple objects 42
 - graphing 38
 - ICMP Out 74
 - MLT 101
 - RMON 123, 126
 - single port 41
 - types 38
 - statistics dialog box
 - multiple objects 42
 - statistics dialog boxes 27
 - Status field 120, 139, 140
 - STG 82
 - StgId field 109, 117
 - Stop button 37
 - SubnetAddr field 109
 - SubnetMask field 109
 - support, Nortel Networks 19
 - switch stack, selecting 31
 - switch unit shortcut menu 34
 - switch, selecting 30
 - sysContact field 52
 - sysDescr field 52
 - sysLocation field 52
 - sysName field 52
 - System tab 52
 - sysUpTime field 52
- ## T
- tagged frame, discarding 114
 - tagged ports
 - configuring 114
 - technical publications 18
 - technical support 19
 - Telnet button 29, 45

- Telnet session 28, 29, 45
- tested port, color 33
- text conventions 17
- Threshold Type field 136
- TimeExcds field 73, 75
- Timeout field 24
- TimestampReps field 73, 75
- Timestamps field 73, 75
- toolbar, Device Manager 28
- topology 119
- Trace field 24
- Transparent Bridging tab 95
- trap log 45
- Trap Log button 28
- Trap Port field 24
- Trap Receivers
 - NetAddr field 60
 - Status field 60
- Trap Receivers tab 59
- troubleshooting
 - locations of Help files 46
 - receiving traps 45
 - selecting switches in device view 31
- TrpRcvrCurEnt field 59
- TrpRcvrMaxEnt field 59
- TrpRcvrNext field 59
- Type 109
- Type field 50, 55, 79, 81, 85, 87, 140
- types of objects 30

U

- UndersizePkts field 97
- UNIX
 - receiving traps 45
- unmanageable port, color 33
- UserDefined field 117

- UserDefinedPid field 109

V

- ValidFlag tab 58
- Value field 136, 138
- value, changed 37
- Variable field 136, 137
- Ver field 55, 57
- Viewing 77
- VLAN 80
- VLAN Basic tab 108
- VLAN dialog box 109, 116
- VLAN menu 27
- VLAN tab 81
- VLAN tab for multiple ports 86
- VlanIds field 81, 87
- VLANs
 - creating 108
 - default 108
 - limitations 107
 - MAC-SA-based 112
 - managing 116
 - port-based 108
 - protocol-based 110

W

- window, Device Manager 27
- Write Community field 25
- Write Community, SNMP 25, 26