Part No. 313195-A
October 2001

4401 Great America Parkway
Santa Clara, CA 95054

# Managing the Passport 8000 Series Switch Using Device Manager Release 5.x.x

NORTEL NETWORKS™

## Copyright © 2001 Nortel Networks



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 Inc.

## Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, OPTera, and BayStack are trademarks of Nortel Networks.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.

Netscape and Navigator are trademarks of Netscape Communications Corporation.

IPX is a trademark of Novell Inc.

UNIX is a trademark of X/Open Company Limited.

## Statement of conditions

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

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

## Nortel Networks 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 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 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 Inc., 2375 N. Glenville Dr., Richardson, TX 75082.

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

# Figures

# Tables

# Preface

Welcome to Device Manager, the Nortel Networks* management software for the Passport 8000 Series* switches. Device Manager is a set of graphical network management applications used to configure and manage an Passport chassis.

This guide provides information about using the features and capabilities of the Device Manager graphical user interface (GUI) to perform general network management operations on an Passport switch.

For information about using Device Manager to configure layer 2 (switching) and layer 3 (routing) functions, refer to *Configuring Switching and Routing Operations for the Passport 8000 Series Switch Using Device Manager Release 5.x.x*

An Passport switch has one of two types of modules installed in it: Passport 8100 modules or Passport 8600 modules. The Passport 8100 modules offer high-performance, low-cost, high-density switching. The Passport 8600 modules provide very high-speed packet forwarding combined with the ability to route Internet Protocol (IP) and Internetwork Packet Exchange (IPX*) Protocol traffic.

## Before you begin

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

- Basic knowledge of networks, Ethernet bridging, and IP routing
- Familiarity with networking concepts and terminology
- Basic knowledge of network topologies
- Experience with windowing systems or GUIs

# Text conventions

This guide uses the following text conventions:

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

| | |
|---|---|
| *italic text* | Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore.<br>Example: If the command syntax is `show at <valid_route>`, `valid_route` is one variable and you substitute one value for it. |
| `plain Courier text` | Indicates command syntax and system output, for example, prompts and system messages.<br>Example: `Set Trap Monitor Filters` |
| separator ( > ) | Shows menu paths.<br>Example: Protocols > IP identifies the IP command on the Protocols menu. |
| vertical line ( \| ) | Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command.<br>Example: If the command syntax is `show ip {alerts\|routes}`, you enter either `show ip alerts` or `show ip routes`, but not both. |

# Related publications

For more information about using a Passport 8000 Series switch, the resident CLI, or Device Manager, refer to the hardware and software publications listed here.

## Chassis and component documentation

For more information about the Passport 8000 Series hardware, refer to the following publications:

- *Installing and Maintaining the Passport 8010co Chassis and Components* (part number 312746-B)

  Provides instructions for installing the Passport 8010co Chassis in an equipment rack and for installing and replacing fan trays, power supplies, modules, gigabit interface converters, and media dependent adapters. This guide describes some of the routine tasks of operating the Passport 8010co Chassis and includes technical specifications for the chassis and the modules.

- *Installing the Breaker Interface Panel for the Passport 8010co Chassis* (part number 312755-B)

  Describes how to install the breaker interface panel in an equipment rack, connect cables, and interpret LEDs. It includes technical specifications for the breaker interface panel.

- *Installing and Maintaining the Passport 8010 Chassis and Components* (part number 312747-B)

  Provides instructions for installing the Passport 8010 Chassis in an equipment rack and for installing and replacing fan trays, power supplies, modules, gigabit interface converters, and media dependent adapters. This guide describes some of the routine tasks of operating the Passport 8010 Chassis and includes technical specifications for the chassis and the modules.

- *Installing and Maintaining the Passport 8006 Chassis and Components* (part number 312748-B)

  Provides instructions for installing the Passport 8006 Chassis in an equipment rack and for installing and replacing fan trays, power supplies, modules, gigabit interface converters, and media dependent adapters. This guide describes some of the routine tasks of operating the Passport 8006 Chassis and includes technical specifications for the chassis and the modules.

- *Installing and Maintaining the Passport 8003 Chassis and Components* (part number 313074-B)

  Provides instructions for installing the Passport 8003 Chassis in an equipment rack and for installing and replacing fan trays, power supplies, modules, gigabit interface converters, and media dependent adapters. This guide describes some of the routine tasks of operating the Passport 8003 Chassis and includes technical specifications for the chassis and the modules.

- *Installing Passport 8600 Switch Modules* (part number 312749-B)

  Provides instructions for installing the Passport 8600 modules in a chassis.

- *Installing Passport 8100 Switch Modules* (part number 312750-A)

  Provides instructions for installing the Passport 8100 modules in a chassis.

- *Installing Media Dependent Adapters for the Passport 8672ATME Module* (part number 313071-A)

  Provides instructions for installing media dependent adapters in the Passport 8672ATME module.

- *Installing Media Dependent Adapters for the Passport 8683POSE Module* (part number 313072-A)

  Provides instructions for installing media dependent adapters in the Passport 8683POSE module.

- *Installing Media Dependent Adapters (MDAs)* (part number 313073-A)

  Provides instructions for installing media dependent adapters in Passport 8000 Series modules, BayStack* equipment, and BPS 2000 equipment.

- *Installing an AC Power Supply in a Passport 8000 Series Switch* (part number 312751-A)

  Provides instructions for installing an AC power supply in a Passport 8000 Series switch.

- *Installing a DC Power Supply in a Passport 8000 Series Switch* (part number 313070-A)

  Provides instructions for installing a DC power supply in a Passport 8000 Series switch.

- *Installing a Fan Tray in a Passport 8000 Series Switch* (part number 312752-A)

  Provides instructions for installing a fan tray in a Passport 8000 Series switch.

- *Installing Gigabit Interface Converters (GBICs)* (part number 312865-A)

  Provides instructions for installing GBICs in selected Passport 8000 Series modules.

## Software documentation

For more information about the Passport 8000 Series software, refer to the following publications:

- *Networking Concepts for the Passport 8000 Series Switch* (part number 313196-A)

  Provides general information and a description of how a Passport 8000 Series switch handles various networking features, such as VLANs, MultiLink Trunking, OSPF, RIP, and IPX.

- *Getting Started with the Passport 8000 Series Switch Management Software* (part number 313189-A)

  Provides instructions for installing management software and describes initial setup procedures.

- *Managing the Passport 8000 Series Switch Using the Command Line Interface Release 3.2* (part number 313194-A)

  Describes the command line interface (CLI) structure and the commands used to perform basic switch management operations, such as modifying the switch boot sequence, working with switch files, and setting up security features.

- *Configuring Switching and Routing Operations for the Passport 8000 Series Switch Using the Command Line Interface Release 3.2* (part number 313191-A)

  Describes the CLI commands and parameters for configuring layer 2 (switching) and layer 3 (routing) operations.

- *Configuring Switching and Routing Operations for the Passport 8000 Series Switch Using Device Manager Release 5.x.x* (part number 313193-A)

Describes how to use Device Manager to configure and manage layer 2 (switching) and layer 3 (routing) functions, including procedures and illustrations of pertinent screens.

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

You can purchase selected documentation sets, CDs, and technical publications through 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 |
|---|---|
| Europe, Middle East, and Africa | (33) (4) 92-966-968 |
| North America | (800) 4NORTEL or (800) 466-7835 |
| Asia Pacific | (61) (2) 9927-8800 |
| China | (800) 810-5000 |

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

# Chapter 1
# Device Manager basics

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

- Instructions on how 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 (page 34)

## Starting Device Manager

To start Device Manager:

➔ Do one of the following:

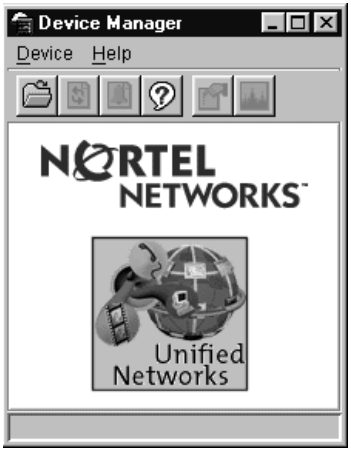
- In the Windows* environment, from the Windows Start menu, choose Programs > Nortel Networks Device Manager > Device Manager.
- In a UNIX* environment, verify that the Device Manager installation directory is in your search path; then type:

  ```
  JDM
  ```

An abbreviated Device Manager window opens, as shown in 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** Abbreviated Device Manager window




## Setting the Device Manager properties

Device Manager uses the Simple Network Management Protocol (SNMP) to configure and manage Passport 8000 Series switches. You can use the Device Manager Properties dialog box to configure important communication parameters such as the polling interval, timeout, and retry count. You can set these parameters at any time before or after you open a device.

To set the Device Manager properties:

1. From the abbreviated Device Manager window menu bar, choose Device > Properties.

   The Device Manager Properties dialog box (Figure 2) opens.

2. Select properties you want to change and set their values.

3. Click OK.

**Figure 2** Properties dialog box

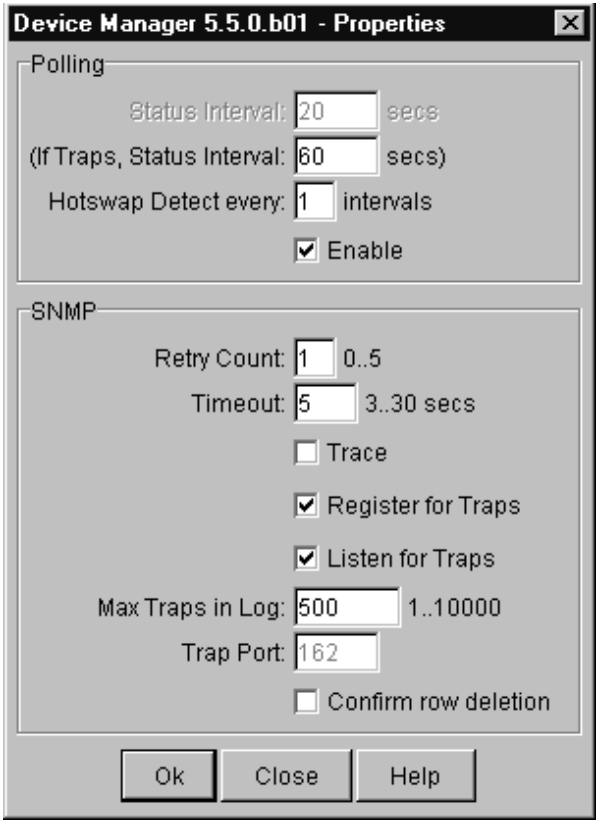



Table 1 describes the Properties dialog box fields.

**Table 1** Properties dialog box fields

| Field | Description |
|---|---|
| Status Interval | Interval at which statistics and status information are gathered (default is 20 seconds). |
| (IfTraps, Status Interval) | If the Register for Traps box is checked, interval, in seconds, at which statistics and status information are gathered. |
| Hotswap Detect every | Enter a number for the number of intervals at which Device Manager will check for module hot swaps. |

**Table 1** Properties dialog box fields (continued)

| Field | Description |
|---|---|
| Enable | If checked, Device Manager will poll the switch according to the settings listed above the Enable box. |
| Retry Count | If Device Manager cannot transmit polling information at startup, the number of times Device Manager retransmits polling information. |
| Timeout | Length of each retry of each polling waiting period. When accessing the device through a slow link, you may want to increase the timeout interval and then change the Retransmission Strategy to superlinear. |
| Trace | If checked, you have the ability to perform trace routes. |
| Register for Traps | If checked, Device Manager will register a trap. |
| Listen for Traps | If checked, Device Manager will listen for a trap. |
| Max Traps in Log | The specified number of traps that may exist in the trap log. The default is 500. |
| Trap Port | The number of the port that trap messages will be captured on. The default is 162. |
| Confirm row deletion | If checked, Device Manager will send a message when a system table row was deleted. |

# Opening a device

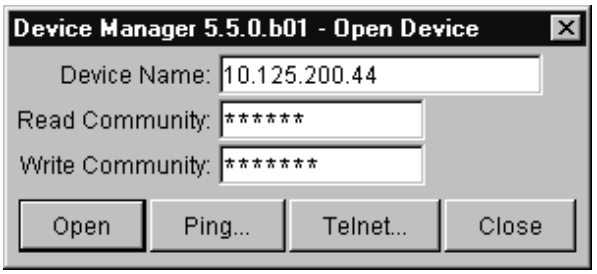
"Opening" a device displays the device view, a picture of the device. Before you can display the device view, you must enter community strings that determine the access level granted to the device.

To open a device:

1 From the abbreviated Device Manager window menu bar, choose Device > Open. Or from the Device Manager toolbar, click the open device button.

The Open Device dialog box opens (Figure 3).

**Figure 3** Open Device dialog box




2 Identify the device by typing the DNS name or IP address of the device in the Device Name field.

3 Type the proper community strings in the Read Community and Write Community fields.

4 Click Ping to check if the switch is reachable, or Telnet to initiate a Telnet session.

5 Click Open.

**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.

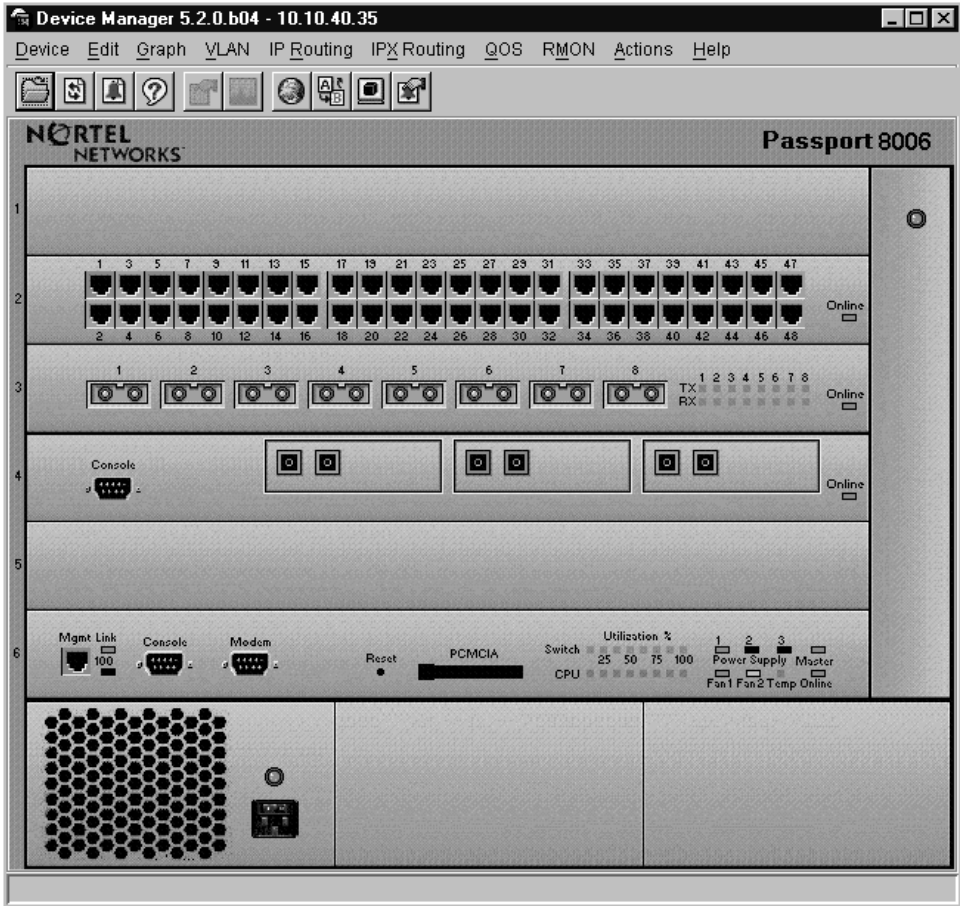
Table 2 shows the default access community strings for the Passport Device Manager software.

**Table 2** SNMP community string default values

| Access Level | Description |
|---|---|
| read-only | Public |
| Layer 1 read/write | Private |
| Layer 2 read/write | Private |
| Layer 3 read/write | Private |
| read/write | Private |
| read/write/all | Secret |

Device Manager automatically determines what version of software the selected device is running. The Device Manager window opens, showing a picture of the device (Figure 4) that represents the physical features of the device.

**Figure 4** Device Manager window showing a Passport 8000 Series switch



# Troubleshooting the opening of a device

If a device does not open, Device Manager displays a timeout message.

To troubleshoot opening a device:

- In slower networks, increase the retransmission retries and timeout interval.
- In the Open Device dialog box, make sure you entered the correct read and write community information.
- If you cannot reach the switch through an IP address or the management station cannot communicate with the switch, check the following possibilities:

  - Is the switch connected to the network?

  - Is the switch turned on?

  - Does the switch have an incorrect IP address?

  - Is the incorrect IP address specified in the Open Device field in Device Manager?

  - Is the network misconfigured?

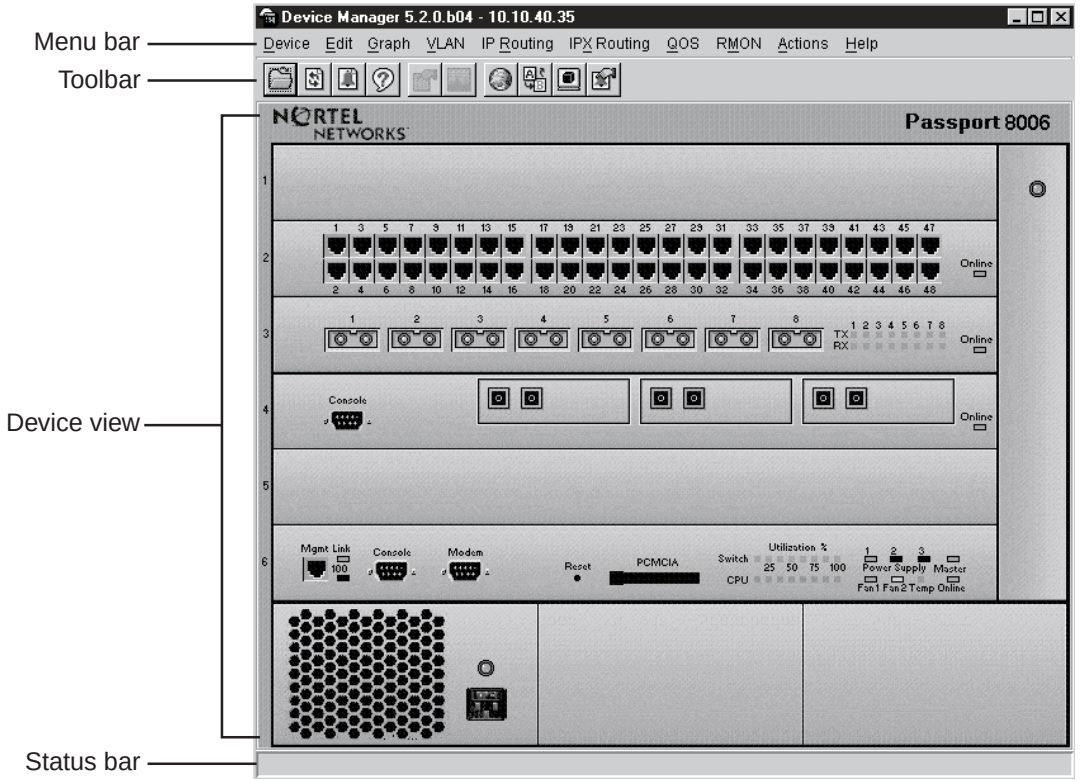
# Understanding the Device Manager window

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

- Menu bar
- Toolbar
- Device view
- Status bar

Figure 5 displays the parts of the Device Manager Window.

**Figure 5** Parts of the Device Manager window



## Menu bar

The menu bar on the Device Manager window (Figure 6) provides menus with commands that let you monitor a device.

**Figure 6** Menu bar


Table 3 describes the menu bar fields.

**Table 3** Device Manager menu bar description

| Menu | Description |
|---|---|
| Device | The Device menu lets you open a device, refresh the device view, and set polling and SNMP properties.This menu also allows you to open and view the Trap Log and Log. |
| Edit | The Edit menu lets you view parameters for the chassis or for selected objects. The object can be a card, fan, MDA, port, power supply or any other object. This menu also lets you set security parameters, run diagnostic tests, and select all objects in the device. |
| Graph | The Graph menu lets you view Device Manager statistics and produce graphs of the chassis or port statistics. |
| VLAN | The VLAN menu lets you view information about VLANs, spanning tree groups (STGs), MultiLink Trunks, and MAC Learning. |
| IP Routing | The IP Routing menu lets you set up IP routing functions for the switch, including OSPF, RIP, VRRP, Multicast, IGMP, DVMRP, DHCP, UDP forwarding, filters, and policies. |
| IPX Routing | The IPX Routing menu lets you set up IPX routing functions, including RIP and SAP. |
| QOS | The QOS menu lets you set up and view QoS filters and profiles. |
| RMON | The RMON menu lets you set up RMON alarms and view the alarm log and history log. This menu also allows you to enable or disable RMON history or statistics on all ports. |
| Actions | The Actions menu provides quick access to selected actions without going through other menus and submenus. Use this menu to initiate a Telnet session, to open the Web management interface, to save runtime configurations, or to save boot configurations. |
| Help | The Help menu lets you view online Help topics for Device Manager. This menu also provides a legend for the port colors in the device view. |

## Toolbar

The toolbar buttons provide quick access to commonly used commands and some additional actions (Table 4).

**Table 4** Toolbar buttons

| Button | Name | Description | Menu equivalent |
|---|---|---|---|
|  | Open Device | Opens a device. | 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 window. | Help > Device Manager |
|  | Edit Selected | Displays configuration data windows for the selected chassis object. | Edit > Chassis<br>Edit > Card<br>Edit > Fan<br>Edit > MDA<br>Edit > Mgmt Port<br>Edit > Port<br>Edit > Power Supply<br>Edit > Serial Port |
|  | Graph Selected | Opens statistics and graphing windows. | Graph > Chassis<br>Graph > Port |
|  | Open Device's Home Page | Opens the Web management interface home page. | Actions > Open Home Page |
|  | Save Runtime Config | Saves the current run-time configuration. | Actions > Save Runtime Config |

**Table 4** Toolbar buttons (continued)

| | | | |
|---|---|---|---|
|  | Telnet | Opens a Telnet session. | Actions > Telnet |
|  | Alarm Manager | Opens the RMON Alarm Manager window. | Rmon > Alarm Manager |

# Using the Device view

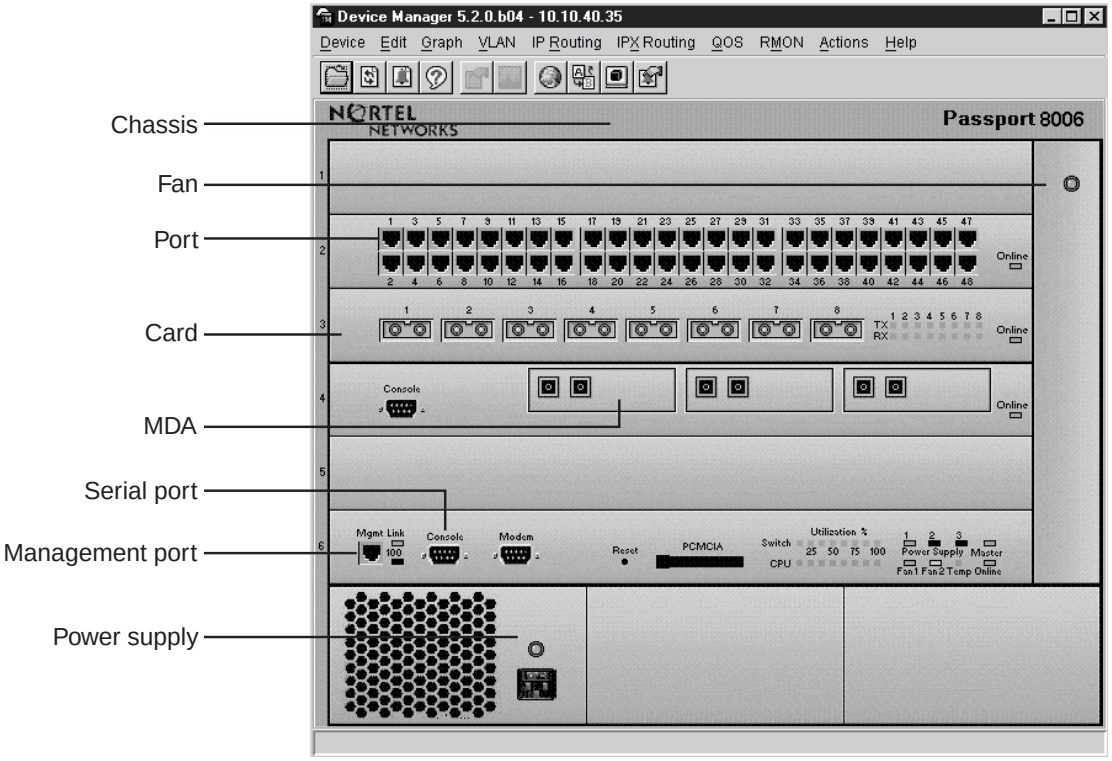
The device view allows you to determine at a glance the operating status of the various modules and ports in your hardware configuration. You also use the device view to perform management tasks on specific objects.

## Selecting objects

In the device view (Figure 7), you can select the following types of objects:

- The entire chassis
- A card (module) or multiple cards
- A port or multiple ports
- A power supply
- A fan
- An MDA
- A management port
- A serial port

**Figure 7** Objects in a Passport 8000 Series switch device view




OPT0002A

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.

To select multiple objects of the same type (such as ports or modules), use *one* of the following actions:

- For a block of contiguous ports or modules, drag to select the group of objects.

  or

- For multiple ports or modules anywhere in the switch chassis, [Ctrl]-click the objects anywhere in the device view.

## Interpreting the status of LEDs and ports

The conventions on the device view are similar to the actual switch appearance. Module LEDs are in one of three states: on, off, or blinking. For a full description of what each state means, refer to the documentation that came with the module.

The ports on the device view are color coded to provide at-a-glance port status. Table 5 shows the status assigned to each color.

**Table 5** Device Manager port color codes

| Color | Description |
|---|---|
| Green | Port is up and 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. |
| Grey | Port is not reachable by Device Manager. |

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

## Using shortcut menus

Objects in the device view such as the chassis, ports, and cards have shortcut menus. These menus provide a faster path for editing objects and applying changes; however, you can access the same options through the menu bar or the toolbar.

To display the chassis shortcut menu (Figure 8), select the chassis and right click.

**Figure 8** Chassis shortcut menu


Table 6 describes the chassis shortcut menu options.

**Table 6** Chassis shortcut menu options

| Option | Description |
|---|---|
| Edit | Edit chassis parameters. |
| Graph | Graph chassis statistics. |
| Save Runtime Config | Save any changes made as a run-time configuration. |
| Save Boot Config | Save any changes made as a boot configuration. |
| Reset Counters | Reset all the statistics counters for the switch. |
| Hard Reset | Perform a hard reset of the switch. |
| Soft Reset | Perform a soft reset of the switch. |

To display the port shortcut menu (Figure 9), select one or more ports and right click.

**Figure 9** Port shortcut menus

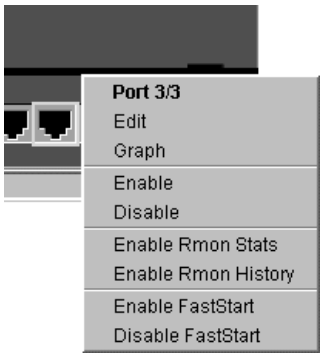



Table 7 describes the I/O port shortcut menu options.

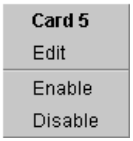
**Table 7** Port shortcut menu options

| Option | Description |
|---|---|
| Edit | Display edit port menu. |
| Graph | Graph port statistics. |
| Graph POS | Displays on POS ports only. |
| Enable | Administratively bring a port up. |
| Disable | Administratively shut down a port. |
| Enable Rmon Stats | Enable Rmon statistics logging on this port or ports. Does not display on ATM or POS ports. |
| Enable Rmon History | Enable Rmon history logging on this port or ports. This field does not display on ATM or POS ports. |
| Enable FastStart | Enable FastStart spanning tree operation on this port or ports. This field does not display on ATM ports. |
| Disable FastStart | Disable FastStart spanning tree operation on this port or ports. This field does not display on ATM ports. |

The card shortcut menu provides a quick way to view the card's parameters. When the selected card is an I/O module, you can click on the Edit option on the shortcut menu to open the Edit Card dialog box.

To display the card shortcut menu (Figure 10), select a card and right click.

**Figure 10** Card shortcut menu (I/O module)




### Status bar

At the bottom of the Device Manager window is the status bar. This area displays error and informational messages from the software application. These messages are not related to the device being managed.

## Using Device Manager dialog boxes

Many Device Manager dialog boxes contain editable fields that allow you to enter parameter values, and many of the parameters have predetermined possible values. For example, a port may be set to be enabled or disabled. Other parameter values are ranges of user-determined values. For example, the value for a system contact will be a name you enter in the SysContact field.

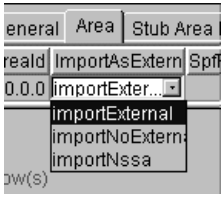
Editable fields in Device Manager dialog boxes are displayed in white.

To change the value in a field:

1 Click the field.

The possible choices for that parameter are displayed (Figure 11).

**Figure 11** Parameter selection menu




2 Click a new value from the list.

3 Click Apply.

For fields that do not have preset values, click the field and type the value.

When you enter values for IP addresses, MAC addresses, or time, follow these guidelines:

- Enter an IP address in decimal format:

  `<xxx>.<xxx>.<xxx>.<xxx>`
- Enter a MAC address in hexadecimal format:

  `xx:xx:xx:xx:xx:xx`
- Time is a value based on the delta from the switch boot-up time.

## Using the buttons in Device Manager dialog boxes

Table 8 describes buttons that appear in Device Manager dialog boxes and tabs. Not all buttons appear in all dialog boxes.

**Table 8** Device Manager buttons

| Button | Description |
|---|---|
| Apply | Applies the changes you have entered in fields on a tab or dialog box. The button is grayed out until you change a parameter. Changes are displayed as **bold** text or numbers. |
| 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. |
| Delete | Deletes a selected entry. |

**Table 8** Device Manager buttons (continued)

| Button | Description |
|---|---|
| Refresh | Refreshes the information in the window. Every time you click on Refresh, new information is polled from the switch and displayed. |
| Close | Closes the tab or dialog box and disregards any changes you have made to fields. |
| Help | Opens context-sensitive online Help. |
| Resize Columns | Resizes table columns to fit the data in them. |
| Stop | Stops the current action (polling). |
| Copy | Will copy selected items to your computer's memory clipboard. |
| Paste | Will paste the contents of your computer's clipboard. |
| Reset changes | Resets any configuration values you have changed back to their original value. |
| Export data | Allows you to copy data to external media. |
| Print Table | Prints the contents of any table that is displayed. |
| Graph | Graphs selected data. |
| Export (on Graph dialog boxes) | Saves the current table in ASCII format in a file you specify. The table contains tabs so you can then import this file into a text editor or spreadsheet for further analysis. |
| Print (on Graph dialog boxes) | Prints the current table. |

## Editing objects

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

- Select an object; from the Device Manager toolbar, click Edit Selected. The edit dialog box opens for that object.
- From the shortcut menu for a chassis, card, port, or any other object, choose Edit. The edit dialog box opens for that object.
- Double-click an object. The edit dialog box opens for that object.
- From the Device Manager menu bar, choose Edit > Selected All. Then choose an object type from the list.

When you change values in a field, you can see fields that have been changed but not applied. Click Apply to apply the changes to the device.

Most tabs and dialog boxes contain a Refresh button. After you apply changes to fields, click Refresh to display the new information in the tab or dialog box. In Windows and UNIX environments, the changed value is displayed in **bold.**

**Note:** To make changes in the running configuration, click Apply. Changes are not applied to Device Manager until you click Apply. To make the changes permanent, from the Device Manager menu bar, click Actions > Save Runtime Config.

# 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 Help. To display online Help correctly, Nortel Networks recommends using the following Web browsers:

- Microsoft Internet Explorer 5.0 or later
- Netscape Navigator 4.7 or later

If, for some reason, the Web browser does not launch, the location of the Help files are the default install directories listed in Table 9.

**Table 9** Help file locations

| Help files | Default path |
|---|---|
| Device Manager | *Jdm/help/dm* |
| Device specific help | *default install directory..../help* |

# Chapter 2
# Security

This chapter describes how to set the security features with Device Manager. It includes the following sections that explain how to:

- Control access to a switch (next).
- Lock a port to prevent other users from changing its configuration (page 50).
- Control access to the command line interface (page 51).
- Modify the SNMP community strings (page 53).
- Control access to the Web interface (page 56).
- Configure RADIUS authentication (page 58).

## Controlling access to a switch

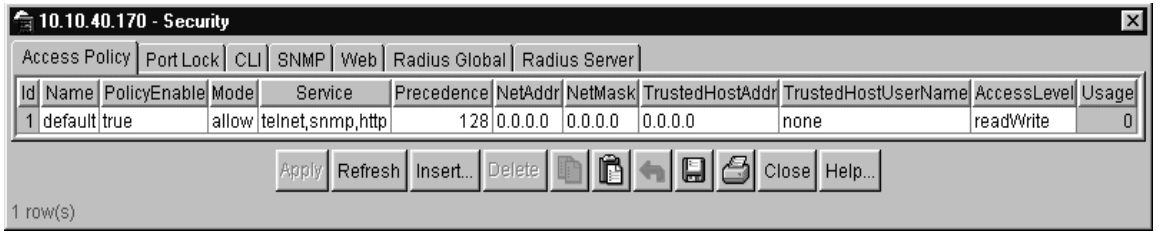
You can control access to the switch by inserting a new access policy. The access policy specifies the hosts or networks that can access the switch through various services.

To insert a new access policy:

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

The Security dialog box (Figure 12) opens with the Access Policy tab active.

**Figure 12** Security dialog box—Access Policy tab




2 In the Security dialog box, click Insert.

   The Security, Insert Access Policies dialog box (Figure 13) opens. Refer to Table 10 for field descriptions. All fields are optional except ID.

3 Make sure PolicyEnable is checked.

4 Select the mode to allow or deny a service.

5 Select a service.

6 Set a precedence number for the service (lower numbers mean higher precedence).

7 Enter an IP address in the NetAddr field.

8 Enter the NetMask used for the NetAddr field.

9 Enter an IP address for the trusted host.

10 Enter a user name for the trusted host.

11 Select the access level for the service.

12 Click Insert.

**Figure 13** Security, Insert Access Policies dialog box

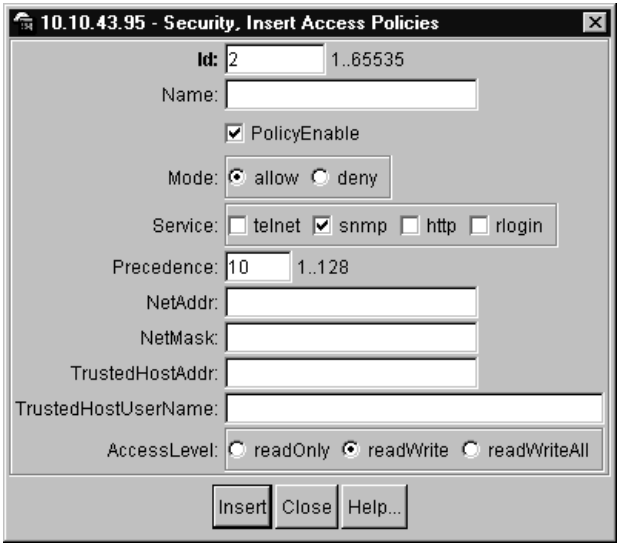



**Table 10** Security, Insert Access Policies fields

| Field | Description |
|---|---|
| Id | Policy ID. |
| Name | Name of this policy. |
| PolicyEnable | Select to activate the access policy. |
| Mode | Indicates whether a packet having a source IP address that matches this entry should be permitted to enter the device or denied access. |
| Service | Selects the protocol to which this entry should be applied. |
| Precedence | Indicates the precedence of the policy. The lower the number, the higher the precedence (1 to 128). |
| NetAddr | Source network IP address. An address of 0.0.0.0 specifies any address on the network. |
| NetMask | Source network masks. |
| TrustedHostAddr | Trusted IP address of the host performing rlogin or rsh into the device. Applies only to rlogin and rsh.<br>**Note:** You cannot use wildcard entries. |

**Table 10** Security, Insert Access Policies fields (continued)

| Field | Description |
|---|---|
| TrustedHostUserName | User name assigned to the trusted host. Applies only to rlogin and rsh.<br>**Note:** You cannot use wildcard entries. The user must already be logged in with the user name to be assigned to the trusted host. |
| AccessLevel | Access level of the trusted host (readOnly, readWrite, or readWriteAll). |

# Locking a port

The Port Lock feature allows you to administratively lock a port or ports to prevent other users from changing port parameters or modifying port action. Locked ports cannot be modified in any way until the port is first unlocked.

To set port locking and unlocking:

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

   The Security dialog box opens with the Access Policy tab displayed.

2. Click the Port Lock tab.

   The Port Lock tab opens (Figure 14). Refer to Table 11 for field descriptions.

**Figure 14** Security dialog box—PortLock tab

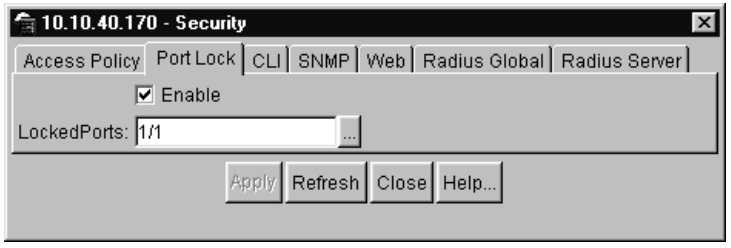


**Table 11** Port Lock tab fields

| Field | Description |
|---|---|
| Enable | Selecting this box locks the ports selected. |
| LockedPorts | Lists the locked ports. Click on the ellipsis button to select the ports you want to lock. |

# Controlling access to the CLI

If you have read/write/all access authority, you can use Device Manager to change the passwords for access to the CLI through a console or Telnet session. If you do not have read/write/all privileges, the user name and password fields will be blank.

The CLI tab allows you to specify the number of allowed Telnet sessions and rlogin sessions. To prohibit Telnet or rlogin access to the switch, specify zero (0) as the number of allowed sessions.

To change passwords for access to the CLI:

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

   The Security dialog box opens with the Access Policy tab displayed.

2. Click the CLI tab.

   The CLI tab opens (Figure 15).

**Figure 15** Security dialog box—CLI tab

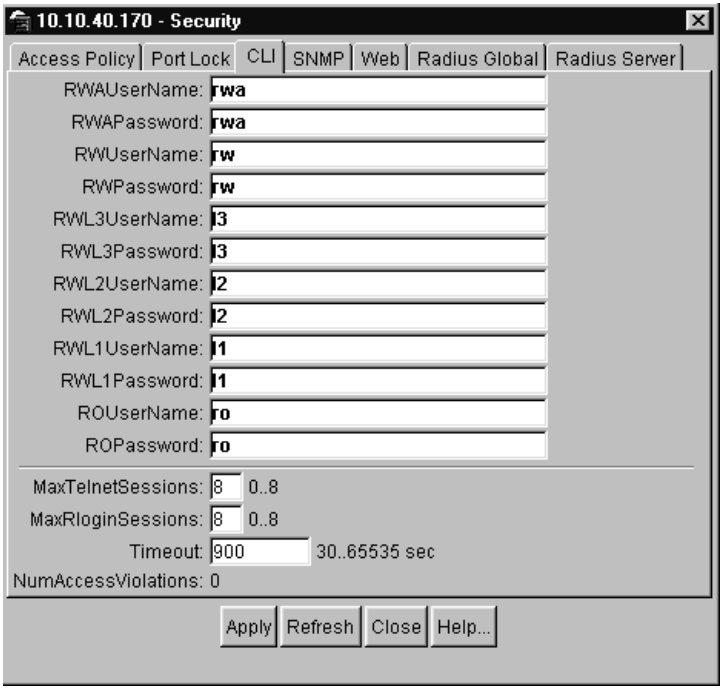



Table 12 describes the Security CLI tab fields.

**Table 12** Security CLI tab fields

| Field | Description |
|---|---|
| RWAUserName | User name for the read/write/all CLI account. |
| RWAPassword | Password for the read/write/all CLI account. |
| RWUserName | User name for the read/write CLI account. |
| RWPassword | Password for the read/write CLI account. |
| RWL3UserName | User name for the Layer 3 read/write CLI account. |
| RWL3Password | Password for the Layer 3 read/write CLI account. |
| RWL2UserName | User name for the Layer 2 read/write CLI account. |
| RWL2Password | Password for the Layer 2 read/write CLI account. |
| RWL1UserName | User name for the Layer 1 read/write CLI account. |
| RWL1Password | Password for the Layer 1 read/write CLI account. |

**Table 12** Security CLI tab fields

| Field | Description |
|---|---|
| ROUserName | User name for the read-only CLI account. |
| ROPassword | Password for the read-only CLI account. |
| MaxTelnetSessions | Maximum number of concurrent Telnet sessions that are allowed (from none to 8). |
| MaxRloginSessions | Maximum number of concurrent Rlogin sessions that are allowed (from none to 8). |
| Timeout | Number of seconds of inactivity for a Telnet or Rlogin session before automatic timeout and disconnect (30 to 65535 seconds). |

# Modifying the SNMP community strings

If you have read/write/all access authority, you can modify the SNMP community strings for access to the device through Device Manager.

To change SNMP community strings:

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

   The Security dialog box opens with the Access Policy tab displayed.

2. Click the SNMP tab.

The SNMP tab opens (Figure 16).

**Figure 16** Security dialog box—SNMP tab

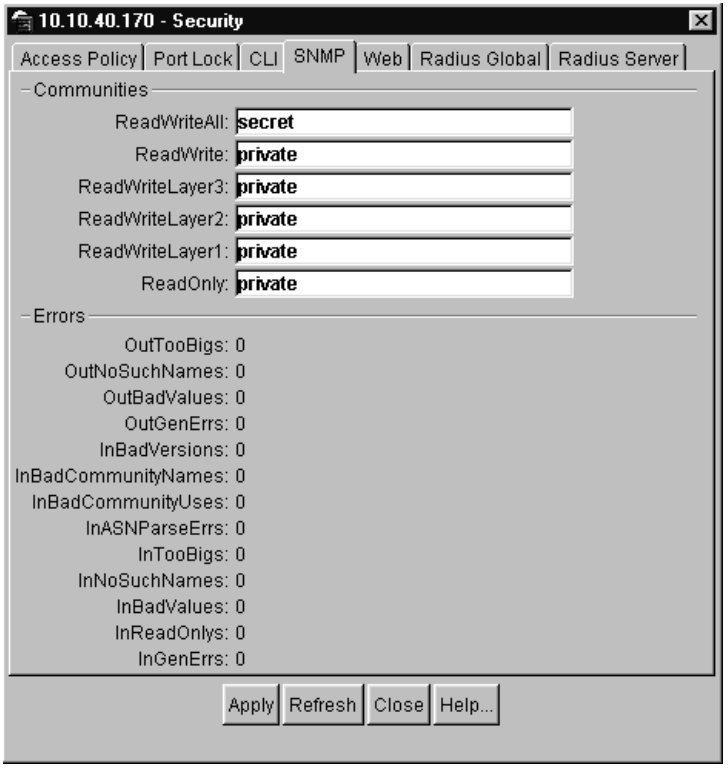



Table 13 describes the SNMP tab fields.

**Table 13** SNMP tab fields

| Field | Description |
|---|---|
| ReadWriteAll | When an SNMP message is received, the community string in the message is compared with this string first. If it matches, read/write access is granted to all items in the MIB. If it does not match, the read/write string is compared next. |
| ReadWrite<br>ReadWriteLayer3<br>ReadWriteLayer2<br>ReadWriteLayer1 | When an SNMP message is received, the community string in the message is compared with these strings second, third, and fourth, respectively. If it matches, read/write access is granted to the appropriate items in the MIB except community strings. (Community strings appear empty when read and return a noSuchName error when an attempt is made to write them.) If it does not match, the ReadOnly string is compared next. |

**Table 13** SNMP tab fields (continued)

| Field | Description |
|---|---|
| ReadOnly | When an SNMP message is received by this entity, the community string in the message is compared with this string fifth. If it matches, read-only access is granted to all items in the MIB except community strings. (Community strings appear empty when read.) If it does not match, no access is granted, no response is sent back to the SNMP requester, and SNMP traps are sent to the SNMP trap receivers if configured. |
| OutTooBigs | The total number of SNMP PDUs that were generated by the SNMP protocol entity and for which the value of the error-status field is “tooBig.” |
| OutNoSuchNames | The total number of SNMP PDUs that were generated by the SNMP protocol entity and for which the value of the error-status is “noSuchName.” |
| OutBadValues | The total number of SNMP PDUs that were generated by the SNMP protocol entity and for which the value of the error-status field is “badValue.” |
| OutGenErrors | The total number of SNMP PDUs that were generated by the SNMP protocol entity and for which the value of the error-status field is “genErr.” |
| InBadVersions | The total number of SNMP messages that were delivered to the SNMP protocol entity and were for an unsupported SNMP version. |
| InBadCommunity Names | The total number of SNMP messages delivered to the SNMP protocol entity that used an SNMP community name not known to said entity. |
| InBadCommunity Users | The total number of SNMP messages delivered to the SNMP protocol entity 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 entity when decoding received SNMP messages. |
| InTooBigs | The total number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is “tooBig.” |
| InNoSuchNames | The total number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is “noSuchName.” |
| InBadValues | The total number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is “badValue.” |

**Table 13** SNMP tab fields (continued)

| Field | Description |
|---|---|
| InReadOnlys | The total number valid SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is “read-only”. It should be noted that it is a protocol error to generate an SNMP PDU that contains the value “read-only” in the error-status field; as such this object is provided as a means of detecting incorrect implementations of the SNMP. |
| InGenErrors | The total number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is “genErr.” |

# Controlling access to the Web interface

In Device Manager, use the Web tab to set Web access parameters, including passwords.

To set Web access:

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

   The Security dialog box opens with the Access Policy tab displayed.

2. Click the Web tab.

   The Web tab opens (Figure 17).

   The ROUserName and ROPassword fields allow you to specify the user name and password for access to the Web interface. (All Web pages are read-only pages.) The other fields allow you to specify the path and file name for the Web Help files and to set the number of rows allowed in the Web display.

**Figure 17** Security dialog box—Web tab

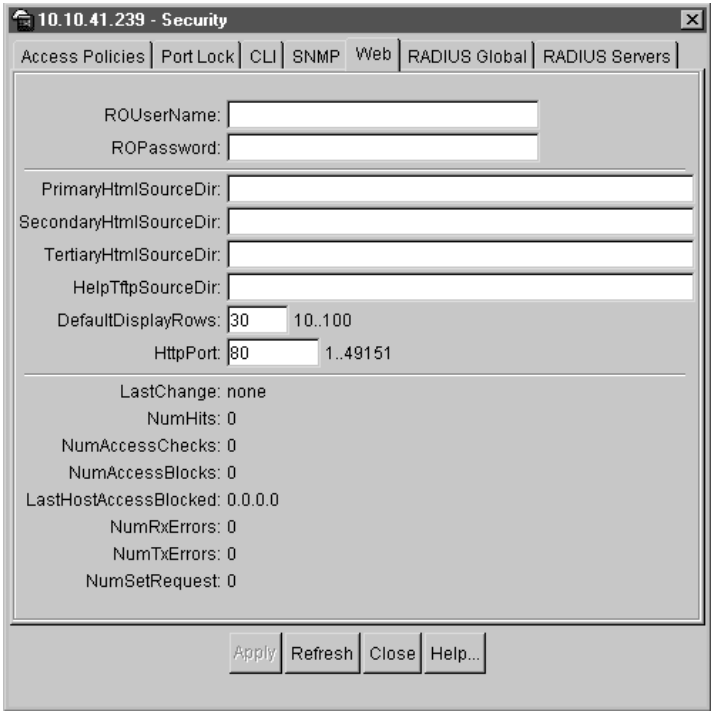


Table 14 describes the Web tab fields.

**Table 14** Web tab fields

| Field | Description |
|---|---|
| ROUserName | The user name for the read-only Web server account. |
| ROPassword | The password for the read-only Web server account. |
| PrimaryHtmlSourceDir | The primary HTML source directory. |
| SecondaryHtmlSourceDir | The secondary HTML source directory. |
| TertiaryHtmlSourceDir | The tertiary HTML source directory. |
| HelpTftpSourceDir | The TFTP source directory for Help files. |
| DefaultDisplayRows | The default display rows for the HTML pages. |
| HttpPort | The port number that allows Web access to the switch. The default is 80. |
| LastChange | The time of the most recent change to the switch configuration using the Web interface. This field always reads none. |
| NumHits | Number of times pages in the Web interface have been accessed. |
| NumAccessChecks | Number of times access attempts have been authenticated. |
| NumAccessBlocks | Number of times access has been attempted and denied. |
| LastHostAccessBlocked | The last host accessed blocked. |
| NumRxErrors | Number of receive errors. |
| NumTxErrors | Number of transmit errors. |
| NumSetRequest | Number of set-requests sent to the Web server. |

# Understanding RADIUS authentication

Remote Authentication Dial In User Service (RADIUS) allows the remote RADIUS server rather than the switch to authenticate logins. The RADIUS server also provides access authority. The Passport 8000 Series software supports BaySecure Access Control (BSAC)* and the Merit Network servers.

RADIUS assists network security and authorization by managing a database of users. Use of the database allows the switch to verify user names and passwords as well as information about the type of access priority available to the user.

The RADIUS software provides the following features:

- Additional user names

  Additional user names can be used to access the switch, in addition to the five existing user names of ro, L1, L2, L3, and rwa. The RADIUS server authenticates the user name and assigns one of the existing access priorities to that name. Unauthenticated user names are denied access to the switch.

- User configurability
  - Up to 10 RADIUS servers in each switch for fault tolerance (Each server is assigned a priority and is contacted in that order.)
  - A secret key for each server to authenticate the RADIUS client
  - The server's UDP port
  - Maximum retries allowed
  - Time-out period for each attempt
- Changeable passwords

  Users can change passwords by logging in to the RADIUS server. However, access priorities are not configurable by individual users; access privileges are maintained by the system administrator.

# Enabling Radius authentication globally

To enable RADIUS authentication globally:

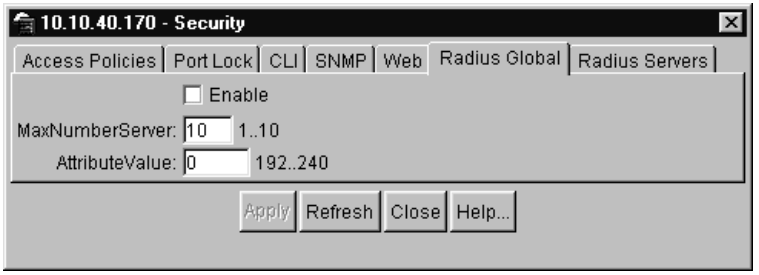
1. From the Device Manager menu bar, choose Edit > Security.

   The Security dialog box opens with the Access Policy tab displayed.

2. Click the Radius Global tab.

   The Radius Global tab opens (Figure 18).

**Figure 18** Security dialog box—Radius Global tab




3 Click Enable.

4 Enter the maximum number of servers.

5 Enter the access policy attribute.

6 Click Apply.

Table 15 describes the Radius Global tab fields.

**Table 15** Radius Global tab fields

| Field | Description |
|---|---|
| Enable | Click this check box to enable or disable the RADIUS authentication feature globally. |
| MaxNumberServer | Enter the maximum number of servers, between 1 and 10, that you want to use. |
| AttributeValue | Integer value for Access-Priority attribute. The default is 192. |

# Viewing Radius server configuration

The Radius Servers tab contains information about the RADIUS servers configured.

To view RADIUS server configuration:

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

The Security dialog box opens with the Access Policy tab displayed.

2 Click the Radius Servers tab.

The Radius Servers tab opens (Figure 19).

**Figure 19** Security dialog box—RADIUS Servers tab

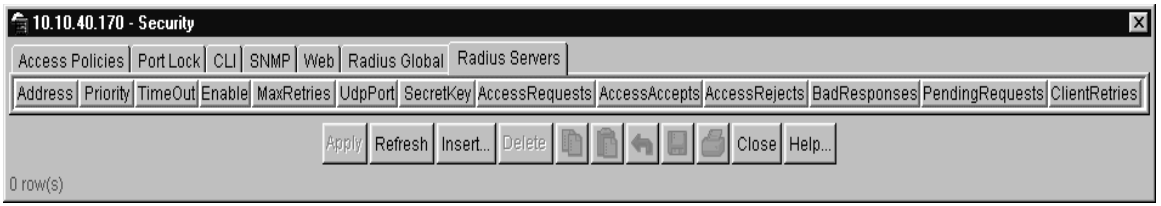



Table 16 describes the Radius Servers tab fields.

**Table 16** Radius Servers tab fields

| Field | Description |
|---|---|
| Address | Displays the IP address of the RADIUS server. |
| Priority | Displays the priority of each server, or the order of servers to send authentication. |
| TimeOut | Displays the time interval before the client will retransmit the package. |
| Enable | Displays whether the server is enabled or disabled. |
| MaxRetries | Displays the maximum number of retransmissions allowed. |
| UdpPort | Displays the UDP port the client uses to send requests to the server. |
| SecretKey | Identifies the RADIUS authentication client. |
| AccessRequests | Displays the number of access-response packets sent to the server; does not include retransmissions. |
| AccessAccepts | Displays the number of access-accept packets, valid or invalid, received from the server. |
| AccessRejects | The number of access-reject packets, valid or invalid, received by the RADIUS server. |
| BadResponses | The number of invalid access-response packets received by the RADIUS server. |

**Table 16** Radius Servers tab fields (continued)

| Field | Description |
|---|---|
| PendingRequests | The number of pending access-requests packets sent to the RADIUS server that have not yet received a response or timed out. |
| ClientRetries | The number of authentication retransmissions to the RADIUS server. |

# Inserting a RADIUS server

To insert a RADIUS server:

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

   The Security dialog box opens with the Access Policy tab displayed.

2. Click the Radius Servers tab.

   The RADIUS Servers tab opens.

3. In the Radius Servers tab; click Insert.

   The Security, Insert RADIUS Servers dialog box opens (Figure 20). Refer to Table 17 for field descriptions.

4. Enter the appropriate fields, and click Insert.

**Figure 20** Security, Insert RADIUS Servers dialog box

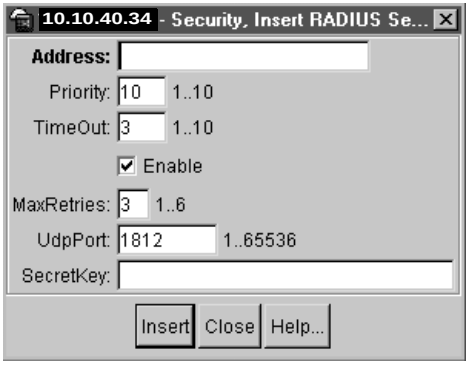


**Table 17** Security, Insert RADIUS Servers fields

| Field | Description |
|---|---|
| Address | Enter the IP address of the new server. |
| Priority | Enter the priority between 1 and 10 of the new RADIUS server. |
| TimeOut | Enter the number of seconds, between 1 and 10, that you want between retransmissions from the client to the RADIUS server. |
| Enable | Enables the RADIUS server. |
| MaxRetries | Enter the maximum number of retries, between 1 and 6, that you want to allow requests to the server. |
| UdpPort | Enter the UDP port number, between 1 and 65536, that the client will use to send requests to the server.<br>**Note:** The UDP port value set for the client must be the same as the value set for the Radius server. |
| SecretKey | Enter the secret key of the authentication client. |

# Chapter 3
# Chassis configuration and graphing

This chapter describes editing and graphing a Passport 8000 Series chassis using Device Manager. The first three sections describe how you can use Device Manager to configure your Passport 8000 Series switch. The last section describes how to use Device Manager to graph switch statistics.

To configure your Passport 8000 Series switch, see:

- "Editing the chassis," next
- "Editing cards" on page 78
- "Editing objects" on page 86

To graph switch statistics, see:

"Graphing chassis statistics" on page 102

## Editing the chassis

Use the tabs in the chassis dialog box to edit the Passport 8000 Series chassis.

To edit the Passport 8000 Series chassis:

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

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

## Editing system information

You can edit system information such as the contact person, the name of the device and where it is located. Other information cannot be edited, but is very useful, such as what version of the software is running on the device.

To open the System tab:

➔ On the Device Manager menu bar, choose Edit > Chassis.

The chassis dialog box opens with the System tab displayed (Figure 21).

**Figure 21** Chassis dialog box—System tab

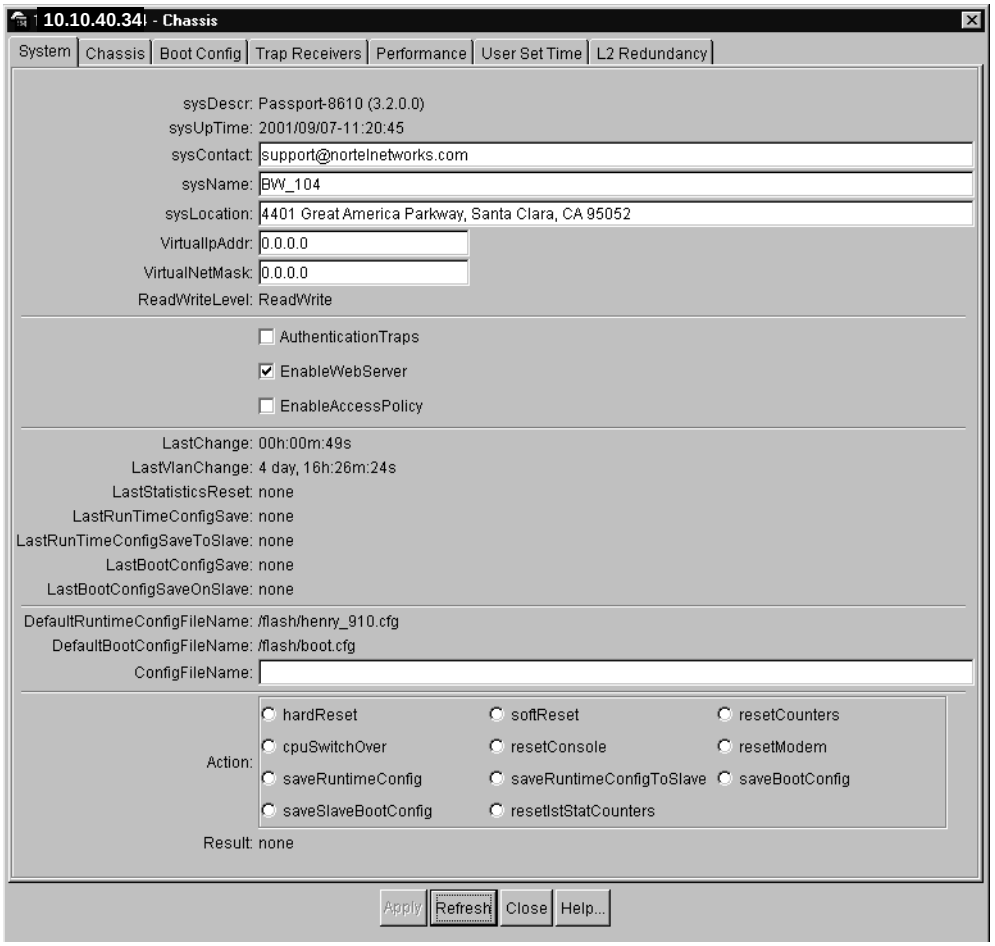



Table 18 describes the System tab fields.

**Table 18** System tab fields

| Field | Description |
|---|---|
| sysDescr | The system assigned name and the software version it is running. |
| sysUpTime | The time since the system was last booted. |

**Table 18** System tab fields (continued)

| Field | Description |
|---|---|
| sysContact | The contact information (in this case, an e-mail address) for the Nortel Networks support group. |
| sysName | The name of this device. |
| sysLocation | The physical location of this device. |
| VirtualIPAddr | The virtual IP address is the IP address advertised by the master CPU. Unlike the management port IP address, this address is stored in the switch configuration file and not the boot configuration file. |
| VirtualNetMask | The net mask of the virtual management IP address. |
| ReadWriteLevel: | Displays the access level of the trusted host (readOnly, readWrite, or readWriteAll) |
| AuthenticationTraps | Enables or disables authentication traps. When you enable, SNMP traps are sent to trap receivers for all SNMP access authentication.<br>To view traps, click the Trap Log button on the Device Manager toolbar.<br>  |
| EnableWebServer | Enables or disables the Web HTML server. When enabled, it allows the system to be monitored using a Web browser. |
| EnableAccess Policy | Enables or disables Access Policy settings. |
| LastChange | The time since the last configuration change. |
| LastVlanChange | The time since the last VLAN change. |
| LastStatisticsReset | The time since the statistics counters were last reset. |
| LastRunTimeConfigSave | The last run-time configuration that was saved. |
| LastRunTimeConfigSaveToSlave | The last run-time configuration that was saved to the standby device. |
| LastBootConfigSave | The last boot configuration that was saved. |
| LastBootConfigSaveOnSlave | The last boot configuration that was saved on the standby device. |
| DefaultRuntimeConfigFileName | The default Runtime Configuration File directory name. |
| DefaultBootConfigFileName | The default Boot Configuration File directory name. |
| ConfigFileName | Allows you to type the name of a new configuration file. |

**Table 18** System tab fields (continued)

| Field | Description |
|---|---|
| Action | Can be one of the following actions:<br>• hardReset—Resets the device and runs power-on tests.<br>• softReset—Resets the device without running power-on tests.<br>• resetCounters—Resets all statistic counters.<br>• cpuSwitchOver—Switch control from one CPU to another.<br>• resetConsole—Reinitializes the hardware UART drivers. Use only if the console or modem connection is hung.<br>• resetModem—Reinitializes the UART drivers on the modem port. Use only if the console or modem connection is hung.<br>• saveRuntimeConfig—Saves the current run-time configuration.<br>• saveRuntimeConfigToSlave—Saves the current run-time configuration to the standby CPU.<br>• saveBootConfig—Saves the current boot configuration.<br>• saveBootConfigOnSlave—Saves the current boot configuration to the standby CPU. |
| Result | Displays a message after you click Apply. |

## Editing chassis information

You can edit chassis information to enable features described in Table 19. However, most of the chassis information describes the hardware specifications and cannot be edited.

To edit the chassis information:

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

   The chassis dialog box opens with the System tab displayed.

2. Click on the Chassis tab.

   The Chassis tab opens (Figure 22).

**Figure 22** Chassis dialog box—Chassis tab

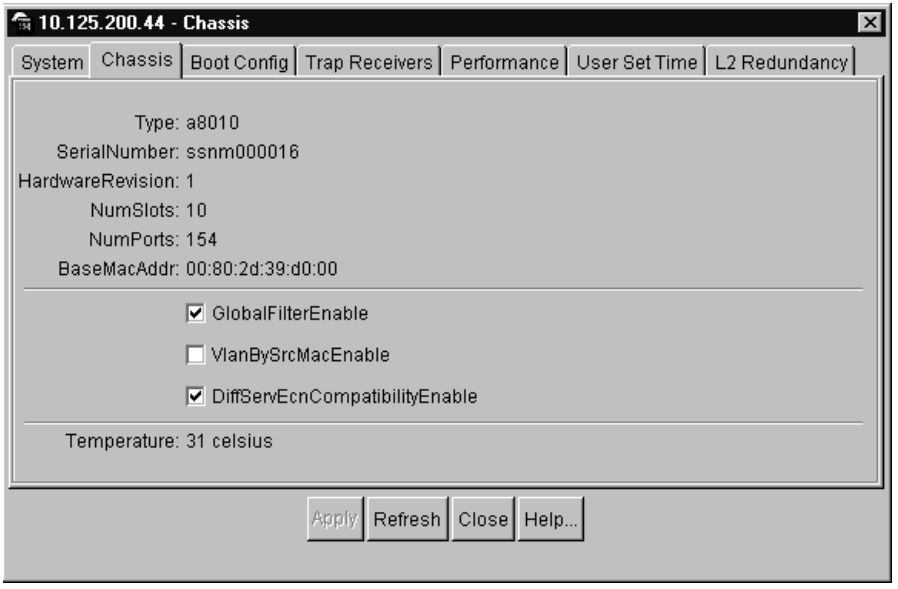



Table 19 describes the Chassis tab fields.

**Table 19** Chassis tab fields

| Field | Description |
|---|---|
| Type | The Passport module type. |
| SerialNumber | A unique chassis serial number. |
| HardwareRevision | The current hardware revision of the device chassis. |
| NumSlots | The number of slots (or cards) this device can contain. |
| NumPorts | The number of ports currently on this device. |
| BaseMacAddr | Starting point of the block of MAC addresses used by the switch for logical and physical interfaces. |
| GlobalFilterEnable | Used to enable/disable global filters in the system. |
| VlanBySrcMacEnable | Used to enable/disable source MAC based VLANs in the system. |

**Table 19** Chassis tab fields (continued)

| Field | Description |
|---|---|
| DiffServEcnCompatibilityEnable | Used to enable/disable the Explicit Congestion Notification(ECN) compatibility feature. When set to enable, the system will mask the ECN bits in the DS field while marking DSCP and will not match on ECN capable flows if filter is set on DSmatch. When set to disable, it will preserve the ECN bits in the DS field while marking DSCP and will match on full 8-bit DS field. The default is enable. |
| Temperature | The current ambient temperature of the chassis. |

## Viewing the boot configuration

You can view the boot source, as well as to see the source from which the switch booted last.

To view the boot configuration:

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

   The chassis dialog box opens with the System tab displayed.

2. Click on the Boot Config tab.

   The Boot Config tab opens (Figure 23).

**Figure 23** Chassis dialog box—Boot Config tab

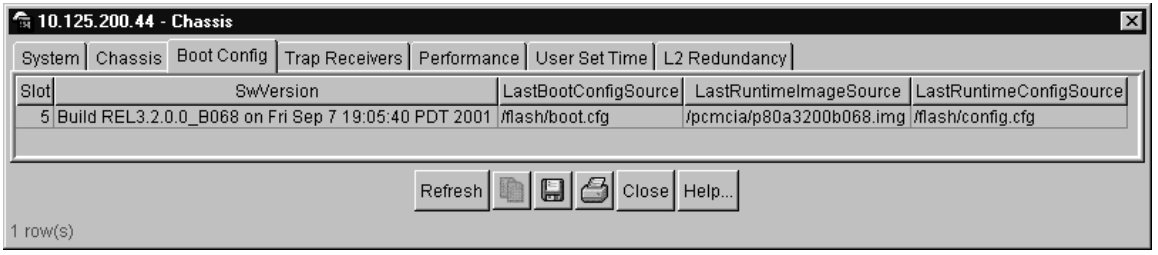



Table 20 describes the Boot Config tab fields.

**Table 20** Boot Config tab fields

| Field | Description |
|---|---|
| Slot | The slot number of the device. |
| SwVersion | The software version that is currently running. |
| LastBootConfigSource | The last source from which the switch booted. |
| LastRuntimeImageSource | The last source from which the run-time image was taken. |
| LastRuntimeConfigSource | The last source from which the run-time configuration was taken. |

## Editing trap receivers

You can edit how machines will receive SNMP traps by editing the community strings and the SNMP version format.

When Device Manager opens a device, it automatically adds the machine on which it is running to the Trap Receivers list only if the *Register for Traps* box on the Properties dialog box is checked.

**Note:** If the Trap Receivers tab takes a long time to open, it may be that the IP address of a trap receiver cannot be resolved to a DNS name. By default, Device Manager attempts to resolve IP addresses to DNS names.

To edit how traps will be received:

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

   The chassis dialog box opens with the System tab displayed.

2. Click on the Trap Receivers tab.

   The Trap Receivers tab opens (Figure 24).

**Figure 24** Chassis dialog box—Trap Receivers tab

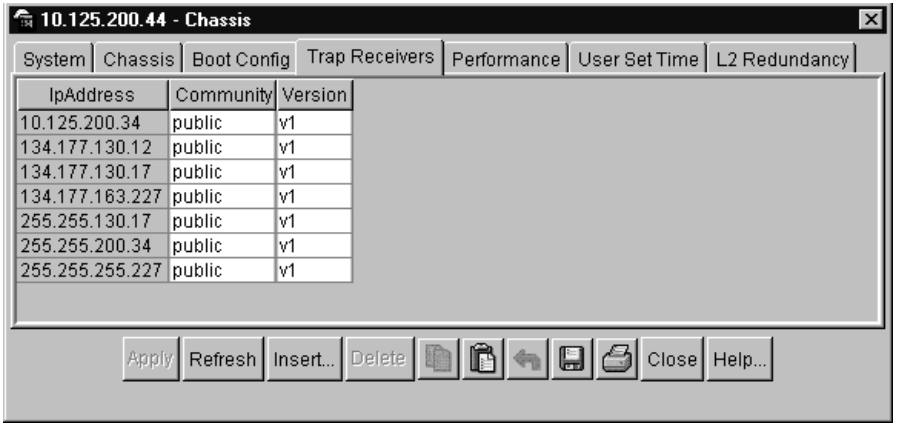



Table 21 describes the Trap Receivers tab fields.

**Table 21** Trap Receivers tab fields

| Field | Description |
|---|---|
| IpAddress | IP address for the trap receiver. (This value may be displayed as a DNS host name, but it was entered originally as an IP address.) |
| Community | Community string used for trap messages to this trap receiver. |
| Version | By default, traps are sent in SNMP V2c format. If you are using an older NMS that supports only V1 traps (for example, HP OpenView) you should select that field. Note that UNIX management stations must run Device Manager as Root to receive traps. |

## Checking the system's performance

You can check the system's performance with the Performance tab.

To open the Performance tab:

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

   The chassis dialog box opens with the System tab displayed.

2. Click on the Performance tab.

The Performance tab opens (Figure 25).

**Figure 25** Chassis dialog box—Performance tab

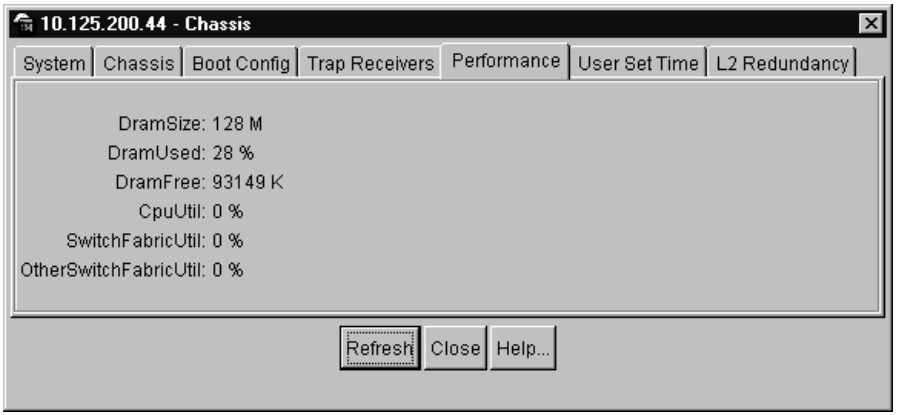



Table 22 describes the Performance tab fields.

**Table 22** Performance tab fields

| Field | Description |
|---|---|
| DramSize | The DRAM size in megabytes |
| DramUsed | The percentage of DRAM space used. |
| DramFree | The amount of DRAM free in kilobytes. |
| CpuUtil | Percentage of CPU utilization. |
| SwitchFabricUtil | Percentage of switch fabric utilization. This field will display 0% when the Passport 8100 module is installed. |
| OtherSwitchFabricUtil | Percentage of other switch fabric utilization. This field will display 0% when the Passport 8100 module is installed. |

## Setting the time

You can set the date and time on the switch with the User Set Time tab.

To open the User Set Time tab:

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

The chassis dialog box opens with the System tab displayed.

**2** Click on the User Set Time tab.

The User Set Time tab opens (Figure 26).

**Figure 26** Chassis dialog box—User Set Time tab


Table 23 describes the User Set Time tab fields.

**Table 23** User Set Time tab fields

| Field | Description |
|---|---|
| Year | The year (integer 1999...2010). |
| Month | The month (integer 1..12). |
| Day | The day (integer 1..31). |
| Hour | The hour (integer 0..23). |
| Minute | The minute (integer 0..59). |
| Second | The second (integer 0..59). |

## Enabling L2 Redundancy status

The *ha-cpu* option has been added to the `bootconfig flags` CLI command to enable or disable the L2 Redundancy feature. For information about layer 2 redundancy or about how to enable or disable this feature using the CLI, see *Managing the Passport 8000 Series Switch Using the Command Line Interface Release 3.2*.

You can enable the L2 redundancy status using Device Manager.

To enable or view the L2 redundancy status:

1. Select the chassis.
2. From the Device Manager menu bar, choose Edit > Chassis.

   The Chassis dialog box opens with the System tab displayed ().
3. Click on the L2 Redundancy tab.

   The L2 Redundancy tab opens (Figure 27).

**Figure 27** Chassis dialog box—L2 Redundancy tab

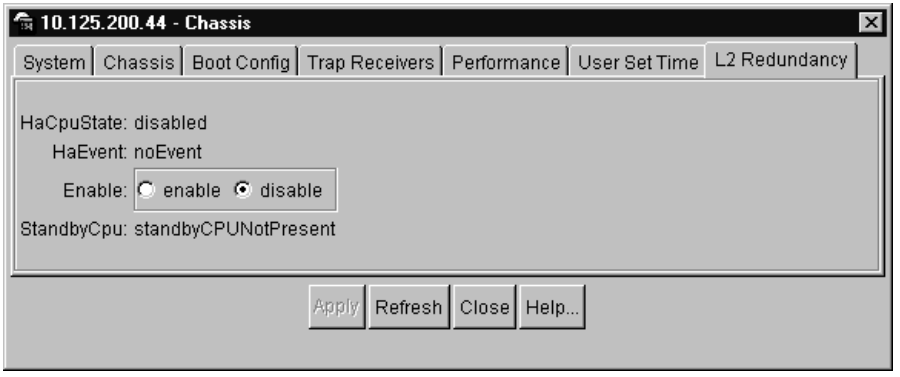



Table 24 describes the L2 Redundancy tab fields.

**Table 24** L2 Redundancy tab fields

| Field | Description |
|---|---|
| HaCpuState | This field indicates the state of the CPUs. The possible CPU states area:<br>• initialization - The two CPUs establish a connection and exchange version information.<br>• oneWayActive - modules that need to be synchronized have been registered.<br>• twoWayActive - modules that need to be synchronized have registered with the redundancy framework on both CPUs.<br>• synchronized - table based synchronization was completed on the current CPU.<br>• remote incompatible - the CPUs software versions are incompatible.<br>• error - If an invalid event is generated in a given state the CPU displays the error state. |
| Ha Event | This field displays the event status. The possible event status values are:<br>• Restart.<br>• Transfer to a One Way or Two Way Active state.<br>• Transfer to a synchronized state.<br>• Transfer go to a remote incompatible state.<br>• No event has occurred. |
| Enable | Allows you to enable or disable L2 redundancy on the master CPU. |
| StandbyCpu | This field indicates if the L2 Redundancy is enabled on the standby CPU. The possible states are:<br>• hotStandbyCPU<br>• warmStandbyCPU<br>• standbyCPUNotPresent |

# Editing cards

Use Device Manager card editing capabilities to view status information for two types of cards, I/O cards and CPU cards.

To edit the Passport 8000 Series modules (cards):

1. Select one or more modules.
2. Do *one* of the following:
   - Double-click the module.
   - Right-click the module. On the shortcut menu, choose Edit.
   - From the Device Manager menu bar, choose Edit > Card.
   - From the Device Manager menu bar, choose Edit > Select All > Cards. Then choose Edit > Card.
   - On the Device Manager toolbar, choose the Edit Selected button.

The following sections provide a description of the two different card types in the Edit> Card dialog box and details about each field on the tabs.

## Editing card information

You can use the Card tab on the Card dialog box to view status for all I/O cards except the CPU card.

To open the Card tab:

1. Select the card.
2. From the Device Manager menu bar, choose Edit > Card.

   The Card dialog box opens with the Card tab displayed (Figure 28).

**Figure 28** Card dialog box—Card tab

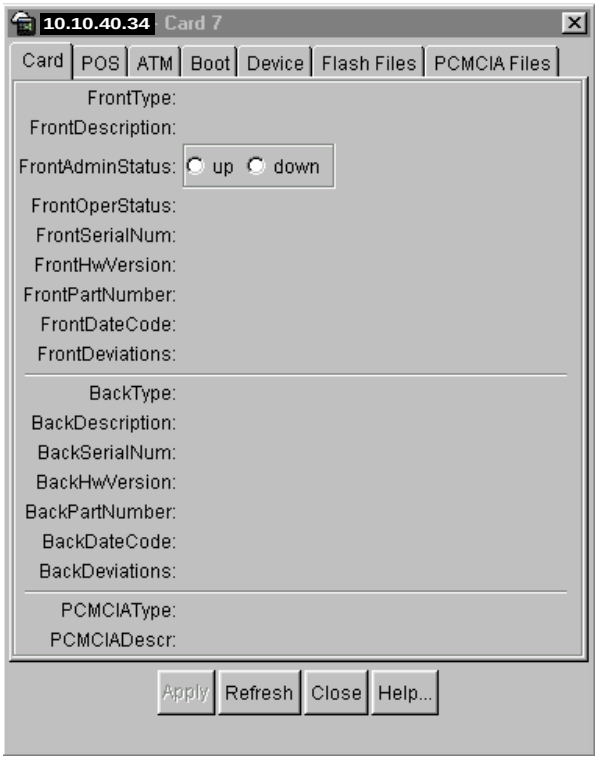



Table 25 describes the Card tab fields.

**Table 25** Card tab fields

| Field | Description |
|---|---|
| FrontType<br>BackType | Used to indicate card types in the Passport 8000 Series. *Front* refers to the I/O portion of the module, the I/O card. |
| FrontDescription<br>BackDescription | Model number of the module (for example, 8608GT). |
| FrontAdminStatus | Indicates the administrative status of the card. |
| FrontOperStatus | Indicates the operational status of this module. |
| FrontSerialNum<br>BackSerialNum | Serial number of the I/O card. |

**Table 25** Card tab fields

| Field | Description |
|---|---|
| FrontHwVersion<br>BackHwVersion | Hardware version of the I/O card. |
| FrontPartNumber<br>BackPartNumber | Part number of the I/O card. |
| FrontDateCode<br>BackDateCode | Manufacturing date code for the I/O card. |
| FrontDeviations<br>BackDeviations | Deviations. |
| PCMCIAType | Used to indicate the type of PCMCIA card currently installed in this CPU card, if any.<br>For non-CPU cards, this variable has no meaning and will always be set to none. |
| PCMCIADescr | PCMCIA description. |

## Editing boot file

You can use the Boot tab to specify, among other things, boot source and order for your switch.

To open the Boot tab:

1. Select a CPU card.
2. From the Device Manager menu bar, choose Edit > Card.

   The Card dialog box opens with the Card tab displayed.
3. Click the Boot tab.

   The Boot tab opens (Figure 29).

**Figure 29** Card dialog box—Boot tab

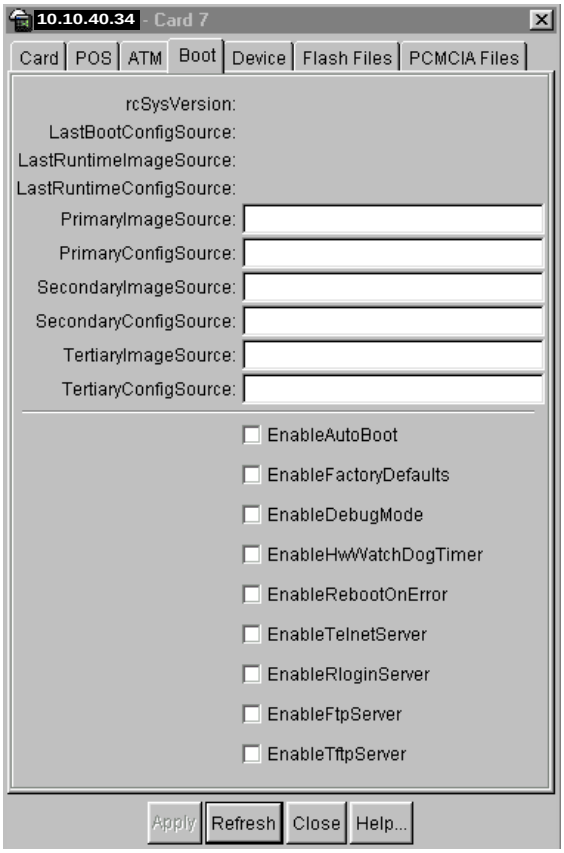



Table 26 describes the Boot tab fields.

**Table 26** Boot tab fields

| Field | Description |
|---|---|
| SwVersion | The software version that is currently running. |
| LastBootConfigSource | The boot configuration file used when the switch most recently booted. |
| LastRuntimeImageSource | The run-time image that was loaded most recently. |
| LastRuntimeConfigSource | The run-time configuration that was loaded most recently. |
| PrimaryImageSource | The primary image source file. |

**Table 26** Boot tab fields (continued)

| Field | Description |
|---|---|
| PrimaryConfigSource | The primary configuration source file. |
| SecondaryImageSource | The secondary image source file. |
| SecondaryConfigSource | The secondary configuration source file. |
| TertiaryImageSource | The tertiary image source file. |
| TertiaryConfigSource | The tertiary configuration source file. |
| EnableAutoBoot | Enables the autoboot option.<br>When you apply power, the switch waits 5 seconds and then boots. If this option is set to false, the boot process stops at the Boot Monitor. |
| EnableFactoryDefaults | Enables factory defaults option. |
| EnableDebugMode | Enables debug mode option. |
| EnableHwWatchDogTimer | Enables hardware watchdog timer option. |
| EnableRebootOnError | Enables reboot on error option. |
| EnableTelnetServer | Enables Telnet server option. |
| EnableRloginServer | Enables Rlogin server option. |
| EnableFtpServer | Enables FTP server option. |
| EnableTftpServer | Enables TFTP server option. |

## Displaying flash and PCMCIA statistics

The Passport 8000 Series switch has two types of flash memory, the onboard flash memory, and an optional installed PCMCIA card. You can view device flash and PCMCIA file information on the Device tab in the Card dialog box.

To open the Device tab:

1. Select a CPU card.
2. From the Device Manager menu bar, choose Edit > Card.

   The Card dialog box opens with the Card tab displayed.
3. Click the Device tab.

   The Device tab opens (Figure 30).

**Figure 30** Card dialog box—Device tab

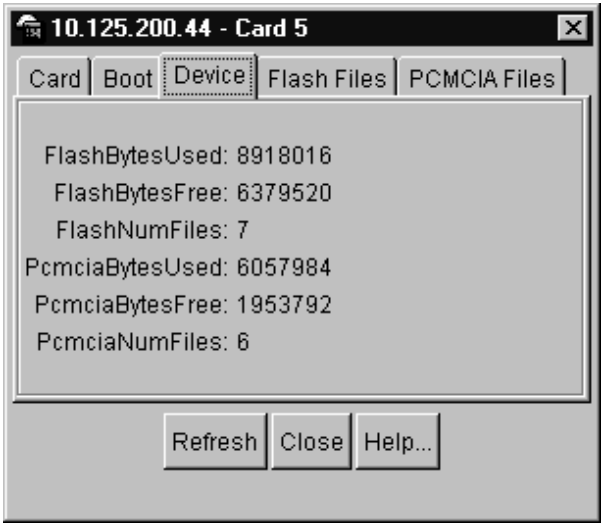



Table 27 describes the Device tab fields.

**Table 27** Device tab fields

| Field | Description |
|---|---|
| FlashBytesUsed | Number of flash bytes used. |
| FlashBytesFree | Number of flash bytes not used. |
| FlashNumFiles | Number of files in flash memory. |
| PCMCIABytesUsed | Number of PCMCIA bytes used. |
| PCMCIABytesFree | Number of PCMCIA bytes not used. |
| PCMCIANumFiles | Number of PCMCIA files. |

## Displaying flash file information

You can obtain information about the files in flash memory from the Flash Files tab.

To open the Flash Files tab:

1. Select a CPU card.
2. From the Device Manager menu bar, choose Edit > Card.

   The Card dialog box opens with the Card tab displayed.
3. Click the Flash Files tab.

   The Flash Files tab opens (Figure 31).

**Figure 31** Card dialog box—Flash Files tab

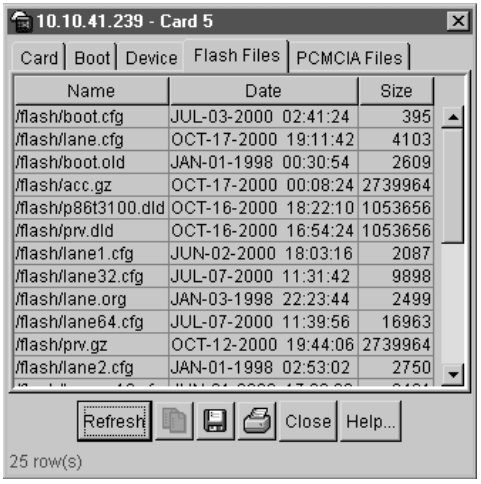



Table 28 describes the Flash Files tab fields.

**Table 28** Flash Files tab fields

| Field | Description |
|---|---|
| Name | Directory name of the flash file. |

**Table 28** Flash Files tab fields (continued)

| Field | Description |
|---|---|
| Date | Creation or modification date of the flash file. |
| Size | Size of the flash file. |

## Displaying PCMCIA file information

You can use the PCMCIA Files tab to provide information about the files stored in the switch PCMCIA card. It includes the same information as the Flash tab.

To open the PCMCIA Files tab:

1. Select a CPU card.
2. From the Device Manager menu bar, choose Edit > Card.

   The Card dialog box opens with the Card tab displayed.
3. Click the PCMCIA Files tab.

   The PCMCIA Files tab opens (Figure 32).

**Figure 32** Card dialog box—PCMCIA Files tab

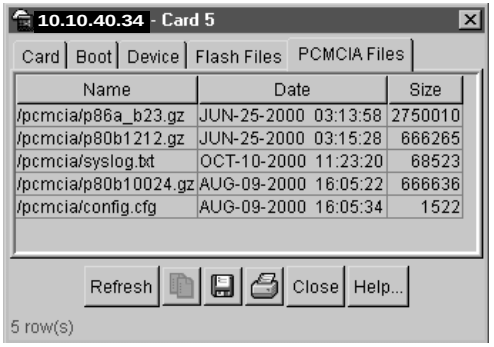



Table 29 describes the PCMCIA Files tab fields.

**Table 29** PCMCIA Files tab fields

| Field | Description |
|---|---|
| Name | The directory name of the PCMCIA file. |
| Date | The creation or modification date of the PCMCIA file. |
| Size | The size of the PCMCIA file. |

# Editing objects

The following sections describe each hardware and software object of the Passport 8000 Series switch.

## Editing management port

The management port on the switch fabric/CPU module is a 10/100 Mb/s Ethernet port that can be used for an out-of-band management connection to the switch.

You can use the Mgmt Port dialog box to specify, among other things, management information for the device and to set device configuration.

To edit the Passport 8000 Series switch Management port:

1. Select the management port.
2. Do *one* of the following:
   - Double-click the Management port.
   - Right-click the Management port; click Edit.
   - From the Device Manager menu bar, choose Edit > MgmtPort.
   - From the Device Manager menu bar, choose Edit > Select All > MgmtPort. Then choose Edit > Mgmt Port.
   - On the Device Manager toolbar, click the Edit Selected button.

To open the Mgmt Port dialog box:

1. Select the management port object.
2. From the Device Manager menu bar, choose Edit > Mgmt Port.

   The Mgmt Port dialog box opens (Figure 33).

**Figure 33** Mgmt Port dialog box

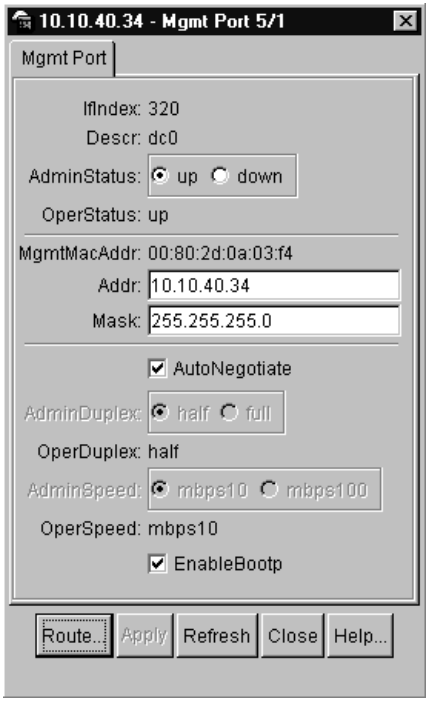



Table 30 describes the Mgmt Port dialog box fields.

**Table 30** Mgmt Port dialog box fields

| Field | Description |
|---|---|
| Ifindex | The slot and port number of the management port. |
| Descr | The description of the management port. |
| AdminStatus | The administrative status of the device. |
| OperStatus | The operational status of the device. |
| MgmtMacAddr | The MAC address of the management device. |
| Addr | The IP address of the device. |
| Mask | The subnet IP mask. |
| AutoNegotiate | The autonegotiate value. |
| AdminDuplex | Specifies the administrative duplex setting for this port. |

**Table 30** Mgmt Port dialog box fields (continued)

| Field | Description |
|---|---|
| OperDuplex | The operational duplex setting for this port. |
| AdminSpeed | Specifies the administrative speed setting for this port. |
| OperSpeed | Indicates the operational duplex setting for this port. |
| EnableBootp | Enables or disables BootP. |

## Editing management port route table

You can use the Mgmt Port Route Table dialog box to view and specify network and gateway IP addresses used to remotely manage the device.

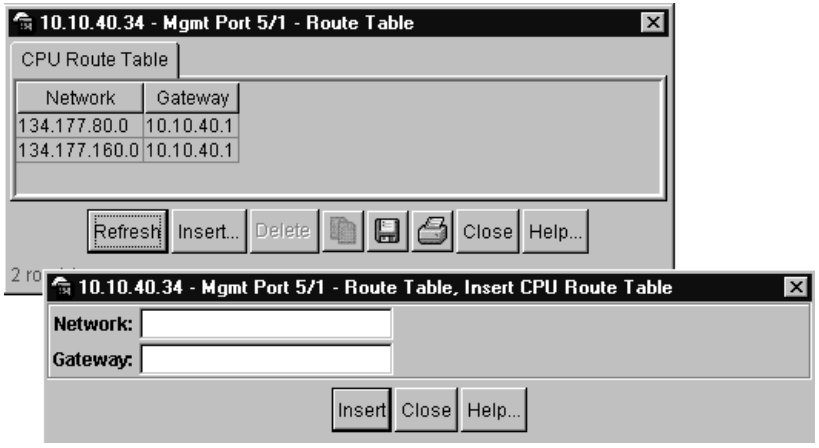
To open the Mgmt Port Route Table dialog box:

1. Select the management port object.
2. From the Device Manager menu bar, choose Edit > Mgmt Port.

   The Mgmt Port dialog box opens (Figure 33).
3. On the Mgmt Port dialog box, click Route.

   The Mgmt Port Route Table dialog box opens (Figure 34).

**Figure 34** Mgmt Port Route Table, Insert CPU Route Table dialog box



To add more Network and Gateway IP addresses:

1. On the Mgmt Port Route Table dialog box, click Insert.

   The Mgmt Port Route Table, Insert CPU Route Table dialog box opens (Figure 34)

2. In the Mgmt Port Route Table, Insert CPU Route Table dialog box; enter new Network and Gateway IP addresses.

3. In the Mgmt Port Route Table, Insert CPU Route Table dialog box, click Insert.

Table 31 describes the Mgmt Port Route Table, Insert CPU Route Table dialog box fields.

**Table 31** Mgmt Port Route Table, Insert CPU Route Table dialog box fields

| Field | Description |
|---|---|
| Network | The network IP address. |
| Gateway | The gateway IP address of the device. |

## Editing serial ports

The serial ports on the switch fabric/CPU module include the modem port and the console port.

Use the Serial Port dialog box to specify serial port communication settings.

To edit the Passport 8000 Series switch serial ports:

1. Select the serial port.
2. Do *one* of the following:
   - Double-click the serial port.
   - Right-click the serial port and click Edit.
   - From the Device Manager menu bar, choose Edit > Serial Port.

- From the Device Manager menu bar, choose Edit > Select All > Serial Ports. Then choose Edit > Serial Port.
- On the Device Manager toolbar, click the Edit Selected button.

To open the Serial Port dialog box:

1. Select the serial port object.
2. From the Device Manager menu bar, choose Edit > Serial Port.

   The Serial Port dialog box opens (Figure 35).

**Figure 35** Serial Port dialog box

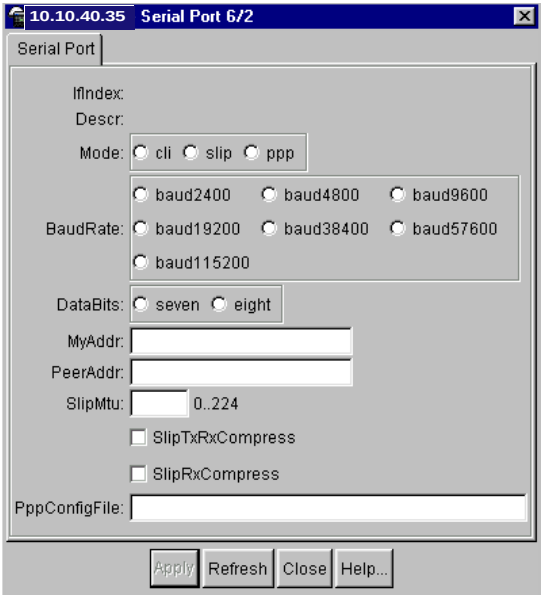



Table 32 describes the Serial Port dialog box fields.

**Table 32** Serial Port dialog box fields

| Field | Description |
|---|---|
| IfIndex | The slot and port number of the serial port. |
| Descr | The description of the serial port. |
| Mode | Specifies the mode this port should operate in. |
| BaudRate | Specifies the baud rate of this port. |
| DataBits | Specifies the number of data bits, per byte of data, this port should send/receive. |
| MyAddr | Specifies this port's IP address. It is used for both “slip” and “ppp” modes. |
| PeerAddr | Specifies the peer's IP address. It is used for both “slip” and “ppp” modes. |
| SlipMtu | Specifies the MTU for this port. |
| SlipTxRxCompress | Enables or disables compression of TCP/IP packet headers on this port. Used for “slip” mode only. |
| SlipRxCompress | Enables or disables compression for receiving packets on this port. Used for “slip” mode only. |
| PppConfigFile | Specifies the configuration file to use PPP. |

## Editing fans

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

To view the fan information:

1. Select the fan object.
2. Do *one* of the following:
   - Double-click the fan object.
   - Right-click the fan object and click Edit.
   - From the Device Manager menu bar, choose Edit > Fan.
   - From the Device Manager menu bar, choose Edit > Select All > Fan. Then choose Edit > Fan.
   - On the Device Manager toolbar, click the Edit Selected button.

To open the Fan dialog box:

1. Select the Fan object.
2. From the Device Manager menu bar, choose Edit > Fan.

   The Fan dialog box opens (Figure 36).

**Figure 36** Fan dialog box

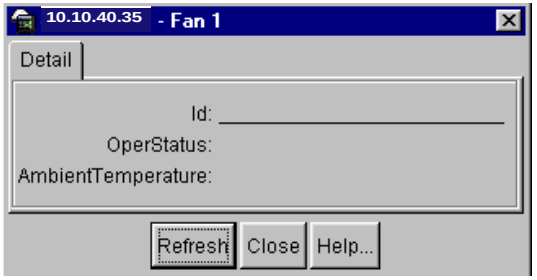



Table 33 describes the Fan dialog box fields.

**Table 33** Fan dialog box fields

| Field | Description |
|---|---|
| Id | The fan ID. |
| OperStatus | Actual status of the Fan:<br>• unknown(1) - status cannot be determined.<br>• up(2) - present and supplying power.<br>• down(3) - present, but failure indicated. |
| AmbientTemperature | Used to indicate the temperature of the air entering the fan. |

## Editing MDAs

The MDA dialog box provides read-only information about the operating status of the switch MDAs.

To view the MDA information:

1. Select the MDA object.
2. Do *one* of the following:
   - Double-click the MDA object.
   - Right-click the MDA object and click Edit.
   - From the Device Manager menu bar, choose Edit > MDA.
   - From the Device Manager menu bar, choose Edit > Select All > MDA. Then choose Edit > MDA.
   - On the Device Manager toolbar, click the Edit Selected button.

To open the MDA dialog box:

1. Select the MDA object.
2. From the Device Manager menu bar, choose Edit > MDA.

   The MDA dialog box opens (Figure 37).

**Figure 37** MDA dialog box

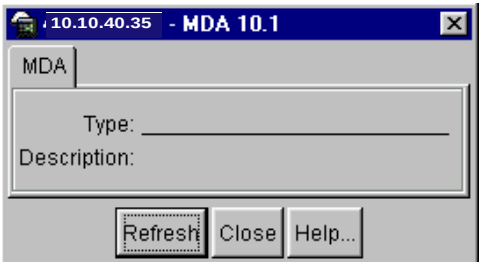



Table 34 describes the MDA fields.

**Table 34** MDA dialog box fields

| Field | Description |
|---|---|
| Type | This field displays the media type of the MDA, either:<br>• OC-3 SMF MDA<br>• OC-3 MMF MDA<br>• OC-12 SMF MDA<br>• OC-12 MMF MDA—rc2klx0c12cBaseMM |
| Description | This field displays a description of the MDA, either:<br>• OC-3 SMFMDA—Quad OC-3 SM<br>• OC-3 MMFMDA—Quad OC-3 MM<br>• OC-12 SMF MDA—Single Port OC-12 SM<br>• OC-12 MMF MDA —Single Port OC-12 MM |

## Editing power supplies

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

To view the power supply information:

1. Select the power supply object.
2. Do *one* of the following:
   - Double-click the power supply object.
   - Right-click the power supply object and click Edit.
   - From the Device Manager menu bar, choose Edit > Power Supply.
   - From the Device Manager menu bar, choose Edit > Select All > Power Supplies. Then choose Edit > Power Supply.
   - On the Device Manager toolbar, click the Edit Selected button.

To open the PowerSupply dialog box:

1. Select the power supply object.
2. On the Device Manager menu bar, choose Edit > Power Supply.

   The PowerSupply dialog box opens (Figure 38).

**Figure 38** PowerSupply dialog box

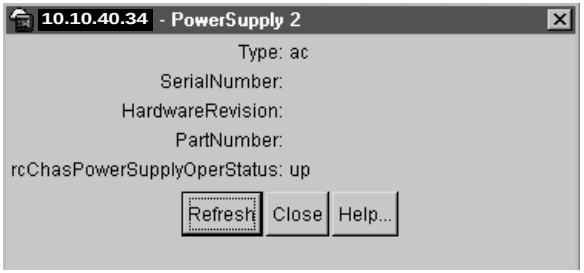



Table 35 describes the Power Supply dialog box fields.

**Table 35** PowerSupply dialog box fields

| Field | Description |
|---|---|
| Type | This field describes the type of power used— AC or DC. |
| SerialNumber | This field defines the serial number of the power supply. |
| HardwareRevision | This field contains the hardware revision number. |
| PartNumber | This field displays the part number of the power supply. |
| rcChasPowerSupplyOperStatus | This field displays the status of the power supply. |

## Editing FileSystem

The FileSystem dialog box allows you to copy files and provides information about flash and PCMCIA files. File copying and file information are all related to files on the switch CPU module.

## Editing copy files

Use the Copy File tab to copy files to or from the switch CPU modules.

To open the Copy File tab:

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

  The FileSystem dialog box opens with the Copy File tab active (Figure 39).

**Figure 39** FileSystem dialog box—Copy File tab

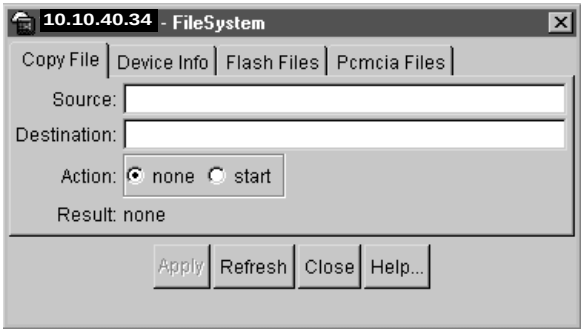



Table 36 describes the Copy File tab fields.

**Table 36** Copy File tab fields

| Field | Description |
|---|---|
| Source | The name or location of the source file to be copied. |
| Destination | The destination name or location where the file is to be copied. |
| Action | Start or Cancel. |
| Result | The result of the copy operation. |

## Displaying flash and PCMCIA statistics

Use the Device Info tab to display flash and PCMCIA file statistics.

To open the Device Info tab:

1. From the Device Manager menu bar, choose Edit > File System.

   The FileSystem dialog box opens with the Copy File tab active.

2. Click the Device Info tab.

   The Device Info tab opens (Figure 40).

**Figure 40** FileSystem dialog box—Device Info tab

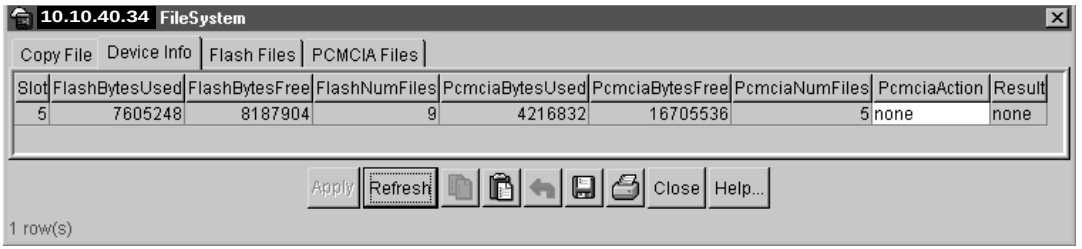



Table 37 describes the Device Info tab fields.

**Table 37** Device Info tab fields

| Field | Description |
|---|---|
| Slot | This is the slot number of the CPU module. |
| FlashBytesUsed | The number of Flash bytes used. |
| FlashBytesFree | The number of Flash bytes free. |
| FlashNumFiles | The number of Flash files. |
| PcmciaBytesUsed | The number of PCMCIA bytes used. |
| PcmciaBytesFree | The number of PCMCIA bytes free. |
| PcmciaNumFiles | The number of PCMCIA files. |
| PcmciaAction | The type of action. None or reset PCMCIA. |
| Result | The results of the last action taken on the device. The valid values are none, in progress, success, or fail. |

## Displaying flash file information

Use the Flash Files tab to display Flash file information.

To open the Flash Files tab:

1 From the Device Manager menu bar, choose Edit > File System.

The FileSystem dialog box opens with the Copy File tab active.

2 Click the Flash Files tab.

The Flash Files tab opens (Figure 41).

**Figure 41** FileSystem dialog box—Flash Files tab

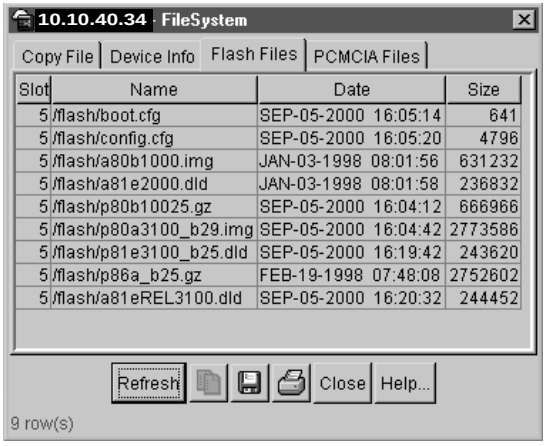



Table 38 describes the Flash Files tab fields.

**Table 38** Flash Files tab fields

| Field | Description |
|---|---|
| Slot | The slot number of the CPU module. |
| Name | The name of the Flash file. |
| Date | The date and time the Flash file was created or modified. |
| Size | The size of the Flash file in bytes. |

## Displaying PCMCIA file information

Use the PCMCIA Files tab to display PCMCIA file information.

To open the PCMCIA Files tab:

1 From the Device Manager menu bar, choose Edit > File System.

The FileSystem dialog box opens with the Copy File tab active.

2 Click the PCMCIA Files tab.

The PCMCIA Files tab opens (Figure 42).

**Figure 42** FileSystem dialog box—PCMCIA Files tab

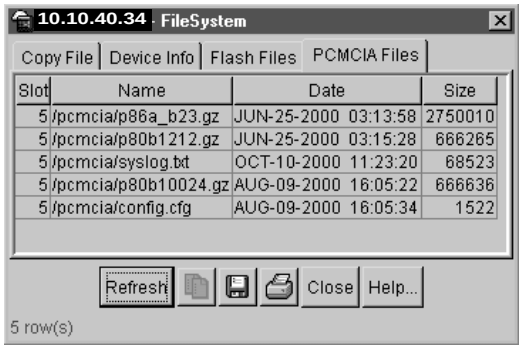



Table 39 describes the Flash Files tab fields.

**Table 39** PCMCIA Files tab fields

| Field | Description |
|---|---|
| Slot | The slot number of the CPU module. |
| Name | The name of the PCMCIA file. |
| Date | The date and time the PCMCIA file was created or modified. |
| Size | The size of the PCMCIA file in bytes. |

## Editing ATM and POS

For complete information on using ATM and POS, refer to *Configuring Switching and Routing Operations for the Passport 8000 Series Switch Using Device Manager Release 5.x.x.*

# Graphing chassis statistics

The following sections discuss the different chassis statistics tabs in the Graph Chassis dialog box with descriptions of the statistics fields.



All graphing chassis tables have the following buttons: Line Chart, Area Chart, Bar Chart, Pie Chart, Export Data, Print table, Clear Counter, Close, and Help. To reset the statistics counters, use the "Clear Counter" button. When you click this button, all Cumulative, Average, Minimum, Maximum, and LastVal columns are reset to zero and automatically begin to recalculate statistical data. (Note that the AbsoluteValue column is NOT cleared.)

To graph chassis statistics:

➔ Select the chassis.

- On the shortcut menu, choose Graph.
- From the Device Manager menu bar, choose Graph > Chassis.
- On the Device Manager toolbar, choose the Graph Selected button.

## Graphing SNMP statistics

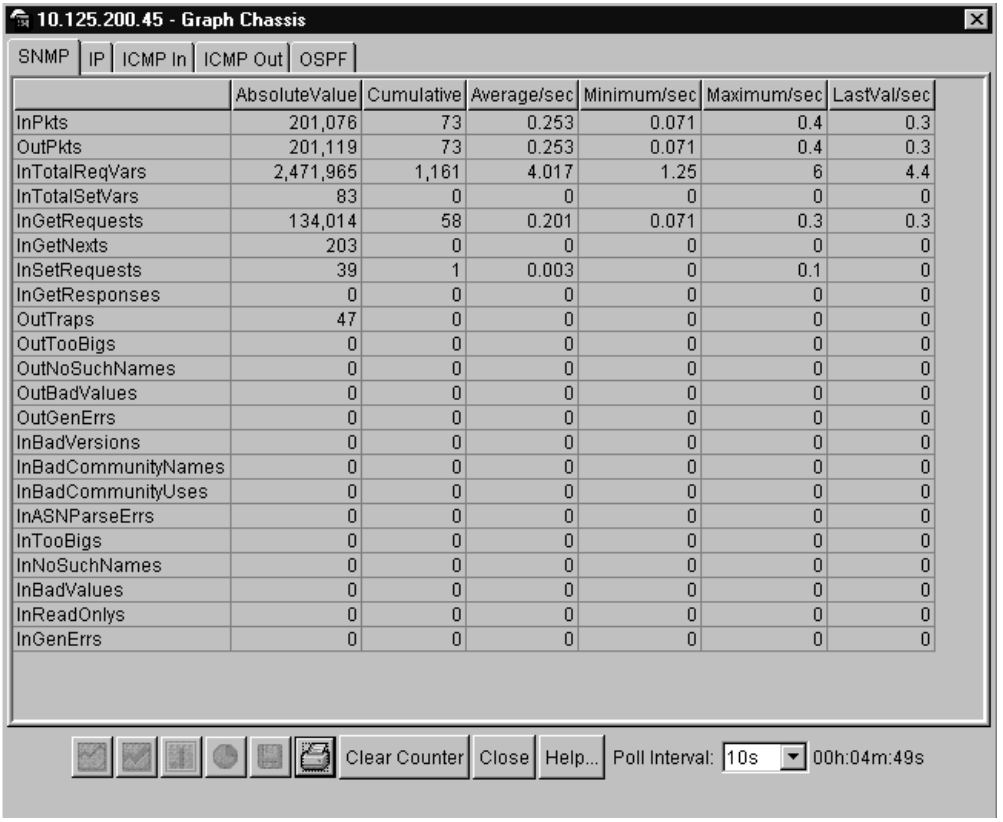
You can graph statistics for all SNMP packets that enter the chassis from different interfaces.

To graph SNMP statistics:

1 From the Device Manager Menu bar, choose Graph > Chassis.

The Graph Chassis dialog box opens with the SNMP tab displayed (Figure 43).

**Figure 43** Graph Chassis dialog box—SNMP tab




| | AbsoluteValue | Cumulative | Average/sec | Minimum/sec | Maximum/sec | LastVal/sec |
|---|---|---|---|---|---|---|
| InPkts | 201,076 | 73 | 0.253 | 0.071 | 0.4 | 0.3 |
| OutPkts | 201,119 | 73 | 0.253 | 0.071 | 0.4 | 0.3 |
| InTotalReqVars | 2,471,965 | 1,161 | 4.017 | 1.25 | 6 | 4.4 |
| InTotalSetVars | 83 | 0 | 0 | 0 | 0 | 0 |
| InGetRequests | 134,014 | 58 | 0.201 | 0.071 | 0.3 | 0.3 |
| InGetNexts | 203 | 0 | 0 | 0 | 0 | 0 |
| InSetRequests | 39 | 1 | 0.003 | 0 | 0.1 | 0 |
| InGetResponses | 0 | 0 | 0 | 0 | 0 | 0 |
| OutTraps | 47 | 0 | 0 | 0 | 0 | 0 |
| OutTooBigs | 0 | 0 | 0 | 0 | 0 | 0 |
| OutNoSuchNames | 0 | 0 | 0 | 0 | 0 | 0 |
| OutBadValues | 0 | 0 | 0 | 0 | 0 | 0 |
| OutGenErrs | 0 | 0 | 0 | 0 | 0 | 0 |
| InBadVersions | 0 | 0 | 0 | 0 | 0 | 0 |
| InBadCommunityNames | 0 | 0 | 0 | 0 | 0 | 0 |
| InBadCommunityUses | 0 | 0 | 0 | 0 | 0 | 0 |
| InASNParseErrs | 0 | 0 | 0 | 0 | 0 | 0 |
| InTooBigs | 0 | 0 | 0 | 0 | 0 | 0 |
| InNoSuchNames | 0 | 0 | 0 | 0 | 0 | 0 |
| InBadValues | 0 | 0 | 0 | 0 | 0 | 0 |
| InReadOnlys | 0 | 0 | 0 | 0 | 0 | 0 |
| InGenErrs | 0 | 0 | 0 | 0 | 0 | 0 |

Table 40 describes the SNMP tab fields.

**Table 40** SNMP tab fields

| Field | Description |
|---|---|
| InPkts | The total number of messages delivered to the SNMP entity from the transport service. |
| OutPkts | The total number of SNMP messages passed from the SNMP protocol entity to the transport service. |
| InTotalReqVars | The total number of MIB objects retrieved successfully by the SNMP protocol entity 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 entity as the result of receiving valid SNMP Set-Request PDUs. |
| InGetRequests | The total number of SNMP Get-Request PDUs that have been accepted and processed by the SNMP protocol entity. |
| InGetNexts | The total number of SNMP Get-Next PDUs accepted and processed by the SNMP protocol entity. |
| InSetRequests | The total number of SNMP Set-Request PDUs accepted and processed by the SNMP protocol entity. |
| InGetResponses | The total number of SNMP Get-Response PDUs accepted and processed by the SNMP protocol entity. |
| OutTraps | The total number of SNMP Trap PDUs generated by the SNMP protocol entity. |
| OutTooBigs | The total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is tooBig. |
| OutNoSuchNames | The total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is noSuchName. |
| OutBadValues | The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field is ‘badValue’. |
| OutGenErrs | The total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is genErr. |
| InBadVersions | The total number of SNMP messages delivered to the SNMP protocol entity for an unsupported SNMP version. |

**Table 40** SNMP tab fields (continued)

| Field | Description |
|---|---|
| InBadCommunityNames | The total number of SNMP messages delivered to the SNMP protocol entity that used an SNMP community name not known to said entity. |
| InBadCommunityUses | The total number of SNMP messages delivered to the SNMP protocol entity 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 entity when decoding received SNMP messages. |
| InTooBigs | The total number of SNMP PDUs delivered to the SNMP protocol entity for which the value of the error-status field is tooBig. |
| InNoSuchNames | The total number of SNMP PDUs delivered to the SNMP protocol entity for which the value of the error-status field is noSuchName. |
| InBadValues | The total number of SNMP PDUs delivered to the SNMP protocol entity for which the value of the error-status field is badValue. |
| InReadOnlys | The total number of SNMP PDUs delivered to the SNMP protocol entity 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 entity for which the value of the error-status field is genErr. |

## Graphing IP statistics

You can graph statistics for all IP packets that enter the chassis from different interfaces.

To graph IP statistics:

1 From the Device Manager Menu bar, choose Graph > Chassis.

The graphChassis dialog box opens with the SNMP tab displayed.

**2** Click the IP tab.

The IP tab opens (Figure 44).

**Figure 44** graphChassis dialog box—IP tab

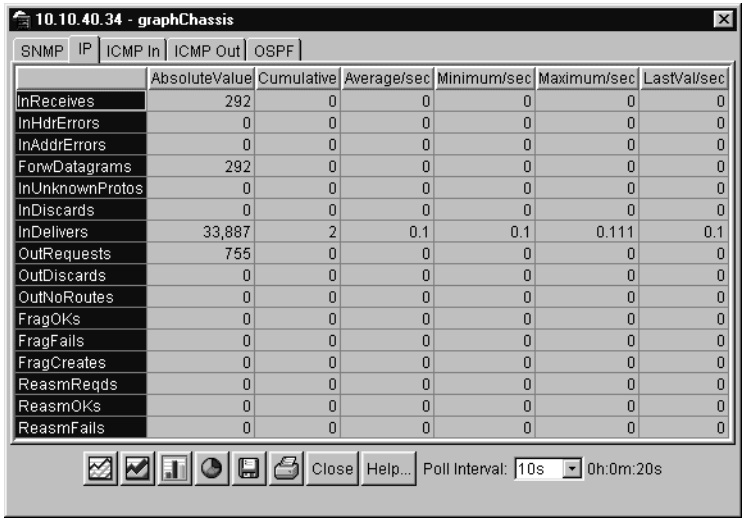



Table 41 describes the IP tab fields.

**Table 41** 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 their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities 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 41** 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. In entities that do not act as IP Gateways, this counter will include only those packets that were Source-Routed by way of this entity 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. This counter 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 41** 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, and so on). Note that this number 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. |

## Graphing ICMP In statistics

You can graph statistics for all ICMP packets received into the chassis from different interfaces.

To graph ICMP In statistics:

1. From the Device Manager menu bar, choose Graph > Chassis.

   The graphChassis dialog box opens with the SNMP In tab displayed.

2. Click the ICMP In tab.

   The ICMP In tab opens (Figure 45).

**Figure 45** graphChassis dialog box—ICMP In tab

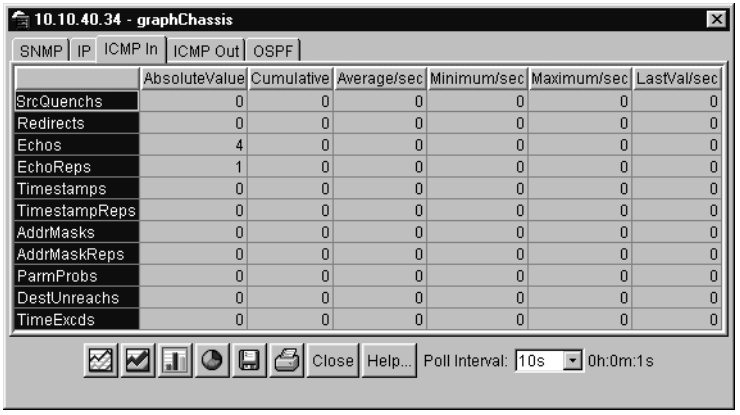


Table 42 describes the ICMP In tab fields.

**Table 42** 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. |

## Graphing ICMP Out statistics

You can graph statistics for all ICMP messages sent.

To graph ICMP Out statistics:

1 From the Device Manager menu bar, choose Graph > Chassis.

The graphChassis dialog box opens with the SNMP Out tab displayed.

2 Click the ICMP Out tab.

The ICMP Out tab opens (Figure 46).

**Figure 46** graphChassis—ICMP Out tab

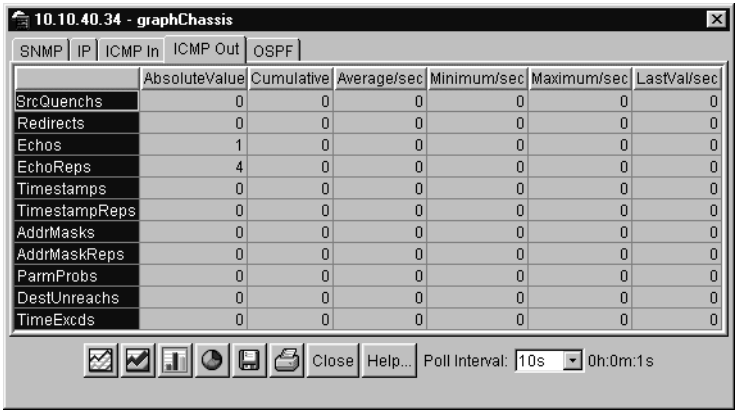



Table 43 describes the ICMP Out tab fields.

**Table 43** 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. |

**Table 43** ICMP Out tab fields (continued)

| Field | Description |
|---|---|
| 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. |

## Graphing OSPF statistics

You can graph statistics for all OSPF packets transmitted by the switch.

To graph OSPF statistics:

1. From the Device Manager menu bar, choose Graph > Chassis.

   The graphChassis dialog box opens with the SNMP tab displayed.

2. Click the OSPF tab.

   The OSPF tab opens (Figure 47).

**Figure 47** graphChassis dialog box—OSPF tab

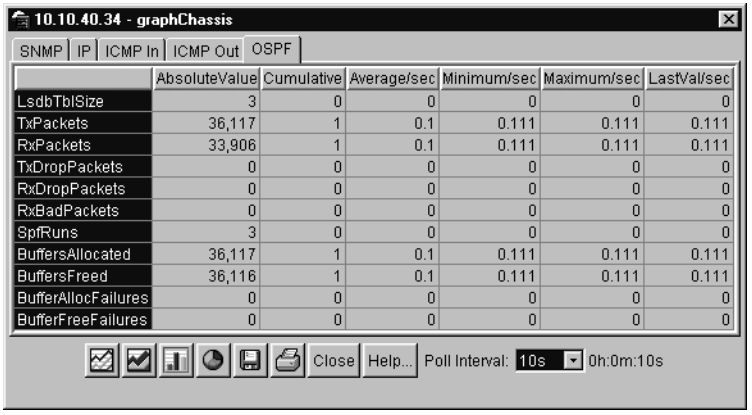


Table 44 describes the OSPF tab fields.

**Table 44** OSPF tab fields

| Field | Description |
|---|---|
| LsdbTblSize | The number of entries in the link state database table. |
| TxPackets | The number of packets transmitted by OSPF. |
| RxPackets | The number of packets received by OSPF. |
| TxDropPackets | The number of packets dropped before being transmitted by OSPF. |
| RxDropPackets | The number of packets dropped before they are received by OSPF. |
| RxBadPackets | The number of packets received by OSPF that are bad. |
| SpfRuns | The number of SPF calculations performed by OSPF. |
| BuffersAllocated | The number of buffers allocated for OSPF. |
| BuffersFreed | The number of buffers freed by OSPF. |
| BufferAllocFailures | The number of times that OSPF has failed to allocate buffers. |
| BufferFreeFailures | The number of times that OSPF has failed to free buffers. |

# Chapter 4
# Port configuration and graphing

This chapter describes editing and graphing layer 2 port functions on a Passport 8000 Series switch and contains the following topics:



## Configuring a port

This section describes the following topics:

## Editing ports

To edit a single port or multiple ports:

1. Select the port or ports you want to edit.
2. Do *one* of the following:
   - Double-click a port.
   - Right-click a port. On the shortcut menu, choose Edit.
   - From the Device Manager menu bar, choose Edit > Port.
   - On the Device Manager toolbar, choose the Edit Selected button.

**Note:** When you edit a single port, dialog boxes and tabs that are not applicable are not available for selection.

When you edit multiple ports, some options are not available, and other options appear to be available even though the dialog box or tab is not applicable. When a dialog box or tab does not apply for a given port, NoSuchObject is displayed.

## Setting a basic configuration

You can set options for a basic port configuration through the Interface tab in the Port dialog box (Figure 48).

**Note:** Additional tabs and screen entries for module-specific functions appear when applicable. For example, on the Interface dialog box for a port, tabs for layer 3 (routing) functions would appear if Device Manager were accessing a Passport 8600 module.

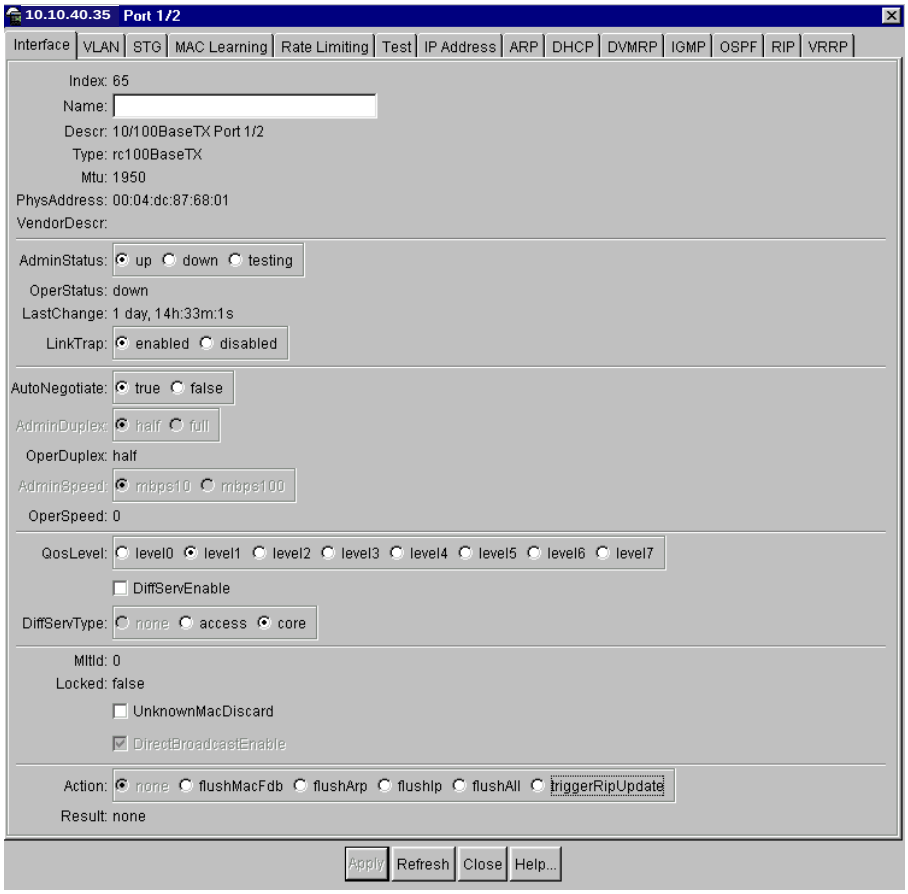
To set a basic configuration:

1. On the device view, select a port or multiple ports.

**2** From the Device Manager menu bar, choose Edit > Port.

The Port dialog box opens with the Interface tab displayed (Figure 48).

**Figure 48** Port dialog box—Interface tab




**Note:** The 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, the settings can be manually configured for the link in question. Check the Nortel Networks Web site (nortelnetworks.com) for the latest compatibility information.

Table 45 describes the Interface tab fields.

**Table 45** Interface tab fields

| Field | Description |
|---|---|
| Index | A unique value assigned to each interface. The value ranges between 64 and 511. |
| Name | The name given to the port. |
| Descr | The port type of this interface. |
| Type | The media type of this interface. |
| Mtu | The size of the largest packet, in octets, that can be sent/ received on the interface. |
| PhysAddress | The MAC address assigned to a particular interface. |
| VendorDescr | The name of the interface chipset. (May not apply to all port types.) |
| AdminStatus | One of the following states:<br>• up<br>• down<br>• testing<br>When a managed system initializes, all interfaces start with AdminStatus in the up state. As a result of either explicit management action or per configuration information retained by the managed system, AdminStatus is then changed to either the down or the testing state (or remains in the down state). The testing state indicates that no operational packets can be passed. |
| OperStatus | The current operational state of the interface. One of the following states:<br>• up<br>• down<br>• testing<br>The testing state indicates that no operational packets can be passed. If AdminStatus is down, then OperStatus should be down. If AdminStatus is changed to up, then OperStatus should change to up if the interface is ready to transmit and receive network traffic. It should remain in the down state if and only if there is a fault that prevents it from going to the up state. |

**Table 45** Interface tab fields (continued)

| Field | Description |
|---|---|
| LastChange | The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero. |
| LinkTrap | Indicates whether or not link Up/link Down traps should be generated for this interface. |
| AutoNegotiate | Indicates whether this port is enabled for autonegotiations or not (only 10/100BASE ports). |
| AdminDuplex | Indicates the port's current duplex value (half-duplex or full-duplex mode). |
| OperDuplex | The current operational duplex mode of the port (half or full). |
| AdminSpeed | Indicates the port's speed (10 Mb/s or 100 Mb/s). |
| OperSpeed | The current operating speed of the port. |
| QosLevel | Quality of service level. |
| DiffServEnable | Used to enable differentiated services on this port. |
| DiffServType | Sets the type of differentiated service to none, access or core. |
| MltId | The MultiLink Trunk to which the port is assigned (if any). |
| Locked | Indicates whether or not the port is locked. When locked, the port configuration cannot be changed. To lock or unlock a port, select Edit > Security > Port Lock. |
| UnknownMacDiscard | If rcUnknownMacDiscard is set to True, then a packet with an unknown source MAC address is dropped on that port, and other ports then will discard any packets with this MAC address in the destination field. For example, suppose 11:22:33:44:55:66 is an unknown source MAC. Packets with source MAC 11:22:33:44:55 coming from this port are discarded; furthermore, packets with destination MAC 11:22:33:44:55:66 coming from other ports are also discarded, unless this address is later learned on another port or the restriction ages out. |
| DirectBroadcastEnable | Used to indicate whether this interface should forward direct broadcast traffic. |

**Table 45** Interface tab fields (continued)

| Field | Description |
|---|---|
| Action | One of the following port-related actions:<br>• none<br>• flushMacFdb—flush MAC forwarding table for port<br>• flushArp—flush ARP table for port<br>• flushIp—flush IP route table for port<br>• flushAll—flush all tables for port<br>• triggerRipUpdate—manually update the RIP table |
| Result | The result of port-related actions. |

## Defining primary and backup connectors

If you have ports with redundant connectors, a Dual tab appears. This tab allows you to define which of the connectors is the Primary connector.

To open the Dual tab:

1. On the device view, select a port or multiple ports.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.
3. Click the Dual tab.

   The Dual tab opens (Figure 49).

**Figure 49** Port dialog box—Dual tab

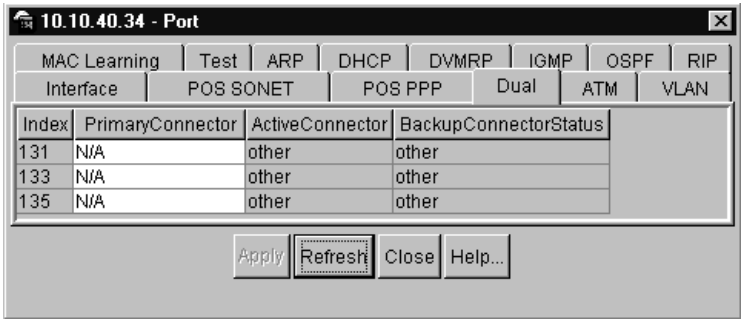


Table 46 describes the Port Dual tab fields.

**Table 46** Dual tab fields

| Field | Description |
|---|---|
| PrimaryConnector | Indicates which connector to use as the active connector on the port the next time that the port is placed into the ifAdminStatus=up. |
| ActiveConnector | Indicates which connector is currently the active connector. Only one connector can be active at any time. |
| BackupConnectorStatus | Indicates the status of the link attached to the backup (nonactive) connector. |

## Configuring VLANs

You can configure VLANs to tag or untag discarded frames for a port.

To configure VLANs:

1. On the device view, select a port or multiple ports.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.
3. Click the VLAN tab.

   The VLAN tab opens (Figure 50).

**Figure 50** Port dialog box—VLAN tab

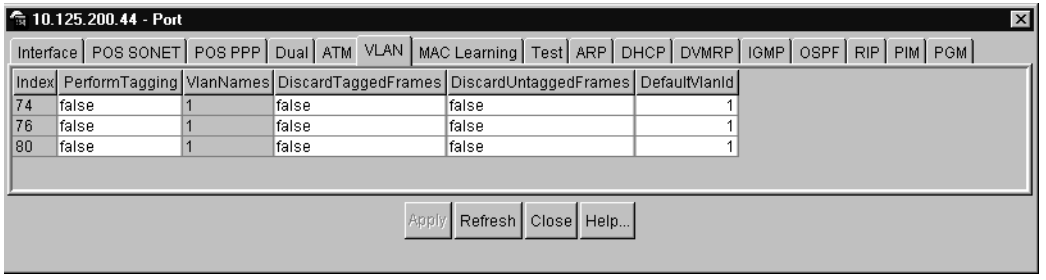


Table 47 describes the VLAN tab fields.

**Table 47** VLAN tab fields

| Field | Description |
|---|---|
| Index | |
| PerformTagging | Enable or disable the port on the current VLAN to perform tagging on the incoming and outgoing traffic. |
| VlanNames | This field is used to identify which VLANs this port is assigned. Each VLAN ID is stored as a two octet value. The first octet in the pair holds bits 15-8 of the VLAN ID, the second octet holds bits 7-0 of the VLAN ID. |
| DiscardTaggedFrames | This flag is used to determine how to process tagged frames received on this access port. When the flag is set, these frames are discarded by the forwarding process. When the flag is reset, these frames are processed normally. |
| DiscardUntaggedFrames | This flag is used to determine how to process untagged frames received on this tagged port. When the flag is set, these frames are discarded by the forwarding process. When the flag is reset, these frames are assigned to the VLAN specified by the DefaultVlanId. |
| DefaultVlanId | The VLAN ID assigned to untagged frames. |

## Configuring spanning tree groups

You can configure a port's spanning tree parameters through the STG (Spanning Tree Group) tab in the Port dialog box.

**Note:** When you edit multiple ports, the spanning tree options are not displayed.

To configure a spanning tree group:

1 On the device view, select a port.

2 From the Device Manager menu bar, choose Edit > Port.

The Port dialog box opens with the Interface tab displayed.

3 Click the STG tab.

The STG tab opens (Figure 51).

**Figure 51** Port dialog box—STG tab

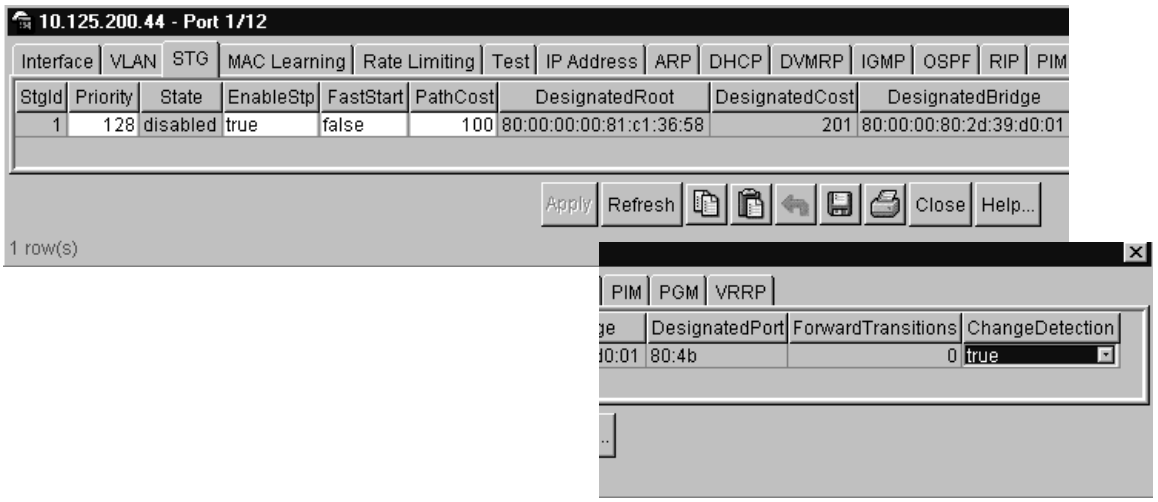



Table 48 describes the STG tab fields.

**Table 48** STG tab fields

| Field | Description |
|---|---|
| StgID | The spanning tree group ID. |
| 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 given by the value of dot1dStpPort. |
| State | The port's current state as defined by application of the Spanning Tree Protocol. This state controls what action a port takes on reception of a frame. If the bridge has detected a port that is malfunctioning, it will place that port into the broken state. For ports that are disabled (see EnableStp), this object will have a value of disabled. |

**Table 48** STG tab fields (continued)

| Field | Description |
|---|---|
| EnableStp | The enabled/disabled spanning tree status of the port, which will affect only the operation of the Spanning Tree Protocol on the port. Disabling STP at the spanning tree group will take precedence over what is configured here. |
| FastStart | When FastStart is true, the port is enabled in the Forwarding state upon being enabled. If the port receives a spanning tree BPDU, the port will start normal STP negotiations. |
| 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. |
| ChangeDetection | If this field is disabled, topology change notifications are not sent for the port. |

## Configuring MAC learning parameters

You can configure the MAC learning parameters to control high-security environments that restrict access to the network. This feature is based on the layer 2 media access control (MAC) address of the network devices connected to the Passport switch.

To configure the MAC learning parameters:

**1** On the device view, select a port or multiple ports.

2 From the Device Manager menu bar, choose Edit > Port.

The Port dialog box opens with the Interface tab displayed.

3 Click the MAC Learning tab.

The MAC Learning tab opens (Figure 52).

**Figure 52** Port dialog box—MAC Learning tab

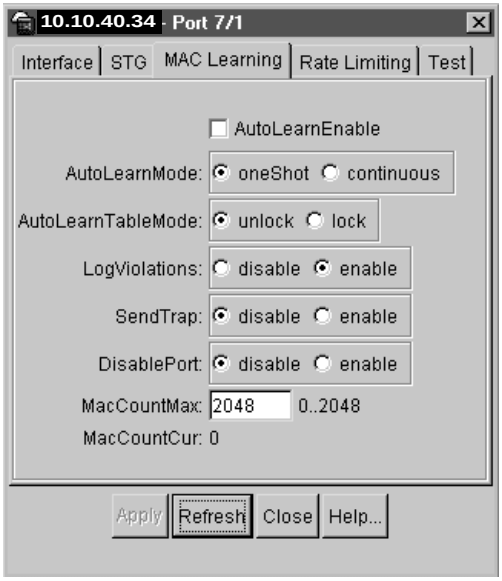



Table 49 describes the MAC Learning tab fields.

**Table 49** MAC Learning tab fields

| Field | Description |
|---|---|
| AutoLearnEnable | Sets the port to autolearn addresses for the allowed MAC table. |
| AutoLearnMode | Sets the autolearn mode on the port for populating the allowed MAC table. |
| AutoLearnTableMode | Sets the allowed MAC table to current state. When locked, no new MAC addresses will be learned. |

**Table 49** MAC Learning tab fields (continued)

| Field | Description |
|---|---|
| LogViolations | Enables the system to create a system log entry when a disallowed MAC address attempts to send traffic through the selected port. |
| SendTrap | Enables the system to send an SNMP trap when a disallowed MAC address attempts to send traffic through the selected port. |
| DisablePort | Enables the system to administratively down the port when a disallowed MAC address attempts to send traffic. To bring the port back up, the administrator must manually enable the selected port or reboot the system. Choosing enable in this field automatically disables the selected port when an intrusion occurs. |
| MacCountMax | This variable represents the maximum number of MAC addresses that can be added to a port. |
| MacCountCur | This variable represents the current number of MAC addresses that have been added to a port. |

## Setting rate limits

You can set the rate limit of broadcast or multicast packets for a port.

To set the rate limit:

1. On the device view, select a port or multiple ports.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.
3. Click the Rate Limiting tab.

   The Rate Limiting tab opens (Figure 53).

**Figure 53** Port dialog box—Rate Limiting tab

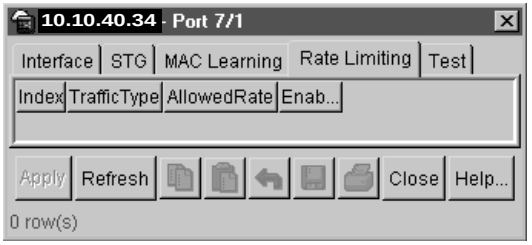



Table 50 describes the Rate Limiting tab fields.

**Table 50** Rate Limiting tab fields

| Field | Description |
|---|---|
| Index | The port number. |
| TrafficType | The type of traffic being rate limited—either broadcast or multicast traffic. |
| AllowedRatePps | This variable is the allowed traffic rate limit for the port.<br>For Passport 8100 Switch switches, 1.. 25 sets the limit in a percentage of the total bandwidth on the port between 1% and 25%.<br>For Passport 8600 Switch switches, 1... 65535 sets the limit in packets per second. |
| Enable | Enable or disable rate limiting. |

## Testing ports

A DRAM memory test and an internal loopback test are run during the automatic boot sequence. However, you can also run external and internal loopback tests on the port.

**Note:** You can run only one loopback test at a time. You *must* stop a loopback test before you start one on another port.

To open the Test tab:

1 On the device view, select a port or multiple ports.

2 From the Device Manager menu bar, choose Edit > Port.

The Port dialog box opens with the Interface tab displayed.

3 Click the Test tab.

The Test tab opens (Figure 54).

**Figure 54** Port dialog box—Test tab

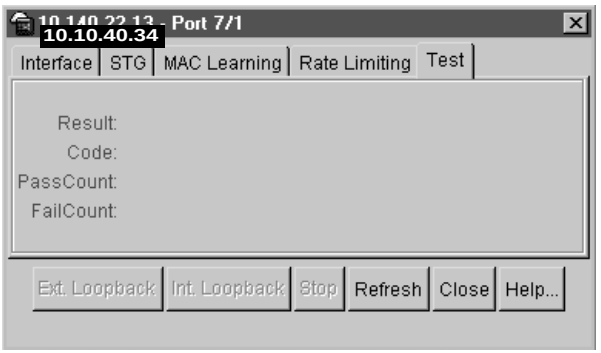



Table 51 on page 129 describes the Test tab fields.

## Performing an external loopback test

An external loopback test uses a loopback connector connected to the port to loop data back to the same port.

**Note:** For information about performing F5 loopback testing, see *Using the Passport 8672ATME Module*.

**Note:** You must supply the loopback connector.

To perform an external loopback test on a port:

1 Plug in an external loopback connector.

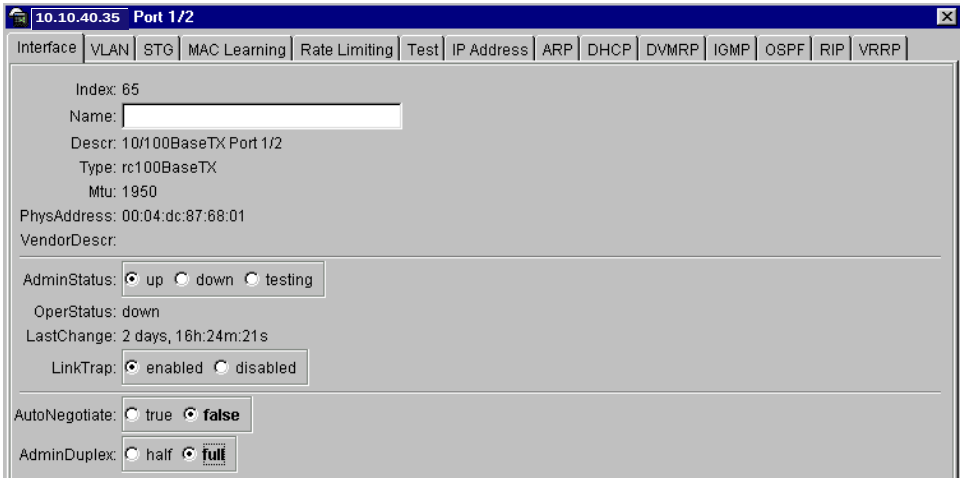
2 From the Device Manager menu bar, choose Edit >Port.

The Port dialog box opens with the Interface tab displayed (Figure 55).

3 Set AutoNegotiate to false.

4 Set Admin Duplex to full.

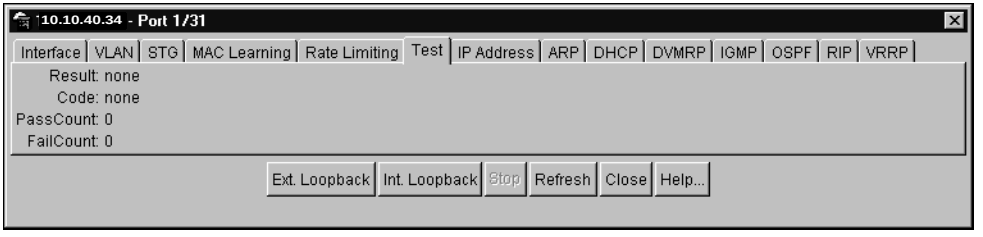
**Figure 55** Interface tab




5 Click the Test tab.

The Test tab opens (Figure 56).

**Figure 56** Test tab




6 Click Ext. Loopback.

Let the test run for several seconds.

7 Click Stop to stop the test.

The result, Fail or Success, is shown along with packet counts.

## Performing an internal loopback test

During an internal loopback test, packets are looped back at the PHY device. No connector is needed, as in the external loopback test, and you can run the test with or without another device attached to the test port.

To perform an internal loopback test on a port:

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

   The Port dialog box opens with the Interface tab displayed.

2. Set AdminStatus to testing.
3. Click the Test tab.

   The Test tab opens (Figure 56).

4. Click Int. Loopback.

   Let the test run for several seconds.

5. Click Stop to stop the test.

   The result, Fail or Success, is shown along with packet counts.

Table 51 describes the Test tab fields.

**Table 51** Test tab fields

| Field | Description |
|---|---|
| Result | The result of the most recently run (or current) test:<br>• None<br>• Success<br>• InProgress<br>• NotSupported<br>• unAbleToRun<br>• Aborted<br>• Failed<br>The code contains more specific information on the test result (for example, an error code after a failed test):<br>• NoReceive (timeout on a send)<br>• BadSeq (packets received out of sequence)<br>• BadLen (packet length mismatch)<br>• BadData (packet data mismatch) |
| Code | This object contains a code which contains more specific information on the test results, for example an error-code after a failed test. Error codes and other values this object may take are specific to the type of interface and/or test. The value may have the semantics of either the Autonomous Type or InstancePointer textual conventions as defined in RFC 1443. The identifier: testCodeUnknown OBJECT IDENTIFIER ::={0 0} is defined for use if no additional result code is available. |
| PassCount | The number of iterations of the loopback test completed successfully. |
| FailCount | The number of iterations of the loopback test failed. |

## Configuring routing operations

The following tabs in the Port dialog box are used for layer 3 routing and are discussed in *Configuring Switching and Routing Operations for the Passport 8000 Series Switch Using Device Manager Release 5.x.x*:

- IP Address tab
- ARP tab
- DHCP tab

- DVMRP tab
- IGMP tab
- OSPF tab
- RIP tab
- VRRP tab

**Note:** This information applies to Passport 8600 modules only.

# Graphing port statistics

The following sections discuss the different port statistics tabs in the Graph Port dialog box with descriptions of the statistics fields.

All graphing port tables have the following buttons: Line Chart, Area Chart, Bar Chart, Pie Chart, Export Data, Print table, Clear Counter, Close, and Help. To reset the statistics counters, use the “Clear Counter” button. When you click this button, all Cumulative, Average, Minimum, Maximum, and LastVal columns are reset to zero and automatically begin to recalculate statistical data. (Note that the AbsoluteValue column is NOT cleared.)

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

To graph port statistics for a single or multiple ports:

1. Select the port or ports you want to graph.
2. Do *one* of the following:
   - Right-click a port or ports. On the shortcut menu, choose Graph**.**
   - From the Device Manager menu bar, choose Graph > Port.
   - On the Device Manager toolbar, click the Graph Selected button.

## Graphing interface statistics

Use the Graph Interface tab to graph interface statistics.

To graph interface statistics:

1. On the device view, select a port or multiple ports.
2. From the Device Manager menu bar, choose Graph > Port.

   The graphPort dialog box opens with the Interface tab displayed (Figure 57).

**Figure 57** graphPort dialog box—Interface tab

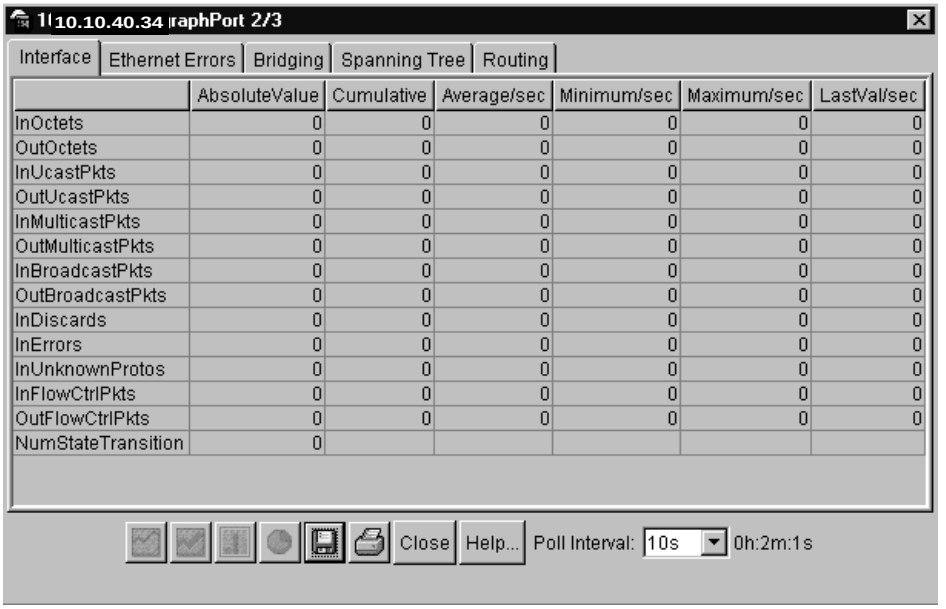



Table 52 describes the Interface tab fields in the graphPort dialog box.

**Table 52** Interface tab fields

| Field | Description |
|---|---|
| InOctets | The total number of octets received on the interface, including framing characters. |
| OutOctets | The total number of octets transmitted out of the interface, including framing characters. |
| InUcastPkts | 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. |
| OutUcastPkts | 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 not sent. |
| InMulticastPkts | The number of packets delivered by this sublayer to a higher sublayer that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses. |
| OutMulticastPkts | The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a multicast address at this sublayer, including those that were discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses. |
| InBroadcastPkts | The number of packets delivered by this sublayer to a higher sublayer that were addressed to a broadcast address at this sublayer. |
| OutBroadcastPkts | The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this sublayer, including those that were discarded or not sent. |
| InDiscards | The number of inbound packets that were discarded because of frames with errors or invalid frames or, in some cases, to fill 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 52** Interface tab fields (continued)

| Field | Description |
|---|---|
| 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. |
| InFlowCtrlPkts | The total number of flow control packets received by this interface. |
| OutFlowCtrlPkts | The total number of flow control packets transmitted by this interface. |
| NumStateTransition | The number of times the port went in and out of service; the number of state transitions from up to down. |

## Graphing Ethernet error statistics

Use the Ethernet Errors tab to graph Ethernet error statistics.

To graph Ethernet Error statistics:

1. On the device view, select a port or multiple ports.
2. From the Device Manager menu bar, choose Graph > Port.

   The graphPort dialog box opens with the Interface tab displayed.
3. Click the Ethernet Errors tab.

   The Ethernet Errors tab opens (Figure 58).

**Figure 58** graphPort dialog box—Ethernet Errors tab

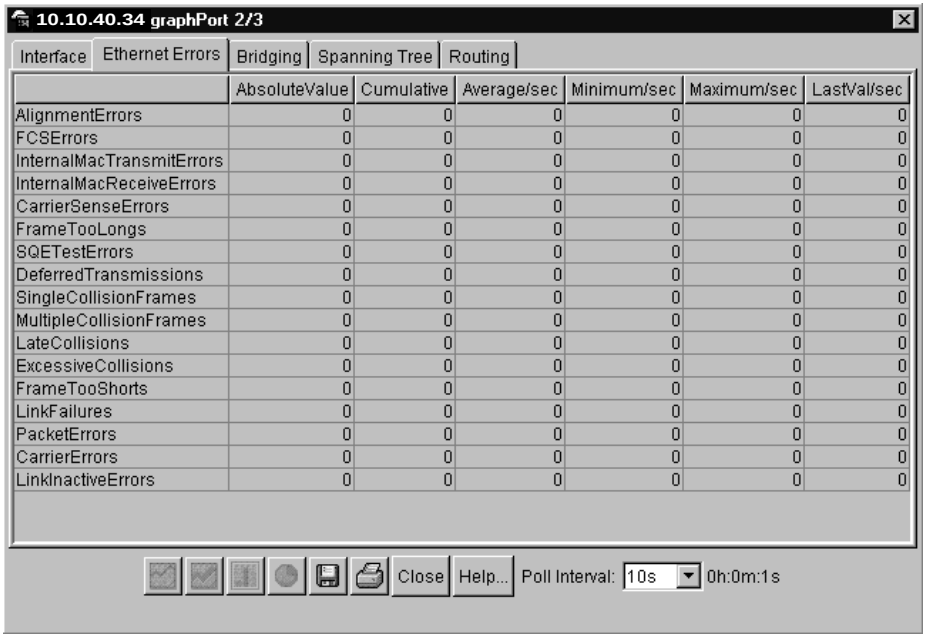



Table 53 describes the Ethernet Errors tab fields.

**Table 53** 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 obtain 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 obtained 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 dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors 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 transmission errors on a particular interface that are not otherwise counted. |
| InternalMacReceiveErrors | A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsFrameTooLongs object, the dot3StatsAlignmentErrors object, or the dot3StatsFCSErrors 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. |

**Table 53** Ethernet Errors tab fields (continued)

| Field | Description |
|---|---|
| CarrierSenseErrors | The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt. |
| FrameTooLongs | A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. |
| SQETestErrors | A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation described in section 7.2.4.6 of the same document. |
| DeferredTransmissions | A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions. |
| SingleCollisionFrames | A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, objects and is not counted by the corresponding instance of the dot3StatsMultipleCollisionFrames object. |
| MultipleCollisionFrames | A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, objects and is not counted by the corresponding instance of the dot3StatsSingleCollisionFrames 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; 512 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. |

**Table 53** Ethernet Errors tab fields (continued)

| Field | Description |
|---|---|
| ExcessiveCollisions | A count of frames for which transmission on a particular interface fails due to excessive collisions. |
| FrameTooShorts | The total number of frames that are too short that were encountered on this interface. |
| LinkFailures | The total number of link failures encountered on this interface. |
| PacketErrors | The total number of packet errors encountered on this interface. |
| CarrierErrors | The total number of carrier errors encountered on this interface. |
| LinkInactiveErrors | The total number of link inactive errors encountered on this interface. |

## Graphing bridging statistics

Use the Bridging tab to graph port bridging statistics.

To graph Bridging statistics:

1. On the device view, select a port or multiple ports.
2. From the Device Manager menu bar, choose Graph > Port.

   The graphPort dialog box opens with the Interface tab displayed.
3. Click the Bridging tab.

   The graphPort dialog box opens with the Bridging tab displayed (Figure 59).

**Figure 59** graphPort dialog box—Bridging tab

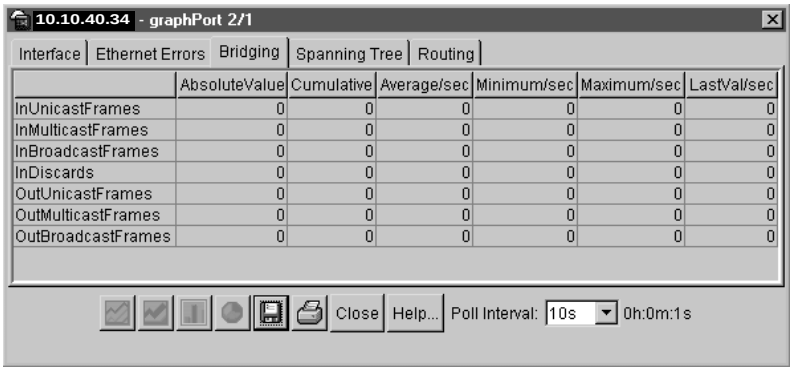



Table 54 describes the Bridging tab fields.

**Table 54** Bridging tab fields

| Field | Description |
|---|---|
| InUnicastFrames | The total number of incoming unicast frames bridged. |
| InMulticastFrames | The total number of incoming multicast frames bridged. |
| InBroadcastFrames | The total number of incoming broadcast frames bridged. |
| InDiscards | The total number of frames discarded by the bridging entity. |
| OutUnicastFrames | The total number of outgoing unicast frames bridged. |
| OutMulticastFrames | The total number of outgoing multicast frames bridged. |
| OutBroadcastFrames | The total number of outgoing broadcast frames bridged. |

## Graphing spanning tree statistics

Use the Spanning Tree tab to graph port spanning tree statistics.

To graph spanning tree statistics:

1. On the device view, select a port or multiple ports.
2. From the Device Manager menu bar, choose Graph > Port.

   The graphPort dialog box opens with the Interface tab displayed.

**3** Click the Spanning Tree tab.

The graphPort dialog box opens with the Spanning Tree tab displayed (Figure 60).

**Figure 60** graphPort dialog box—Spanning Tree tab

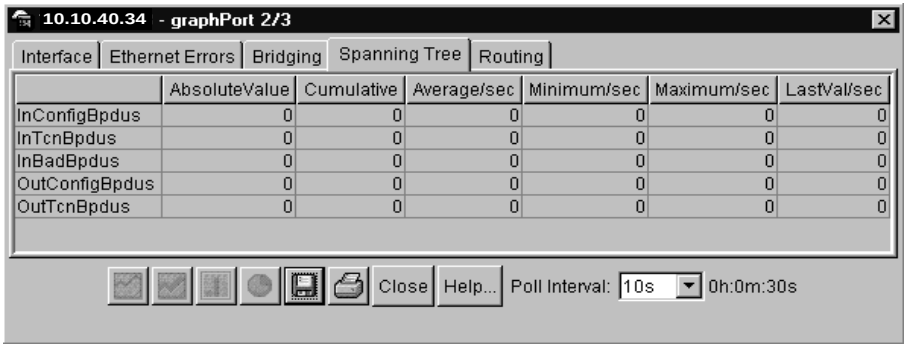



Table 55 describes the Spanning Tree tab fields.

**Table 55** Spanning Tree tab fields

| Field | Description |
|---|---|
| InConfigBpdus | The number of Config BPDUs received. |
| InTcnBpdus | The number of Topology Change Notification BPDUs received. |
| InBadBpdus | The number of unknown or malformed BPDUs received. |
| OutConfigBpdus | The number of Config BPDUs transmitted. |
| OutTcnBpdus | The number of Topology Change Notification BPDUs transmitted. |

## Graphing unicast and multicast traffic statistics

Use the Routing tab to graph port routing statistics.

To graph unicast and multicast traffic statistics:

**1** On the device view, select a port or multiple ports.

2 From the Device Manager menu bar, choose Graph > Port.

The graphPort dialog box opens with the Interface tab displayed.

3 Click the Routing tab.

The graphPort dialog box opens with the Routing tab displayed (Figure 61).

4 Select the statistic(s) you want to graph.

5 In the Poll Interval box, select the polling interval.

6 Click the Graph button (bar, pie, chart, line).

**Figure 61** graphPort dialog box—Routing tab

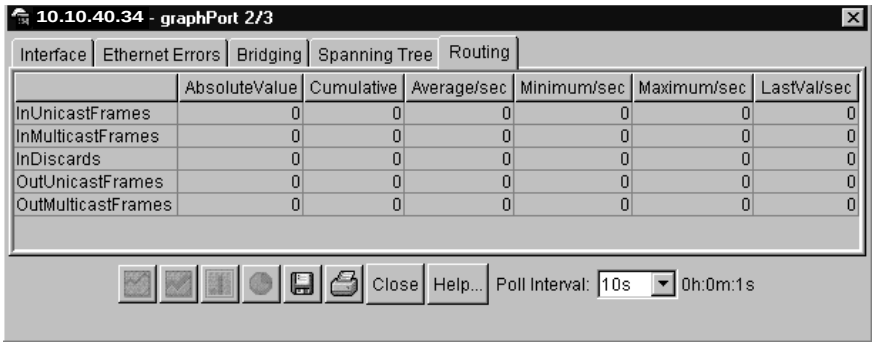



Table 56 describes the Routing tab fields.

**Table 56** Routing tab fields

| Field | Description |
|---|---|
| InUnicastFrames | The total number of incoming unicast frames routed. |
| InMulticastFrames | The total number of incoming multicast frames routed. |
| InDiscards | The total number of frames discarded by the routing entity. |
| OutUnicastFrames | The total number of outgoing unicast frames routed. |
| OutMulticastFrames | The total number of outgoing multicast frames routed. |

# Graphing RMON statistics

Use the following procedure to enable RMON globally, enable Rmon Stats on a selected port, and use the RMON tab to graph RMON statistics.

To graph RMON statistics for a single port or multiple ports:

1. From the Device Manager menu bar, choose RMON > Options.
2. Click Enable.
3. Click Apply and then Close.
4. Right click on the port you want to graph.
5. Select Enable Rmon Stats.
6. From the Device Manager menu bar, choose Graph > Port.

   The graphPort dialog box opens with the Interface tab displayed.
7. Click the RMON tab.

   The RMON tab opens (Figure 62).

**Figure 62** graphPort dialog box—RMON tab

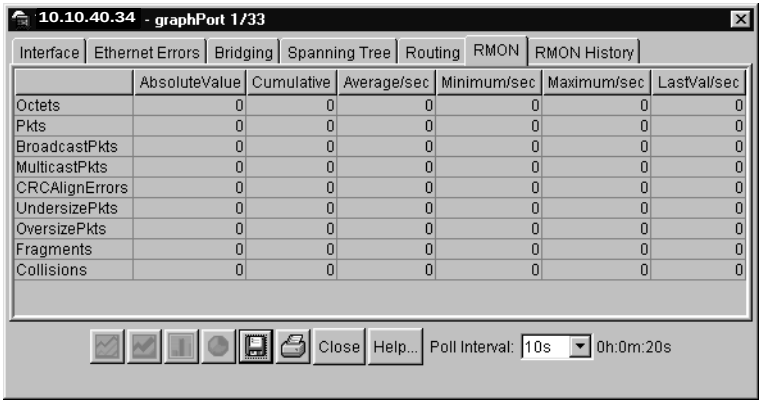



Table 57 describes the fields in the RMON tab.

**Table 57** 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. |
| Packets | 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 number does not include multicast packets. |
| MulticastPkts | The total number of good packets received that were directed to the multicast address. Note that this number does not include packets directed to the broadcast address. |
| CRCAlignErrors | 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 more than 1518 octets long (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 long (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. |
| Cumulative | The total count since the statistics tab was first opened. The elapsed time for the cumulative counter is displayed at the bottom of the graph dialog box. |
| 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. |
| Last value | The average for the counter over the last polling interval. |

# Graphing RMON History statistics

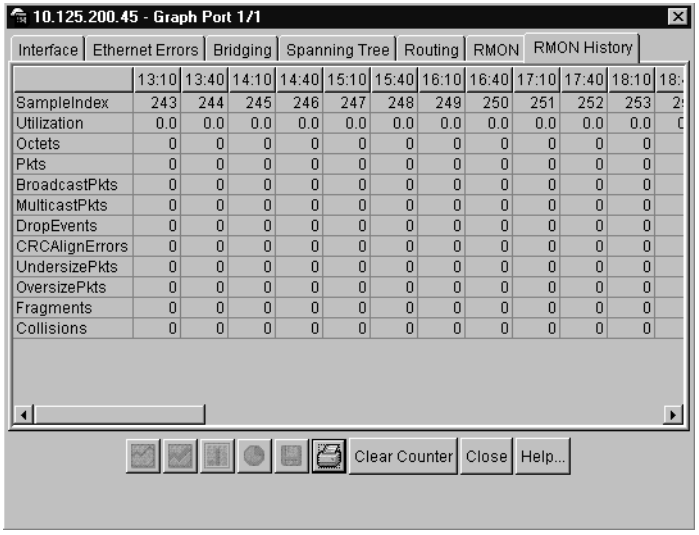
To graph RMON History statistics for a single port or multiple ports:

1. If you haven't already done so, enable RMON by choosing RMON > Options from the Device Manager menu bar.
2. Right click on the port you want to graph.
3. Select Enable Rmon History.
4. From the Device Manager menu bar, choose Graph > Port.

   The graphPort dialog box opens with the Interface tab displayed.
5. Click the RMON History tab.

   The RMON History tab opens (Figure 63).

**Figure 63** graphPort dialog box—RMON History tab




| | 13:10 | 13:40 | 14:10 | 14:40 | 15:10 | 15:40 | 16:10 | 16:40 | 17:10 | 17:40 | 18:10 | 18: |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SampleIndex | 243 | 244 | 245 | 246 | 247 | 248 | 249 | 250 | 251 | 252 | 253 | 2 |
| Utilization | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0 |
| Octets | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Pkts | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| BroadcastPkts | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| MulticastPkts | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| DropEvents | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| CRCAlignErrors | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| UndersizePkts | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| OversizePkts | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Fragments | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Collisions | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |

Table 58 describes the fields in the RMON History tab.

**Table 58** RMON History tab fields

| Field | Description |
|---|---|
| SampleIndex | Uniquely identifies a specific etherStats entry. The value range is 1 to 65535. |
| Utilization | If greater precision is required, you should sample the etherStstsPkts and etherStatsOctets objects before and after a common interval. The differences in the sampled values are Pkts and Octets, respectively. The number of seconds in the interval is Interval. These values are used to calculate the utilization as follows:<br>$$\text{Utilization} = \frac{\text{Pkts} \times (9.6 + 6.4) + (\text{Octets} \times 0.8)}{\text{Interval} \times 10000}$$<br>The result of this equation is the value Utilization, which is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent. |
| Octets | The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). You can use this object as a reasonable estimate of Ethernet utilization. For greater precision, sample the etherStatsPkts and etherStatsOctets objects before and after a common interval. |
| Packets | 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 number 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. |
| DropEvents | The total number of events in which packets were dropped by the probe due to lack of resources during this interval. Note that this number is not necessarily the number of packets dropped, it is just the number of times this condition has been detected. |
| CRCAlignErrors | 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. |

**Table 58** RMON History tab fields (continued)

| Field | Description |
|---|---|
| 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. |

# Graphing DCHP statistics

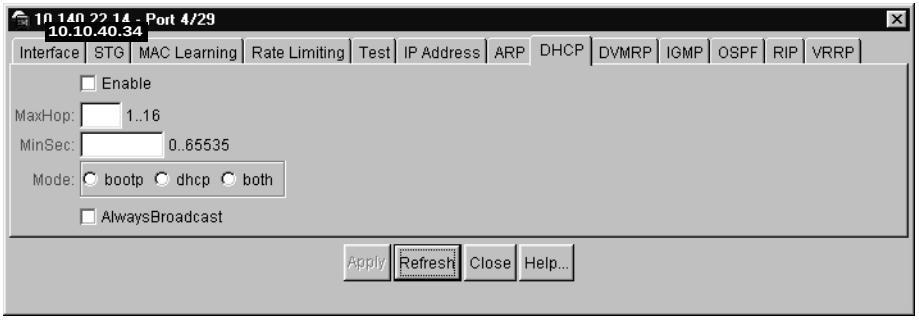
To graph DHCP statistics for a single port or multiple ports:

1. On the device view, select a port or multiple ports.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.
3. Click the DHCP tab.

   The DHCP tab opens (Figure 64).

**Figure 64** Port dialog box—DHCP tab




4. Click Enable to select the DHCP option.
5. Click Apply and then Close.
6. From the Device Manager menu bar, choose Graph > Port.

   The graphPort dialog box opens with the Interface tab displayed.

7 Click the DHCP tab.

The DHCP tab opens (Figure 65).

**Figure 65** graphPort dialog box—DHCP tab

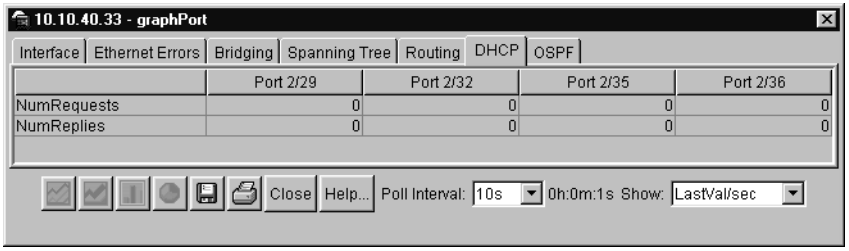



Table 59 describes the fields in the DHCP tab.

**Table 59** DHCP tab fields

| Field | Description |
|---|---|
| NumRequests | The total number of DHCP and/or BootP requests seen on this interface. |
| NumReplies | The total number of DHCP and/or BootP replies seen on this interface. |

# Graphing OSPF statistics

To graph OSPF statistics for a single port or multiple ports:

1 On the device view, select a port or multiple ports.

2 From the Device Manager menu bar, choose Graph > Port.

The graphPort dialog box opens with the Interface tab displayed.

3 Click the OSPF tab.

The OSPF tab opens (Figure 66).

**Figure 66** graphPort dialog box—OSFP tab

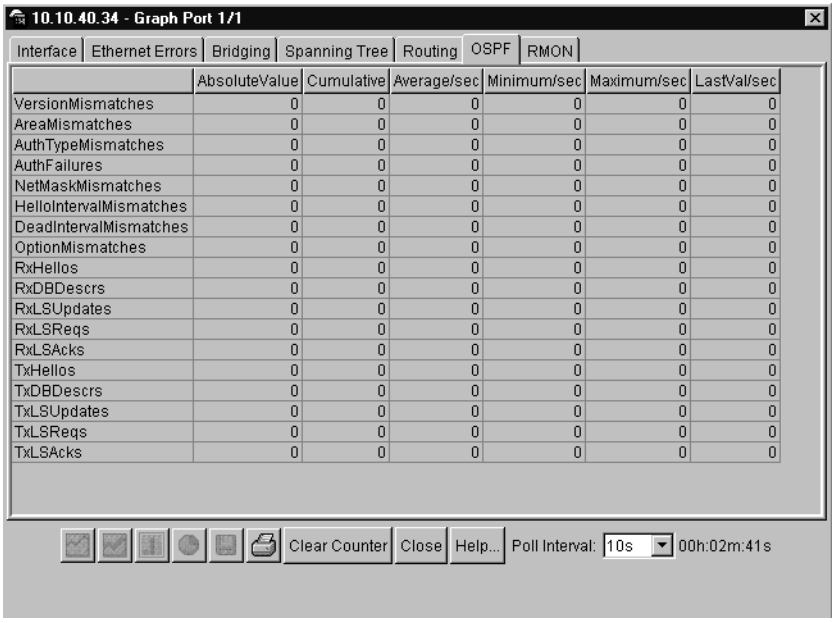



Table 60 describes the OSPF tab fields.

**Table 60** OSPF tab fields

| Field | Description |
|---|---|
| VersionMismatches | The number of version mismatches received by this interface. |
| AreaMismatches | The number of area mismatches received by this interface. |
| AuthTypeMismatches | The number of authentication type mismatches received by this interface. |
| AuthFailures | The number of authentication failures. |
| NetmaskMismatches | The number of net mask mismatches received by this interface. |
| HelloIntervalMismatches | The number of hello interval mismatches received by this interface. |
| DeadIntervalMismatches | The number of dead interval mismatches received by this interface. |
| OptionMismatches | The number of option mismatches in the Hello interval or Dead interval fields received by this interface. |

**Table 60** OSPF tab fields (continued)

| Field | Description |
|---|---|
| RxHellos | The number of hello packets received by this interface. |
| RxDBDescrs | The number of database descriptor packets received by this interface. |
| RxLSUpdates | The number of link state update packets received by this interface. |
| RxLSReqs | The number of link state request packets received by this interface. |
| RxLSAcks | The number of link state acknowledge packets received by this interface. |
| TxHellos | The number of hello packets transmitted by this interface. |
| TxDBDescrs | The number of database descriptor packets transmitted by this interface. |
| TxLSUpdates | The number of link state update packets transmitted by this interface. |
| TxLSReqs | The number of link state request packets transmitted by this interface. |
| TxLSAcks | The number of link state acknowledge packets transmitted by this interface. |

# Graphing VRRP statistics

To graph VRRP statistics:

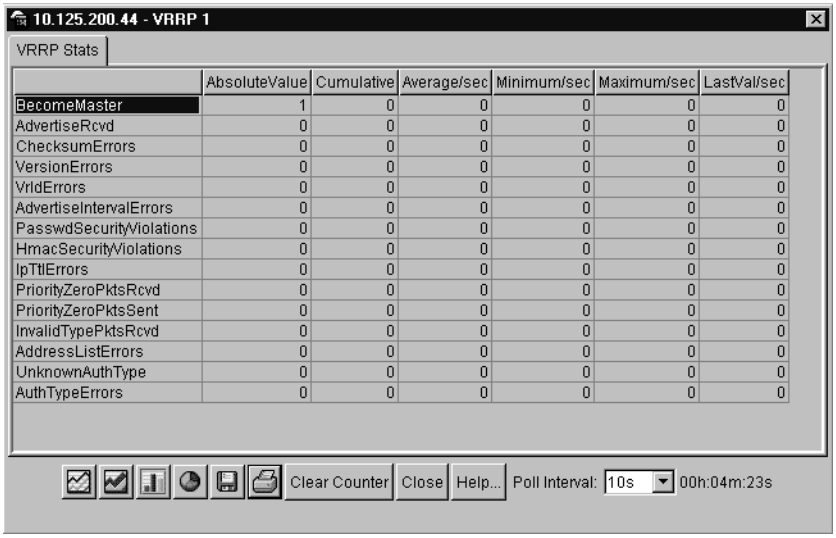
1. On the device view, select a port.
2. From the Device Manager menu bar, choose VLAN > VLANs.

   The VLAN dialog box opens with the Basic tab displayed.
3. From the VLAN dialog box, Basic tab, select a row and click IP.

   The IP, VLAN dialog box opens with the IP Address tab displayed.
4. From the IP,VLAN dialog box, click VRRP.
5. From the VRRP tab, select a row and click Graph.

   The VRRP Stats tab opens (Figure 67).

**Figure 67** VRRP dialog box—VRRP Stats tab




**6** Select the statistics that you want to graph.

**7** Click Graph.

Table 61 describes the fields in the VRRP Stats tab.

**Table 61** VRRP tab fields

| Field | Description |
|---|---|
| BecomeMaster | The total number of times that the state of this virtual router has transitioned to master. |
| AdvertiseRcvd | The total number of VRRP advertisements received by the virtual router. |
| ChecksumErrors | The total number of VRRP packets received with an invalid VRRP checksum value. |
| VersionErrors | The total number of VRRP packets received with an unknown or unsupported version number. |
| VrIDErrors | The total number of VRRP packets received with an invalid VrID for this virtual router. |
| AdvertiseIntervalErrors | The total number of VRRP advertisement packets received for which the advertisement interval is different than that configured for the local virtual router. |

**Table 61** VRRP tab fields (continued)

| Field | Description |
|---|---|
| PasswdSecurityViolations | The total number of VRRP packets received that do not pass the simple text password authentication check. |
| HmacSecurityViolations | The total number of VRRP packets received that do not pass the HMAC-MD5-96 authentication check. |
| IpTtlErrors | The total number of VRRP packets received by the virtual router with IP time-to-live (TTL) not equal to 255. |
| PriorityZeroPktsRcvd | The total number of VRRP packets received by the virtual router with a priority of zero. |
| PriorityZeroPktsSent | The total number of VRRP packets sent by the virtual router with a priority of zero. |
| InvalidTypePktsRcvd | The total number of VRRP packets received by the virtual router with an invalid value in the "type" field. |
| AddressListErrors | The total number of VRRP packets received for which the address list does not match the locally configured list for the virtual router. |
| UnkknownAuthType | The total number of VRRP packets received with an unknown authentication type. |
| AuthTypeErrors | The total number of VRRP packets received with Auth Type not equal to the locally configured authentication method. |

# Chapter 5
# Device Manager diagnostics

This chapter describes the diagnostic techniques you can run on a Passport 8000 Series switch, and includes the following topics:



## Testing the switch fabric and address resolution table

The Test tab allows you to perform two tests. You can test the switch fabric and check the address resolution (AR) table for consistency.

The Fabric test causes the CPU to generate traffic and send it through the switch fabric. Given the forwarding rate of Passport 8000 Series switches, the CPU does not generate much traffic, but it performs a simple test of the switch fabric memory.

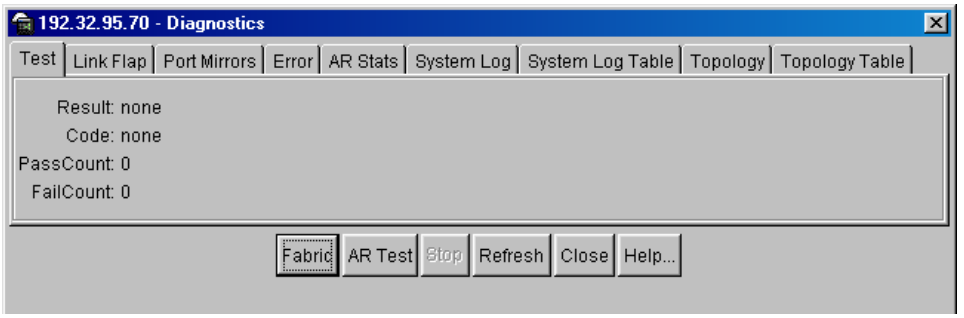
The AR table test performs a consistency check on address resolution table entries.

To test the fabric or address resolution table:

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

The Diagnostics dialog box opens with the Test tab displayed (Figure 68).

**Figure 68** Diagnostics dialog box—Test tab




The following test options are available:

- Test the Address Resolution Table (AR Test)
- Test the switch fabric (Fabric)
- Stop a test in progress

Table 62 describes the Test tab fields on the Diagnostics dialog box.

**Table 62** Test tab fields

| Field | Description |
|---|---|
| Result | The result of the most recently run (or current) test:<br>• none<br>• success<br>• inProgress<br>• notSupported<br>• unAbleToRun<br>• aborted<br>• failed |
| Code | The code contains more specific information about the test result (for example, an error code after a failed test):<br>• none<br>• NoReceive (timeout on a send)<br>• BadSeq (packets received out of sequence)<br>• BadLen (packet length mismatch)<br>• BadData (packet data mismatch) |
| PassCount | The number of iterations of the test case that completed successfully. |
| FailCount | The number of iterations of the test case that failed. |

# Monitoring how often a port goes down

You can monitor the number of times a link is going up or down rapidly (that is, flapping) on a port. This action can be detrimental to network stability because it could trigger spanning tree and routing table recalculation. If the number exceeds a given boundary during a specified interval, the port is forced out of service.

To monitor a port:

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

   The Diagnostics dialog box opens with the Test tab displayed.

2. Click the Link Flap tab.

   The Link Flap tab opens (Figure 69).

**Figure 69** Diagnostics dialog box—Link Flap tab

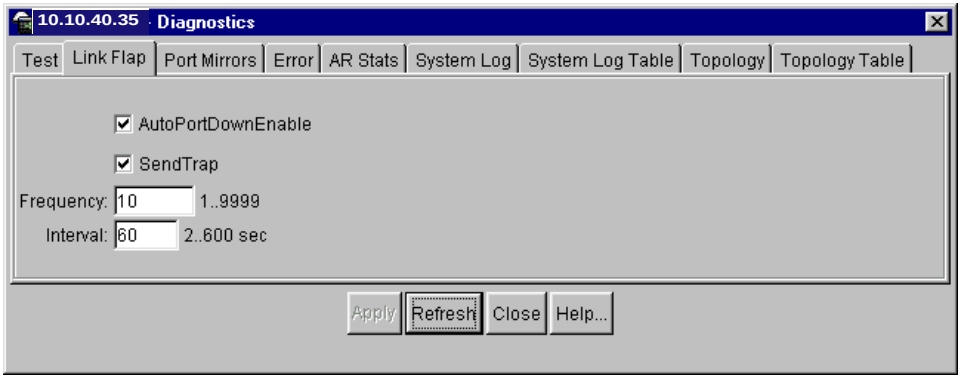



Table 63 describes the Link Flap tab fields on the Diagnostics dialog box.

**Table 63** Link Flap tab fields

| Field | Description |
|---|---|
| AutoPortDownEnable | Enables or disables the Link Flap Detect feature. |
| SendTrap | Specifies whether or not a trap should be sent if the port is forced out of service. |
| Frequency | Specifies the number of times the port can go down. The default is 10. |
| Interval | Specifies the interval (in minutes). The default is 60. |

# Configuring and monitoring port mirroring

You can use port mirroring to specify a destination port on which you want to see mirrored traffic and specify the source ports from which traffic is mirrored. Any packets entering or leaving the specified ports are forwarded normally and a *copy* of the packets is sent out the mirror port. You can configure up to 100 entries in the MirroredPort field for mirroring, and you can have up to 25 entries active (enabled) at any given time. When the port mirroring feature is active, all packets received on the port(s) specified by the MirroredPort field are copied to MirroringPort. The mirroring operation is nonintrusive; mirrored traffic is always treated in the lowest priority queue.

You can also use the port mirroring feature to monitor traffic from MAC addresses where traffic with a given MAC source address (SA) or MAC destination address (DA) is copied to the mirror port. This feature is enabled by setting the Monitor field to true for a MAC address in the Forwarding dialog box.

**Note:** Monitoring of MAC address traffic must be within the context of a VLAN (see "Viewing the forwarding database," in *Configuring Switching and Routing Operations for the Passport 8000 Series Switch Using Device Manager Release 5.x.x*).

## Configuring port mirroring ports

To configure ports for port mirroring:

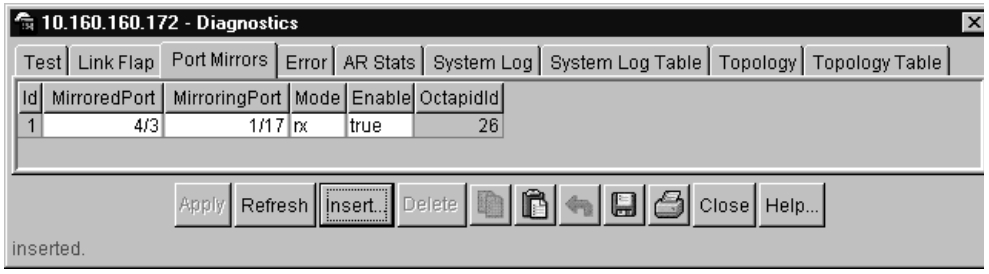
1. From the Device Manager menu bar, choose Edit > Diagnostics.

   The Diagnostics dialog box opens with the Test tab displayed (Figure 68).

2. Click the Port Mirrors tab.

   The Port Mirrors tab opens (Figure 70).

**Figure 70** Diagnostics dialog box—Port Mirrors tab



**3** Click Insert.

The Diagnostics, Insert Port Mirrors dialog box opens (Figure 71).

**Figure 71** Diagnostics, Insert Port Mirrors dialog box

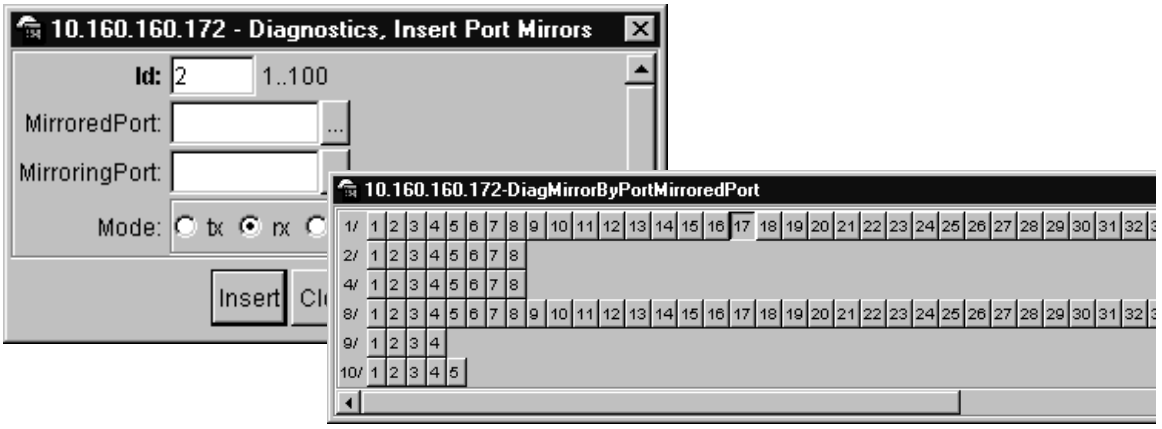



Table 64 describes the Diagnostics, Insert Port Mirrors dialog box fields.

**Table 64** Diagnostics, Insert Port Mirrors dialog box fields

| Field | Description |
|---|---|
| Id | An assigned identifier for the configured port mirroring instance. |
| MirroredPort | Allows you to specify a port to be mirrored (source port). You can select ports from any module in your configuration by clicking the ellipses button to the right of the field (Figure 71). |
| MirroringPort | Allows you to specify a destination port (the port to which the mirrored packets are forwarded). You can select ports from any module in your configuration by clicking the ellipses button to the right of the field (see "Selecting ports for mirroring," next). |
| Mode | Allows you to specify the traffic direction of the packet being mirrored—Rx, Tx, or both. The default configuration is Rx. |
| Enable | Allows you to enable or disable this port mirroring instance. The default value is Enable. |
| OctapidId | This field is the Octapid Id for a port. |

## Selecting ports for mirroring

To select ports for port mirroring:

1. On the device view, select a mirrored (source) port:
   a. Click the ellipses button in the MirroredPort field.

      The DiagMirrorByPortMirroredPort dialog box opens (Figure 72).

**Figure 72** DiagMirrorByPortMirrored/MirroringPort dialog box


   b. Select a source port.
   c. Click Ok.

      The Diagnostics, Insert Port Mirrors dialog box displays the new entry in the MirroredPort field.

2. ???Where do I select? Select a destination port.
   a. Click the ellipses button in the MirroredPort field.

      The DiagMirrorByPortMirroringPort dialog box opens.

   b. ??? Where do I select? Select a destination port.
   c. Click Ok.

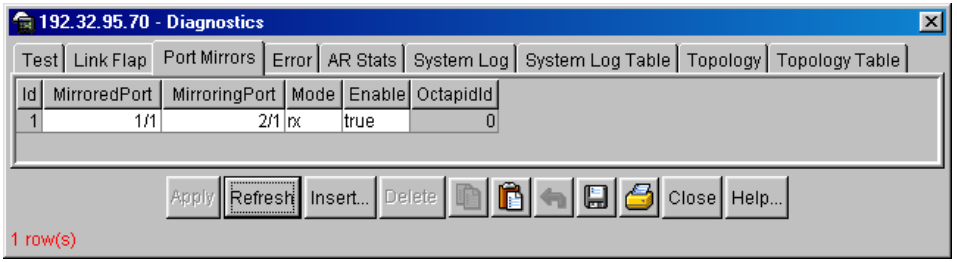
      The Diagnostics, Insert Port Mirrors dialog box displays the new entry in the MirroringPort field.

3. In the Diagnostics, Insert Port Mirrors dialog box, select the appropriate mode value (tx, rx, or both) to specify the traffic direction of the mirrored packet. The default configuration is rx.
4. Select the appropriate value (Enable or Disable) to enable or disable this instance of mirroring. The default value is Enable.

**5** Click Insert to accept your configuration choices.

The Diagnostic dialog box displays your new entry for port mirroring (Figure 73).

**Figure 73** Diagnostics dialog box




## Editing existing port mirroring values

This section describes how to edit existing port mirroring values. The following topics are covered:

- "Sorting entries," next.
- "Displaying configured port mirroring entries" on page 158
- "Editing existing mirrored or mirroring ports" on page 160
- "Editing the Mode field values" on page 161
- "Editing the Enable field values" on page 161

### Sorting entries

You can click on the column heading of any entry listed in the Port Mirrors tab to sort the entries in ascending or descending numerical order, or you can sort to group entry values.

### Displaying configured port mirroring entries

To display existing port mirroring entries:

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

The Diagnostics dialog box opens with the Test tab displayed (Figure 68).

**2** Click the Port Mirrors tab.

The Port Mirrors tab opens, displaying the configured port mirroring entries (Figure 74).

**Figure 74** Diagnostics dialog box—Port Mirrors tab

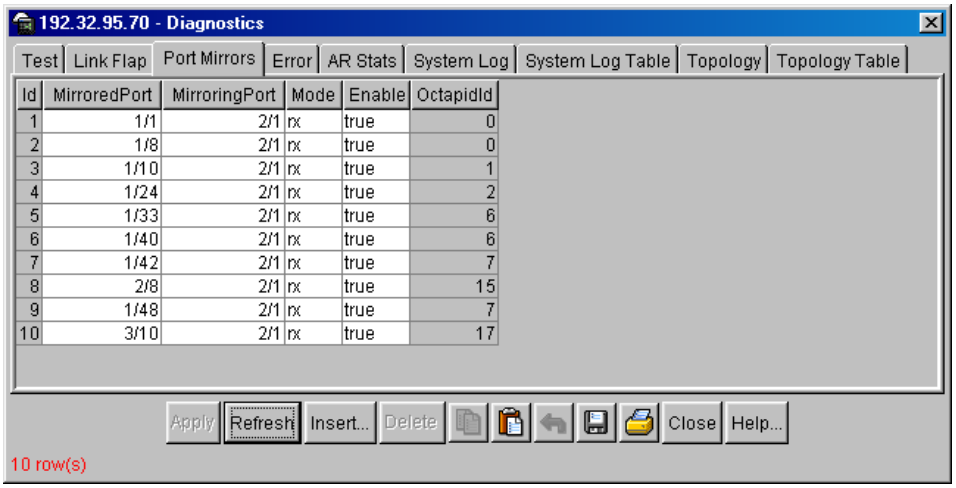



Table 65 describes the Port Mirrors tab fields on the Diagnostics dialog box.

**Table 65** Port Mirrors tab fields

| Field | Description |
|---|---|
| Id | Read-only field—displays the assigned identifier for the existing port mirroring instances. |
| MirroredPort | Displays existing port(s) from which packets are being copied (also referred to as *source* ports). |
| MirroringPort | Displays the existing port(s) that are performing the mirroring, that is, the port(s) to which the mirrored packets are forwarded (also referred to as *destination* ports). |
| Mode | Specifies the traffic direction of the packets being mirrored for each existing entry—Rx, Tx, or Both. |

**Table 65** Port Mirrors tab fields (continued)

| Field | Description |
|---|---|
| Enable | Specifies the status of existing entries—true (enabled) or false (disabled). |
| OctapidId | Read-only field—displays the OctaPID ID assignment for existing entries. The interface automatically assigns an OctaPID ID according to the switch fabric in specific Passport 8000 modules and a fixed set of configuration rules.<br>Each OctaPID ID supports up to 8 port members. Source ports that are members of the same OctaPID ID can only be mirrored to the same destination port. |

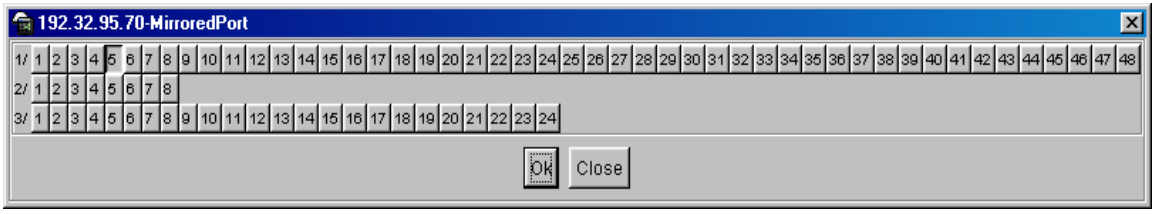
## Editing existing mirrored or mirroring ports

To modify an existing mirrored or mirroring port:

1. From the Port Mirrors dialog box, double click on an entry you want to modify in the MirroredPort or MirroringPort column heading.

   The MirroredPort dialog box opens with the port you clicked to modify shown selected (Figure 75).

**Figure 75** MirroredPort dialog box




2. Click on the port you want as a replacement.
3. Click Ok.

   The entry in the Port Mirrors tab is replaced with the new port.

### Editing the Mode field values

To modify an existing entry in the Mode field:

1. Click on the entry to display the pop up menu.

   A pop up widow displays the following options: Rx, Tx, or Both.
2. Click on the option you want for replacement.

   The Apply button becomes highlighted.
3. Click Apply to accept the option.

### Editing the Enable field values

To modify an existing entry in the Enable field:

1. Click on the entry to display the pop up menu.

   A pop up widow displays the following options: true or false.
2. Click on the option you want for replacement.

   The Apply button is highlighted.
3. Click Apply to accept the option.

## Trapping errors

You can specify that errors generate an SNMP trap. All errors detected are then sent to a log that you can view in Device Manager.

To trap errors:

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

   The Diagnostics dialog box opens with the Test tab displayed.
2. Click the Error tab.

   The Error tab opens (Figure 76).

**Figure 76** Diagnostics dialog box—Error tab

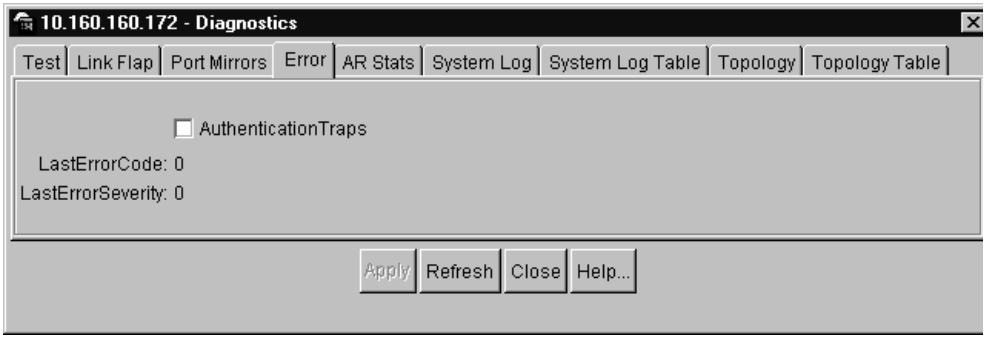



Table 66 describes the Error tab fields on the Diagnostics dialog box.

**Table 66** Error tab fields

| Field | Description |
|---|---|
| AuthenticationTrap | When enabled, sends a trap upon receiving an error in the system. |
| LastErrorCode | The last error reported in the system. This value is intended to help customer support personnel isolate system problems. |
| LastErrorSeverity | The last error reported in the system. The meanings of this value are:<br>0= Informative Information<br>1= Warning Condition<br>2= Error Condition<br>3= Manufacturing Information<br>4= Fatal Condition |

# Viewing address resolution statistics

The AR Stats tab shows statistics for the internal state of the address translation table. These statistics are debugging aids, and you should use them only when consulting with Nortel Networks support personnel.

The statistic of most interest is the NoSpace counter, which indicates the number of entries the address resolution (AR) table could not add because of lack of space.

To access the AR Stats tab:

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

   The Diagnostics dialog box opens with the Test tab displayed.

2. Click the AR Stats tab.

   The AR Stats tab opens.

**Figure 77** Diagnostics dialog box—AR Stats tab

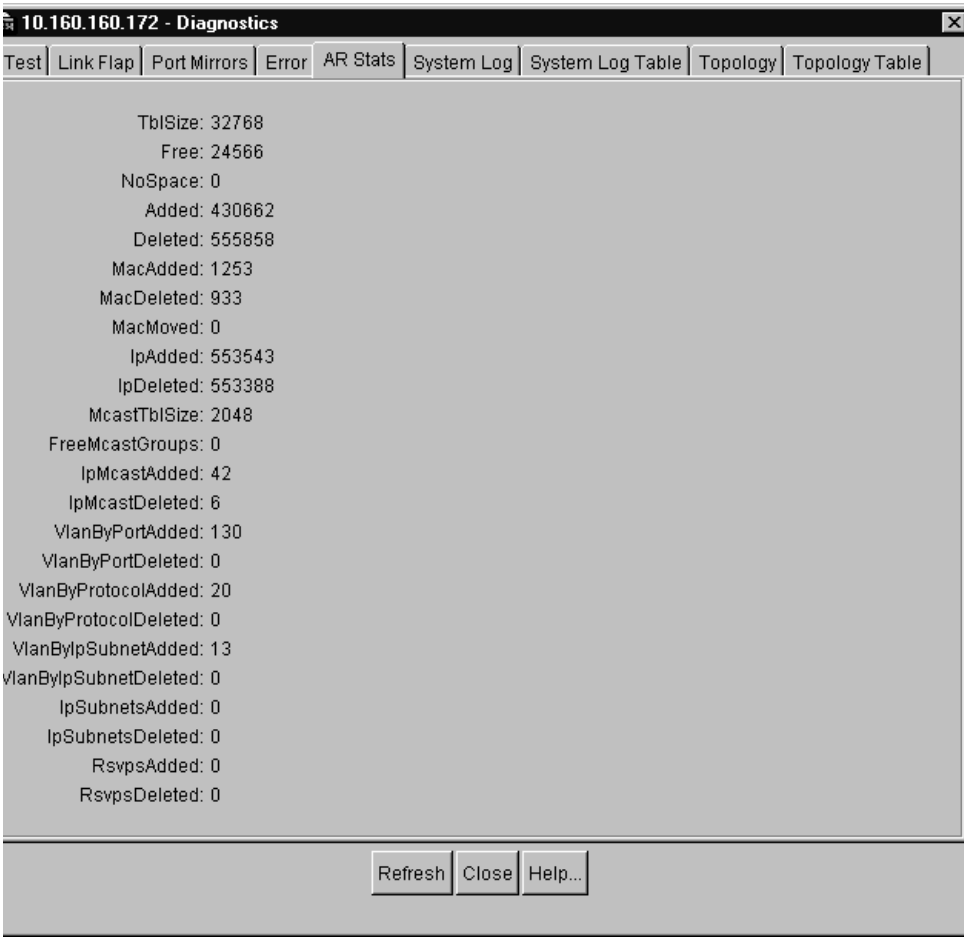



Table 67 describes the AR Stats tab fields on the Diagnostics dialog box.

**Table 67** AR Stats tab fields

| Field | Descriptions |
|---|---|
| TblSize | The size of the address resolution (AR) translation table. |
| Free | The number of free entries that are available in the AR translation table. |
| NoSpace | The number of entries that were not added to the AR translation table because of lack of space. |
| Added | The number of entries added to the AR translation table. |
| Deleted | The number of entries deleted from the AR translation table. |
| MacAdded | The number of MAC entries added to the AR translation table. |
| MacDeleted | The number of MAC entries deleted from the AR translation table. |
| MacMoved | The number of MAC entries moved in the AR translation table. |
| IpAdded | The number of IP entries added to the AR translation table. |
| IpDeleted | The number of IP entries deleted from the AR translation table. |
| McastTblSize | The size of the Multicast AR translation table. |
| FreeMcastGroups | The number of free multicast groups available in the AR table. |
| IpMcastAdded | The number of IP multicast entries added to the AR table. |
| IpMcastDeleted | The number of IP multicast entries deleted from the AR table. |
| VlanByPortAdded | The number of VLAN by Port entries added to the AR table. |
| VlanByPortDeleted | The number of VLAN by Port entries deleted from the AR table. |
| VlanByProtocolAdded | The number of VLAN by Protocol Type entries added to the AR table. |
| VlanByProtocolDeleted | The number of VLAN by Protocol Type entries deleted from the AR table. |
| VlanByIpSubnetAdded | The number of VLAN by IP Subnet entries added to the AR table. |
| VlanByIpSubnetDeleted | The number of VLAN by IP Subnet entries deleted from the AR table. |
| IpSubnetsAdded | The number of IP Subnet entries added to the AR table. |
| IpSubnetsDeleted | The number of IP Subnet entries deleted from the AR table. |
| RsvpsAdded | The number of RSVP entries added to the AR table. |
| RsvpsDeleted | The number of RSVP entries deleted from the AR table. |

# Enabling the system log

You can enable the system log feature globally to send messages to up to 10 syslog hosts. By default, five hosts are supported.

To enable the system log feature globally:

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

   The Diagnostics dialog box opens with the Test tab displayed.

2. Click the System Log tab.

   The System Log tab opens (Figure 78).

3. Set Enable to true.

4. Set the maximum number of hosts (1 to 10).

**Figure 78** Diagnostics dialog box—System Log tab

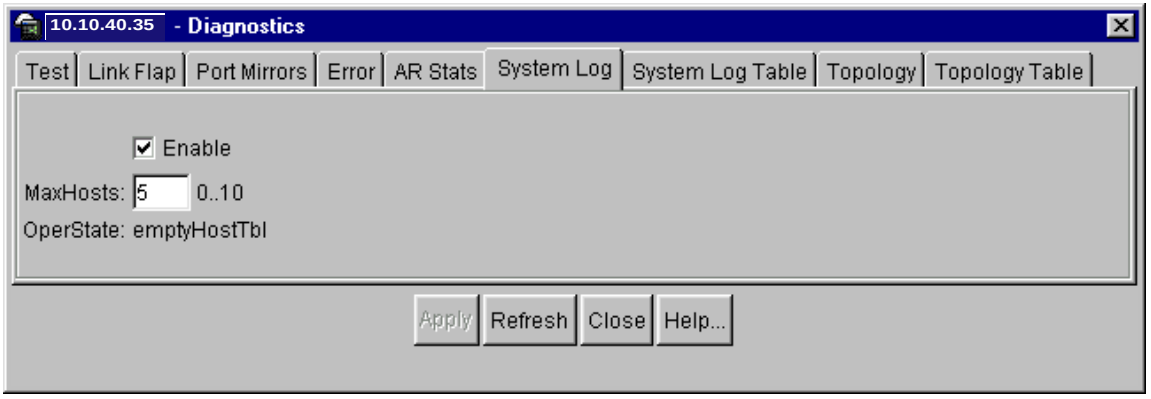



Table 68 describes the System Log tab fields on the Diagnostics dialog box.

**Table 68** System Log tab fields

| Field | Descriptions |
|---|---|
| Enable | Used to enable/disable the syslog feature. When enabled, this feature sends a message to a server on a network that is configured to receive and store diagnostic messages from this device. The type of messages sent is user configurable. |
| MaxHost | The maximum number of remote hosts considered active and able to receive messages from the syslog service. |
| OperState | The operational state of the syslog service. |

# Receiving system log messages

You can use the system log messaging feature of the Passport to manage switch event messages on any UNIX-based management platform. The Passport syslog software supports this functionality by communicating with a counterpart software component named *syslog* on your management workstation. The UNIX daemon syslogd is a software component that receives and locally logs, displays, prints, and/or forwards messages that originate from sources internal and external to the workstation. For example, syslogd on a UNIX workstation concurrently handles messages received from applications running on the workstation, as well as messages received from Passports running in a network accessible to the workstation.

At a remote UNIX management workstation, the system log messaging feature does the following:

- Receives system log messages from the Passport
- Examines the severity code in each message
- Uses the severity code to determine appropriate system handling for each message

- Based on the severity code in each message, dispatches each message to any or all of the following destinations:
  - — Workstation display
  - — Local log file
  - — Designated printer
  - — One or more remote hosts

Internally the Passport has four severity levels for log messages:

- Info
- Warning
- Error
- Fatal

The system log feature supports eight different severity levels:

- Debug
- Info
- Notice
- Warning
- Error
- Critical
- Alert
- Emergency

Table 69 shows the default mapping of internal severity levels to syslog severity levels.

**Table 69** Default severity levels and system log severity levels

| UNIX system error codes | System log severity level | Internal Passport severity level |
|---|---|---|
| 0 | Emergency | Fatal |
| 1 | Alert | - |
| 2 | Critical | - |

**Table 69** Default severity levels and system log severity levels

| UNIX system error codes | System log severity level | Internal Passport severity level |
|---|---|---|
| 3 | Error | Error |
| 4 | Warning | Warning |
| 5 | Notice | - |
| 6 | Info | Info |
| 7 | Debug | - |

# Changing the severity level mapping

To change the severity level mapping:

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

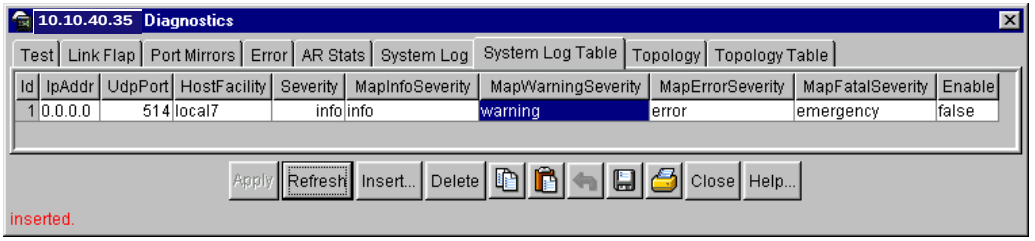
   The Diagnostics dialog box opens with the Test tab displayed.

2. Click the System Log Table tab.

   The System Log Table tab opens (Figure 79).

3. For each severity type, use the MapWarningSeverity list to change the severity level.

**Figure 79** Diagnostics dialog box—System Log Table tab




To insert a system log table member:

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

   The Diagnostics dialog box opens with the Test tab displayed.

2 Click the System Log Table tab.

The System Log Table tab opens.

3 In the Diagnostics dialog box, click Insert.

The Diagnostics, Insert System Log Table dialog box opens (Figure 80).

4 Select the appropriate items.

5 Click Insert.

**Figure 80** Diagnostics, Insert System Log Table dialog box

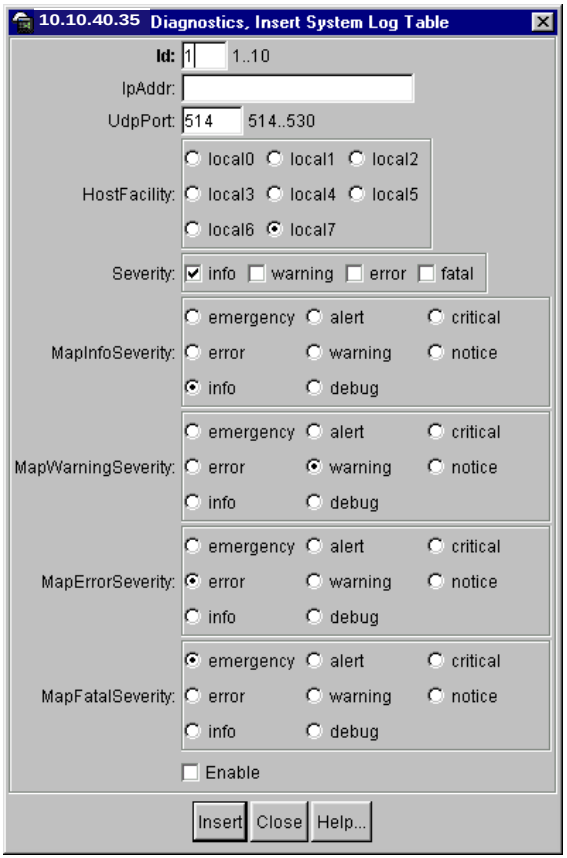



Table 70 describes the System Log Table tab fields and Diagnostics, Insert System Log Table dialog box.

**Table 70** Diagnostics, Insert System Log Table dialog box fields

| Field | Description |
|---|---|
| Id | ID for the syslog host being created. |
| IpAddr | IP address of the syslog host. |
| UdpPort | The UDP port to use to send messages to the syslog host (514 to 530). |
| HostFacility | The syslog host facility used to identify messages (LOCAL0 to LOCAL7) |
| Severity | The Passport message severity for which syslog messages will be sent. |
| MapInfoSeverity | The fields that map Passport severity levels to syslog severity. |
| MapWarningSeverity | The fields that map Passport warning severity levels to syslog severity. |
| MapErrorSeverity | The fields that map Passport error severity levels to syslog severity. |
| MapFatalSeverity | The fields that map Passport fatal severity levels to syslog severity. |
| Enable | Enables or disables sending messages to the syslog host. |

# Checking the MIB status

Use the Topology tab to view Nortel Management MIB (NMM) status information.

To view topology status information:

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

   The Diagnostics dialog box opens with the Test tab displayed.

2. Click the Topology tab.

   The Topology tab opens (Figure 81).

**Figure 81** Diagnostics dialog box—Topology tab

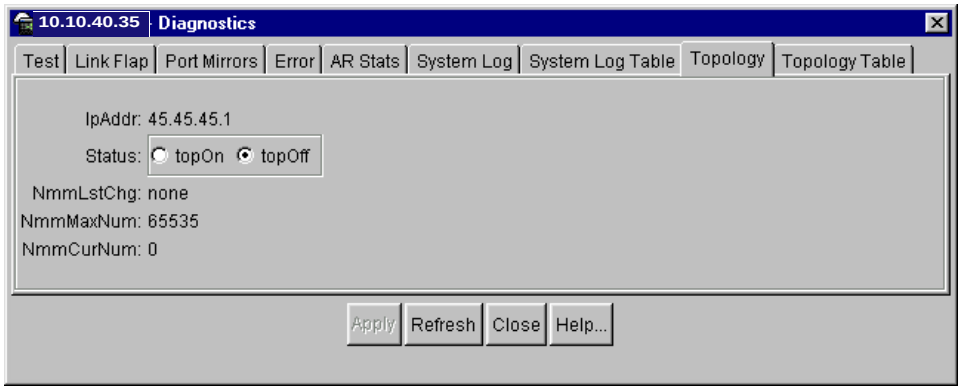



Table 71 describes the Topology tab fields on the Diagnostics dialog box.

**Table 71** Topology tab fields

| Field | Description |
|---|---|
| IpAddr | The IP address of the device. |
| Status | Whether Nortel Networks topology is on or off for the device. |
| 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. |

# Checking the details of the MIB status

Use the Topology Table tab to view details of Nortel Management MIB (NMM) status information.

To view topology table information:

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

   The Diagnostics dialog box opens with the Test tab displayed.

2. Click the Topology Table tab.

   The Topology Table tab opens (Figure 82).

**Figure 82** Diagnostics dialog box—Topology Table tab

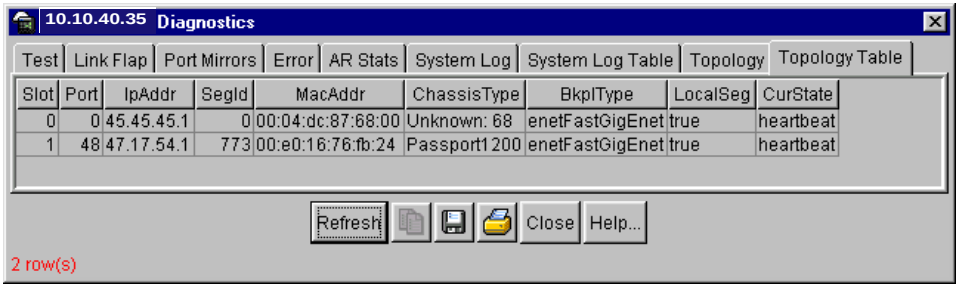



Table 72 describes the Topology Table tab fields.

**Table 72** 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. |

**Table 72** Topology Table tab fields (continued)

| Field | Description |
|---|---|
| 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:<br>• topChanged—Topology information has recently changed.<br>• heartbeat—Topology information is unchanged.<br>• new—The sending agent is in a new state. |

# Chapter 6
# RMON

The RMON MIB is an interface between the RMON agent on the Passport 8000 Series switch and an RMON management application, such as the Device Manager. It defines objects that are suitable for the management of any type of network, but some groups are targeted for Ethernet networks in particular. Enabling RMON on the switch allows the RMON agent to continuously collect statistics and proactively monitor switch performance. This data can then be viewed 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

**Note:** Before using RMON functions, you must globally enable RMON. In addition, you should specify certain options to control how RMON operates on the switch.

## Enabling RMON globally

Enable RMON globally before using any RMON function. If you attempt to enable any functions when the global flag is disabled, Device Manager informs you that the flag is disabled and prompts for automatic enabling of the flag. See the appropriate sections about RMON functionality for details on other RMON parameters that will be automatically created and set to default parameters.

To enable and set RMON options:

➔ From the Device Manager menu bar, choose RMON > Options.

The RMONOptions dialog box opens displaying the default values.

If you want to use nondefault RMON parameter values, you should set them before enabling RMON or when you create the specific RMON function.

# Using Ethernet statistics

You can use Device Manager to gather and graph Ethernet statistics in a variety of formats, or you can save them to a file and export them into an outside presentation or graphing application.

**Note:** This implementation of RMON requires a “control” row for Ethernet statistics. This control row appears as “port” 0/1 when you choose RMON > Control > Ethernet Statistics. The row ID is reserved for the control row. Therefore, some automated tests, such as ANVL, may fail when the test attempts to create a row 1.

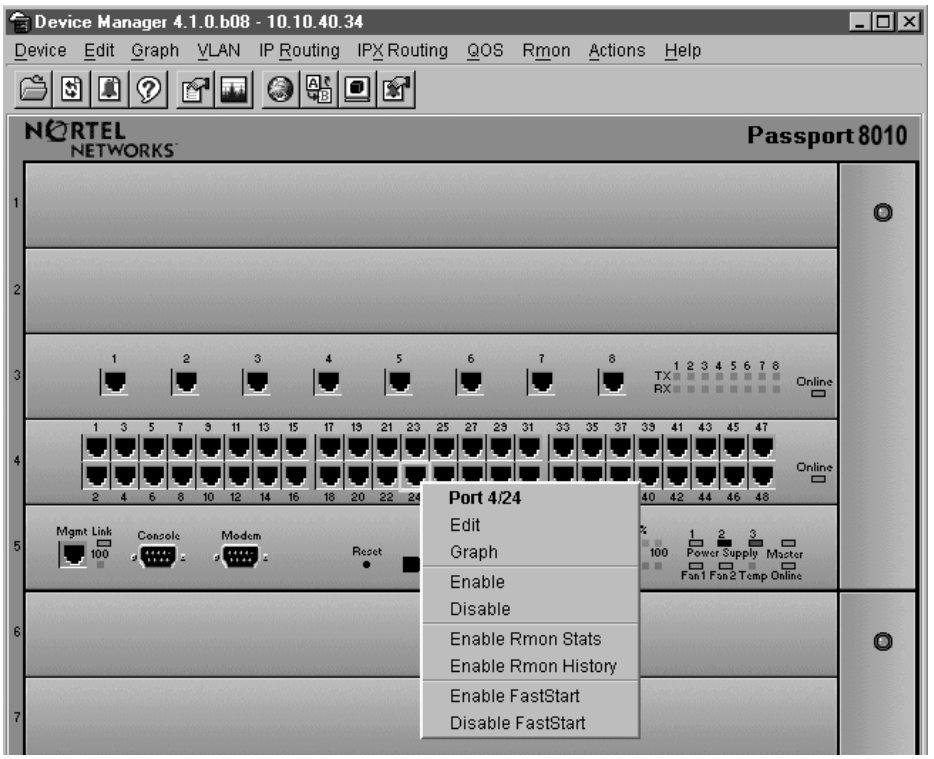
## Enabling RMON statistics (default)

To enable RMON statistics:

1. On the device view, select a port or multiple ports.
2. Right-click the selected ports.

   The Port shortcut menu opens (Figure 83).
3. In the Port shortcut menu, select Enable Rmon Stats.

**Figure 83** Enabling RMON statistics on a port




**Note:** If RMON statistics have not yet been globally enabled, Device Manager prompts you to do so.

## Verifying RMON statistics

To verify that RMON statistics are enabled:

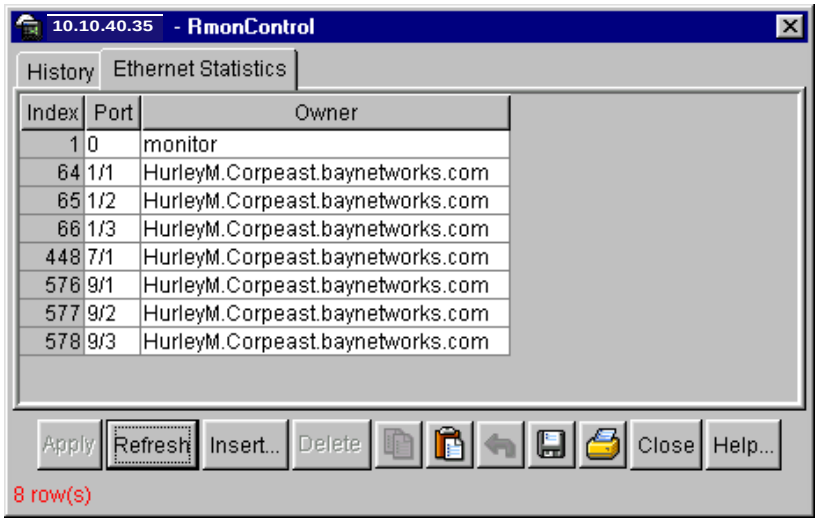
1 From the Device Manager menu bar, choose RMON > Control.

The RmonControl dialog box opens with the History tab displayed.

2 Click the Ethernet Statistics tab.

The Ethernet Statistics tab opens (Figure 84). Note that the default owner displayed is the host name on which Device Manager is running.

**Figure 84** RmonControl dialog box—Ethernet Statistics




## Enabling RMON statistics (nondefault)

The default owner of the RMON statistics port is the host name on which the Device Manager software is running.

To insert another host name:

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

   The RmonControl dialog box opens with the History tab displayed.

2. Click the Ethernet Statistics tab.

   The Ethernet Statistics tab opens.

3. On the RmonControl dialog box, click Insert.

   The RmonControl, Insert Ethernet Statistics dialog box opens (Figure 85).

4. Click the Port ellipsis button, and select a port.

5. On the RmonControl, Insert Ethernet Statistics dialog box, click Insert.

**Figure 85** RmonControl and Insert Ethernet Statistics dialog boxes

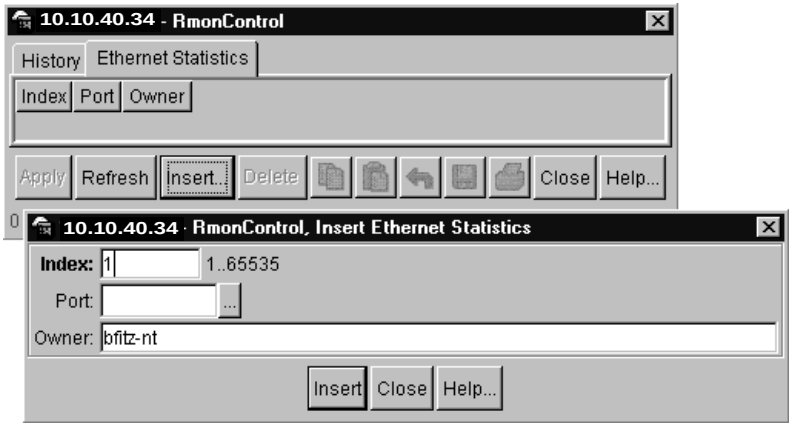



Table 73 describes the RmonControl, Insert Ethernet Statistics dialog box fields.

**Table 73** RmonControl, Insert Ethernet Statistics dialog box fields

| Field | Description |
|---|---|
| Index | The value of this object uniquely identifies this etherStats entry. |
| Port | This object identifies the source of the data that this etherStats entry is configured to analyze. This source can be any Ethernet interface on this device. In order to identify a particular interface, this object shall identify the instance of the ifIndex object, defined in [4,6], for the desired interface. For example, if an entry were to receive data from interface #1, this object would be set to ifIndex 1. The statistics in this group reflect all packets on the local network segment attached to the identified interface. This object may not be modified if the associated etherStatsStatus object is equal to valid(1). |
| Owner | The entity that configured this entry and is therefore using the resources assigned to it. |

## Disabling RMON statistics

To disable RMON statistics on a port:

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

The RmonControl dialog box opens with the History tab displayed.

2 Click the Ethernet Statistics tab.

The Ethernet Statistics tab opens.

3 Select the row that contains the port ID you want to disable.

4 Click Delete.

## Viewing statistics

To view RMON statistics:

1 Select a single port.

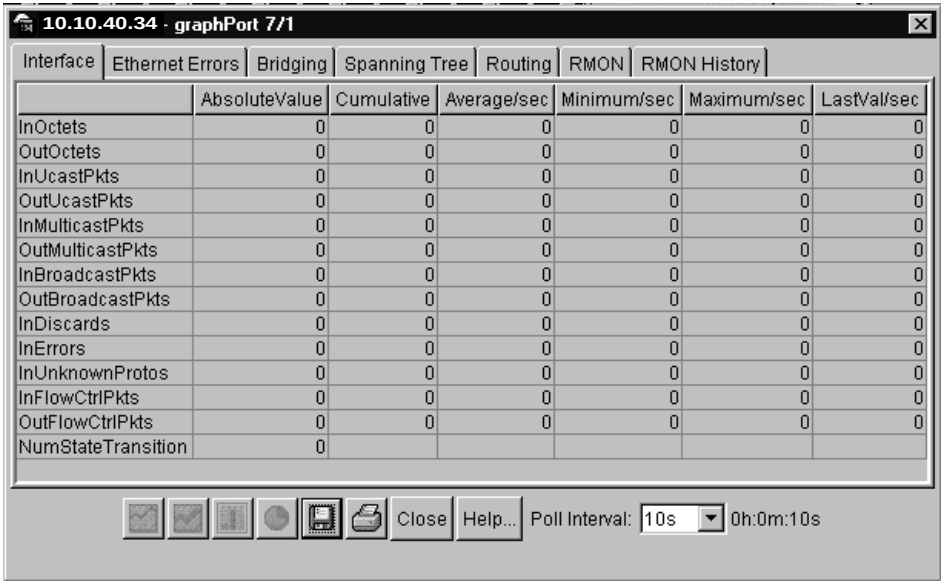
2 On the Device Manager toolbar, click the graphing icon.

The graphPort dialog box for the port object opens with the Interface tab displayed (Figure 86).

3 Click RMON.

The RMON tab opens and displays RMON statistics.

**Figure 86** graphPort dialog box—Interface tab




| | AbsoluteValue | Cumulative | Average/sec | Minimum/sec | Maximum/sec | LastVal/sec |
|---|---|---|---|---|---|---|
| InOctets | 0 | 0 | 0 | 0 | 0 | 0 |
| OutOctets | 0 | 0 | 0 | 0 | 0 | 0 |
| InUcastPkts | 0 | 0 | 0 | 0 | 0 | 0 |
| OutUcastPkts | 0 | 0 | 0 | 0 | 0 | 0 |
| 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 |
| InDiscards | 0 | 0 | 0 | 0 | 0 | 0 |
| InErrors | 0 | 0 | 0 | 0 | 0 | 0 |
| InUnknownProtos | 0 | 0 | 0 | 0 | 0 | 0 |
| InFlowCtrlPkts | 0 | 0 | 0 | 0 | 0 | 0 |
| OutFlowCtrlPkts | 0 | 0 | 0 | 0 | 0 | 0 |
| NumStateTransition | 0 | | | | | |

# Understanding RMON history

The RMON History group records periodic statistical samples from a network. A sample is called a history and is gathered in time intervals referred to as "buckets." By enabling and creating histories, you establish a time-dependent method for gathering RMON statistics on a port. Following are the default values for history:

- 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.

## Enabling RMON history (default)

To enable RMON history on a port basis:

1. On the device view, select a port or multiple ports.
2. Right-click on the selected ports.

   The Port shortcut menu opens (Figure 83 on page 177).
3. In the port shortcut menu, select Enable Rmon History.
4. From the Device Manager menu bar, choose RMON > Control

   The RmonControl dialog box opens with the History tab displayed (Figure 87 on page 182). Rows with RMON history enabled are displayed.

To verify that RMON statistics are enabled:

➔ From the Device Manager menu bar, choose RMON > Control.

The RmonControl dialog box opens with the History tab displayed (Figure 87 on page 182). Rows with RMON history enabled are displayed.

## Enabling RMON history (nondefault)

You can use RMON to collect statistics at intervals. For example, if you wanted RMON statistics to be gathered over the weekend, you would want enough buckets to cover two days. To do this, you would set the history to gather one bucket over every 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 menu bar, choose RMON > Control.

   The RmonControl dialog box opens with the History tab displayed.

2. Click Insert.

   The RmonControl, Insert History dialog box opens (Figure 87).

3. In the Port field, select a port.
4. In the Buckets Requested field, enter the number of discrete time intervals to save data.
5. Enter the Interval in seconds.
6. Click Insert.

**Figure 87** RmonControl and RmonControl, Insert History dialog boxes

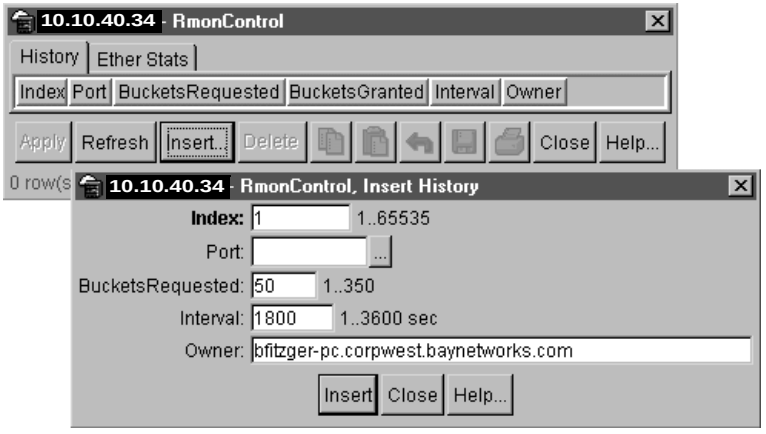



Table 74 describes the RMON History tab fields.

**Table 74** RmonControl dialog box fields

| Field | Description |
|---|---|
| Index | An index that uniquely identifies an entry in the historyControl table. Each such entry defines a set of samples at a particular interval for an interface on the device. |
| Port | This object identifies the source of the data for which historical data was collected and placed in a media-specific table on behalf of this historyControlEntry. This source can be any interface on this device. In order to identify a particular interface, this object shall identify the instance of the ifIndex object, defined in [4,6], for the desired interface. For example, if an entry were to receive data from interface #1, this object would be set to ifIndex.1. The statistics in this group reflect all packets on the local network segment attached to the identified interface. This object may not be modified if the associated historyControlStatus object is equal to valid(1). |
| 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 historyControl entry. When this object is created or modified, the probe should set historyControlBucketsGranted as closely to this object as is possible for the particular probe implementation and available resources. |

**Table 74** RmonControl dialog box fields (continued)

| Field | Description |
|---|---|
| BucketsGranted | The number of discrete sampling intervals over which data shall be saved in the part of the media-specific table associated with this history control entry. When the associated BucketsRequested object is created or modified, the probe should set this object as closely to the requested value as possible for the particular probe implementation and available resources. The probe must not lower this value except as a result of a modification to the associated BucketsRequested object. There will be times 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 will be added to the media-specific table. When the number of buckets reaches the value of this object and a new bucket is to be added to the media-specific table, the oldest bucket associated with this entry shall be deleted by the agent so that the new bucket can be added. When the value of this object changes to a value less than the current value, entries are deleted from the media-specific table associated with this entry. Enough of the oldest of these entries shall be deleted by the agent so that their number remains less than or equal to the new value of this object. When the value of this object changes to a value greater than the current value, the number of associated media-specific entries may be allowed to grow. |
| 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 historyControl entry. This interval can be set 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, a prudent manager will take into account 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. This object may not be modified if the associated historyControlStatus object is equal to valid(1). |
| Owner | The entity that configured this entry and is therefore using the resources assigned to it. |

## Disabling RMON history

To disable RMON history on a port:

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

   The RmonControl dialog box opens with the History tab displayed (Figure 87 on page 182).
2. Select the row that contains the port ID you want to delete.
3. Click Delete.

## Viewing history

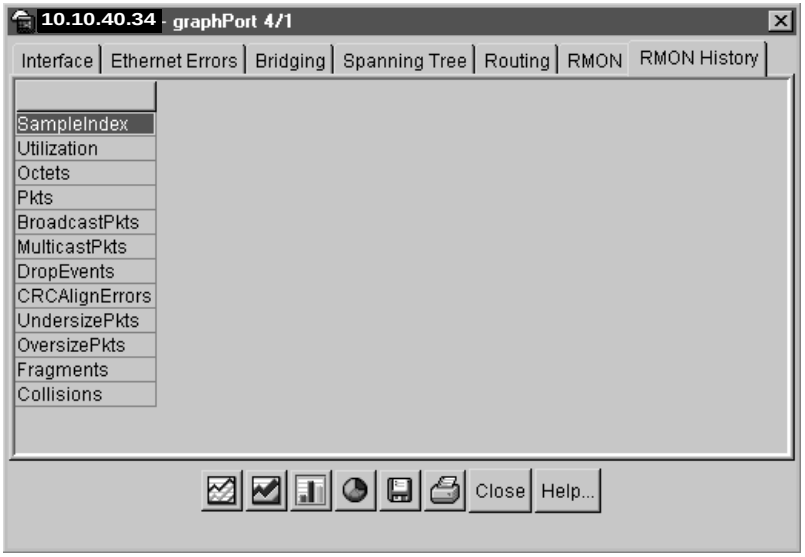
To view RMON history:

1. Select a port.
2. On the Device Manager toolbar, click the graphing icon.

   The graphPort dialog box opens with the Interface tab displayed.
3. Click the RMON History tab.

   The RMON History tab opens (Figure 88).

**Figure 88** graphPort dialog box—RMON History tab




# Configuring RMON alarms

Alarms are useful when the network administrator needs to know when the value of some variable goes out of range. RMON alarms can be defined on any MIB variable that resolves to an integer value. In other words, string variables (such as system description) cannot be used as alarm variables.

All alarms share the following characteristics:

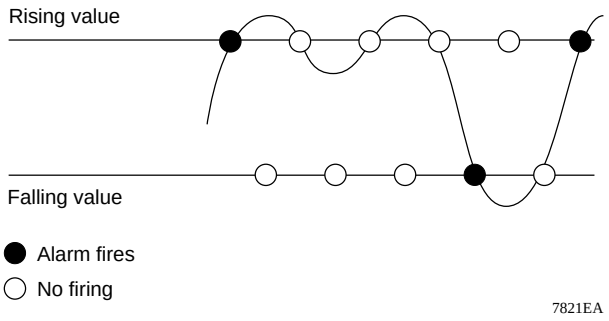
- An upper and lower threshold value defined on it
- A corresponding rising and falling event
- An alarm interval or polling period

When alarms are “fired,” or 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.

The alarm variable is polled and the result is compared against upper and lower limit values selected when the alarm is created. 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 89).

**Figure 89** How alarms fire



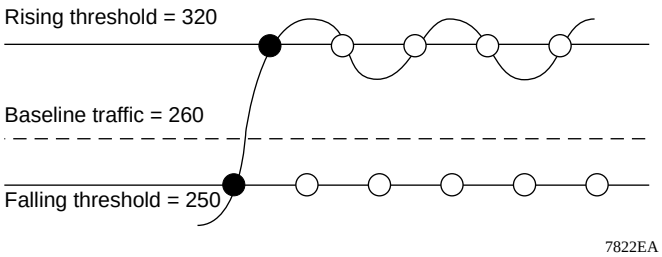

It is important to note that the alarm fires during the first interval that the sample goes out of range. No additional events are generated for that threshold until the opposite threshold is crossed. Therefore, it is important to carefully define the rising and falling threshold values for alarms to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

A general "rule of thumb" is to define one of the threshold values to an expected, baseline value, 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 90). The reason is that for the rising alarm to fire a second time, the falling alarm (the opposite threshold) must fire. Unless the port goes 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 90** Alarm example—threshold less than 260




## Creating alarms

When you create an alarm, you select a variable from the variable list (Appendix B, “RMON alarm variables”) and a port, or other switch component, to which it is connected. Some variables require port IDs, card IDs, or other indexes (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. Therefore, if you keep track of the current values of a given delta-valued alarm and add them together, the result is twice the actual value. (This result is not an error in the software.)

**Note:** The example alarm described here will generate 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 in a real world scenario.

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

1. Make sure that RMON is globally enabled.

   When you enable RMON globally, you also create a default rising and falling event. The default for the events is log-and-trap, meaning you will receive notification through a trap as well as through a log file.

2. From the Device Manager menu bar, choose RMON > Alarm Manager.

   The Alarm Manager dialog box opens (Figure 91).

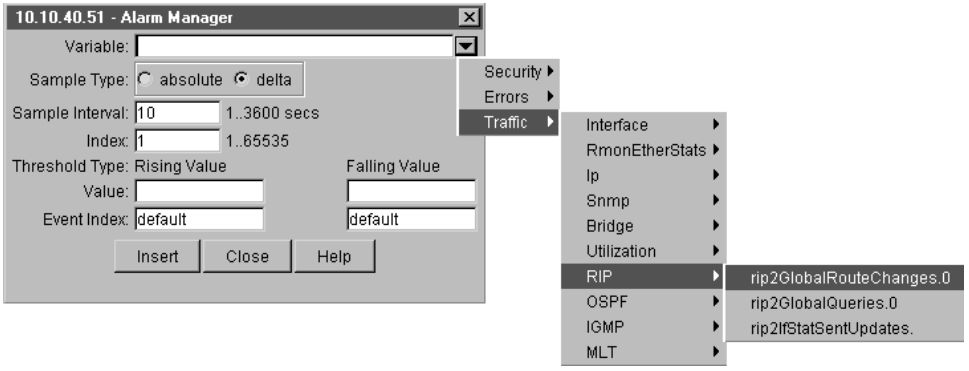
3. In the Variable field, select a variable for the alarm and a port (or other ID) on which you want to set an alarm.

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

- A chassis, power supply, or fan-related alarm ends in x where the x index is hard-coded. No further information is required.
- A card, spanning tree group (STG), RIP or OSPF, 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).

In the example displayed in Figure 91, “rip2GlobalRouteChanges.0” has been selected from the variable list under RIP. (A list of variable definitions is located in Appendix B, “RMON alarm variables.”)

**Figure 91** Alarm Manager dialog box




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, and click Insert.

(If you want to make field changes, refer to the field descriptions in Table 76.)

Table 75 describes the RMON Alarm Manager dialog box fields.

**Table 75** Alarm Manager dialog box fields

| **Field** | **Description** | |
|---|---|---|
| Variable | Name and type of alarm—indicated by the format:<br>• *alarmname.x,* where x=0 indicates a chassis alarm, x=1 or 2 indicates a power supply or fan alarm with 1 being the primary unit and 2 the secondary unit.<br>• *alarmname,* where the user must specify the index. This value is 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), an IP address for RIP or OSPF alarms (RIP/OSPF must be enabled on the VLAN or router port and enabled globally), or the Ether Statistics Control Index for RMON Stats alarms.<br>• *alarmname* with no dot or index is a port-related alarm and results in display of the port picker tool. | |
| Sample Type | Can be either absolute or delta. | |
| 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.) |

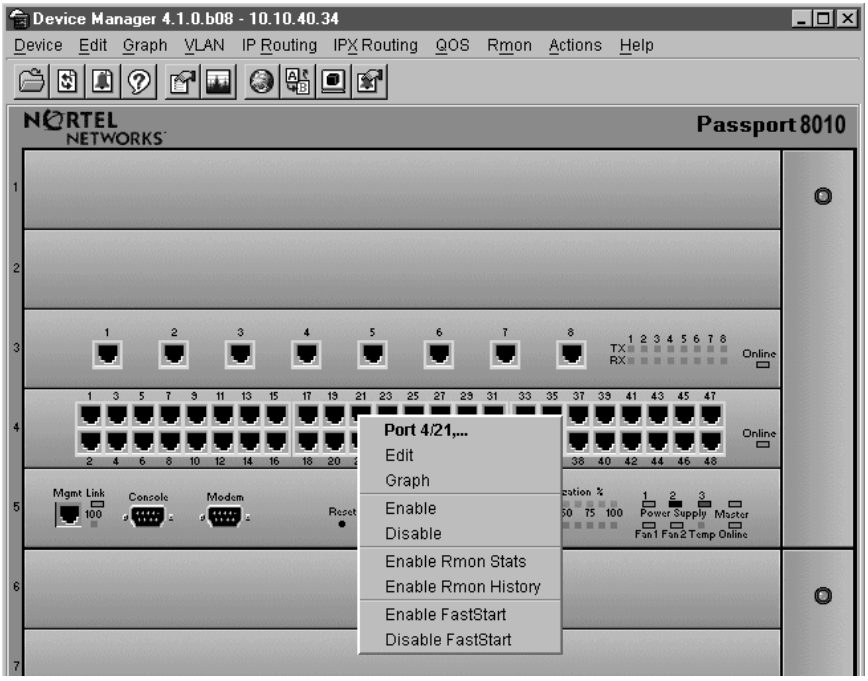
## Creating a port history alarm

To create a port history alarm:

1. Select the port on which you have created an alarm.
2. Right-click the mouse.

   The Port shortcut menu opens (Figure 92).
3. Choose Enable Rmon Stats and Enable Rmon History.

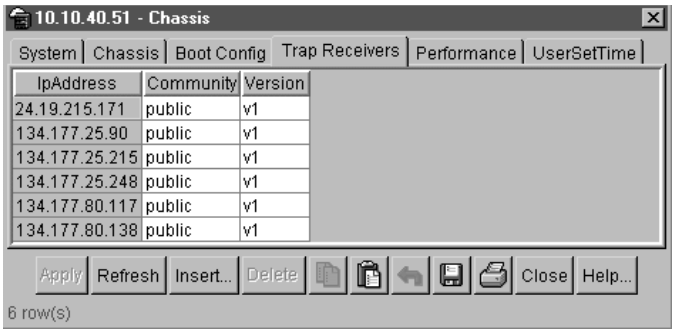
**Figure 92** Enabling RMON statistics and history




4. If trapping is not enabled, enable trapping.

   On the Device Manager menu bar, choose Edit > Chassis, and then click on the Trap Receivers tab (see Figure 93). Two trap versions are available: Version 1 (v1) and Version 2c (v2c). In general, select Version 2c trapping. If you are using HP OpenView or other network managers that are RMON management applications, select Version 1.

**Figure 93** Chassis dialog box—Trap Receivers tab




## Viewing RMON statistics

To view RMON statistics and history:

1. Select the port on which you have created an alarm.
2. On the Device Manager toolbar, click the graph icon.
3. On the graphPort dialog box, click RMON History.

   The graphPort dialog box opens with the RMON History tab displayed (Figure 88 on page 186).
4. On the graphPort dialog box, click the graph button.

## Viewing log files

To view the RMON log and the events log:

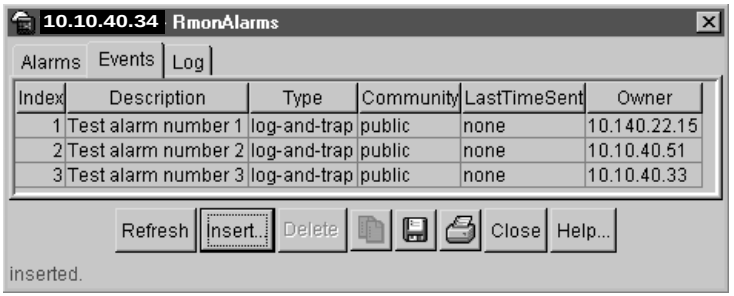
➔ On the Device Manager toolbar, click the bell icon.

To view the Rmon Alarms, Events, or Log information:

1. From the Device Manager menu bar, choose RMON > Alarms.
2. Click the Alarms, Events, or Log tab.

   An example is shown in Figure 94.

**Figure 94** RmonAlarms dialog box—Events tab




## Deleting alarms

To delete an alarm:

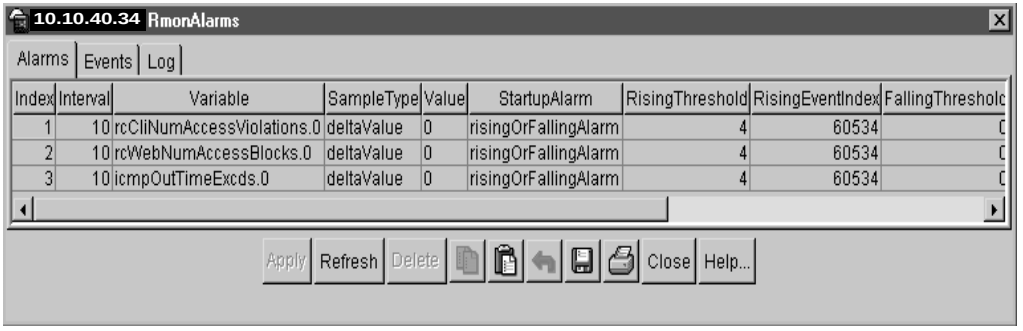
1. From the Device Manager menu bar, choose RMON > Alarms.

   The RmonAlarms dialog box opens with the Alarms tab displayed (Figure 95).

2. Select the alarm you want to delete.

3. Click Delete.

**Figure 95** Deleting an alarm



# Understanding RMON events

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

An event specifies whether a trap, a log, or a trap and a log will be 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, both a trap and a log track the "firing" of the alarm. 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.

## Creating events (default)

To create a default rising and falling event:

1. From the Device Manager menu bar, choose RMON > Alarms.

   The RmonAlarms dialog box opens with the Alarms tab displayed.

2. Click the Events tab.

   The Events tab opens.

3. Click Insert.

   If Rmon is not globally enabled, a dialog box displays the following message:

   "RMON is currently disabled. Do you want to enable it now?"

4. Click Yes.

When you create events in this manner, you create two default events (a rising event and a falling event).

## Creating events (nondefault)

To create events with nondefault parameter values:

1. From the Device Manager menu bar, choose RMON > Alarms.

   The RmonAlarms dialog box opens with the Alarms tab displayed.

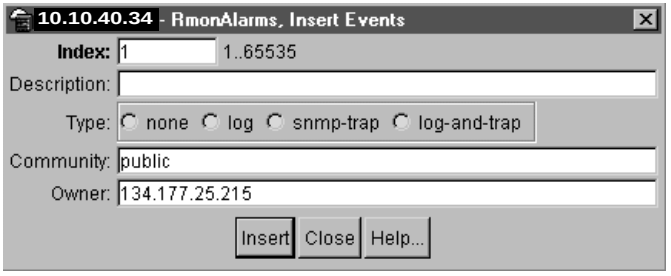
2. Click the Events tab.

   The Events tab opens.

3. Click Insert.

   The RmonAlarms, Insert Events dialog box opens (Figure 96).

**Figure 96** RmonAlarms, Insert Events dialog box




4. Type a name for the event in the Description field.

5. Select the type of event you want.

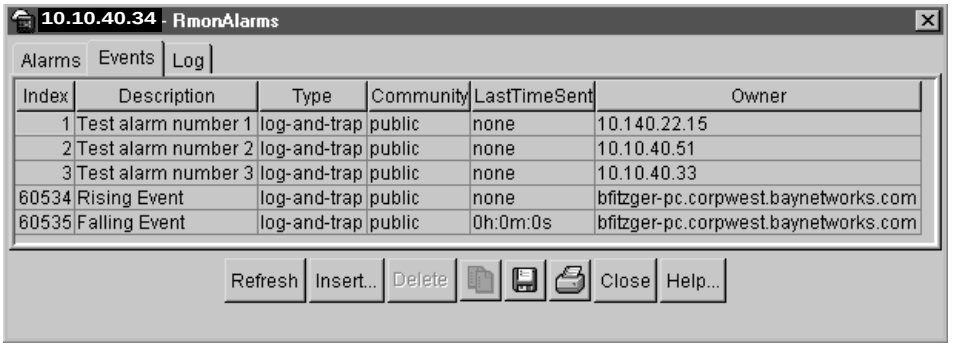
   The default setting is log-and-trap. You may opt to set the event type to log to save memory or to snmp-log to reduce traffic from the switch.

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

6. Click Insert.

   The new event is displayed in the Events tab of the RmonAlarms dialog box (Figure 97).

**Figure 97** RmonAlarms dialog box—Events tab




## Viewing events

To view a table of Rmon Alarm events:

1. From the Device Manager menu bar, choose RMON > Alarms.

   The RmonAlarms dialog box opens with the Alarms tab displayed.
2. Click the Events tab.

   The Events tab opens (Figure 97).

## Deleting events

To delete an event:

1. From the Device Manager menu bar, choose RMON > Alarms.

   The RmonAlarms dialog box opens with the Alarms tab displayed.
2. Click the Events tab.

   The Events tab opens.
3. Select the event you want to delete.
4. Click Delete.

Table 76 describes the RmonAlarms dialog box—Evens tab fields.

**Table 76** Events tab fields

| Field | Description |
|---|---|
| Index | An index that 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:<br>• none<br>• log<br>• trap<br>• 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. |

# 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, enter the following:

```
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:.
```

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

MIB files are shipped with the Device Manager, and you can find them in the following directory:

*dm/dmdb/acc/OV/mibs*

Load each of the MIB files in the following order:

- rfc1213.mib
- rfc1253rcc.mib
- rfc1271_te.mib
- rfc1271_te.trp (trap configuration)
- rfc1389.mib
- rfc1493.mib
- rfc1573rcc.mib
- rfc1643.mib
- rfc1850t_rcc.mib
- accelar.mib

Now you can start HP OpenView.

## Understanding the “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 will not be displayed in the event browser version 5.0, because this bug is fixed. If users are not aware that version 4.0 had a problem, then they may erroneously assume that the switch is not sending these traps. In this case, you can view the ASCII trap log file:

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

In doing so, 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 is the process that receives the trap. HP OpenView then passes the trap to Device Manager. In a sense, it intercepts the trap message. 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. Select Event Configuration under Options.
2. Select enterprise name snmpTraps.
3. Double-click the event (trap) name in question.
4. Change the category from Log Only to any event type: Error Events, Threshold Events (normally used for RMON alarms), Status Events, Configuration Events, or Application Alert Events.
5. Click OK.
6. Choose File and then Save.

## Working around the private management trap bug

A problem with the private management traps in HP OpenView 4.0 and 5.0 affects the following variables:

- rcCardDown
- rcCardUp
- rcErrorNotification
- rcStpNewRoot
- rcStpTopologyChange

Although the trap MIB is defined correctly and loads without problems, HP OpenView does not properly process event object identifiers (OIDs) that have embedded zeros. HP OpenView appears to ignore “0” and drops it from the OID. This bug results in HP OpenView logging these traps as undefined.For example, rcCardDown is defined with OID 1.3.6.1.4.1.2272.1.21.0.1, but HP OpenView processes it with an OID of 1.3.6.1.4.1.2272.1.21.1 in its event configuration file.

To work around this problem:

1. Select Event Configuration under Options.
2. Select enterprise name rcMgmt.
3. Select Copy event under Edit.
4. Enter a new event name (for example, xlrCardDown instead of rcCardDown).
5. Add 0 to the beginning of the editable portion of the event OID (for example, “21.1” becomes “0.21.1” for the xlrCardDown event). Optionally, change the event category from Log only to Status Events if you want the trap to be displayed in the events browser.
6. Click OK.
7. Choose File and then Save.

# Appendix A
# Error messages and codes

This appendix provides a table of error codes, messages, and descriptions (Table 77).

**Table 77** Error codes, messages, and descriptions

| Code Number | Error Message | Description |
|---|---|---|
| 101 | resourceNotAvailable | The system is out of a resource required by the specified operation. For example, if the system is running low on memory, the user should turn off features that are not critical (Web server, RMON). |
| 102 | operationNotAllowed | The specified operation is not allowed. Select another operation. |
| 103 | operationInProgress | A previous operation is still in progress. Wait until the previous operation is finished; then retry the requested operation. |
| 104 | invalidPortNumber | The specified port number is invalid. Retry the operation with the valid port number. |
| 105 | invalidSubnetAddress | The specified IP subnet address is invalid or already in use. Specify a valid or alternate IP subnet address. |
| 106 | invalidSubnetMask | The specified IP subnet mask is invalid or already in use. Specify a valid or alternate IP subnet mask. |
| 107 | invalidVlanId | The specified VLAN ID is invalid or already in use. Specify a valid or alternate VLAN ID number. |
| 108 | invalidVlanName | The specified VLAN name is invalid or already in use. Specify a valid or alternate VLAN name. |
| 109 | invalidVlanType | The specified VLAN type is invalid or already in use. Specify a valid or alternate VLAN type. |
| 110 | invalidStgId | The specified STG ID is invalid or already in use. Specify a valid or correct STG ID. |
| 111 | invalidProtocolId | The specified protocol ID is invalid or already in use. Specify a valid or correct protocol ID. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 112 | invalidPortMembers | The specified port members bit map is invalid. The bit field is used to identify which ports in the system are members (static or dynamic) to this VLAN. The bit field is 32 octets long and represents ports 0 to 255 (inclusive). |
| 113 | invalidStaticMembers | The specified static members bit map is invalid. The bit field is used to identify how ports are members of this VLAN. A one (1) value in a bit means the port is a static member of this VLAN. A zero (0) value in a bit means the port is a dynamic member of this VLAN.The bit field is 32 octets long, representing ports 0 to 255 (inclusive). |
| 114 | invalidNotAllowedMembers | The specified NotAllowToJoin bit map is invalid. The bit field is used to identify which ports are not allowed to join this VLAN. A one (1) value in a bit means the port is not allowed to join a VLAN. A zero (0) value in a bit means the port is allowed to join a VLAN. The bit field is 32 octets long, representing ports 0 to 255 (inclusive). |
| 115 | destinationNotReachable | The specified destination is not reachable. The system has no route to the destination specified. Verify the destination IP address to ensure that it is correct. |
| 116 | tableisFull | There is no more room in the trap receive table. Remove entries that are no longer needed before adding additional entries. |
| 117 | nondualConnectorGigPort | This port is not a dual-connector Gigabit port. Select a dual-connector Gigabit port when you want to perform a Gigabit port-specific operation. |
| 118 | testIdNotPresent | The test ID is not present in the SET PDU. The SET PDU is incorrectly formatted. Refer to the Enterprise MIB specification for the proper format. |
| 119 | invalidTestId | The test ID is not valid and does not match TestAndIncr. Refer to the Enterprise MIB specification for the proper format. |
| 120 | invalidStatusChange | An invalid status change has been performed. |
| 121 | invalidCpuCard | The card is not a CPU card. Select an SSF module when you want to perform an operation specific to the Passport SSF modules. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 122 | invalidSrcPortChoice | The specified source port is the same as the specified destination port. Choose a different port; then resubmit the operation. |
| 123 | dstPortUnspecified | The mirror destination port is not set. Specify the destination port; then resubmit the operation. |
| 124 | srcPortOneUnspecified | The mirror source port #1 is not set. Specify source port #1; then resubmit the operation. |
| 125 | srcPortTwoUnspecified | The mirror source port #2 is not set. Specify the source port #2; then resubmit the operation. |
| 126 | notSupported | This functionality is not supported. |
| 127 | nonUniqueUserName | The user name is not unique. Enter a new user name. |
| 128 | InvalidUsernameLen | The length of the user name is invalid. Reenter the user name, ensuring that the user name does not exceed the 20-character maximum. |
| 129 | invalidPasswordLen | The length of the password is invalid. Reenter the password, ensuring that the password does not exceed the 20-character maximum. |
| 130 | cannotModifyThisField | It is illegal to change this field. This field is not editable. Please select another field associated with the operation that you want to perform. |
| 131 | invalidUserPasswordLength | The length of the user password is invalid. Reenter the password, ensuring that the password does not exceed the 20-character maximum. |
| 132 | thisUsernameExists | An entry exists with this user name. Choose a different user name; then resubmit the operation. |
| 133 | invalidIpAddress | The specified IP address is invalid. Enter a valid IP address in dotted-decimal notation (<xxx>.<xxx>.<xxx>.<xxx>). The following are examples of valid IP addresses:<br>• 209.99.99.1<br>• 107.85.21.2<br>• 134.177.160.14 |
| 134 | invalidMacAddress | The specified MAC address is invalid. Enter a valid MAC address in the format:<br>xx-xx-xx-xx-xx-xx. An example of a valid MAC address is 00-00-ef-01-db-40. |
| 135 | nosuchEntry | The specified entry is invalid. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 136 | anotherLoopbackTestAlreadyRunning | A user can run only one loopback test at a time. This error is returned if another loopback test is already in progress. To determine if a test is already running:<br>• From the CLI, use the command `test show` to determine if another test is running. Use the command `test stop` to stop a test.<br>• From Device Manager, choose Diagnostics > Options > Testing to show or stop a test in progress. |
| 137 | protocolIdNotRoutable | The routing protocol type requested is invalid. Specify IP routing as the routing protocol type, and retry the operation. |
| 138 | invalidAdminSpeedSpecified | User attempted to set AdminSpeed or AdminDuplex on a port where AutoNegotiate is enabled. Disable autonegotiation on the port; then retry the attempted operation. |
| 139 | noActionSpecified | User attempted to execute an operation, but no action is specified. Review the actions available, select an action, and then retry the operation. |
| 140 | invalidActionSpecified | User attempted to execute an operation, but an invalid action is specified. Review the actions available, select the correct action, and then retry the operation. |
| 141 | cannotModifyAutoNegotiateIsOn | User attempted to modify AdminSpeed or AdminDuplex on a port where AutoNegotiate is enabled. Disable autonegotiation on the port; then retry the attempted modification. |
| 142 | cannotModifyAutoPortIsFiber | User attempted to enable autonegotiation on a fiber port. Retry the operation on a valid 10/100BASE-T port. |
| 143 | autoNegotiationNotSupported | User attempted to enable autonegotiation on a port that does not support autonegotiation. Retry the operation on a valid port. |
| 144 | cannotSetAdminSpeed | User attempted to set AdminSpeed on a port that does not support this operation (for example, 100BASE-F or 1000BASE-F ports). Retry the operation on a valid port type. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 145 | cannotSetAdminDuplex | User attempted to specify half-duplex mode on a port that does not support this operation (for example, a Gigabit port operates only in full-duplex mode). Retry the operation on a valid port type. |
| 146 | OspfRtrDeadIntIsnotMultOfHelloInt | Router dead interval should be a multiple of the hello interval. (For example, if the hello interval is 6, the router dead interval could be specified as 24, 36, or 60.) |
| 147 | OspfRtrDeadIntILessThan4timesHelloInt | Router dead interval should be at least four times the value of the hello interval. (For example, if the hello interval is 4, the router dead interval must be a minimum of 16.) |
| 148 | invalidOrInconsistentValue | A bad value has been specified. Retry the operation using a correct value. |
| 149 | ospfBadAuth | An invalid authentication key has been specified. A valid authentication key syntax is the area's authorization type as a simple password and the key, which is shorter than 8 octets. The agent will left adjust and zero fill to 8 octets. |
| 150 | ospfRouterOn | The requested operation cannot be performed when OSPF is enabled. Disable OSPF; then resubmit the operation.<br>• To disable OSPF from the CLI, use the command `ospf set {enable\| disable}`<br>• To disable OSPF from Device Manager, choose Routing > OSPF > General. |
| 151 | ospfAreaNotFound | The specified area ID cannot be found. Enter a valid area ID; then resubmit the operation. A valid area ID is a 32-bit identifier that on creation can be derived from the instance. |
| 152 | ospfBBArea | The backbone area cannot be deleted. Specify a nonbackbone area; then resubmit the operation. |
| 153 | notInTestMode | The port is not in test mode. Put into test mode before attempting a test. |
| 154 | ospfInvalidAreaRangeMask | The specified area range mask is invalid. Specify the correct subnet that pertains to the net or subnet. |
| 155 | ospfDuplicateEntry | This entry already exists. Specify a unique entry; then resubmit the operation. |
| 156 | ospfRangeNotAllocated | Invalid area range specified. Specify a valid area range; then resubmit the operation. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 157 | ospfAreaRangeNotFound | The specified area range cannot be found. |
| 158 | testRunning | A test is running. |
| 159 | nvramLimitExceeded | The NVRAM limit has been exceeded for some static entry. |
| 160 | flowAlreadyExists | The specified flow already exists. |
| 161 | flowNotFound | The specified flow cannot be found. |
| 162 | ispfInvalidAreaRangeNet | The specified area range net is invalid. |
| 163 | duplicateIpAddress | A duplicate IP address has been entered. Verify the correct IP address and enter. |
| 164 | conflictingIpAddress | A conflicting IP address has been entered. |
| 165 | invalidRouteCost | An invalid route cost has been entered. Enter a valid route cost. |
| 166 | invalidNextHop | An invalid next hop address has been entered. Enter a valid next hop address. |
| 167 | duplicateRoute | A duplicate route has been entered. |
| 168 | cannotFindRoute | An invalid route has been specified. |
| 169 | cannotDeleteLocalRoute | The local route cannot be deleted. |
| 170 | badDhcpMinSec | The DHCP minimum seconds value is out of range. Enter a valid value. |
| 171 | badDhcpMaxHop | The DHCP maximum hops value is out of range. Enter a valid value. |
| 172 | badDhcpMode | An invalid DHCP mode value has been entered. Enter a valid value. |
| 173 | badAgentAddress | An invalid DHCP agent address has been entered. Enter a valid address. |
| 174 | dhcpNotEnabled | DHCP is not enabled and should be enabled for the requested action. Enable DHCP before proceeding. |
| 175 | dhcpForwardNotFound | A DHCP forward record was not found. |
| 176 | dhcpDupForward | A duplicate DHCP forward entry was found. |
| 177 | dhcpMaxForward | The maximum number of DHCP forwarding records has been reached. |
| 178 | dhcpBadEnable | A bad DHCP enable value has been found. |
| 179 | deviceInvalidFileNum | The device has an invalid device file number. |
| 180 | deviceNotExecuteFile | The device has a device file that is not executable. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 181 | deviceDeletedFile | The device has a deleted device file. |
| 182 | devicePcmciaNotPresent | The PCMCIA for the device is not present. |
| 183 | devicePcmciaWrProtect | The device's PCMCIA card is write-protected. Unprotect the PCMCIA card before attempting to write on it. |
| 184 | disContiguousSubnetMask | The specified subnet mask is discontiguous. |
| 185 | ospfInvalidMetric | An attempt was made to delete a local route. You cannot delete a local route. |
| 186 | ospfHostRouteEntryNotFound | The OSPF host route entry was not found. |
| 187 | mltInvalidMltID | The MultiLink Trunk has an invalid ID. Specify a valid MLT ID. |
| 188 | mltInvalidMltName | The MultiLink Trunk name is invalid. Specify a valid MLT name. |
| 189 | mltOnePort | There is only one port entered in the MultiLink Trunk. Add one or more ports. |
| 190 | mltTooManyPorts | More than four ports have been added to the MultiLink Trunk. An MLT can have only four ports. |
| 191 | mltInvalidQuids | The specified MultiLink Trunk ports are in different QUIDs. |
| 192 | mltInvalidPort | The specified MultiLink Trunk port is already in another MultiLink Trunk. |
| 193 | mltInvalidVlan | The MultiLink Trunk VLAN ID is invalid. Enter a valid VLAN ID. |
| 194 | snoopNonExistIpMcastAddr | The specified multicast group address was not found in the group database. |
| 195 | snoopInvalidIpMcastAddr | The specified multicast IP address is not valid. |
| 196 | portIsLocked | The specified port is locked and cannot be modified. |
| 197 | accessRestriction | Access is restricted for the specified action. |
| 198 | invalidFilenameLength | The allowed file name length was exceeded. Enter another file name shorter in length. |
| 199 | duplicateAccessPolicyId | A duplicate access policy ID has been specified. Specify another policy ID. |
| 200 | noDesiredAccessPolicyItem | The specified access policy item does not exist. |
| 201 | ipFilterNonExist | The specified IP filter does not exist. Specify another IP filter. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 202 | ipfInvalidVlanPriority | The specified IEEE VLAN priority number is invalid. Specify a valid priority number. |
| 203 | ipfInvalidDestinationAddr | The specified destination address is either a duplicate or nonexistent. Specify a valid destination address. |
| 204 | ipfInvalidSourceAddr | The specified source address is either a duplicate or nonexistent. Specify a valid source address. |
| 205 | ipFilterDuplicate | You are attempting to create an IP filter that already exists. |
| 206 | ipfGlobalListSuplicate | You are trying to create an IP filter global list that already exists. |
| 207 | ifGlobalListNonExist | The desired IP global list does not exist. Specify another global list. |
| 208 | ipfBaseListDuplicate | You are trying to create an IP filter base list that already exists. |
| 209 | ipfBaseListNonExist | The specified IP base list does not exist. Specify another IP base list. |
| 210 | ipfPortDuplicate | You are trying to create an IP filtered port that already exists. |
| 211 | ipfPortNonExist | The specified IP filtered port does not exist. Specify another IP filtered port. |
| 212 | ipfListNonExist | The specified IP filter global or base list does not exist. Specify another. |
| 213 | snoopDisabled | IGMP snooping is not enabled. |
| 214 | invalidHostIpAddr | The host IP address is Invalid. |
| 215 | snoopStaticGroupExists | A static entry already exists for the group. |
| 216 | announceRipPolicyEntryNotFound | The specified RIP announce policy entry was not found. Enter another RIP announce policy. |
| 217 | announceRipPolicyDuplicateEntry | The specified RIP announce policy entry is a duplicate. |
| 218 | announceOspfPolicyEntryNotFound | The specified OSPF announce policy entry was not found. Enter another OSPF announce policy. |
| 219 | announceOspfPolicyDuplicateEntry | The specified OSPF announce policy entry is a duplicate. |
| 220 | policytNetEntryNotFound | The policy network entry was not found. Enter another policy network. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 221 | policyNetDuplicateEntry | The specified policy network entry is a duplicate. |
| 222 | policyAddrListEntryNotFound | The specified policy match list entry was not found. |
| 223 | policyAddrListDuplicateEntry | The specified policy match list entry is a duplicate. |
| 224 | polictAddrListIdEntryNotFound | The specified policy route list entry route ID was not found. |
| 225 | policyExactNetListidNotFound | The specified policy exact net list ID was not found. |
| 226 | policyRangeNetListidNotFound | The specified policy range net list ID was not found. |
| 227 | policyRipGatewayListidNotFound | The specified policy RIP interface gateway list ID was not found. |
| 228 | policyRipIntfListidNotFound | The specified policy RIP interface list ID was not found. |
| 229 | policyOspfRtrListidNotFound | The specified policy OSPF router list ID was not found. |
| 230 | policyAnnounceIntfListidNotFound | The specified policy announce interface list ID was not found. |
| 231 | policyAdvertNetListidNotFound | The specified policy advertise network list ID was not found. |
| 232 | policyInjectNetListidNotFound | The specified policy inject network list ID was not found. |
| 233 | policyInvalidIdListSize | The list size of the policy is invalid. |
| 234 | policyAddrEntryNotFound | The specified IP policy address list entry was not found. |
| 235 | policyAddrDuplicateEntry | The specified IP policy address list entry is a duplicate. |
| 236 | ipfPortDisableFirst | Before completing the specified action, you must first disable the filtered port. |
| 237 | multinettingNotSupported | Multinetting is not supported. |
| 238 | ipfGlobalToBaseList | You are attempting to add a global filter to a nonglobal list. |
| 239 | nonblobalToGlobalList | You are attempting to add a nonglobal filter to a global list. |
| 240 | ipfSetModeAlso | You are attempting to enable ports without setting the port mode. |
| 241 | ipfSetEnableAlso | You are attempting to set port mode without enabling or disabling the port. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 242 | ipfInvalidMode | The specified IP filter port mode is invalid. |
| 243 | acceptRipPolicyDuplicateEntry | The specified entry in the RIP accept policy is a duplicate. |
| 244 | acceptRipPolicyEntryNotFound | The specified RIP accept policy was not found. |
| 245 | acceptOspfPolicyDuplicateEntry | The specified entry in the OSPF accept policy is a duplicate. |
| 246 | acceptOspfPolicyEntryNotFound | The specified OSPF accept policy cannot be found. |
| 247 | invalidAccPolicyName | The access policy name is invalid. |
| 248 | invalidAccPolicyPolicyEnable | An invalid access policy is active. |
| 249 | invalidAccPolicyMode | The access policy mode is invalid. |
| 250 | invlaidAccPolicyService | The access policy service is invalid. |
| 251 | invalidAccPolicyPrecedence | The access policy precedence is invalid. |
| 252 | invlaidAccPolicyNetAddr | The access policy net address is invalid. |
| 253 | invlaidAccPolicyTrustedHostAddr | The access policy trusted host address is invalid. |
| 254 | invlaidAccPolicyTrustedHost-UserName | The access policy trusted host user name is invalid. |
| 255 | invalidAccPolicyAccessLevel | The access policy access level is invalid. |
| 256 | invalidAccPolicyLog | The policy log setting is invalid. |
| 257 | invalidAccPolicyId | The access policy ID is invalid. |
| 258 | invalidAreaOptions | The area options stub and import combinations are invalid. |
| 259 | areaIntfCountNotZero | You cannot delete an area interface count greater than zero. |
| 260 | ospfIntfNotFound | The specified OSPF interface was not found. |
| 261 | ospfIntfAreaConflictsWithAreaRange | The interface area ID conflicts with the configured range. |
| 262 | ipfGlistDuplicateFilter | A duplicate global filter was applied to the port. |
| 263 | mltPortDifferentType | The specified MultiLinkTrunking ports are different types. |
| 264 | mltAddPortFail | The MultiLink Trunk add port command failed. |
| 265 | mltRemovePortFail | The MultiLink Trunk remove port command failed. |
| 266 | mirrorPortInMlt | The mirror port is a MultiLink Trunk port. |
| 267 | badDhcpAlwaysBroadcast | DHCP is always broadcasting values out of range. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 268 | interfaceIsSetToTxRipv1 | The RIP transmit for this interface is set to v1. |
| 269 | ripInterfaceDoesnotExist | The specified RIP interface does not exist. |
| 270 | interfaceIsNotRunningRip | The specified interface is not running RIP protocol. |
| 271 | cannotCreateVlinksThroughStubArea | You cannot create virtual links through a stub area. |
| 272 | invalidSyslogGlobalEnable | The specified Syslog global enable/disable settings are invalid. |
| 273 | invlaidSyslogEnabledHost | The specified Syslog maximum hosts setting is invalid. |
| 274 | invlalidSyslogHostIpaddr | The specified Syslog host IP address is invalid. |
| 275 | invlalidSyslogHostUdpPort | The specified Syslog host UDP port is invalid. |
| 276 | invlalidSyslogHostFacility | The specified Syslog host facility is invalid. |
| 277 | invalidSyslogHostModuleId | The specified Syslog host module ID is invalid. |
| 278 | invlalidSyslogSeverity | The specified Syslog severity is invalid. |
| 279 | invlalidSyslogMapInfoSeverity | The specified Syslog map Information severity is invalid. |
| 280 | invlalidSyslogMapWarningSeverity | The specified Syslog map Warning severity is invalid. |
| 281 | invalidSyslogMapErrorSeverity | The specified Syslog map Error severity is invalid. |
| 282 | invalidSyslogMapMfgSeverity | The specified Syslog map Manufacturing severity is invalid. |
| 283 | invalidSyslogMapFatalSeverity | The specified Syslog map Fatal severity is invalid. |
| 284 | invalidSyslogMapTraceMsg | The specified Syslog map trace message is invalid. |
| 285 | invalidSyslogMapTrapMsg | The specified Syslog map trap message is invalid. |
| 286 | invalidSyslogLogTraceMsg | The specified Syslog log trace message is invalid. |
| 287 | invalidSyslogLogTrapMsg | The specified Syslog log trap message is invalid. |
| 288 | invalidSyslogHostEnable | The specified Syslog host enable/disable setting is invalid. |
| 289 | syslogMacEnabledHostsExceed | The maximum allowable number of enabled syslog hosts has been exceeded. |
| 290 | invlalidSyslogHostID | The specified syslog host entry ID is invalid. |
| 291 | syslogHostExists | The specified syslog host entry already exists. |
| 292 | syslogHostTblFull | The syslog host table is full. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 293 | noDesiredSyslogHostItem | No desired syslog host entry was found. |
| 294 | invalidHoldDownTime | The specified holddown time value is invalid. |
| 295 | incompatibleAruHardware | The specified feature is not supported on this ARU hardware version. |
| 296 | invalidVRID | The specified virtual router ID is invalid. |
| 297 | duplicateVrrpEntry | The VRRP entry is a duplicate. |
| 298 | noVrrpIpAddressSpecified | No VRRP IP address was specified. Enter a VRRP IP address. |
| 299 | invalidVrrpControl | The specified VRRP control value is not valid. |
| 300 | invalidVrrpPrio | The specified VRRP priority value is not valid. |
| 301 | invalidVrrpAdvertInt | The specified VRRP advertisement interval is not valid. |
| 302 | tooManyVrrps | The maximum number of VRRP entries has been exceeded. |
| 303 | policyNetListEntryNotFound | The specified policy match list entry was not found. |
| 304 | policyNetListDuplicateEntry | The specified announce match entry is a duplicate. |
| 305 | policyNetListIdEntryNotFound | The specified policy route list entry route ID was not found. |
| 306 | ipfFilterOnEnabledPort | You are attempting to delete a filter that is on an enabled port. |
| 307 | ipfListOnEnabledPort | You are attempting to delete a list that is on an enabled port. |
| 308 | invalidIpFilterSrsOption | The specified filter source IP address is not valid. |
| 309 | invalidIpFilterDstOption | The specified filter destination IP address is not valid. |
| 310 | invalidospfAreaImportextOption | The OSPF area import text is not valid. |
| 311 | invalidOspfInterfaceMd5KeyIdLength | The ID length of the specified OSPF interface MD5 authentication key is not valid. |
| 312 | invalidOspfInterfaceMd5KeyLength | The length of the specified OSPF interface MD5 authentication key is not valid. |
| 313 | invalidIPXNetworkNumber | The specified IPX network number is not valid. |
| 314 | ipxCircuitAlreadyExists | The specified IPX circuit already exists. |
| 315 | ipxCircuitDoesNotExist | The specified IPX circuit does not exist. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 316 | encapsulationIsNotAllowedOnSame Segment | You cannot set IPX encapsulation on the same network segment. |
| 317 | encapsulationDoesNotMatchProtocol BasedVLAN | The IPX encapsulation method does not match the protocol-based VLAN. |
| 318 | invalidDvmrpIfTblEnableValue | The enable value in the DVMRP interface table is not valid. |
| 319 | invalidDvmrpIfTblMetricValue | The specified metric in the DVMRP interface table is not valid. |
| 320 | ipHostPartForSubnetAddrIsNonZero | The IP host part of the specified subnet address is not zero. |
| 321 | globalMulticastNotEnabled | Multicasting is not enabled globally. |
| 322 | metricFieldIsCreatedButModified | The specified metric field has been modified. |
| 323 | invalidIpMRouteInterfaceTblTtlValue | The time-to-live value in the Multicast Router interface table is not valid. |
| 324 | invalidUdpPortNumber | The UDP port number is not valid. |
| 325 | invalidUdpProtocolNameLength | The UDP protocol name length is not valid. |
| 326 | cannotModifyUdpProtocolName | The UDP protocol name cannot be modified. |
| 327 | udpProtocolEntryDoesNotExist | The UDP protocol entry does not exist. |
| 328 | duplicateUdpProtocolEntry | The UDP protocol entry is a duplicate. |
| 329 | cannotDelUdpProtocolEntryFwdEntries Exist | You cannot delete existing UPD protocol entry forwarding entries. |
| 330 | udpBroadcastIntfEntryDoesnotExist | The UDP broadcast interface entry does not exist. |
| 331 | duplicateUdpBroadcastIntfEntry | The UDP broadcast interface entry is a duplicate. |
| 332 | invalidUdpConfBroadcastInterface | The UDP configuration broadcast interface is not valid. |
| 333 | udpConfIntfEntryNotEnabledForUdp BcastForwarding | The UDP configuration interface entry is not enabled for UDP broadcast forwarding. |
| 334 | udpPortFwdEntryDoesnotExist | The UDP port forward entry does not exist. |
| 335 | duplicateUdpPortFwdEntry | The UDP port forward entry is a duplicate. |
| 336 | udpPortFwdEntryYUdpPortInterfaceDoes notExist | The UDP port forward entry UDP port interface does not exist. |
| 337 | udpPortFwdListEntryDoesnotExist | The UDP port forward entry list does not exist. |
| 338 | duplicateUdpPortFwdListEntryDoesnot Exist | The UDP port forward list entry is a duplicate. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 339 | udpPortFwdListEntryPortFwdIdDoesnot Exist | The UDP port forward list entry port forward ID does not exist. |
| 340 | updPortFwdListEntryinvalidFwdIdListSize | The UDP port forward list has an invalid ID list size. |
| 341 | cannotDeleteUdpPortFwdListEntry InterfaceUsingThisList | You cannot delete a UDP forward list entry interface using this list. |
| 342 | invalidIgmpSnoopDestAddress | The IGMP snooping destination address is not valid. |
| 343 | invalidIgmpSnoopHostAddress | The IGMP snooping host address is not valid. |
| 344 | cannotDeleteDefaultUdpProtocolTblEntry | You cannot delete the default UDP protocol table entry. |
| 345 | nextHopRouteIsStaticRoute | The next Hop Route is static. |
| 346 | invalidUpdateIntervalValueInDVMRP GlobalTable | There is an invalid update interval value in the DVMRP Global Table |
| 347 | invalidTriggeredUpdateIntervalValueIn DVMRPGlobalTable | There is an invalid triggered update interval value in the DVMRP Global Table. |
| 348 | invalidLeafTimeoutValueInDVMRPGlobal Table | There is an invalid Leaf timeout value in the DVMRP Global Table. |
| 349 | invalidNbrTimeoutValueInDVMRPGlobal Table | There is an invalid Nbr timeout value in the DVMRP Global Table. |
| 350 | invalidNbrProbeIntervalValueInDVMRP GlobalTable | There is an invalid Nbr probe interval value in the DVMRP Global Table. |
| 351 | invalidQueryIntervalValueInIgmpInterface Table | There is an invalid query interval value in the IGMP Interface Table. |
| 352 | invalidVersionValueInIgmpInterfaceTable | There is an invalid version value in the IGMP Interface Table. |
| 353 | invalidQueryMaxResponseTimeValue InIgmpInterfaceTable | There is an invalid query maximum response time value in the IGMP Interface Table. |
| 354 | invalidRobustnessValueInIgmpInterface Table | There is an invalid robustness value in the IGMP Interface Table. |
| 355 | invalidLastMembQueryIntvlValueInIgmp InterfaceTable | There is an invalid last member query interval value in the IGMP Interface Table. |
| 356 | invalidANDMaskInRcIpTosRuleGroup | There is an invalid AND mask in the Rclp to s Rule Group. |
| 357 | invalidORRule1InRcIpTosRuleGroup | There is an invalid OR rule 1 in the Rclp to s Rule Group. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 358 | invalidORRule2InRcIpTosRuleGroup | There is an invalid OR rule 2 in the Rclp to s Rule Group. |
| 359 | invalidORRule3InRcIpTosRuleGroup | There is an invalid OR rule 3 in the Rclp to s Rule Group. |
| 360 | deleteStaticPortNotValid | It is not valid to delete the static port. |
| 361 | maxEntriesForIgmpAccTbl | The maximum number of entries has been reached for the Igmc access table. |
| 362 | maxMaskNumberOfHostIgmpAccTbl | The maximum mask number of hosts has been reached for the Igmc access table. |
| 363 | dvmrpIgmpExclusive | The DVMRP is exclusive. |
| 364 | theSpecifiedAreaRangeMaskIsInvalid | The specified Area Range Mask is invalid. |
| 365 | invalidLengthOf2kBootConfigImage Source | The length of the 2K Boot Configuration Image Source is invalid. |
| 366 | invalidLengthOf2kBootConfigSource | The length of the 2K Boot Configuration Source is invalid. |
| 367 | preferenceOfStaticRouteIsInvalid | The static route preference is invalid. |
| 368 | copyFileOutOfSpace | The copy file is out of space. |
| 369 | copyFileFileNotFound | The copy of the file is not found. |
| 370 | copyFileInvalidDestination | The destination of the copy file is invalid. |
| 371 | copyFileInvalidSource | The source of the copy file is invalid. |
| 372 | copyFileFail | The copying of the file failed. |
| 373 | invalidLinkFlapDetectAutoPortDown | The Link Flap Detect Auto Port down is invalid. |
| 374 | invalidLinkFlapDetectFrequency | The link flap detect frequency is invalid. |
| 375 | invalidLinkFlapDetectInterval | The link flap detect interval is invalid. |
| 376 | invalidLinkFlapDetectSendTrap | The link flap detect send trap is invalid. |
| 377 | invalidQosLevel | The Qos level is invalid. |
| 378 | invalidQosWeight | The Qos weight is invalid. |
| 379 | invalidQosThreshold | The Qos threshold is invalid. |
| 380 | invalidTagToQosTableIeee1pValue | The Tag to Qos table 1p value is invalid. |
| 381 | invalidTagToQosTableQosLevel | The Tag to Qos Table Qos level is invalid. |
| 382 | invalidDsFieldToQosTableDsField | The Ds Field to Qos Table Ds is invalid. |
| 383 | invalidDsFieldToQosTableQosLevel | The Ds Field to Qos Table Qos is invalid. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 384 | invalidQosToTagTableQosLevel | The Qos to Tag Table Qos level is invalid. |
| 385 | invalidQosToTagTableIeee1pValue | The Qos to Tag Table Ieee1 value is invalid. |
| 386 | invalidQosLevelValue | The Qos level value is invalid. |
| 387 | invalidQosToDsFieldTableDsFieldValue | The Qos to DS Field Table Ds Field value is invalid. |
| 388 | invalidQosToDsFieldTableQosLevel | The Qos to Ds Field Table Qos level is invalid. |
| 389 | invalidDiffServEnable | The different server enabled is invalid. |
| 390 | invalidDiffServType | The different server type is invalid. |
| 391 | invalidIeeeOverride | The Ieee override is invalid. |
| 392 | invalidVlanQosValue | The VLAN Qos value is invalid. |
| 393 | invalidVlanTosValue | The VLAN Tos value is invalid. |
| 394 | operationNotAllowedOnAccessPort | The operation is not allowed to access the port. |
| 395 | operationNotAllowedOnTaggingPort | The operation is not allowed on the tagging port. |
| 396 | invalidFileName | The file name is invalid. |
| 397 | invalidDiaglogueDuplicateMirroredPort | The dialog duplicate mirrored port is invalid. |
| 398 | invalidDiaglogueEnableValue | The dialog enable value is invalid. |
| 399 | invalidDiaglogueEnableSetting | The dialog enable setting is invalid. |
| 400 | invalidDiaglogueModeSetting | The dialog mode setting is invalid. |
| 401 | invalidDiaglogueEntryId | The dialog entry ID is invalid. |
| 402 | srcMacVlanIsNotYetEnabled | The source MacVLAN is not yet enabled. |
| 403 | srcMacVlanIsNotYetDisabled | The source MacVLAN is not yet disabled. |
| 404 | invalidDiaglogueOperation | The dialog operation is invalid. |
| 405 | invalidMacAddressSpecied | The Mac address specified is invalid. |
| 406 | maxResponseTimeGreaterThanQuery Interval | The maximum response time is greater than the query interval. |
| 407 | noModifyDsFltrAllowedOnDiffSrvCorePort | Modifying the DS filter on a different core server is not available. |
| 408 | mltMoreThan4PortsInMgMlt | MLT has more than 4 ports in the MgMlt. |
| 409 | protocolRulesForThePortHasExceeded16 | The number of rules for the port has exceeded 16. |
| 410 | routeDoesNotExistsInTheRroutingTable | The route does not exist in the routing table. |
| 411 | diagMirrorByPortTableAccessError | An error occurred when accessing the diag mirror by port table. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 412 | diagMirrorByPortInvalidMirroringPort Setting | The port setting for diag mirror by port is invalid. |
| 413 | igmpAdminVersionConfiguredLessThan OperatingVersion | The configured IGMP administration version is less than the operating version. |
| 414 | canOnlyConfigureViaMltTable | You can only configure the Via MLT table. |
| 415 | dvmrpInterfaceTableIsFull | The DVMRP interface table is full. |
| 416 | invalidDscpField | The description field is invalid. |
| 417 | invalidDscpReservedField | The description reserved field is invalid. |
| 418 | disablePortPriorToChangingDiffServPort Type | You must disable the port before you change to a different server port type. |
| 419 | ipFilterInvalidId | The IP filter ID is invalid. |
| 420 | rateLimitingExceeded | Rate limiting has been exceeded. |
| 421 | diagEntryMaxExceeded | The maximum diag entries has been exceeded. |
| 422 | onlyOneMirroringPortAllow | Only one mirroring port is allowed. |
| 423 | radiusServerExist | The radius server is available. |
| 424 | radiusServerNotExist | The radius server is not available. |
| 425 | radiusServerInUse | The radius server is in use. |
| 426 | radiusMaxServerNumExceeded | The maximum number of radius servers has been exceeded. |
| 427 | radiusInvalidAttribute | The radius attribute is invalid. |
| 428 | canNotChangeLocking | The locking cannot be changed. |
| 429 | activationDisabled | Activation has been disabled. |
| 430 | zeroMac | Mac is not available. |
| 431 | atmBadVpi | The ATM Vpi is wrong. |
| 432 | atmBadVci | The ATM Vci is wrong. |
| 433 | atmBadFramingMode | The ATM framing mode is wrong. |
| 434 | atmDestroyPvcFailed | The ATM Destroy Pvc has failed. |
| 435 | atmBadName | The ATM name is wrong. |
| 436 | atmBadEnable | The ATM enable is wrong. |
| 437 | atmBadpvcEncapsulation | The ATM encapsulation is wrong. |
| 438 | atmBadPvdServiceType | The ATM Pvd service type is wrong. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 439 | atmBadPeakCellRate | The ATM peak cell rate is wrong. |
| 440 | atmBadSustainedCellRate | The ATM sustained cell rate is wrong. |
| 441 | atmBadMaxBurstSize | The ATM maximum burst size is wrong. |
| 442 | atmBadMaxMtuSize | The ATM maximum MTU is wrong. |
| 443 | atmBadElanId | The ATM ELAN ID is wrong. |
| 444 | atmUnknownOperation | The ATM operation is unknown. |
| 445 | atmDestroy1483ElanFailed | The ATM destroy 1483 ELAN has failed. |
| 446 | atmBadPerformTagging | The ATM tagging is wrong. |
| 447 | atmIlleagalElanDefinition | The ATM ELAN definition is wrong. |
| 448 | atmCreate1483ElanFailed | The ATM Create 1483 ELAN has failed. |
| 449 | atmBadSnmpMessage | The ATM SNMP message is wrong. |
| 450 | atmBadScrambleEnable | The ATM Scramble enabling is wrong. |
| 451 | atmBadSignalingEnable | The ATM signal enabling is wrong. |
| 452 | atmBadClockSource | The ATM clock source is wrong. |
| 453 | atmBadLoopback | The ATM loopback is wrong. |
| 454 | badRowStatus | The row status is wrong. |
| 455 | atmBadLaneConfigMode | The lane configuration mode is wrong. |
| 456 | atmLecCreationFailed | ATM LEC creation has failed. |
| 457 | atmBad1438Inarp | The ATM 1438 Inarp is wrong. |
| 458 | atmF5StartFailed | The ATM F5 Start has failed. |
| 459 | atmBadPvcId | The ATM Pvcld is wrong. |
| 460 | atmBadConnectType | The ATM connect type is wrong. |
| 461 | atmBadIpxEncapMethod | The ATM encap method is wrong. |
| 462 | atmBadUniVersion | The ATM Universion is wrong. |
| 463 | atmCreatePvcFailed | The ATM create Pvc failed. |
| 464 | invalidLoginPromptLength | The login prompt length is invalid |
| 465 | invalidPasswordPromptLength | The password prompt length is invalid |
| 466 | invalidCliBannerLength | The Cli banner length is invalid. |
| 467 | invalidCliBannerSize | The Cli banner size is invalid. |
| 468 | invalidCliMotdLength | The Climotd length is invalid. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 469 | invalidCliMotdSize | The Climotd size is invalid. |
| 470 | invalidPortNameLength | The port name length is invalid. |
| 471 | invalidPortName | The port name is invalid. |
| 472 | invalidMaxAdvertiseInterval | The maximum advertise interval is invalid. |
| 473 | invalidMinAdvertiseInterval | The minimum advertise interval is invalid. |
| 474 | invalidMaxInitialAdvertiseInterval | The maximum initial advertise interval is invalid. |
| 475 | invalidMaxInitalAdvertments | The maximum advertisements is invalid. |
| 476 | invalidNeigborDeadInterval | The neighbor dead interval is invalid. |
| 477 | invalidUserSetTimeYearValue | The Year setting is invalid. |
| 478 | invalidUserSetTimeMonthValue | The Month setting is invalid. |
| 479 | invalidUserSetTimeDateValue | The Date setting is invalid. |
| 480 | invalidUserSetTimeHourValue | The Hour setting is invalid. |
| 481 | invalidUserSetTimeMinuteValue | The Minute setting is invalid. |
| 482 | invalidUserSetTimeSecondValue | The Second setting is invalid. |
| 483 | rtcIsNotPresent | The RTC is not present. |
| 484 | rtcIsNotRunning | The RTC is not running. |
| 485 | maxMacCount | The maximum Mac count has been reached. |
| 486 | maxAdvertiseIntLessThanMinAdvertiseInt | The maximum advertise interval is greater than the minimum advertise interval. |
| 487 | minAdvertiseIntGreaterThanMax AdvertiseInt | The minimum advertise interval is greater than the maximum advertise interval. |
| 488 | dvmrpNotEnabledGlobally | The DVMRP is not enabled globally. |
| 489 | vrrpCriticalIpAddrNotEnable | The critical IP address is not enabled. |
| 490 | vrrpInvalidCriticalIpAddress | The Critical IP address in invalid. |
| 491 | metricConfigNotAllowed | The configuration is not allowed. |
| 492 | posActiveNonBcpEnabledPort | A non-active bridge control protocol is enabled. |
| 493 | posVlanNoMorePorts | There are no more VLAN ports. |
| 494 | posPortCanBeAdded | No more POS ports can be added. |
| 495 | posNonBcpCanNotBeEnabled | A bridge control protocol cannot be enabled. |
| 496 | posImageFilenameTooLong | The image file name is to long. |
| 497 | posNoIpcpEnableOnMltPorts | There is no IPCP enabled on MultiLink Trunk ports. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 498 | posNoIpcpEnableOnTagPort | There is no IPCP enabled on tagged ports. |
| 499 | posNoIpxEnableOnMltPort | No IPX protocol enabled on MultiLink Trunk ports. |
| 500 | posNoIpxcpEnableOnTagPort | No IPXCP enabled on tagged ports. |
| 501 | posDisableTagBeforeBcpDisable | A tagged port is disabled before BCP is disabled. |
| 502 | posAssignIpBeforeIpcpEnable | An IP is assigned before IPCP is enabled. |
| 503 | posAssignIpxBeforeIpxcpEnable | IPX is assigned before IPXCP is enabled. |
| 504 | posAssignIpBeforeRemoteIp | An IP is assigned before a remote IP is assigned. |
| 505 | posKeepRemoteIpInSameSubnet | The remote IP must be in the same subnet. |
| 506 | staticRouteEnabled | A static route is enabled. |
| 507 | cannotChangeAutoLearnState | You cannot change the Auto Learn state. |
| 508 | invalidVirtualIpAddr | Invalid virtual IP address. |
| 509 | virtualAndPhyIpNotInSameSubnet | A virtual and physical IP cannot be in the same subnet. |
| 510 | vidNotAvailable | The VLAN id is not available. |
| 511 | mgidNotAvailable | The MG id is not available. |
| 512 | posNoIpcpEnableOnPolicyVlanPort | No IPCP is enabled on a policy-based VLAN. |
| 513 | posNoIpxcpEnableOnPolicyVlanPort | No IPXCP is enabled on a policy-based VLAN. |
| 514 | posVrrpNotAllowed | VRRP not allowed. |
| 515 | webInvalidHttpPort | Invalid Http port. |
| 516 | cannotAddMulticastStaticMac | Cannot add a multicast static MAC address. |
| 517 | posNoStpEnableWithBCPClosed | No STP enabled with BCP closed. |
| 518 | posAtmNoRipl | No ATM RIP. |
| 519 | ipfFilterNumOverFilterSetLimit | The IP filter number is greater than the filter limit set. |
| 520 | ipfQosTrafficAverageRateOverLimit | The IP Qos traffic is over the rate limit set. |
| 521 | ipfQosTrafficProfileNotExist | The Qos traffic profile does not exist. |
| 522 | atmNoIpIpxConfigOnVlan | No IPX configured on the VLAN. |
| 523 | atmPvcIsInUse | The PVC is in use. |
| 524 | globalFilterNotDisables | The global filter is not disabled. |
| 525 | dhcpNotOnByIpSubnetVlan | No DHCP defined on a byIPSubnet VLAN. |
| 526 | cannotConfigureDefaultGateway | Can not configure a default gateway. |

**Table 77** Error codes, messages, and descriptions (continued)

| Code Number | Error Message | Description |
|---|---|---|
| 527 | routeExists | The route does not exist. |
| 528 | gatewayNotOnMgmtInterfaceSubnet | The gateway is not on the management interface subnet. |
| 529 | mgmtRouteTableFull | The management port route table is full. |
| 530 | routeNotExists | The route does not exist. |
| 531 | invalidMacOffsetRangeForBW | Invalid MAC offset range for BW. |
| 532 | invalidMacOffsetRangeForMG | Invalid MAC offset range for MG. |
| 533 | atmPvcBadPeakCellRate | A bad PVC peak cell rate. |
| 534 | atmPvcBadSustainedCellRate | A bad PVC sustained cell rate. |
| 535 | qosReservedQosLevel | Reserved Qos level. |
| 536 | ipfQosTrafficAvgRateZeroProfileEnable | Qos Traffic Average Rate Zero Profile enabled. |

# Appendix B
# RMON alarm variables

RMON alarm variables are divided into three categories. Each category can have a number of subcategories.

Table 78 lists the alarm variable categories and provides a brief variable description.

**Table 78** Alarm variables

| Category | Subcategory | Variable | Definition |
|---|---|---|---|
| **Security** | | rcCliNumAccess Violations.0 | The number of CLI access violations detected by the system. |
| | | rcWebNumAccess Blocks.0 | The number of accesses blocked by the Web server. |
| | | snmpInBadCommunity Names.0 | The total number of SNMP messages delivered to the SNMP protocol entity that represented an SNMP operation not allowed by the SNMP community named in the message. |
| **Errors** | **Interface** | ifInDiscards | 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. |
| | | ifInErrors | 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. |
| | | ifOutDiscards | The number of outbound packets that 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. |

**Table 78** Alarm variables (continued)

| Category | Subcategory | Variable | Definition |
|---|---|---|---|
| | | ifOutErrors | 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. |
| | **Ethernet** | dot3StatsAlignment Errors | A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the Frame Check Sequence (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 exist are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. |
| | | dot3StatsFCSErrors | 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. |
| | | dot3StatsSingle CollisionFrames | 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 object, the ifOutMulticastPkts object, or the ifOutBroadcastPkts object, and is not counted by the corresponding instance of the dot3StatsMultipleCollisionFrames object. |
| | | dot3StatsMultiple CollisionFrames | 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 object, and is not counted by the corresponding instance of the dot3StatsSingleCollisionFrames object. |

**Table 78** Alarm variables (continued)

| Category | Subcategory | Variable | Definition |
|---|---|---|---|
| | | dot3StatsSQETest Errors | 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. |
| | | dot3StatsDeferred Transmissions | 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. |
| | | dot3StatsLate Collisions | The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet; 512 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. |
| | | dot3StatsExcessive Collisions | A count of frames for which transmission on a particular interface fails due to excessive collisions. |
| | | dot3StatsInternalMac TransmitErrors | 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 dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object.<br>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 transmission errors on a particular interface that are not otherwise counted. |
| | | dot3StatsCarrierSense Errors | The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt. |

**Table 78** Alarm variables (continued)

| Category | Subcategory | Variable | Definition |
|---|---|---|---|
| | | dot3StatsFrameTooLongs | 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 obtained are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. |
| | | dot3StatsInternalMacReceiveErrors | 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 dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object.<br>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 transmission errors on a particular interface that are not otherwise counted. |
| | **IP** | ipInHdrErrors.0 | 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, and errors discovered in processing their IP options. |
| | | ipInDiscards.0 | 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. |
| | | ipOutDiscards.0 | 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. |
| | | ipFragFails.0 | 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. |

**Table 78** Alarm variables (continued)

| Category | Subcategory | Variable | Definition |
|---|---|---|---|
| | | ipReasmFails.0 | The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, and so forth). 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. |
| | | icmpInParmProbs.0 | The number of ICMP In parameter problem messages received. |
| | | icmpOutParmProbs.0 | The number of ICMP Out parameter problem messages received. |
| | **MLT** | rcStatMltEther AlignmentErrors | The number of frames received on an MLT that are not an integral number of octets in length but do not pass the FCS check. |
| | | rcStatMltEtherFCS Errors | The number of frames received on an MLT that are an integral number of octets in length but do not pass the FCS check. |
| | | rcStatMltEtherSingle CollFrames | The number of successfully transmitted frames on a particular MLT for which transmission is inhibited by exactly one collision. |
| | | rcStatMltEtherMultiple CollFrames | The number of successfully transmitted frames on a particular MLT for which transmission is inhibited by more than one collision. |
| | | rcStatMltEtherSQETest Error | A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular MLT. |
| | | rcStatMltEtherDeferred Transmiss | 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. |
| | | rcStatMltEtherLate Collisions | The number of times that a late collision is detected on a particular MLT later than 512 bit-times into the transmission of a packet; 512 bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. |
| | | rcStatMltEther ExcessiveCollis | The number of times that excessive collisions are detected on a particular MLT later than 512 bit-times into the transmission of a packet; 512 bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. |

**Table 78** Alarm variables (continued)

| Category | Subcategory | Variable | Definition |
|---|---|---|---|
| | | rcStatMltEtherMac TransmitError | 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. |
| | | rcStatMltEtherCarrier SenseError | 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. |
| | | rcStatMltEtherFrame TooLong | A count of frames received on a particular MLT that exceed the maximum permitted frame size.<br>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). |
| | | rcStatMltEtherMac ReceiveError | 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. |
| | **Other** | rcTblArNoSpace | Used to indicate the number of entries that could not be added to the address translation table due to lack of space. |
| | | snmpInAsnParseErrs.0 | The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding received SNMP messages. |
| | | rcStgPortInBadBpdus | The number of bad BPDUs received by this port. |
| | | dot1dTpPortInDiscards | Count of valid frames received that were discarded (that is, filtered) by the forwarding process. |
| | | rip2ifStatRcvBad Packets | The number of routes in valid RIP packets that were ignored for any reason. |
| | | rip2ifStatRcvBad Routes | The number of RIP response packets received by the RIP process that were subsequently discarded for any reason. |
| | | rcStatOspfBufferAlloc Failures.0 | The number of times that OSPF has failed to allocate buffers. |

**Table 78** Alarm variables (continued)

| Category | Subcategory | Variable | Definition |
|---|---|---|---|
| | | rcStatOspfBufferFree Failures.0 | The number of times that OSPF has failed to free buffers. |
| **Traffic** | **Interface** | ifInOctets | The total number of octets received on the interface, including framing characters. |
| | | ifInMulticastPkts | The number of packets, delivered by this sublayer to a higher sublayer, that were addressed to a multicast address at this sublayer. For a MAC layer protocol, this number includes both Group and Functional addresses. |
| | | ifInBroadcastPkts | The number of packets, delivered by this sublayer to a higher (sub-)layer, that were addressed to a broadcast address at this sublayer. |
| | | ifInUnkownProtos | 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. |
| | | ifOutOctets | The total number of octets transmitted out of the interface, including framing characters. |
| | | ifOutMulticastPkts | The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a multicast address at this sublayer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. |
| | | ifoutBroadcastPkts | The total number of packets that higher level protocols requested to be transmitted, and that were addressed to a broadcast address at this sub layer, including those that were discarded or not sent. |
| | | ifLastChange | 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, then this object contains a zero value. |

**Table 78** Alarm variables (continued)

| Category | Subcategory | Variable | Definition |
|---|---|---|---|
| | **RmonEther Stats** | etherStatsOctets | The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. For greater precision, sample the etherStatsPkts and etherStatsOctets objects before and after a common interval. |
| | | etherStatsPkts | The total number of packets (including bad packets, broadcast packets, and multicast packets) received. |
| | | etherStatsBroadcast Pkts | The total number of good packets received that were directed to the broadcast address. Note that this number does not include multicast packets. |
| | | etherStatsMulticast Pkts | 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. |
| | | etherStatsCRCAlign Errors | 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). |
| | | etherStatsUndersize Pkts | 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. |
| | | etherStatsOversize Pkts | The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. |
| | | etherStatsFragments | 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).<br>**Note:** It is entirely normal for etherStatsFragments to increment because it counts both runts (which are normal occurrences due to collisions) and noise hits. |
| | | etherStatsCollisions | The best estimate of the total number of collisions on this Ethernet segment. |
| | **IP** | ipInReceives.0 | All incoming IP packets. |
| | | ipInAddrErrors.0 | The number of bad IP destination addresses. |

**Table 78** Alarm variables (continued)

| Category | Subcategory | Variable | Definition |
|---|---|---|---|
| | | ipForwDatagrams.0 | IP packets forwarded. |
| | | ipInUnknownProtos.0 | Number of unsupported IP protocols. |
| | | ipInDelivers.0 | The number of IP In packets delivered. |
| | | ipOutRequests.0 | The total number of IP datagrams that local IP user-protocols supplied to IP in request for transmission. |
| | | ipOutNoRoutes.0 | The number of IP datagrams discarded because no route could be found to transmit to their destination. |
| | | ipFragOKs.0 | The number of IP datagrams that have been successfully fragmented. |
| | | ipFragCreates.0 | The number of IP datagram fragments that have been generated as a result of fragmentation. |
| | | ipReasmReqds.0 | The number of requests to reassemble fragments. |
| | | ipReasmOKs.0 | The number of fragments reassembled successfully. |
| | **ICMP** | IcmpInSrcQuenchs.0 | The number of ICMP Source Quench messages received. |
| | | icmpInRedirects.0 | The number of ICMP redirect messages. |
| | | icmpInEchos.0 | The number of ICMP Echo requests messages received. |
| | | icmpInEchosReps.0 | The number of ICMP Echo reply messages received. |
| | | icmpInTimeStamps.0 | The number of ICMP timestamp request messages received. |
| | | icmpInTimeStamps Reps.0 | The number of ICMP timestamp reply messages received. |
| | | icmpInAddrMasks.0 | The number of ICMP mask request messages reviewed. |
| | | icmpInAddrMasks Reps.0 | The number of ICMP mask reply messages reviewed. |
| | | icmpInDestUnreachs.0 | The number of ICMP destinations unreachable messages received. |
| | | icmpInTimeExcds.0 | The number of ICMP Time Exceeded messages received. |
| | | icmpOutSrcQuenchs.0 | The number of ICMP Source Quench messages sent. |
| | | icmpOutRedirects.0 | The number of ICMP redirect messages sent. |
| | | icmpOutEchos.0 | The number of ICMP Echo request messages sent. |

**Table 78** Alarm variables (continued)

| Category | Subcategory | Variable | Definition |
|---|---|---|---|
| | | icmpOutEchosReps.0 | The number of ICMP Echo reply messages sent. |
| | | icmpOutTimeStamps.0 | The number of ICMP Timestamp request messages sent. |
| | | icmpOutTimeStamps Reps.0 | The number of ICMP Timestamp reply messages sent. |
| | | icmpOutAddrMasks.0 | The number of ICMP Address mask messages sent. |
| | | icmpOutAddrMasks Reps.0 | The number of ICMP Address mask reply messages sent. |
| | | icmpOutDest Unreachs.0 | The number of ICMP destination unreachable messages sent. |
| | | icmpOutTimeExcds.0 | The number of ICMP time exceeded messages sent. |
| | **Snmp** | snmpInPkts.0 | The total number of messages delivered to the SNMP entity from the transport service. |
| | | snmpOutPkts.0 | The total number of SNMP messages that were passed from the SNMP protocol entity to the transport service. |
| | | snmpInBadVersions.0 | The total number of SNMP messages that were delivered to the SNMP protocol entity and were for an unsupported SNMP version. |
| | | snmpInBadCommunity Uses.0 | The total number of SNMP messages delivered to the SNMP protocol entity that represented an SNMP operation that was not allowed by the SNMP community named in the message. |
| | | snmpInTooBigs.0 | The total number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is tooBig. |
| | | snmpInNoSuch Names.0 | The total number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is noSuchName. |
| | | snmpInBadValues. 0 | The total number of SNMP PDUs received that were generated by the SNMP protocol entity and for which the value of the error-status field is badValue. |
| | | snmpInReadOnlys.0 | The total number of valid SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is readOnly. It should be noted that it is a protocol error to generate an SNMP PDU that contains the value readOnly in the error-status field; as such, this object is provided as a means of detecting incorrect implementations of the SNMP. |

**Table 78** Alarm variables (continued)

| Category | Subcategory | Variable | Definition |
|---|---|---|---|
| | | snmpInGenErrs.0 | The total number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is genErr. |
| | | snmpInTotalReqVars.0 | The total number of MIB objects that have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs. |
| | | snmpInTotalSetVars.0 | The total number of MIB objects that have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs. |
| | | snmpInGetRequests.0 | The total number of SNMP Get-Request PDUs that have been accepted and processed by the SNMP protocol entity. |
| | | snmpInGetNexts.0 | The total number of SNMP Get-Next PDUs that have been accepted and processed by the SNMP protocol entity. |
| | | snmpInSetRequests.0 | The total number of SNMP Set-Request PDUs that have been accepted and processed by the SNMP protocol entity. |
| | | snmpInGet Responses.0 | The total number of SNMP Get-Response PDUs that have been accepted and processed by the SNMP protocol entity. |
| | | snmpInTraps.0 | The total number of SNMP Trap PDUs that have been accepted and processed by the SNMP protocol entity. |
| | | snmpOutTooBigs.0 | The total number of SNMP PDUs that were generated by the SNMP protocol entity and for which the value of the error-status field is tooBig. |
| | | snmpOutNoSuch Names.0 | The total number of SNMP PDUs that were generated by the SNMP protocol entity and for which the value of the error-status field is noSuchName. |
| | | snmpOutBadValues.0 | The total number of SNMP PDUs sent that were generated by the SNMP protocol entity and for which the value of the error-status field is badValue. |
| | | snmpOutGenErrs.0 | The total number of SNMP PDUs that were generated by the SNMP protocol entity and for which the value of the error-status field is genErr. |
| | | snmpOutGet Requests.0 | The total number of SNMP Get-Request PDUs that have been generated by the SNMP protocol entity. |
| | | snmpOutGetNexts.0 | The total number of SNMP Get-Next PDUs that have been generated by the SNMP protocol entity. |

**Table 78** Alarm variables (continued)

| Category | Subcategory | Variable | Definition |
|---|---|---|---|
| | | snmpOutSet Requests.0 | The total number of SNMP Set-Request PDUs that have been generated by the SNMP protocol entity. |
| | | snmpOutGet Responses.0 | The total number of SNMP Get-Response PDUs that have been generated by the SNMP protocol entity. |
| | | snmpOutTraps.0 | The total number of SNMP Trap PDUs that have been generated by the SNMP protocol entity. |
| | **Bridge** | rcStgTimeSinceTopologyChange | The time (in hundredths of a second) since the last topology change was detected by the bridge entity. |
| | | rcStgTopChanges | The total number of topology changes detected by this bridge since the management entity was last reset or initialized. |
| | | rcStgMaxAge | The maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded, in hundredths of a second. This is the actual value that this bridge is currently using. |
| | | rcStgPortForward Transitions | The number of times this port has transitioned from the Learning state to the Forwarding state. |
| | | rcStgPortInConfig Bpdus | The number of Config BPDUs received by this port. |
| | | rcStgPortInTcn Bpdus | The number of Topology Change Notification BPDUs received by this port. |
| | | rcStgPortOutConfig Bpdus | The number of Config BPDUs transmitted by this port. |
| | | rcStgPortOutTcn Bpdus | The number of Topology Change Notification BPDUs transmitted by this port. |
| | | dot1dTpPortInFrames | The number of frames that have been received by this port from its segment. Note that a frame received on the interface corresponding to this port is counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames. |
| | | dot1dTpPortOut Frames | The number of frames that have been transmitted by this port to its segment. Note that a frame transmitted on the interface corresponding to this port is counted by this object if and only if it is for a protocol being processed by the local bridging function, including bridge management frames. |

**Table 78** Alarm variables (continued)

| Category | Subcategory | Variable | Definition |
|---|---|---|---|
| | | dot1dTpLearnedEntry Discards.0 | The total number of Forwarding Database entries that have been or would have been learned but have been discarded due to a lack of space to store them in the Forwarding Database. If this counter is increasing, it indicates that the forwarding database is regularly becoming full (a condition that has unpleasant performance effects on the subnetwork). If this counter has a significant value but is not presently increasing, it indicates that the problem has been occurring but is not persistent. |
| | **Utilization** | rcSysCpuUtil.0 | Percentage of CPU utilization. |
| | | rcSysSwitchFabric Util.0 | Percentage of switching fabric utilization. |
| | | rcSysBufferUtil.0 | Buffer utilization as a percentage of the total amount of buffer space in the system. A high value indicates congestion. |
| | | rcSysNVRamUsed.0 | Nonvolatile RAM (NVRAM) in use in kilobytes. |
| | | rcSysLastChange.0 | Last management-initiated configuration change since sysUpTime. |
| | | rcSysLastVlan Change.0 | Last management-initiated VLAN configuration change since sysUpTime. |
| | | rcSysLastSaveTo NVRam.0 | SysUpTime of the last time when the NVRAM on the CPU board was written to. |
| | | rcSysLastSaveTo StandbyNVRam.0 | SysUpTime of the last time when the standby NVRAM (on the backup CPU board) was written to. |
| | **RIP** | rip2GlobalRoute Changes.0 | The number of changes made to the IP Route database by RIP. |
| | | rip2GlobalQueries.0 | The number of responses sent to RIP queries from other systems. |
| | | rip2ifStatSentUpdates | The number of triggered RIP updates actually sent on this interface. |
| | **OSPF** | ospfExternLSACount.0 | The number of external (LSA type 5) link-state advertisements in the link-state database. |
| | | ospfOriginateNew LSAs.0 | The number of new link-state advertisements that have been originated. The number is incremented each time the router originates a new LSA. |
| | | ospfrxNewLSAs.0 | The number of link-state advertisements received determined to be new installations. |

**Table 78** Alarm variables (continued)

| Category | Subcategory | Variable | Definition |
|---|---|---|---|
| | | ospfSpfRuns | Indicates the number of SPF calculations performed by OSPF. |
| | | ospfAreaBdrRtrCount | The total number of area border routers reachable within this area. |
| | | ospfASBdrRtrCount | The total number of autonomous system border routers reachable within this area. |
| | | ospfAreaLSACount | The total number of link-state advertisements in this area's link-state database. |
| | | ospfIfState | This signifies that there has been a change in the state of an OSPF virtual interface. |
| | | ospfIfEvents | The number of times this OSPF interface has changed its state or an error has occurred. |
| | | ospfVirtIfState | The number of times this OSPF interface. |
| | | ospfVirtIfEvents | The number of state changes or error events on this virtual link. |
| | | ospfVirtNbrState | The state of the Virtual Neighbor Relationship. |
| | | ospfVirtNbrEvents | The number of times this virtual link has changed its state or an error has occurred. |
| | **Igmp** | igmpInterfaceWrong Versions | The number of queries received whose IGMP version does not match. IGMP requires that all routers on the LAN be configured to run the same version of IGMP. |
| | | igmpInterfaceJoins | The number of times a group membership has been added on this interface. |
| | | igmpInterfaceLeaves | The number of times a group membership has been deleted on this interface. |
| | **MLT** | rcStatMltIfExtnIfIn MulticastPkts | The total number of multicast packets delivered to this MLT interface. |
| | | rcStatMltIfExtnIfIn BroadcastPkts | The total number of broadcast packets delivered to this MLT Interface. |
| | | rcStatMltIfExtnIfOut MulticastPkts | The total number of MLT interface multicast packets delivered to this MLT interface. |
| | | rcStatMltIfExtnIfOut BroadcastPkts | The total number of MLT interface broadcast packets delivered to this MLT interface. |
| | | rcStatMltIfExtnIfHCIn Octets | The total number of octets received on this MLT interface including framing characters detected by the high-count (64-bit) register. |

**Table 78** Alarm variables (continued)

| Category | Subcategory | Variable | Definition |
|---|---|---|---|
| | | rcStatMltIfExtnIfHCIn UcastPkts | The number of packets delivered by this MLT interface to a higher MLT that were not addressed to a multicast or broadcast address as detected by the high-count (64-bit) register. |
| | | rcStatMltIfExtnIfHCIn MulticastPkt | The total number of multicast packets delivered to this MLT interface detected by the high-count (64-bit) register. |
| | | rcStatMltIfExtnIfHCIn BroadcastPkt | The total number of broadcast packets delivered to this MLT interface detected by the high-count (64-bit) register. |
| | | rcStatMltIfExtnIfHC OutOctets | The total number of octets transmitted out of the MLT interface, including framing characters. |
| | | rcStatMltIfExtnIfHCOut UcastPkts | The number of packets transmitted by this MLT interface to a higher MLT that were not addressed to a multicast or broadcast address as detected by the high-count (64-bit) register. |
| | | rcStatMltIfExtnIfHCOut Multicast | The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a multicast address at this sublayer, including those that were discarded or not sent registered by the high-count (64-bit) register. |
| | | rcStatMltIfExtnIfHCOut Broadcast | The total number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this sublayer, including those that were discarded or not sent registered by the high-count (64-bit) register. |

# Index

## A



## B



## C

## D



## E



## F

## G



## H



## I



## L



## M

## N



## O



## P

## Q



## R



## S

## T

## U



## V



## W