Part No. 314723-C Rev 00
May 2004

4655 Great American Parkway
Santa Clara, CA 95054

Configuring Network Management

Passport 8000 Series Software Release 3.7

NORTEL NETWORKS™

Copyright © 2004 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.

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

Trademarks

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

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

The asterisk after a name denotes a trademarked item.

Restricted rights legend

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

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

Statement of conditions

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

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

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

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

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

Nortel Networks Inc. software license agreement

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

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

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States

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

b Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Figures

Tables

Preface

Nortel Networks* Passport 8000 Series* switch is a flexible and multifunctional switch that supports a diverse range of network architectures and protocols. This guide to network management for the Passport 8000 Series switch provides information about the three switch managment tools, the Dynamic network applications feature, SNMP, and RMON, describes how to configure the Web management interface, and describes how to graph port and chassis statistics.

Before you begin

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

- Basic knowledge of networks, Ethernet bridging, and IP and IPX routing
- Familiarity with networking concepts and terminology
- Basic knowledge of network topologies
- Experience with windowing systems or graphical user interfaces (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. 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. Example: Use the **`dinfo`** command. 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. 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. Example: If the command syntax is `show ip interfaces [-alerts]`, you can enter either `show ip interfaces` or `show ip interfaces -alerts`.
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. 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. Example: `Set Trap Monitor Filters`

separator (>)	Shows menu paths. 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. Example: If the command syntax is `show ip {alerts|routes}`, you enter either `show ip alerts` or `show ip routes`, but not both.

Acronyms

This guide uses the following acronyms:

ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
DVMRP	Distance Vector Multicast Routing Protocol
IGMP	Internet Gateway Message Protocol
IP	Internet Protocol
IPX	Internetwork Packet Exchange
MAC	media access control
OSPF	Open Shortest Path First
PGM	Pragmatic General Multicast
PIM	Protocol Independent Multicast
RIP	Routing Information Protocol
RMON	Remote Monitoring
SNMP	Simple Network Management Protocol

Hard-copy technical manuals

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

How to get help

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

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

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

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www.nortelnetworks.com/help/contact/erc/index.html URL.

Chapter 1
Managing the switch

This chapter describes the three management tools that are available to monitor and manage your routing switch, and provides overviews for Simple Network Management Protocol (SNMP) and Remote monitoring (RMON). It includes the following topics:

Switch management tools

Three management tools are available to monitor and manage your routing switch:

- Command line interface (CLI)
- Device Manager software
- Web management interface

Command line interface (CLI)

To access the CLI initially, you need a direct connection to the switch from a terminal or PC. After Telnet access is enabled, you can access the CLI from a Telnet session on the network.

The CLI consists of two sets of commands that are accessed in different ways. While the switch is booting, you can interrupt the boot process and display the Boot Monitor CLI, which contains commands used to configure boot options and to manage files in flash memory. When the switch completes its boot sequence, the login screen for the Run-Time CLI is displayed. The Run-Time CLI contains commands to configure switch operations and management access.

For information about connecting a console terminal, see *Getting Started*. For information about the Boot Monitor and Run-Time CLIs, see *Managing Platform Operations and Using Diagnostic Tools*.

Device Manager

Device Manager is an SNMP-based graphical user interface (GUI) tool designed to manage single devices. To use Device Manager, you must have network connectivity to a management station running Device Manager in one of the supported environments.

Web management interface

The Web management interface is a Web-based GUI tool that operates in conjunction with a Web browser. It is designed to monitor a single device and is intended for use as a tool to access and monitor devices on your network from various locations within the network. To configure the switch, use the CLI or Device Manager.

To access the Web interface, you need a Web browser and an IP address for the switch. For more information about the Web interface, see Chapter 2.

Dynamic network applications

The remote access services supported on the Passport 8000 Series switch (that is, ftp, tftp, rlogin, and Telnet) use daemons. To enhance security, these daemons are started unconditionally.

When a flag is disabled, all existing connections are abruptly terminated, and the daemon remains idle (does not accept connection requests). Additionally, if HA-CPU is on and you disable a daemon, all the existing connections, even to the standby CPU, are abruptly terminated.

You use the following Dynamic network applications to manage the remote access services:

- Access policies
- Port lock
- CLI access
- SNMP community strings
- Web management interface access

For instructions on enabling remote access services, see *Getting Started*.

For information about setting access policies, locking a port, accessing the CLI, and setting SNMP community strings, see *Configuring and Managing Security.*

For information about accessing the Web management interface, see Chapter 3.

SNMP

SNMP is a simple request/response protocol that communicates management information between two types of SNMP software entities: SNMP applications (also called SNMP managers) and SNMP agents.

SNMP applications contain manager software that runs on a network management station (also known as an SNMP client), such as a PC or a workstation. The manager software implements the protocols used to exchange data with SNMP agents. SNMP applications issue queries to gather information about the status, configuration, and performance of external network devices, called *network elements* in SNMP terminology. Network elements contain an agent and perform the network management function that the network management stations request.

The SNMP agent is a software entity that responds to information and action request messages (SNMP get and set requests) sent by a network management station (for example, a Device Manager workstation). The messages exchanged between manager and switch SNMP agents enable you to access and manage objects in an active or inactive (stored) management information base (MIB) on a switch.

The agents also send unsolicited reports, called *traps*, back to the network management station when certain network activity occurs. An example of a trap is an overload condition as defined by the packet load's crossing some threshold. You use the management station to configure, monitor, and receive trap messages from other network devices configured as SNMP agents. The management station can get and set objects in the agents and can receive traps from the agents. The management station, therefore, has the capability to "manage" a number of agents.

SNMP communities

For security reasons, the SNMP agent validates each request from an SNMP manager before responding to the request, by verifying that the manager belongs to a valid SNMP community. An *SNMP community* is a logical relationship between an SNMP agent and one or more SNMP managers (the manager software implements the protocols used to exchange data with SNMP agents). You define communities locally at the agent.

The agent establishes one community for each combination of authentication and access control characteristics that you choose. You assign each community a unique name (within the agent), and all members of a community have the same access privileges, either read-only or read-write:

Read-only: members can view configuration and performance information.

Read-write: members can view configuration and performance information, and also change the configuration.

By defining a community, an agent limits access to its MIB to a selected set of management stations. By using more than one community, the agent can provide different levels of MIB access to different management stations.

For more information about configuring SNMP settings (including creating community strings and setting traps) using the Device Manager, see *Installing and Using Device Manager* and *Configuring and Managing Security.* For more information about configuring SNMP settings using the CLI, see *Getting Started* and *Configuring and Managing Security.*

RMON

Remote monitoring (RMON) is a management information base (MIB) or a group of "management objects" that you use to "get" or "set" values using Simple Network Management Protocol (SNMP). Using the CLI or Device Manager, you enable RMON globally for devices on the switch. When RMON is enabled globally, you then enable monitoring for individual devices on a port-by-port basis.

RMON has four major functions:

- Setting alarms for user-defined events
- Gathering real-time and historical Ethernet statistics
- Logging events
- Sending traps for events

Within Device Manager, you can set RMON alarms that relate to specific events or variables simply by selecting these variables from a drop-down menu. You specify events associated with alarms to be set to either trap or log-and-trap. In turn, these alarms, when tripped, are trapped or logged.

All RMON information is viewable within both Device Manager and the CLI. Alternatively you can use any management application that supports SNMP traps (such as Optivity NMS* and HP OpenView*) to view RMON trap information.

Chapter 2
Configuring RMON

This chapter describes how to configure and use Remote Network Monitoring (RMON) using Device Manager and the CLI. It includes the following topics:

The Remote Network Monitoring (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 using Device Manager or the CLI.

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.

Configuring RMON using Device Manager

The following sections describe how to configure RMON using Device Manager. It includes the following topics:

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)

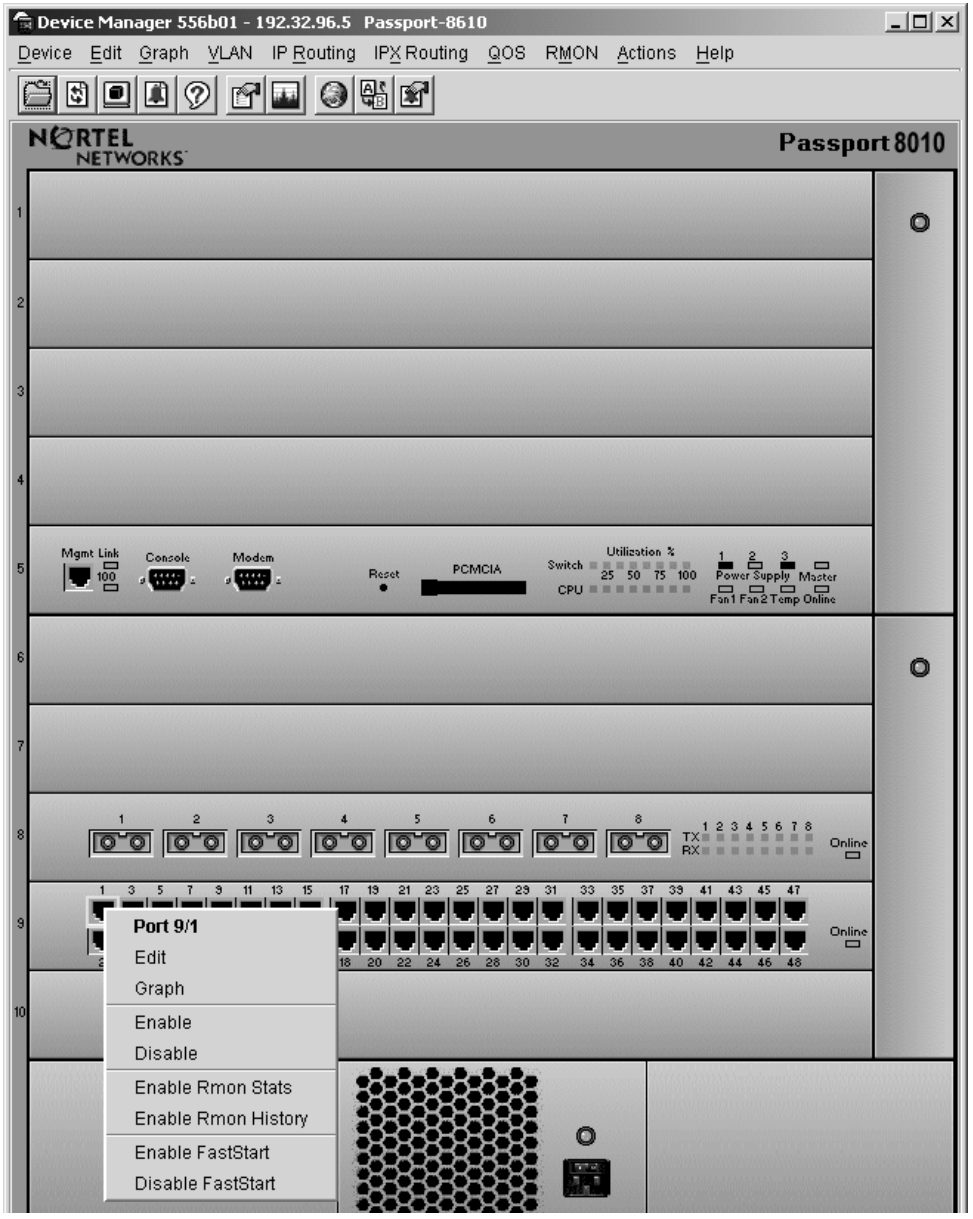
To enable RMON statistics:

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

   The Port shortcut menu opens (Figure 1).

3. In the Port shortcut menu, select Enable Rmon Stats.

Figure 1 Enabling RMON statistics on a port



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

Table 1 describes the Port shortcut menu fields.

Table 1 Port shortcut menu fields

Field	Description
Port	This object identifies the source of the data that this etherStats entry is configured to analyze.
Edit	Make modifications to the port statistics.
Graph	Create a graph of port statistics
Enable	Enable the port.
Disable	Disable the port
Enable RMON stats	Collect RMON statistics on the port.
Enable RMON History	Collect an RMON history on the port.
Enable FastStart	Enable FastStart on the port.
Disable FastStart	Disable FastStart on the port.

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 2). Note that the default owner displayed is the host name on which Device Manager is running.

Figure 2 RmonControl dialog box—Ethernet Statistics

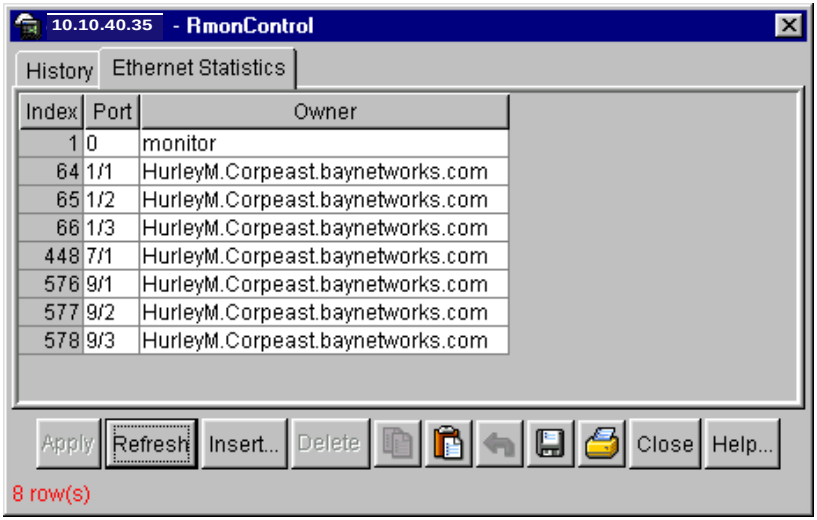


Table 2 describes the RmonControl Ethernet Statistic tab fields.

Table 2 RmonControl Ethernet Statistics tab 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.

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 3).

4. Click the Port ellipsis button, and select a port.
5. On the RmonControl, Insert Ethernet Statistics dialog box, click Insert.

Figure 3 RmonControl and Insert Ethernet Statistics dialog boxes

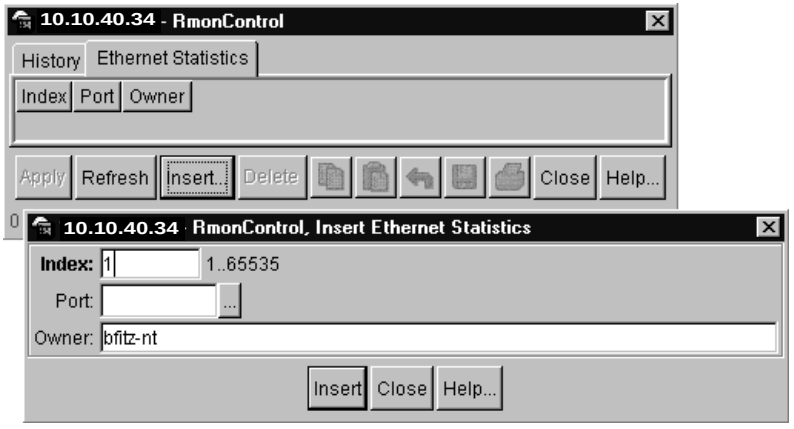


Table 3 describes the RmonControl, Insert Ethernet Statistics dialog box fields.

Table 3 RmonControl, Insert Ethernet Statistics tab fields

Field	Description
Index	An index that uniquely identifies an entry in the Ethernet Statistics table.
Port	This object identifies the source of the data that this etherStats entry is configured to analyze.
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:

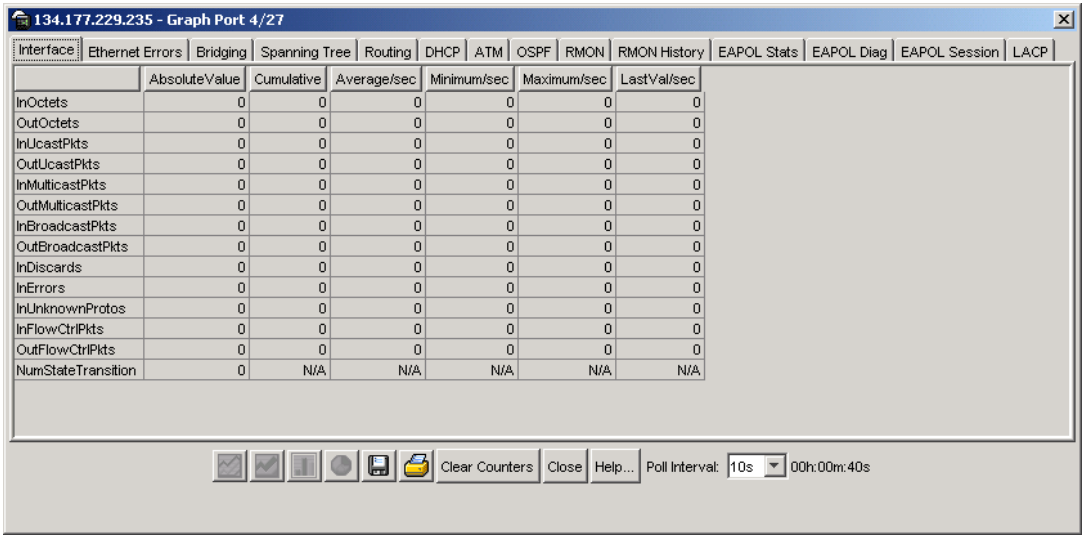
1. Select a single port.
2. On the Device Manager toolbar, click the graphing icon.

   The graphPort dialog box for the port object opens with the Interface tab displayed (Figure 4).

3. Click RMON.

The RMON tab opens and displays RMON statistics.

Figure 4 GraphPort dialog box—Interface tab



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 1 on page 32).

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 5). 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. 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 5).

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 5 RmonControl and RmonControl, Insert History dialog boxes

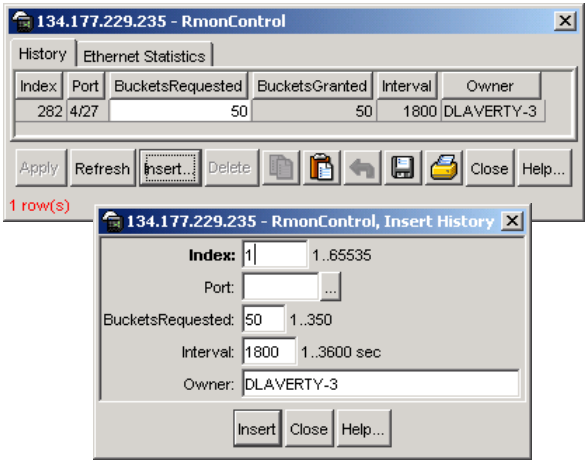


Table 4 describes the RMON History tab fields.

Table 4 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).

Table 4 RmonControl dialog box fields (continued)

Field	Description
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.
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.

Table 4 RmonControl dialog box fields (continued)

Field	Description
Interval	The interval in seconds over which the data is sampled for each bucket in the part of the media-specific table associated with this 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 5 on page 39).

2. Select the row that contains the port ID you want to delete.
3. Click Delete.

Viewing history

To view RMON history:

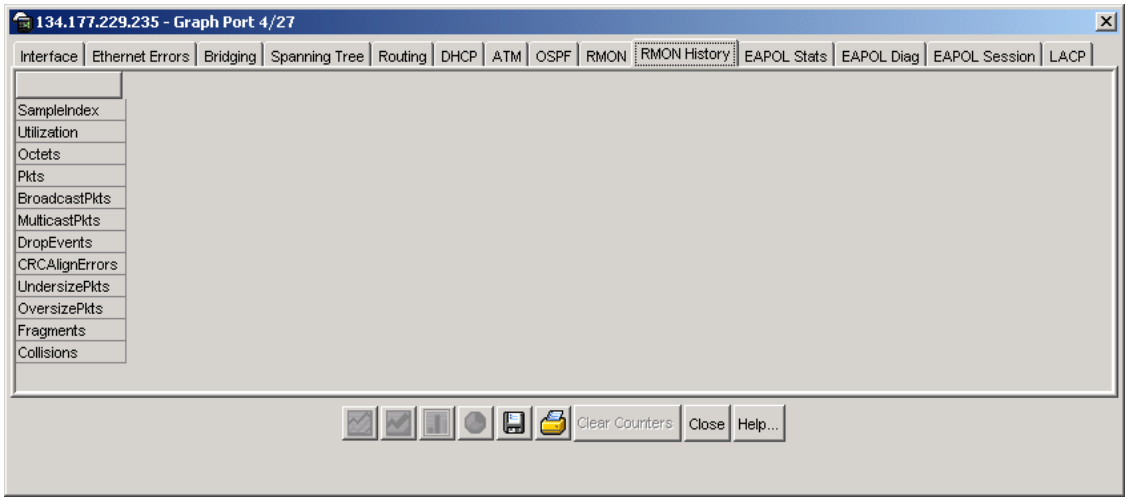
1. Select a port.
2. On the Device Manager toolbar, click the graphing icon.

   The graphPort dialog box opens with the Interface tab displayed.

3 Click the RMON History tab.

The RMON History tab opens (Figure 6).

Figure 6 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:

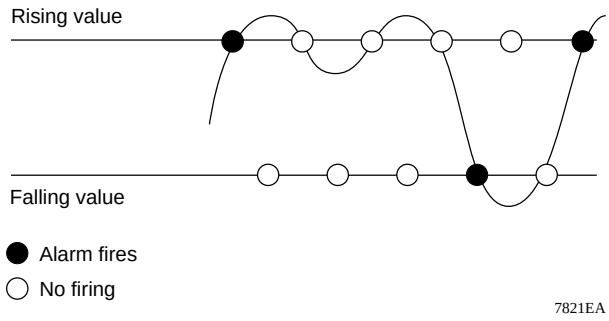
- An upper and lower threshold value defined on it
- A corresponding rising and falling event
- An alarm interval or polling period

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 7).

Figure 7 How alarms fire



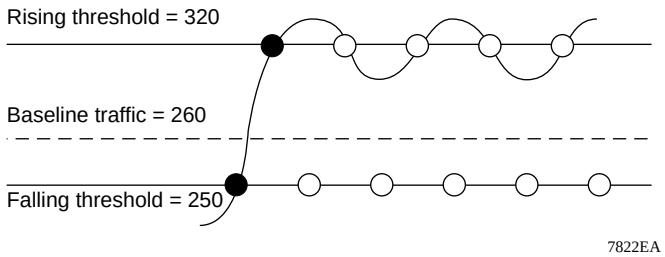
It is important to note that the alarm fires during the first interval that the sample goes out of range. No additional events are generated for that threshold until the opposite threshold is crossed. Therefore, it is important to carefully define the rising and falling threshold values for alarms to 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 8). 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 8 Alarm example—threshold less than 260



Creating alarms

When you create an alarm, you select a variable from the variable list (Appendix A, “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:

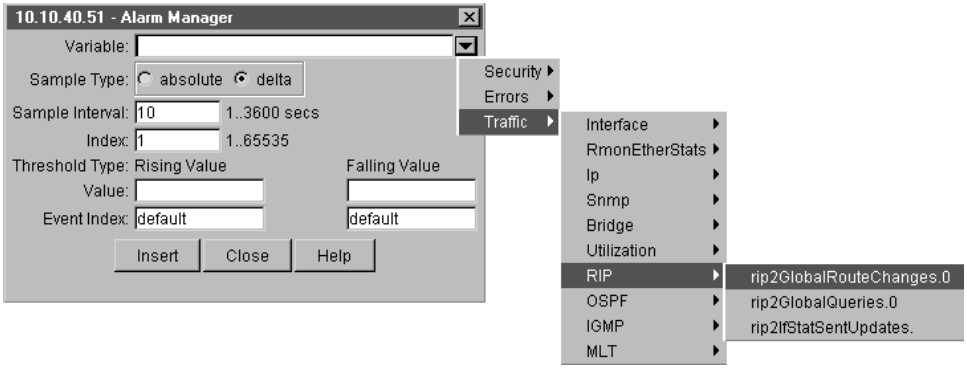
1. Make sure that RMON is globally enabled.

   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 9).

Figure 9 Alarm Manager dialog box



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 9, “rip2GlobalRouteChanges.0” has been selected from the variable list under RIP. (A list of variable definitions is located in Appendix A, “RMON alarm variables.”)

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 5.)

Table 5 describes the RMON Insert Alarm fields.

Creating a port history alarm

Table 5 Alarm Manager dialog box fields

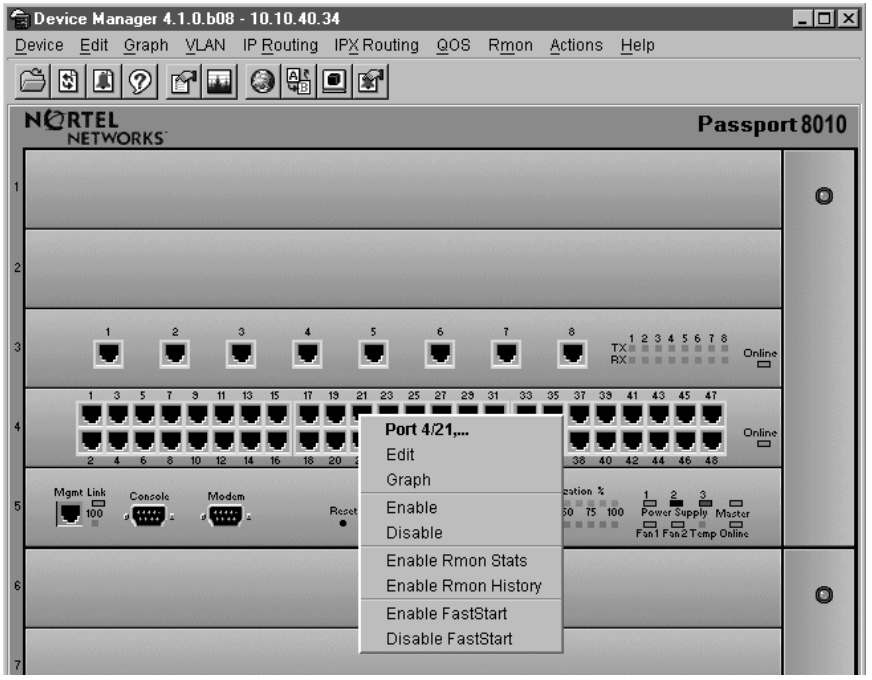
Field	Description	
Variable	Name and type of alarm—indicated by the format: • *alarmname.x,* where x=0 indicates a chassis alarm, x=1 or 2 indicates a power supply or fan alarm with 1 being the primary unit and 2 the secondary unit. • *alarmname,* where the user must specify the index. This value is 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. • *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.)

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 10).

Figure 10 Enabling RMON statistics and history



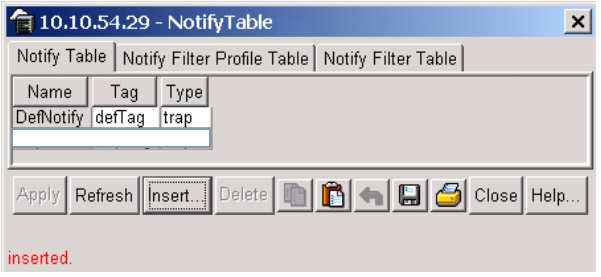
3 Choose Enable Rmon Stats and Enable Rmon History.

4 If trapping is not enabled, enable trapping as follows:

a On the Device Manager menu bar, choose Edit > SnmpV3 > Notify Table.

The NotifyTable tab opens (Figure 11).

Figure 11 NotifyTable tab



b Click Insert.

The NotifyTable, Insert Notify Table dialog box opens.

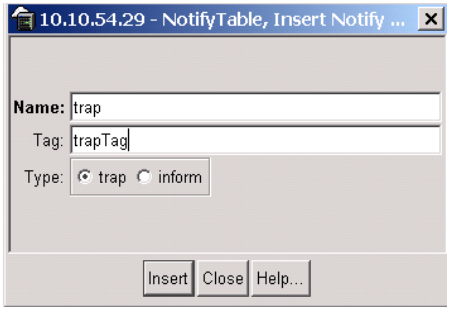
c Enter a name that represents a table index.

d Enter a tag.

e Select Trap for the notification type.

For the purposes of this example, enter trapTag and then select Trap as the notification type (Figure 12).

Figure 12 NotifyTable, Insert Notify Table dialog box



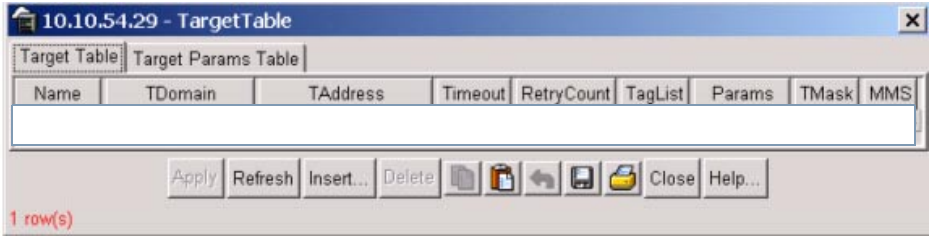
f Click Insert.

g Click Close.

h On the Device Manager menu bar, choose Edit > SnmpV3 > Target Table.

The TargetTable tab opens (Figure 13).

Figure 13 TargetTable tab



i Click Insert.

The TargetTable, Insert Target Table dialog box opens.

j Create a target in the TAddress field in the xx.xx.xx.xx:port format.

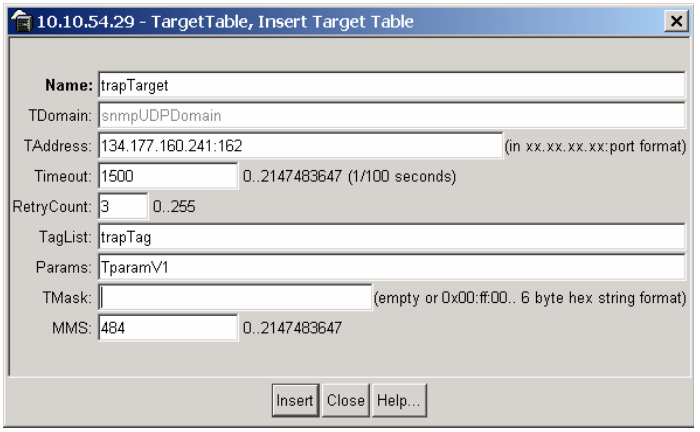
k Enter a TagList in the designated field. Note here that this field has to be an exact match for the Tag field entry in the NotifyTable tab.

l Set the Params field to TParamV1 or TParamV2 to receive a v1 or v2 trap.

TParamV1 and TParamV2 are default entries previously defined in the Target Params Table. If you wish to use another Params name, ensure that you define that entry with the proper attributes in the Target Params Table.

For the purposes of this example, the TAddress is 134.177.160.241 with a port number of 162, the TagList is trapTag, and the Params are set to receive TparamV1 traps. (Figure 14).

Figure 14 TargetTable, Insert Target Table dialog box



m Click Insert

n Click Close.

You should now be able to receive traps.

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 6 on page 42).

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.

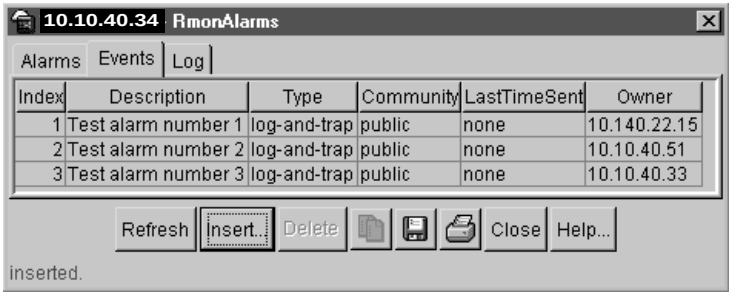
To view the Rmon Alarms, Events, or Log information:

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

2 Click the Alarms, Events, or Log tab.

An example is shown in Figure 15.

Figure 15 RmonAlarms dialog box—Events tab



Deleting alarms

To delete an alarm:

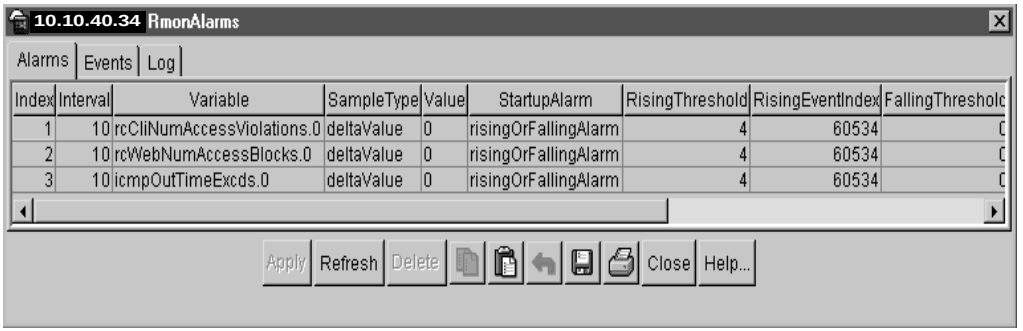
1 From the Device Manager menu bar, choose RMON > Alarms.

The RmonAlarms dialog box opens with the Alarms tab displayed (Figure 16).

2 Select the alarm you want to delete.

3 Click Delete.

Figure 16 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.

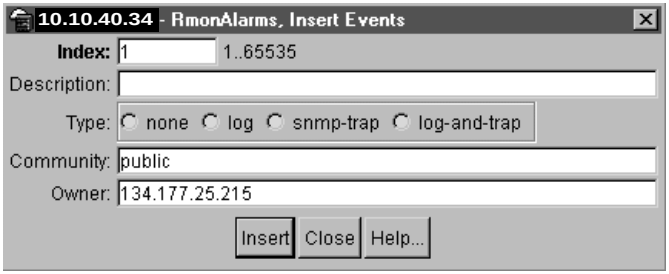
2 Click the Events tab.

The Events tab opens.

3 Click Insert.

The RmonAlarms, Insert Events dialog box opens (Figure 17).

Figure 17 RmonAlarms, Insert Events dialog box



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

5 Select the type of event you want.

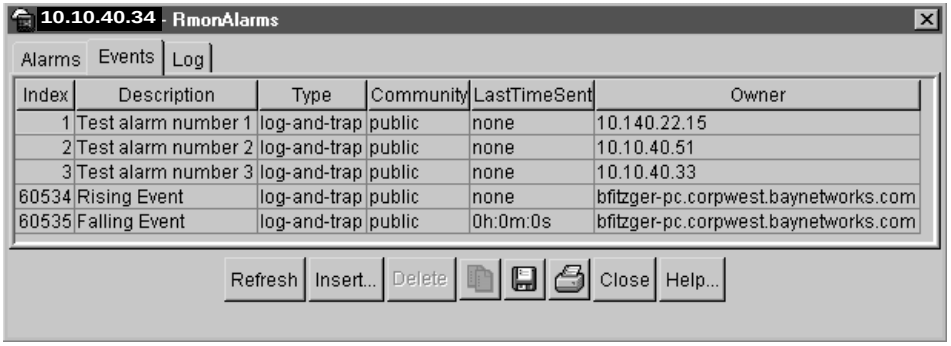
The default setting is log-and-trap. You may opt to set the event type to log to save memory or to snmp-log to reduce traffic from the switch.

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 18).

Figure 18 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 18).

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 6 describes the RmonAlarms dialog box—Evens tab fields.

Table 6 RmonAlarms dialog box—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: • none • log • trap • log-and-trap
Community	The SNMP community string acts as a password. Only those management applications with this community string can view the alarms.
LastTimeSent	The value of sysUpTime at the time this event entry last generated an event. If this entry has not generated any events, this value is zero.
Owner	If traps are specified to be sent to the owner, then this is the name of the machine that will receive alarm traps.

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.

Configuring RMON using the CLI

To configure the RMON functions on the switch, use the following command:

```
config rmon
```

The **`config rmon`** commands include the following options:

`config rmon` followed by:	
`info`	Indicates whether RMON is enabled or disabled on the switch.
`alarm create <id> type <value> intv <value> [variable <value>] [r_th <value>] [r_ev <value>] [f_th <value>] [f_ev <value>] [owner <value>]`	Creates an alarm interface. • *`id`* is the interface index number (1 to 65535). • `type <value>` is the sample type, `absolute` or `delta`. • `intv <value>` is the sample interval (1 to 3600). • `variable <value>` is the variable name or OID, case sensitive (string length 1 to 256). • `r_th <value>` is the rising threshold (0 to 65535). • `r_ev <value>` is the rising event number (0 to 65535). • `f_th <value>` is the falling threshold (0 to 65535). • `f_ev <value>` is the falling event number (0 to 65535). • `owner <value>` is the name of the owner (string length 1 to 48).
`alarm delete <id>`	Deletes the specified RMON alarm.
`alarm info`	Displays information about the RMON alarms.
`disable`	Disables RMON on the switch.
`enable`	Enables RMON on the switch.
`ether-stats create <id> <ports> [owner <value>]`	Creates an ether-stats control interface. • *`id`* is the index number of the ether stats control interface (0 to 65535). • *`ports`* is the single port interface {slot/port[-slot/port][,...]}. • `owner <value>` is name of the owner (string length 1 to 48).

config rmon followed by:	
`ether-stats delete <id>`	Deletes an ether-stats control interface. • *id* is the index number of the ether stats control interface (0 to 65535).
`ether-stats info`	Displays the current ether-stats settings.
`ether-stats owner <id> <name>`	Changes the owner name for the ether-stats control interface. • *id* is the index number of the ether stats control interface (0 to 65535). • *name* is name of the owner (string length 1 to 48).
`event create <id> trap_src <value> trap_dest <value> [desc <value>] [type <value>] [community <value>] [owner <value>]`	Creates an event. • *id* is the event index number (0 to 65535). • `trap_src <value>` is the trap source IP address. • `trap_dest <value>` is the trap destination IP address. • `desc <value>` is the event description (string length 0 to 127). • `type <value>` is the event type, `none`, `log`, `snmp-trap`, or `log-and-trap`. • `community <value>` is the event community (string length 1 to 127). • `owner <value>` is the name of the owner (string length 1 to 48).
`event delete <id>`	Deletes an event. • *id* is the event index number (0 to 65535).
`event info`	Displays the event information.
`history-control create <id> <ports> [buckets <value>] [intv <value>] [owner <value>]`	Creates a history control interface. • *id* is the index number of the history control interface (0 to 65535). • *ports* is the single port interface {slot/port[-slot/port][,...]}. • `buckets <value>` is the number of buckets requested (1 to 350). • `intv <value>` is the time interval in seconds over which the data is sampled for each bucket (1 to 3600). • `[owner <value>` is the name of the owner (string length 1 to 48).
`history-control delete <id>`	Deletes a history control interface. • *id* is the interface index number of the history control interface (0 to 65535).

config rmon followed by:	
`history-control info`	Displays the setting for history control interfaces.
`memsize <`*`memsize`*`>`	Sets the amount of RAM in bytes to allocate for RMON. • *`memsize`* is the memory size in bytes (250000 to 4000000).
`trap-option <toOwner|toAll>`	Controls whether the RMON traps should be sent to the owner or all trap recipients. • `toOwner|toAll` is set to either the owner or all trap recipients.
`util-method <half|duplex>`	Controls whether port utilization is calculated in half or full duplex.

Configuration example

This configuration example uses the above commands to enable RMON. The example also uses the **`info`** command to display RMON function information.

```
8610:5# config rmon
8610:5/config/rmon# enable
8610:5/config/rmon# info
Sub-Context: alarm ether-stats event history-control
Current Context:
                        rmon : enable
                    mansize : 250000
                trap-option : toOwner
8610:5/config/rmon#
```

Viewing RMON settings

To view the various RMON settings, use the following command:

```
show rmon
```

The **show rmon** commands and options are:

show rmon followed by:	
info	Displays the status of RMON on the switch.
alarm	Displays the RMON Alarm table.
ether-stats	Displays the RMON Ethernet statistics table.
event	Displays the RMON event table.
history-control	Displays the RMON history control table.
log	Displays the RMON log table.

Example

The following example shows sample output from each of the **show rmon** options.

```
8610:5# show rmon
8610:5/show/rmon# ether-stats

================================================================================
                    Rmon Ether Stats
================================================================================

INDEX PORT   OWNER
--------------------------------------------------------------------------------
1     cpp    monitor


8610:5/show/rmon# info

RMON Info :

        Status       : enable
        MemorySize   : 250000
        TrapOption   : toOwner
```

```
8610:5/show/rmon# alarm

================================================================================
                     Rmon Alarm
================================================================================

                                              RISING       FALLING

                             SAMPLE   STARTUP THRES EVENT  THRES EVENT

ID INTVAL VARIABLE   VALUE TYPE     ALARM   HOLD  INDEX  HOLD  INDEX  OWNER

--------------------------------------------------------------------------------

 1  10     ifInOctets.72 338   delta    r_or_f  1000  60534  10    60535 TEST
O-WIN2K

8610:5/show/rmon# event

================================================================================

                                       Rmon Event
================================================================================

INDEX DESCRIPTION     TYPE          COMMUNITY OWNER      LAST_TIME_SENT
--------------------------------------------------------------------------------

60534 Rising Event    log-and-trap public@1 TEST-WIN2K none
60535 Falling Event   log-and-trap public@1 TEST-WIN2K none

8610:5/show/rmon# history-control

================================================================================

                                       Rmon Control-History
================================================================================

INDEX PORT   BUCKET_REQUEST  INTERVAL OWNER
--------------------------------------------------------------------------------

72    1/9    50              1800 TEST-WIN2K
```

```
8610:5/show/rmon# log

================================================================================

                                      Rmon Log
================================================================================

INDEX    DESCRIPTION          TIME
--------------------------------------------------------------------------------
```

Chapter 3
Configuring the Web management interface

This chapter describes how to enable the Web management interface. It includes the following topics:

Monitoring the switch using Web management

The Passport 8000 Series switch includes a Web management interface that lets you monitor your switch through a World Wide Web browser from anywhere on your network. The Web interface provides many of the same monitoring features as the Device Manager software.

The Web management interface is protected by a security mechanism that requires you to log in to the device using a user name and password. The switch is shipped with the default user name and password both specified as **`ro`**. For security, the default state of the Web Server is disabled.

This section includes the following topics:

Requirements

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

- A computer connected to any of the network ports
- One of the following browsers:
  - Netscape Navigator, version 4.7 or later
  - Microsoft Internet Explorer Web browser, version 5.0 or later
- The IP address of the Passport 8000 Series switch.

  For instructions on assigning an IP address to the management port, see *Getting Started*.

Note: As long as you have a route to the switch and there are no filters or access policies in effect, you should be able to monitor the switch using the Web interface.

Access to the Web management interface must also be enabled for the switch (the default setting). You can enable or disable Web access using the `config web-server` command in the CLI. For instructions, see "Enabling the Web server using the CLI" on page 71. In Device Manager, you enable or disable Web access by choosing Edit > Chassis > System. On the System tab, set the EnableWebServer parameter to true. For instructions, see "Enabling the Web server using Device Manager" on page 68.

To access the Web management interface, enter your switch IP address as the URL in your Web browser and log on. See "Accessing the Web interface" on page 74 for instructions.

Installing Help files

Online Help for the Web interface consists of a separate set of files included on the *Passport 8000 Switch Software* CD. You must install the files on a TFTP server in the network and specify the IP address of the server and the path to the file, using either the CLI or Device Manager.

Installing Help files in a Windows environment

To install the Help files in a Windows environment:

1. Insert the *Software* CD into the CD driver of your computer.
2. Navigate to the CD and double-click the wm_windows folder.
3. Double-click the installer icon or in WinZip, extract the file, and click wm.exe.
4. Follow the screen prompts.

Installing Help files in a UNIX environment

To install the Help files in a UNIX environment, use the command:

`install_passport_wmfiles` ***`[wm-version] [target-directory]`***

where:

`wm-version` specifies the file name.

`target-directory` specifies the system directory where you are installing the files.

For example:

```
install_passport_wmfiles wm_v300 /opt/Passport/wm
```

Specifying the Help file location

To specify the file location using the CLI, enter:

config web-server html-source-dir help-tftp *<file>*

where *file* specifies the path and file name.

To specify the file location using Device Manager:

1. From the Device Manager menu bar, choose Edit > Security > Web.
2. In the HelpTftpSourceDir field, type the path and file name for the Help files.

Note: If you install the Help files on a PC, place the files in the same drive as the one specified under TFTP server options for your system.

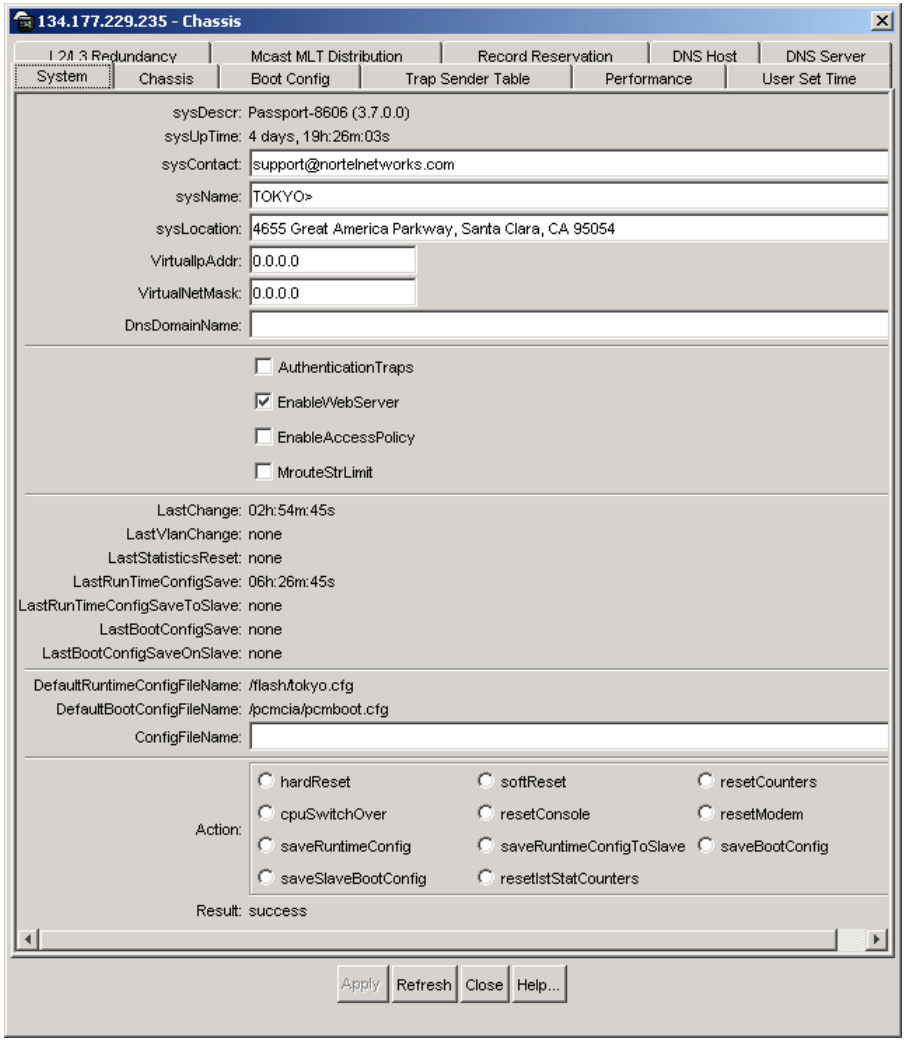
Enabling the Web server using Device Manager

To enable the Web Server using Device Manager:

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

   The Chassis dialog box opens with the System tab displayed (Figure 19).

Figure 19 Chassis dialog box—System tab



2 Select EnableWebServer.

3 Click Apply.

4 Close the dialog box.

The Web Server is enabled.

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 Policies tab displayed.

2. Click the Web tab.

   The Web tab opens (Figure 20).

   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 20 Security dialog box—Web tab

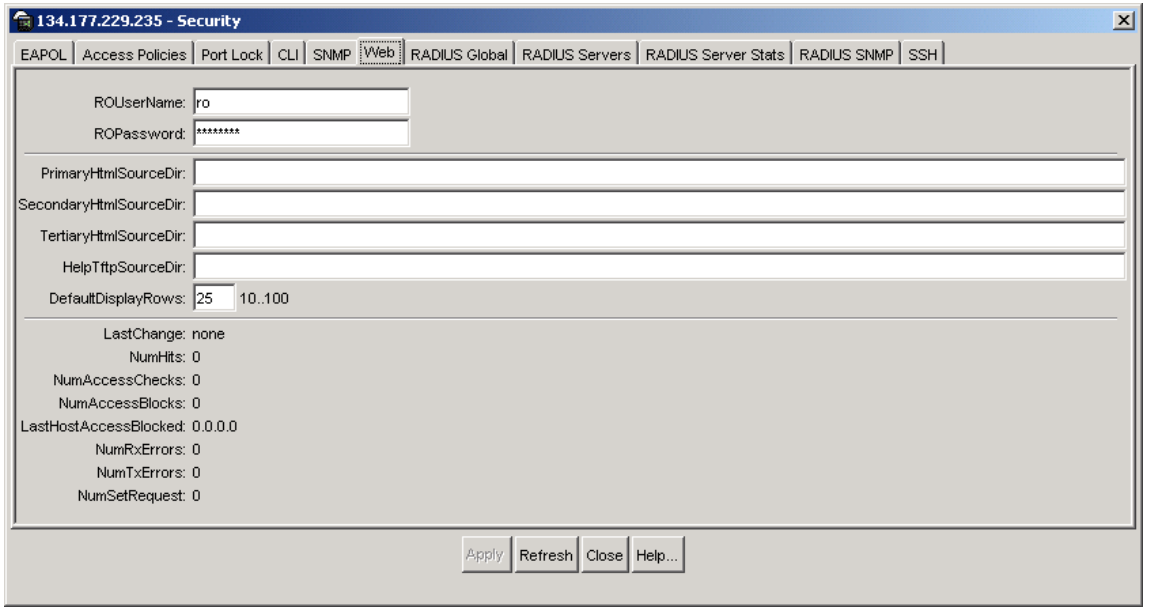


Table 7 describes the Web tab fields.

Table 7 Web tab fields

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

Enabling the Web server using the CLI

To enable and manage the Web Server using the CLI, use the following command:

```
config web-server
```

This command includes the following options:

config web-server followed by:	
info	Indicates whether Web access is enabled or disabled on the switch and displays the current Web user name and password setting.
def-display-rows <*integer*>	Sets the number of rows displayed per page. • *integer* is 10 to 100.
disable	Disables the Passport Web interface.
enable	Enables the Passport Web interface.
html-source-dir help-tftp <*file*>	Specifies the file location and name for the Web server HTML Help file. • *file* specifies the path and file name of the HTML source.
http-port <integer>	Specifies the http port of the Web server. • *integer* is a value from 1 to 49151.
password <*ro*> <*username*> <*passwd*>	Sets passwords for access to the Web interface. • *username* is the user's login name, up to 20 characters long. • *passwd* is the password associated with the login name, up to 20 characters long.

Configuration example

This configuration example uses the above commands to enable the web interface and specify the number of rows in the display. The example also uses the **`info`** command to display web interface parameters.

```
8610:5# config web-server
8610:5/config/web-server# def-display-rows 25
8610:5/config/web-server# enable
8610:5/config/web-server# info

Sub-Context:
Current Context:

                    webserver : enable
                     password :
                     RO - username : ro
                            passwd : ro
              def-display-rows : 25
               html-source-dir :
                    help-tftp :
                    http-port : 80

8610:5/config/web-server#
```

Showing web-server status

To display whether or not Web access is enabled, as well as password and access information, use the following command:

```
show web-server
```

Configuration example

This configuration example uses the above command to display web server status.

```
8610:5/config/web-server# show web-server

Web Server Info :

        Status                    : on
        RO Username               : ro
        RO Password               : ro
        Def-display-rows          : 25
        Html help tftp source-dir :
        HttpPort                  : 80
        NumHits                   : 0
        NumAccessChecks           : 0
        NumAccessBlocks           : 0
        NumRxErrors               : 0
        NumTxErrors               : 0
        NumSetRequest             : 0

8610:5/config/web-server#
```

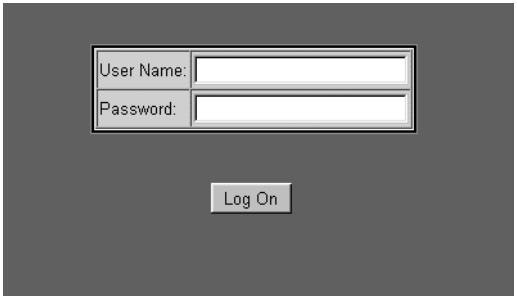
Accessing the Web interface

To access the Web interface:

1. Start your Web browser.
2. Enter the switch IP address as the URL in the Web address field.

   The Web logon page opens (Figure 21).

Figure 21 Web logon page



3 In the User Name and Password text boxes, type `ro`.

4 Click Log On.

The System page opens. This page provides general information about the switch as a whole and its configuration parameters.

The Web interface has a 15-minute timeout period. If there is no activity for 15 minutes, the system logs off the switch Web interface, and you must reenter the password information.

Note: To access a Web browser from Device Manager, on the toolbar, click the Browse Device's Home Page button.

Troubleshooting Web interface access to a switch

If the switch and the PC running the Web browser are in the same network, you may find that even though other applications (such as Device Manager or Telnet) can access a particular switch, the Web management interface cannot. This situation can occur if the Web browser has a proxy server that resolves the *www* path and returns the "reachable" IP address to the browser. If there is no route from the proxy server to the switch, the http query does not reach the switch, and there is no response.

To prevent this problem, make sure that if your Web browser uses a proxy server, a route is specified from the proxy server to the switch.

Chapter 4
Configuring and graphing ports

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 22).

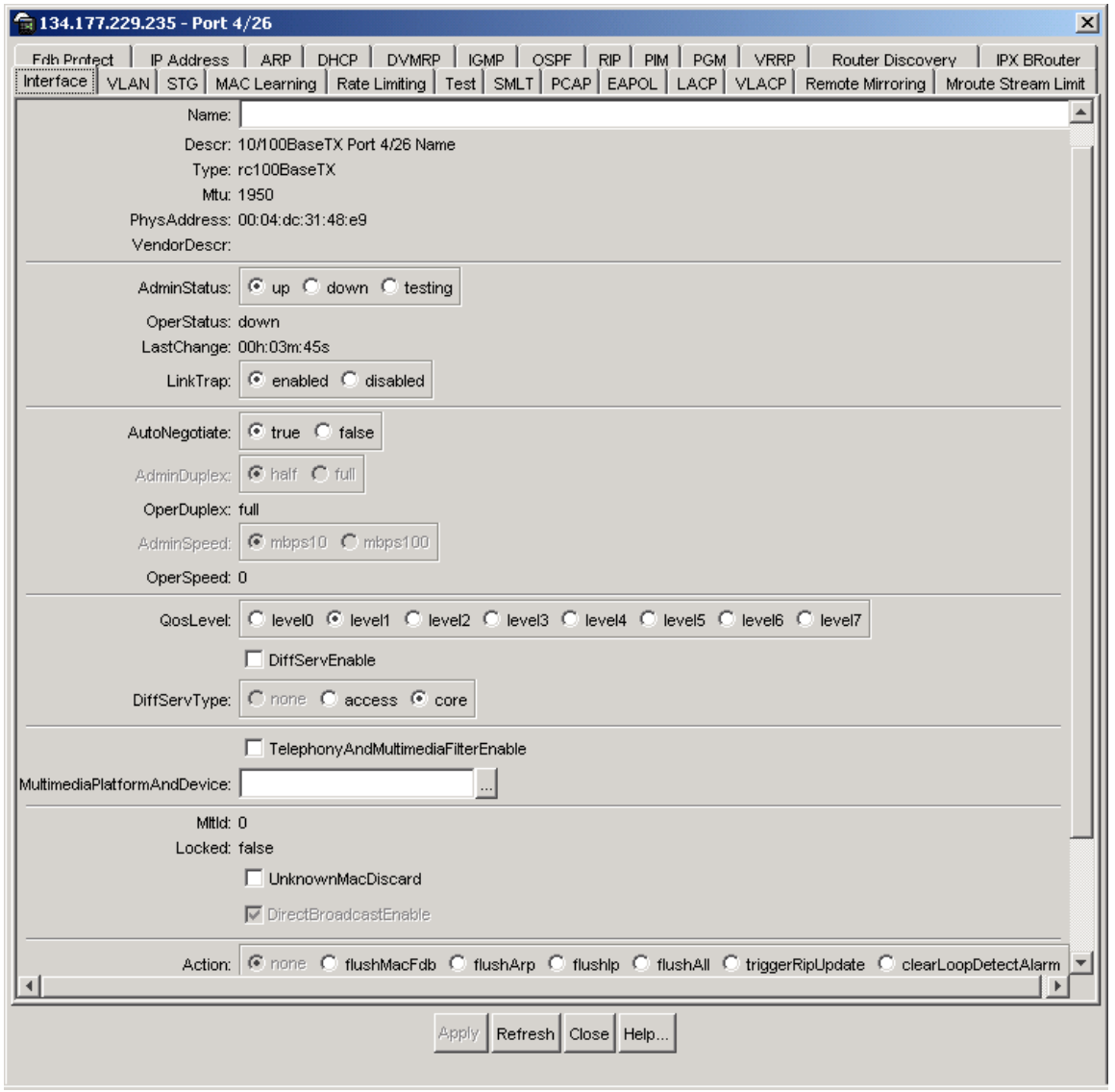
Note: Additional tabs and screen entries for module-specific functions appear when applicable. For example, on the Interface dialog box for a port, tabs for layer 3 (routing) functions would appear if Device Manager were accessing a Passport 8600 module.

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 22).

Figure 22 Port dialog box—Interface tab



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

Table 8 describes the Interface tab fields.

Table 8 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: • up • down • testing 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.

Table 8 Interface tab fields (continued)

Field	Description
OperStatus	The current operational state of the interface. One of the following states: • up • down • testing 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.
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 (only 10/100BASE ports). Nortel Networks recommends that you use autonegotiation whenever it is supported by the devices on both ends of a Gigabit fiber link. When the Passport 8600 Series switch is connected to a device that does not support it, autonegotiation should be disabled and SFFD enabled. For more information, see *Network Design Guidelines*.
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.
MultimediaPlatformAndDevice	Specifies the platform and multimedia device
TelephonyAndMultimediaFilterEnable	Enables telephony and multimedia filters
MltId	The MultiLink Trunk to which the port is assigned (if any).

Table 8 Interface tab fields (continued)

Field	Description
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. **Note:** You cannot set the unknown-mac-discard lock-autolearn-mac disable parameter when autolearn is disabled.
DirectBroadcastEnable	Used to indicate whether this interface should forward direct broadcast traffic.
Action	One of the following port-related actions: • none • flushMacFdb—flush MAC forwarding table for port • flushArp—flush ARP table for port • flushIp—flush IP route table for port • flushAll—flush all tables for port • triggerRipUpdate—manually update the RIP table
Result	The result of port-related actions.
AdminRouting	Enables or disables routing for a port.
OperRouting	Indicates the current state of routing for the port.
HighSecureEnable	Enables or disables the high secure feature.

Opening a dual tab

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 23).

Figure 23 Port dialog box—Dual tab

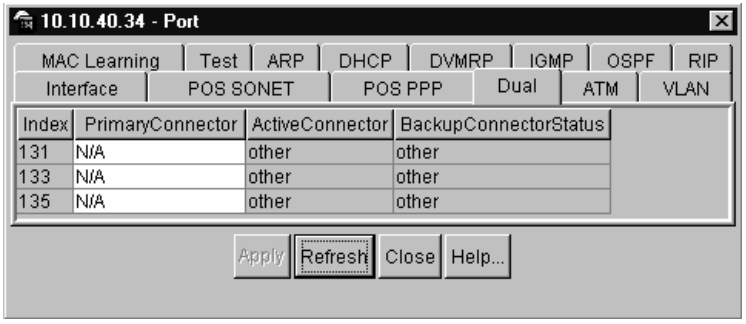


Table 9 describes the Port Dual tab fields.

Table 9 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 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).

Note: For more information on port mirroring, see *Using Diagnostic Tools* in the Passport 8000 Series Software Release 3.7

Configuring remote mirroring

To configure remote mirroring:

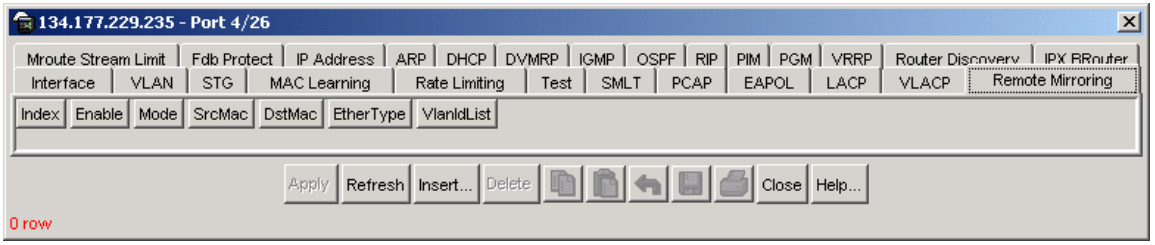
1. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed (Figure 22 on page 79).

2. Click the Remote Mirroring tab.

   The Remote Mirroring tab opens (Figure 24).

Figure 24 Port dialog box—Remote Mirroring tab



3. Click Insert.

   The Port, Insert Remote Mirroring dialog box opens (Figure 25).

Figure 25 Port, Insert Remote Mirroring dialog box

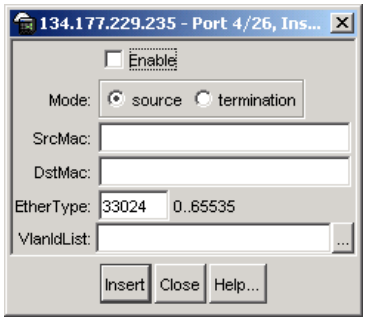


Table 10 describes the Port, Insert Remote Mirroring dialog box fields.

Table 10 Port, Insert Remote Mirroring dialog box fields

Field	Description
Enable	Enables remote mirroring for the port. The default is false
Mode	Identifies the mode in which remote mirroring is enabled
SrcMac	Specifies the source MAC address of the remote mirrored packet. The remote mirroring packet is sent with this source MAC address
DstMac	Specifies the destination MAC address of the remote mirrored packet. Packets are bridged to this MAC address and the remote mirroring packet is also sent here
EtherType	Specifies the Ether Type of the remote mirrored packet. Packets are sent with this Ether Type. Valid values range from 0- 65535.
VlanIdList	Used only if the port is assigned as a remote mirroring termination port. Represents zero or more filter list VLANs in which the Destination MAC address resides. Each VLAN ID is stored as two bytes in this array starting from offset zero. Any unused bytes should be set to zero

Configuring mroute stream limit

To configure the mroute stream limit:

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

The Port dialog box opens with the Interface tab displayed (Figure 21 on page 79).

2 Click the Mroute Stream Limit tab.

The Mroute Stream Limit tab opens (Figure 26).

Figure 26 Port dialog box—Mroute Stream Limit tab

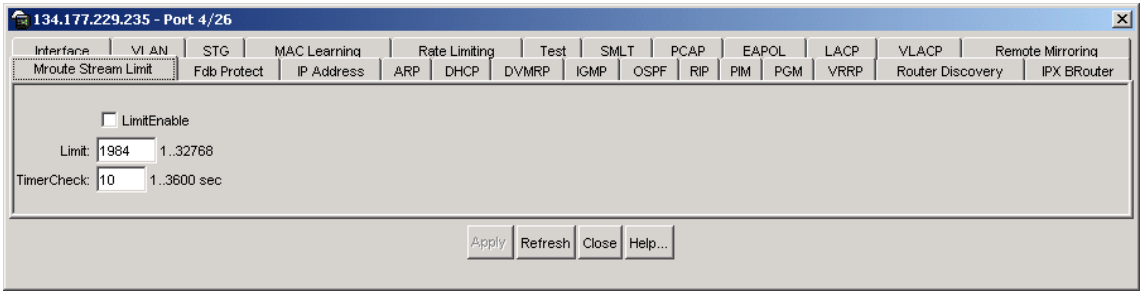


Table 11 describes the Mroute Stream Limit tab fields.

Table 11 Mroute Stream Limit tab fields

Field	Description
LimitEnable	Enables or disables the mroute stream limit on the port.
Limit	Specifies the maximum number of multicast streams that are allowed to ingress the CPU through this port. Valid values range from 1-32768, with a default of 1984.
TimerCheck	Specifies a sampling period (in seconds) for checking the number of multicast streams that has entered the CPU through this port. Valid values range from 1- 3600 seconds, with a default of 10.

Enabling routing operations on a port

The following tabs in the Port dialog box are used for layer 3 routing:

- IP Address tab
- VLAN tab

- STG tab
- MAC Learning tab
- Fdb Protect tab
- Test tab
- ARP tab
- DHCP tab
- DVMRP tab
- IGMP tab
- OSPF tab
- RIP tab
- PIM tab
- PGM tab
- VRRP tab
- Router Discovery
- IPX BRouter
- LACP
- VLACP

Note: This information applies to Passport 8600 modules only.

Each of these is described in the subsections that follow:

Assigning an IP address on a brouter port

When you assign an IP address to a brouter port, keep these rules in mind:

- You cannot edit the IP address, and you can assign only one IP address to any router interface (brouter or virtual).

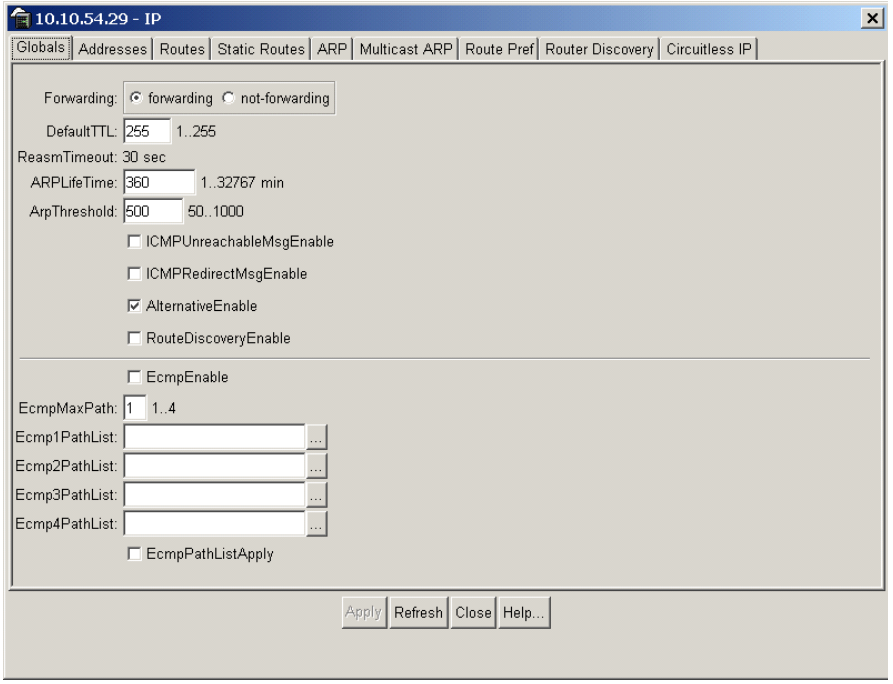
  Attempting to assign a second IP address returns an invalid IP address error.
- You also cannot assign an IP address to a brouter port that is a member of a routed VLAN. To assign an IP address to the brouter port, you must first remove it from the routed VLAN.
- If you want to assign a new IP address to a VLAN or brouter port that already has an IP address, first remove the existing IP address and then insert the new IP address.

To configure an IP address on a brouter port:

1. From the Device Manager menu bar, select IP Routing > IP.

   The IP dialog box opens with the Globals tab displayed (Figure 27).

Figure 27 IP dialog box—Globals tab



2 Click forwarding to enable routing on the device.

3 Do *one* of the following:

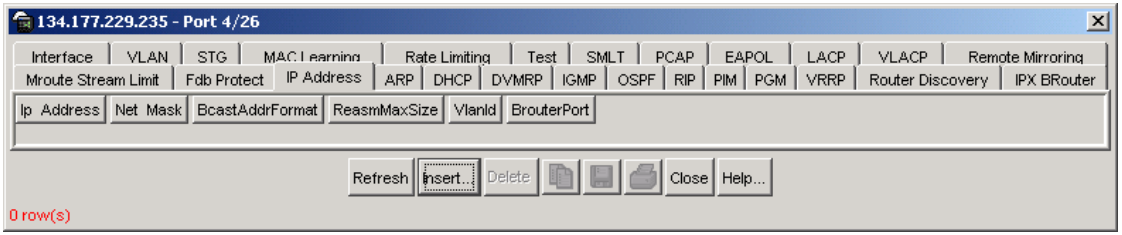
- On the device view, double-click a port.
- On the device view, right-click a port. On the shortcut menu, choose Edit.
- On the device view, select a port. From the Device Manager menu bar, choose Edit > Port.
- On the device view, select a port. On the Device Manager toolbar, choose the Edit Selected button.

The Port dialog box opens with the Interface tab displayed (Figure 22).

4 Click the IP Address tab.

The IP Address tab opens (Figure 28).

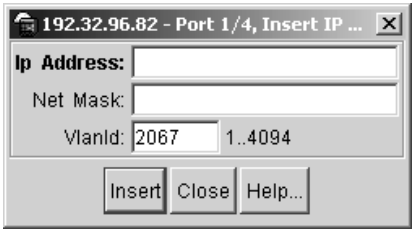
Figure 28 Port dialog box—IP Address tab



5 Click Insert.

The Port, Insert IP Address dialog box opens (Figure 29).

Figure 29 Port, Insert IP Address dialog box



6 Enter the IP address, Netmask, and VlanID.

7 Click Insert.

Table 12 describes the fields in the Port, Insert IP Address dialog box.

Table 12 Port, Insert IP Address dialog box fields

Field	Description
IpAddress	The IP address of the brouter interface on this port. Note that only one IP address can be defined on a given port interface.
NetMask	The subnet mask of the brouter interface on this port.
VlanId	The ID of the VLAN associated with the brouter port. This field is used for tagging ports.

Configuring VLANs

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

To configure VLANs:

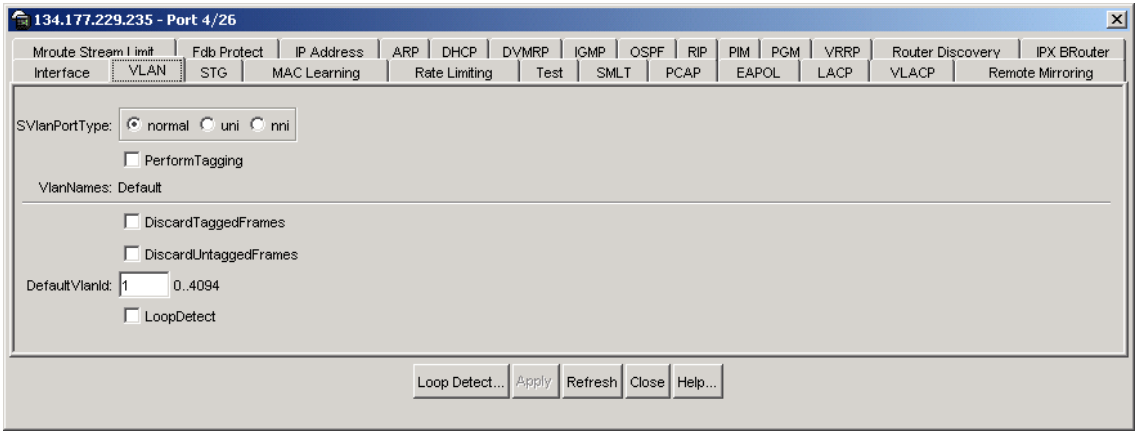
1. On the device view, select a port or multiple ports.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.

3. Click the VLAN tab.

   The VLAN tab opens (Figure 30).

Figure 30 Port dialog box—VLAN tab



4. Click Apply.
5. Click Close.

Table 13 describes the VLAN tab fields.

Table 13 VLAN tab fields

Field	Description
SvlanPortType	Sets the stacked VLAN (SVLAN) port type: • normal (default) • uni (User-to-Network Interface) You must configure ports to which you want to provide VLAN transparency as UNI ports. UNI ports can only belong to one SVLAN. When you designate a port as a UNI port, the DiscardTaggedFrames parameter is automatically configured (Edit > Port > VLAN). This prevents traffic from leaking to other VLANs. • nni (Network-to-Network Interface) NNI ports interconnect the switches in the core network, drop untagged frames on ingress, and insert the SVLAN tag at the egress. When you configure an NNI port, the DiscardUnTaggedFrames parameter is automatically configured (Edit > Port > VLAN). Before configuring a port as uni or nni, you must change the switch level to 1 or above (Edit > VLAN > SVLAN > Level).
PerformTagging	Enable or disable the port on the current VLAN to perform tagging on the incoming and outgoing traffic.
VlanNames	Identifies 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	Determines 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	Determines 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	VLAN ID assigned to untagged frames.
LoopDetect	Enables loop detection.

Detecting VLAN Loops

You can detect VLAN loops to tag or untag discarded frames for a port.

To detect VLAN loops:

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 31).

4. Check LoopDetect to enable loop detection.
5. Click Apply.
6. Click Loop Detected.

   The Loop Detected dialog box displays any loop detection information for the port (Figure 31).

Figure 31 Loop Detected dialog box

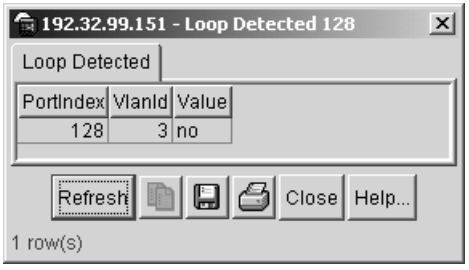


Table 14 describes the LoopDetect dialog box fields.

Table 14 LoopDetect dialog box fields

Field	Description
PortIndex	Port number.
VlanId	The assigned ID of the VLAN.
Value	Specifies that a loop has been detected (yes), or that no loop has been detected (no).

Configuring Spanning Tree Groups (STGs)

You can configure a port's Spanning Tree parameters through the STG tab in the Port dialog box.

Note: When you edit multiple ports, the Spanning Tree options are not displayed.

To configure an STG:

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 32).

Figure 32 Port dialog box—STG tab

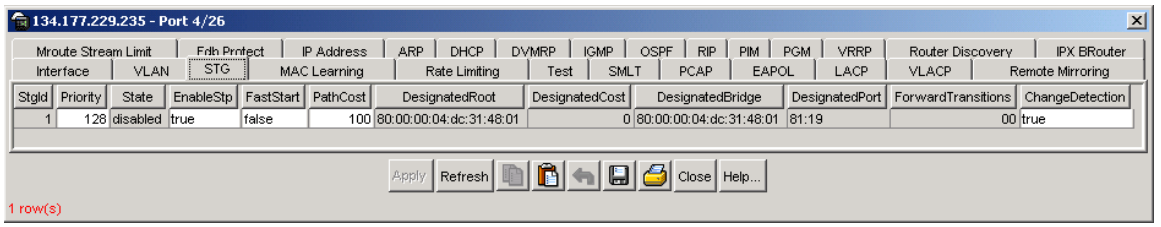


Table 15 describes the STG tab fields.

Table 15 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.
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 8000 Series 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 33).

Figure 33 Port dialog box—MAC Learning tab

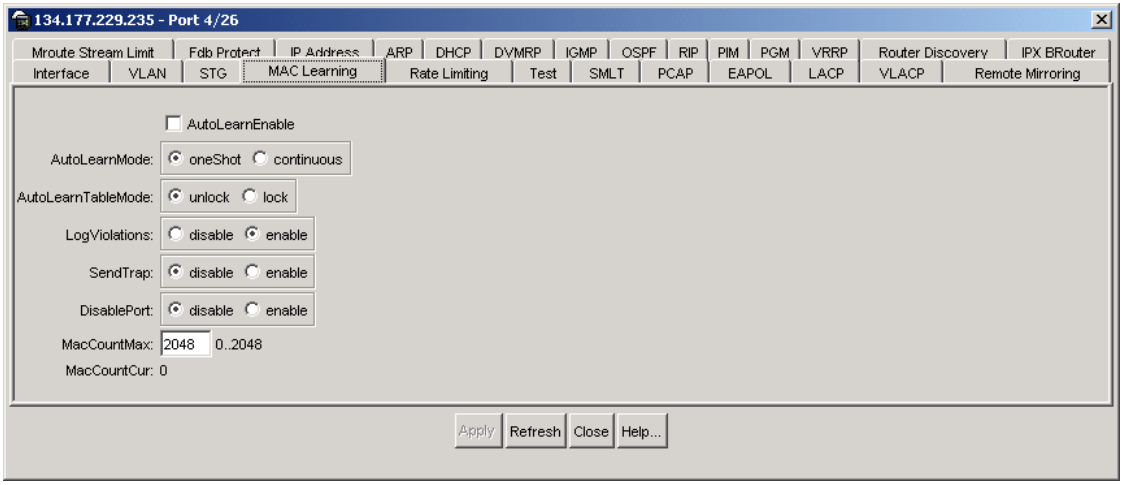


Table 16 describes the MAC Learning tab fields.

Table 16 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.
LogViolations	Enables the system to create a system log entry when a disallowed MAC address attempts to send traffic through the selected port.
SendTrap	Indicates whether a trap should be sent to the management station when a MAC address violation is detected on the selected port. The default is disable.
DisablePort	Indicates whether the selected port should be disabled if a MAC address violation is detected. enable means that the port should be disabled if this event occurs. The default is disable.
MacCountMax	The maximum number of MAC addresses that can be added to the selected port. The valid values are 0 to 2048.
MacCountCur	The current number of MAC addresses that have been added to the selected port.

Configuring the FDB protect feature

To obtain information about the MAC address learning limits for a specific port, configure the FDB protect feature. To configure FDB protect:

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

   The Port dialog box opens with the Interface tab displayed.

2. Click the Fdb Protect tab.

   The Fdb Protect tab opens (Figure 34).

Figure 34 Port dialog box—Fdb Protect tab

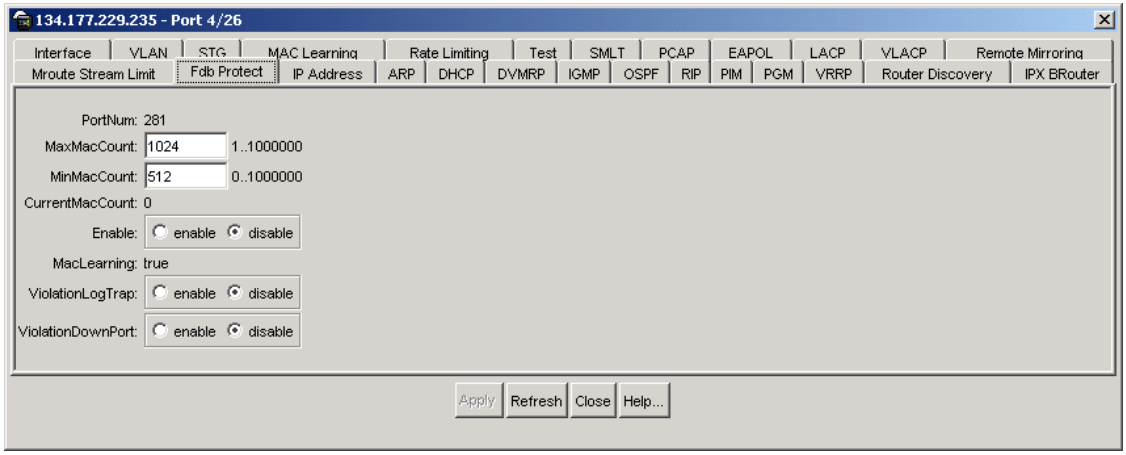


Table 17 describes the Fdb Protect tab fields.

Table 17 Fdb Protect tab fields

Field	Description
PortNum	Identifies the interface on which the MAC address learning limit is applied. This is a read-only field
MaxMacCount	Specifies the maximum number of MAC addresses that can be learned on the port. Valid values range from 1- 1000000, with a default value of 1024.
MinMaxCount	Specifies the minimum number of learned MAC addresses in which MAC address learning is re-enabled on the port. Valid values range from 1- 1000000, with a default value of 512.
CurrentMacCount	Identifies the current number of MAC addresses learned on the port. This is a read-only field.
Enable	Enables or disable the MAC learning limit feature on the port.
MacLearning	Indicates whether or not the port can currently learn new MAC addresses. This is a read-only field.
ViolationLogTrap	Enables or disables logging and sending the SNMP trap, once the MAC learning limit is reached for the port.
ViolationDownPort	Allows you to enable or disable the port once the MAC learning limit is reached.

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 35).

Figure 35 Port dialog box—Rate Limiting tab

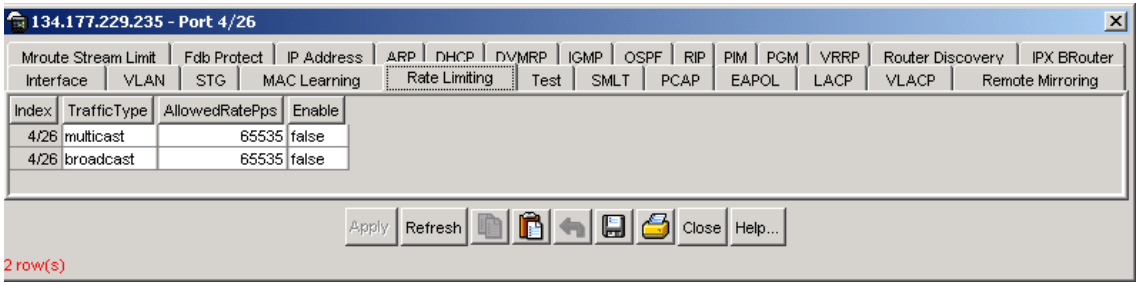


Table 18 describes the Rate Limiting tab fields.

Table 18 Rate Limiting tab fields

Field	Description
Index	The port number.
TrafficType	The type of traffic being rate limited—either broadcast or multicast traffic.

Table 18 Rate Limiting tab fields

Field	Description
AllowedRatePps	This variable is the allowed traffic rate limit for the port. For Passport 8100 switches, 1.. 25 sets the limit in a percentage of the total bandwidth on the port between 1% and 25%. **Note:** On Passport 8100 gigabit ports and MDAs, there may be up to a 2% difference between the configured and actual rate limiting values. For Passport 8600 switches, 1... 65535 sets the limit in packets per second.
Enable	Right click in the field and select to enable (True) or disable (False) 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 36).

Figure 36 Port dialog box—Test tab

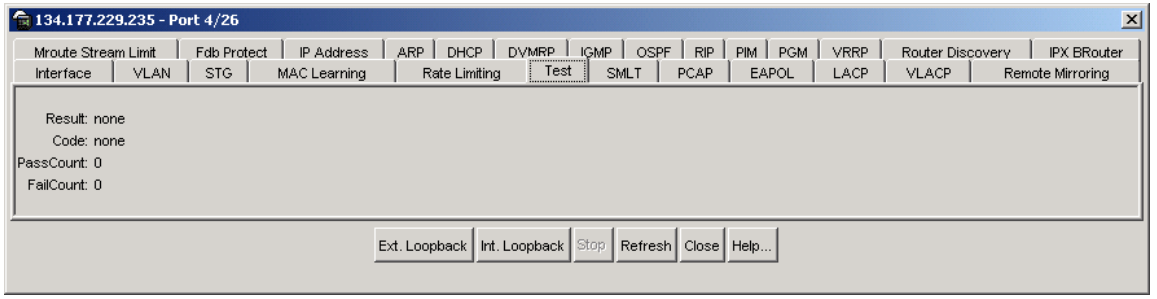


Table 19 describes the Test tab fields.

Table 19 Test tab fields

Field	Description
Result	The result of the most recently run (or current) test: • None • Success • InProgress • NotSupported • unAbleToRun • Aborted • Failed The code contains more specific information on the test result (for example, an error code after a failed test): • NoReceive (timeout on a send) • BadSeq (packets received out of sequence) • BadLen (packet length mismatch) • 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.

Table 19 Test tab fields

Field	Description
PassCount	The number of iterations of the loopback test completed successfully.
FailCount	The number of iterations of the loopback test failed.

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 8672ATME/ATMM Modules*.

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.
3. Set AutoNegotiate to false.
4. Set Admin Duplex to full.
5. Click the Test tab.

   The Test tab opens (Figure 36 on page 101).
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 36 on page 101).

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.

Configuring Address Resolution Protocols (ARP)

To configure ARP on a port:

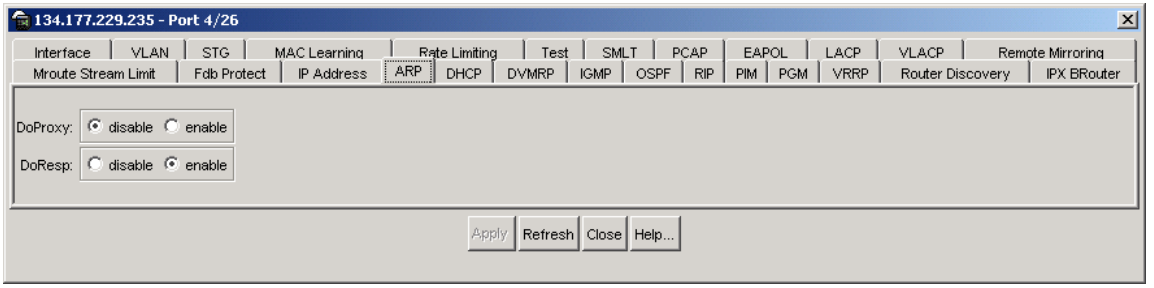
1. Select a port.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.

3. Click the ARP tab.

   The ARP tab opens (Figure 37).

Figure 37 Port dialog box—ARP tab



4 In the DoProxy field, click enable to enable Proxy ARP function.

5 In the DoResp field, click disable or enable to select whether or not to respond to an ARP.

6 Click Apply.

7 Click Close.

Note: Use the ARP dialog box when setting the ARP response behavior on a brouter port. To configure the ARP response for a routing VLAN, use VLAN > VLANs > Basic > IP > ARP. The ARP dialog box is not applicable unless the port or VLAN is routed, that is, it is assigned an IP address.

Table 20 describes the ARP tab fields.

Table 20 ARP tab fields

Field	Description
DoProxy	Proxy ARP allows the 8000 switch to respond to an ARP request from a locally attached host or end station for a remote destination.
DoResp	Sets the Proxy ARP option to respond to an ARP request.

Configuring Dynamic Host Configuration Protocol (DHCP)

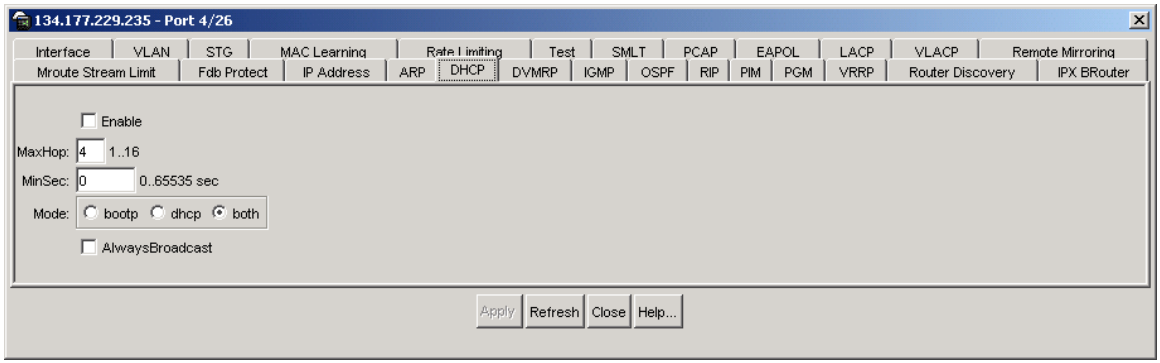
To configure DHCP on a port:

1. 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 DHCP tab.

   The DHCP tab opens (Figure 38).

Figure 38 Port dialog box—DHCP tab



4. Click Enable to select the DHCP option.
5. Enter the appropriate values.
6. Click Apply.
7. Click Close.

Table 21 describes the DHCP tab fields.

Table 21 DHCP tab fields

Field	Description
Enable	Enables or disables BootP/DHCP on the port. The default is disable.
MaxHop	Sets the maximum number of hops before a BootP/DHCP packet is discarded (1 to 16). The default is 4.

Table 21 DHCP tab fields

Field	Description
MinSec	The “secs" field in the BootP/DHCP packet header represents the elapsed time since the client first sent the message. If the "secs" field in the packet header is greater than this value, the switch relays or forwards the packet; otherwise, the packet is dropped. The default is 0 seconds.
Mode	Sets the interface to process only BootP, only DHCP, or both types of packets. The default is both.
AlwaysBroadcast	When enabled, the server reply is sent as a broadcast back to the end station. The default is disable.

Configuring Distance Vector Multicast Routing Protocol (DVMRP)

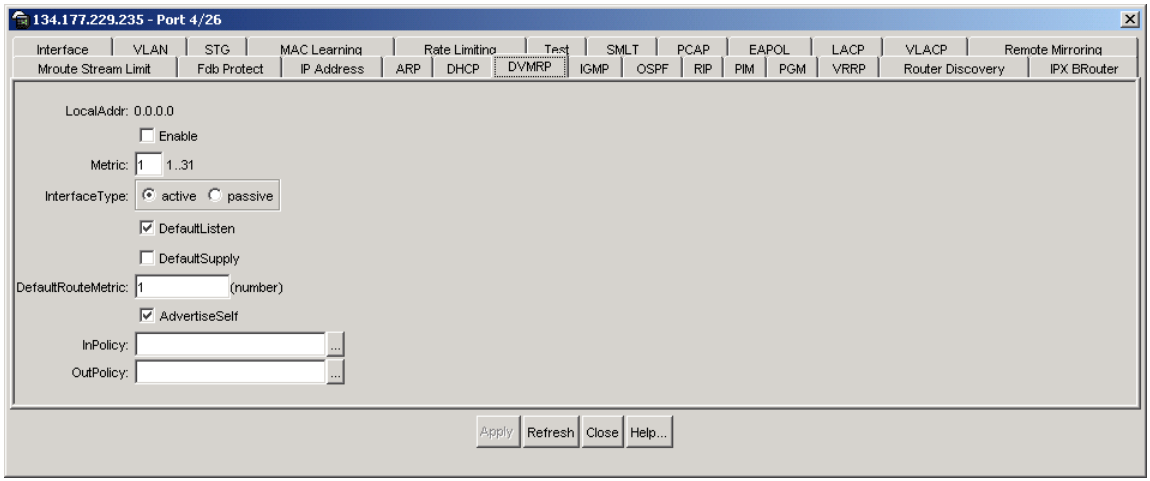
To configure DVMRP on a port:

1. 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 DVMRP tab.

   The DVMRP tab opens (Figure 39).

Figure 39 Port dialog box—DVMRP tab



4 Click the Enable check box to select DVMRP on the port, or click to clear the check box.

5 Enter a metric (cost) in maximum number of hops for DVMRP; the range is 1 to 31.

A default value of 1 means local delivery only. You can use the metric value to control the scope of the DVMRP routes.

6 Click Apply.

7 Click Close.

Table 22 describes the DVMRP tab fields.

Table 22 DVMRP tab fields

Field	Description
LocalAddress	When enabled, the server reply is sent as a broadcast back to the end station. The default is disable.
Enable	Enables (check box selected) or disables (check box not selected) DVMRP on the port.
Metric	Specifies the distance metric for this port, used to calculate distance vectors. The range is 1 to 31 hops.

Table 22 DVMRP tab fields

Field	Description
InterfaceType	Sets the port type as passive or active.
DefaultListen	Sets the port to listen (check box selected) or not listen (check box not selected) for the default route.
DefaultSupply	Sets the port to supply (check box selected) or not supply (check box not selected) only the default route.
DefaultRouteMetric	Sets the metric (number of hops for DVMRP) of the default route. The range is 1 to 31 hops.
AdvertiseSelf	Sets the port to advertise (check box selected) or not advertise (check box not selected) local routes to neighbors.
InPolicy	Selects the name of the DVMRP accept policy applied to the port.
OutPolicy	Selects the name of the DVMRP announce policy applied to the port.

Configuring Internet Group Management Protocol (IGMP)

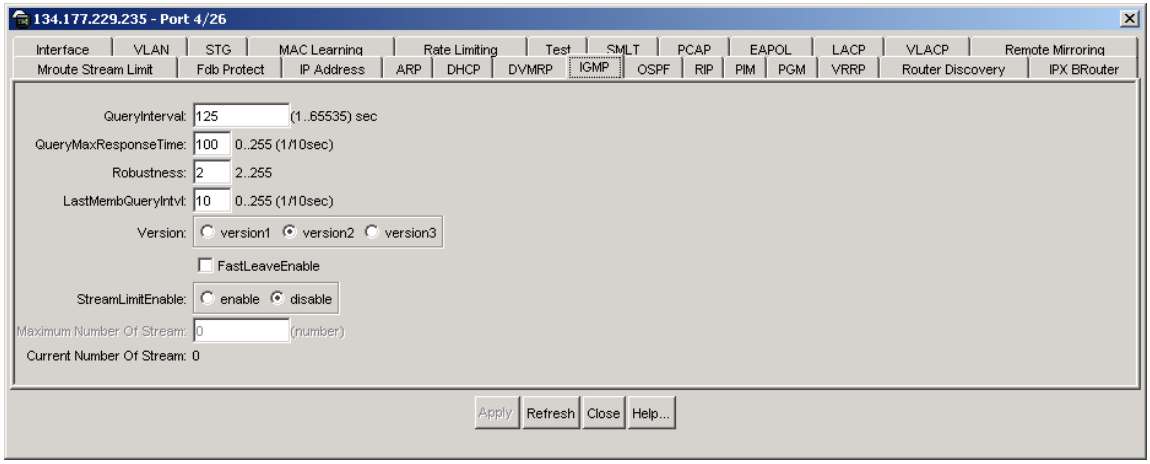
To configure IGMP on a port:

1. 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 IGMP tab.

   The IGMP tab opens (Figure 40).

Figure 40 Port dialog box—IGMP tab



4 Enter the appropriate values.

5 Click Apply.

6 Click Close.

Table 23 describes the IGMP tab fields.

Table 23 IGMP tab fields

Field	Description
QueryInterval	The frequency (in seconds) at which IGMP host query packets are transmitted on the interface. The range is from 1 to 65535, and the default is 125.
QueryMaxResponseTime	The maximum response time (in 1/10 seconds) advertised in IGMPv2 general queries on this interface. This value is can not be configured for IGMPv1. Smaller values allow a router to prune groups faster. The range is from 0 to 255, and the default is 100 tenth seconds (equal to 10 seconds). **Note:** This value must be less than the QueryInterval.

Table 23 IGMP tab fields

Field	Description
Robustness	This parameter allows tuning for the expected packet loss of a network. This value is equal to the number of expected query packet losses per serial query interval, plus 1. If a network is expected to lose query packets, the robustness value should be increased. The range is from 2 to 255, and the default is 2. The default value of 2 means that one query per query interval may be dropped without the querier aging out.
LastMembQueryIntvl	The maximum response time (in 1/10 seconds) that is inserted into group-specific queries sent in response to leave group messages. It is also the time between group-specific query messages. This value can not be configured for IGMPv1. Decreasing the value reduces the time to detect the loss of the last member of a group. The range is from 0 to 255, and the default is 10 tenth seconds. Nortel Networks recommends configuring this parameter to values higher than 3. If a fast leave process is not required, Nortel recommends values above 10. (The value 3 is equal to 0.3 of a second and 10 is equal to 1.0 second).
Version	The version of IGMP (1, 2 or 3) that you want to configure on this interface. For IGMP to function correctly, all routers on a LAN must use the same version. The default is version 2.
FastLeaveEnable	Enables fast leave on the interface.
StreamLimitEnable	Enables stream limitation on this interface.
Maximum Number of Stream	Sets the maximum number of streams allowed on this interface. The range is from 0 to 65535, and the default is 4.
Current Number of Stream	Displays the current number of streams. This is a read-only value.

Configuring Open Shortest Path First (OSPF)

To configure OSPF on a port:

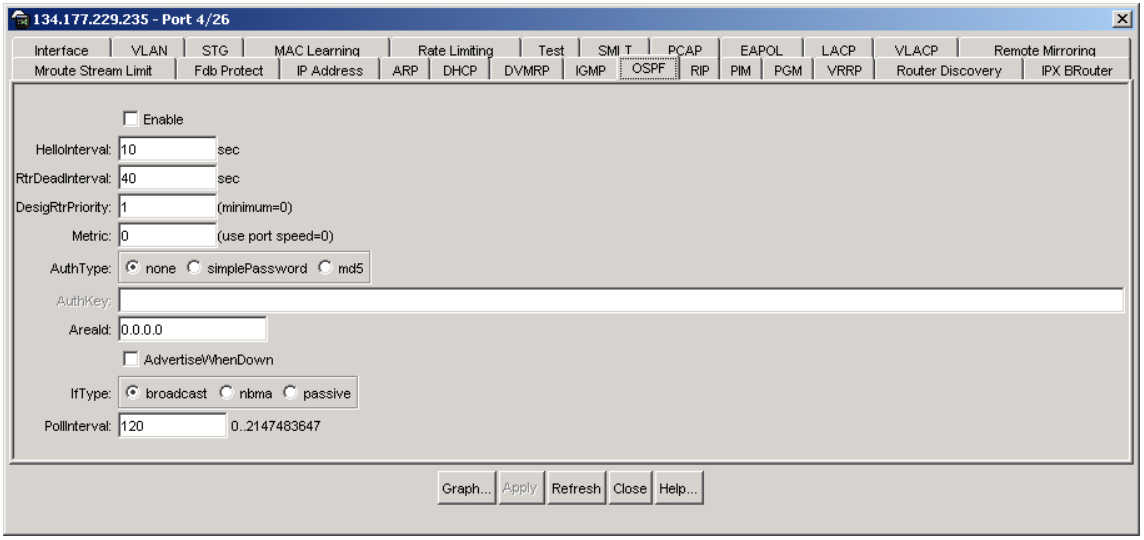
1. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.

2. Click the OSPF tab.

   The OSPF tab opens (Figure 41).

Figure 41 Port dialog box—OSPF tab



3 Check Enable.

4 Specify the HelloInterval.

5 Specify the RtrDeadInterval.

6 Designate a RtrPriority.

7 Enter a metric.

8 If desired, select an authentication type.

9 If you chose a simplePassword authentication type, enter an authentication key.

10 Enter the AreaId.

11 If desired, check AdvertiseWhenDown.

12 Select an IfType.

13 Specify a polling interval.

14 Click Apply.

15 Click Close.

Table 24 describes the OSPF tab fields

Table 24 OSPF tab fields

Field	Description
Enable	Enables or disables OSPF on the port.
HelloInterval	Specifies how long to wait (in seconds) before the router sends out the next hello message to neighboring routers. The default is 30 seconds.
RtrDeadInterval	Specifies the retry interval in seconds
DesigRtrPriority	Specifies the retry priority
Metric	Specifies the distance metric for this port.
AuthType	Type of security. You can choose none, a simplePassword, or md5.
AuthKey	Password for simplePassword Authtype only.
AreaId	The area ID
AdvertiseWhenDown	If true, the network on this interface is advertised as up, even if the port is down. The default is false. **Note:** When you configure a port without any link and enable AdvertiseWhenDown, it does not advertise the route until the port is active. Then the route is advertised even when the link is down. To disable advertising based on link states, disable AdvertiseWhenDown.
IfType	Specifies the interface type: broadcast, nbma, or passive.
PollInterval	The seconds between pollings.

Configuring Routing Information Protocol (RIP)

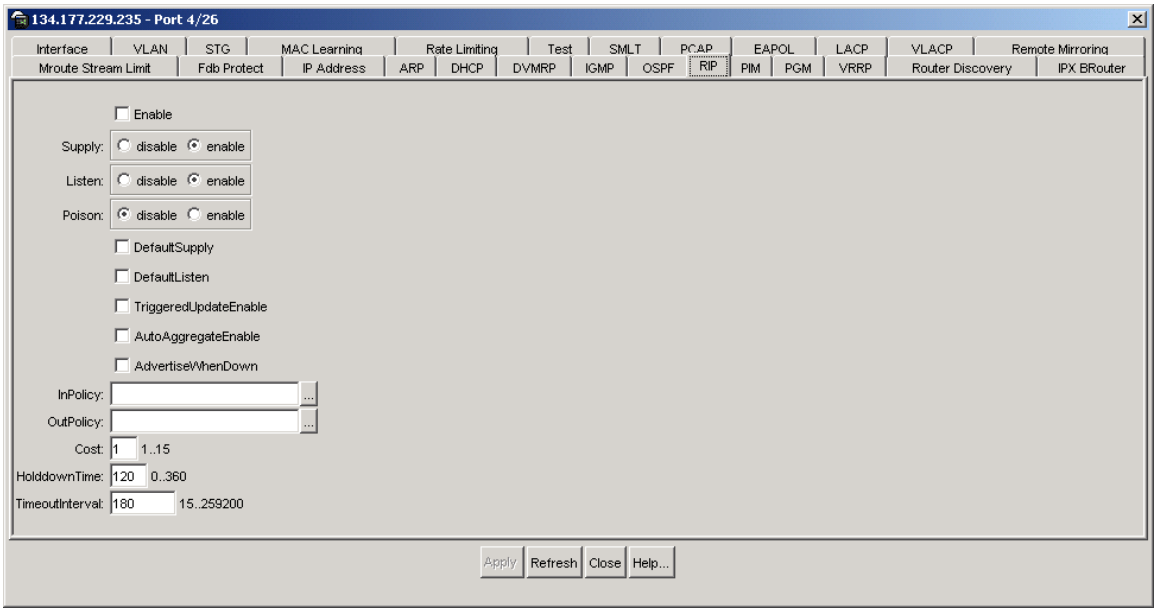
To configure RIP on a port:

1. 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 RIP tab.

   The RIP tab opens (Figure 42).

Figure 42 Port dialog box—RIP tab



4 Check Enable.

5 Click Apply.

6 Click Close.

Table 25 describes the RIP tab fields.

Table 25 RIP tab fields

Field	Description
Enable	If selected, enables RIP on the port.
Supply	Specifies that the routing switch will advertise RIP routes through the interface. The default is enable.
Listen	Specifies that the routing switch will learn RIP routes through this interface. The default is enable.

Table 25 RIP tab fields

Field	Description
Poison	If disabled, split horizon is invoked, meaning that IP routes learned from an immediate neighbor are not advertised back to the neighbor from which the routes were learned. If enabled, the RIP update sent to a neighbor from which a route is learned is "poisoned" with a metric of 16. In this manner, the route entry is not passed along to the neighbor, because historically 16 is "infinity" in terms of hops on a network. The default is disable.
DefaultSupply	Set the value to true if a default route must be advertised out this interface. The default is false. **Note:** The default route will be advertised only if it exists in the routing table.
DefaultListen	Set value to true if default route should be learned on this interface when advertised by another router connected to the interface. The default is false.
TriggeredUpdateEnable	Allows you to enable or disable triggered RIP updates. The default is false (disabled).
AutoAggregateEnable	Allows you to enable or disable RIP automatic aggregation. RIP2 automatically aggregates routes to their natural mask. Auto aggregation can be enabled only in RIP2 mode or RIP1 compatibility mode. The default is false.
AdvertiseWhenDown	If true, the network on this interface will be advertised as up, even if the port is down. The default is false. **Note:** When you configure a port without any link and enable AdvertiseWhenDown, it will not advertise the route until the port is active. Then the route will be advertised even when the link is down. To disable advertising based on link states, disable AdvertiseWhenDown.
InPolicy	Right click in the InPolicy name field and select the policy name to be applied from the PolicyName dialog box. This policy will determine whether to learn a route on this interface. It also specifies the parameters of the route when it is added to the routing table.
OutPolicy	Right click in the OutPolicy name field and select the policy name to be applied from the PolicyName dialog box. This policy will determine whether to advertise a route from the routing table on this interface. This policy also specifies the parameters of the advertisement.
Cost	Indicate the RIP cost for this interface. Enter a value between1 to 15. The default is 1.

Table 25 RIP tab fields

Field	Description
Holddown Time	Indicates a RIP holddown time for this interface. Enter a value from 0- 360.
Timeout Interval	Indicates the RIP timeout interval for this interface. Enter a value from 15- 259200.

Configuring Protocol Independent Multicast (PIM)

To configure PIM on a port:

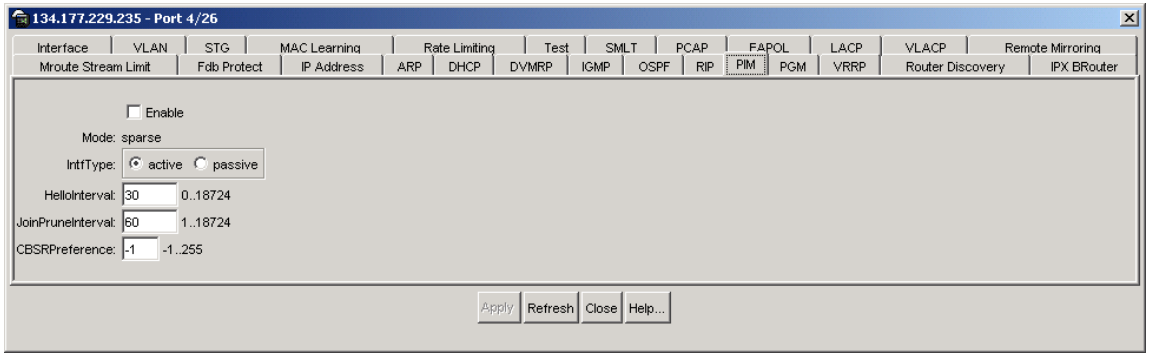
1. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.

2. Click the PIM tab.

   The PIM tab opens (Figure 43).

Figure 43 Port dialog box—PIM tab



3. Check Enable.
4. Click Apply.
5. Click Close.

Table 26 describes the PIM tab fields

Table 26 PIM tab fields

Field	Description
Enable	Enables (true) or disables (false) PIM. You must globally enable PIM before you can enable PIM on a port.
Mode	Displays the mode currently running on the routing switch.
IntfType	Specifies whether the interface type is active or passive.
HelloInterval	Specifies how long to wait (in seconds) before the PIM router sends out the next hello message to neighboring routers. The default is 30 seconds.
JoinPruneInterval	Specifies how long to wait (in seconds) before the PIM router sends out the next join/prune message to its upstream neighbors. The default is 60 seconds.
CBSRPreverence	Sets your preference for this local interface to become a C-BSR. The C-BSR with the highest BSR-priority and address is referred to as the preferred BSR. The default is -1, which indicates that the current interface is not a C-BSR.

Configuring Pragmatic General Multicast (PGM)

To configure PGM on a port:

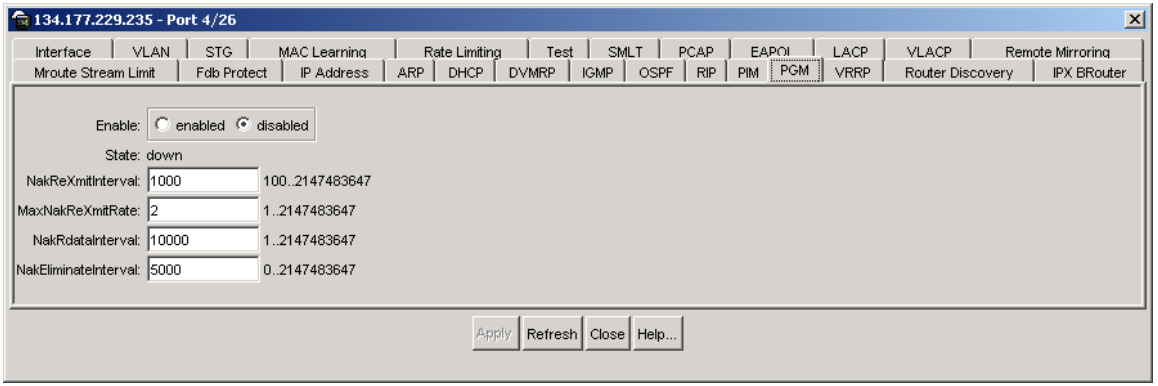
1. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.

2. Click the PGM tab.

   The PGM tab opens (Figure 44).

Figure 44 Port dialog box—PGM tab



3 Click enabled.

4 Click Apply.

5 Click Close.

Table 27 describes the PGM tab fields.

Table 27 PGM tab fields

Field	Description
Enable	Enables or disables PGM on this interface.
State	Indicates the current state (up or down) of PGM.
NakReXmitInterval	Specifies how long to wait for an NCF (in milliseconds) before retransmitting the NAK. The default is 1000 milliseconds.
MaxNakReXmitRate	Configures the maximum number of NAK retransmission packets allowed per second. The default is 2.
NakRdataInterval	Specifies how long to wait for RDATA (in milliseconds) after receiving an NCF. The default is 10000 milliseconds.
NakEliminateInterval	Specifies the length of time (in milliseconds) during which a network element (NE) eliminates duplicate NAKs. When this interval expires, the NE suspends NAK elimination until the first duplicate arrives. Once this NAK is forwarded, the NE once again eliminates duplicate NAKs for the specified interval. This parameter must be less than NakRdataInterval. The default is 5000 milliseconds.

Configuring Virtual Router Redundancy Protocol (VRRP)

To configure VRRP on a port:

To discover a router on a port:

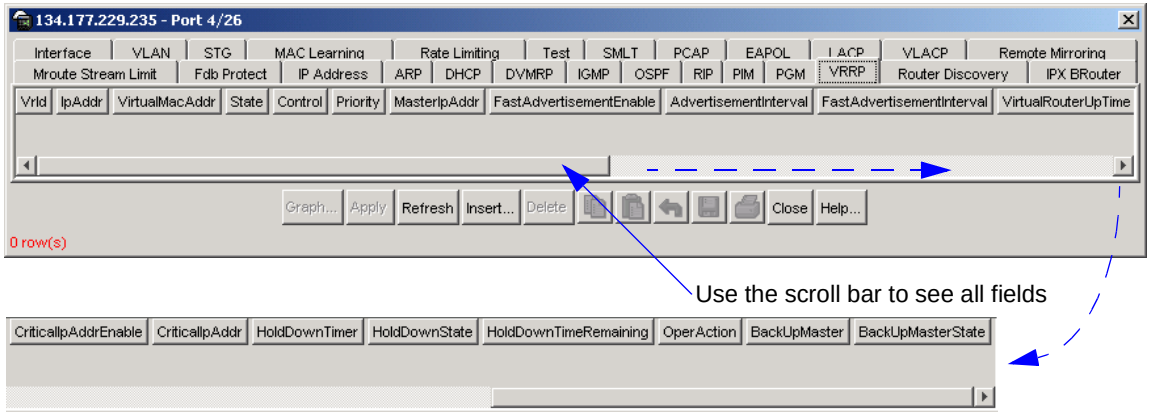
1. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.

2. Click the VRRP tab.

   The VRRP tab opens (Figure 45).

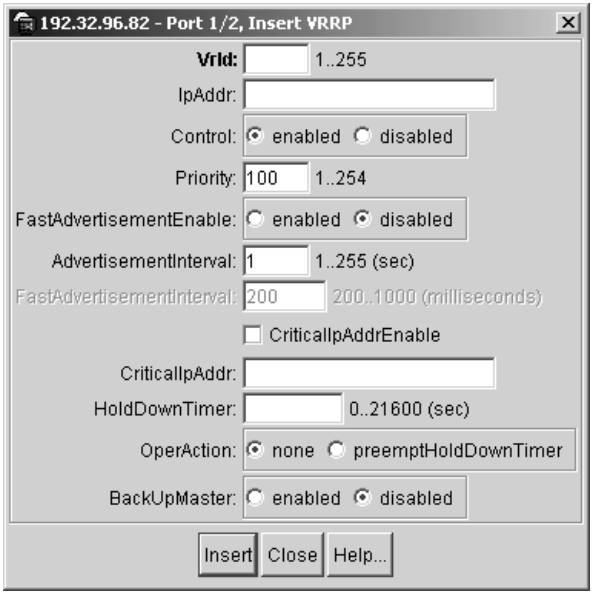
Figure 45 Port dialog box—VRRP tab



3. Click Insert.

   The Port, Insert VRRP dialog box opens (Figure 46).

Figure 46 Port, Insert VRRP dialog box



4 Enter a VrId.

5 Enter an IP address.

6 Click enabled in the Control field.

7 Enter an advertisement interval.

8 Check CriticalIpAddrEnable.

9 Enter a critical IP address.

10 Specify the number of seconds for the HoldDown timer.

11 If desired, select an OperAction.

12 Click enabled to enable BackUpMaster.

13 Click Insert.

14 Click Close.

Table 28 describes the VRRP tab fields.

Table 28 VRRP tab fields

Field	Description
Vrld	A number that uniquely identifies a virtual router on a given VRRP router. The virtual router acts as the default router for one or more assigned addresses (1 to 255).
IpAddr	IP address of the virtual router interface.
VirtualMacAddr	The virtual MAC address of the virtual router. The first three octets consist of the IANA's OUI, the next two octets indicate the address block of the VRRP protocol, and the remaining octets consist of the VRID (for example, 00-00-5E-00-01-<*vrid*>).
State	The current state of the virtual router. This is a read-only field. The valid options are initialize (1) -- the virtual router is starting up backup (2 -- the virtual router is monitoring the state/ availability of the master router master (3) -- the virtual router is functioning as the master router
Control	Whether VRRP is enabled or disabled for the port or VLAN.
Priority	Priority value to be used by this VRRP router. Set a value from 1 to 255, where 255 is reserved for the router that owns the IP addresses associated with the virtual router. The default is 100.
MasterIpAddr	The master router's real (primary) IP address. This is the IP address listed as the source in VRRP advertisement last received by this virtual router. This is read-only field.
FastAdvertisementEnable	Enables or disables the Fast Advertisement Interval. When disabled the regular advertisement interval is used. Default is disable.
AdvertisementInterval	The time interval (in seconds) between sending advertisement messages. Set from 1 to 255 seconds with a default of 1 second. Only the master router sends advertisements.
FastAdvertisementInterval	Sets the Fast Advertising Interval, the time interval between sending VRRP advertisement messages. The interval can be between 200 and 1000 milliseconds, and it must be the same on all participating routers. The default is 200. The values must be entered in multiples of 200 milliseconds.

Table 28 VRRP tab fields

Field	Description
VirtualRouterUpTime	The time interval (in hundredths of a second) since this virtual router was initialized. This is a read-only field.
CriticalIpAddrEnable	Sets the IP interface on the local router to enable or disable the backup.
CriticalIpAddr	Indicates if a user-defined critical IP address should be enabled. There is no effect if a user-defined IP address does not exist. No--use the default IP address (0.0.0.0)
HoldDownTimer	The time interval (in seconds) a router is delayed for the following conditions: The VRRP holddown timer is executed when the switch transitions from Init to backup to master. This occurs only on a switch bootup. The VRRP holddown timer is NOT executed under the following condition: In a non-bootup condition the Backup switch will become master after the Master Downtime Interval. (3 * hello interval), if the master VR goes down. The VRRP holddown timer also applies to the VRRP BackupMaster feature.
HoldDownState	Indicates the hold-down state of this VRRP interface. If the hold-down timer is operational, this field is set to active (2). If it is not operational, it is set to dormant (1).
HoldDownTimeRemaining	Indicates the amount of time (in seconds) left before the hold-down timer will expire. This is a read-only field.
OperAction	Use the action list to manually override the delay timer and force preemption: preemptHoldDownTimer--preempt the timer none--allow the timer to keep working
BackUpMaster	Enables or disables the VRRP backup master feature. This option is only supported on Split-MLT ports.
BackUpMasterState	Indicates the state of the VRRP backup master. The options are up (1) and down (2). The default is down. This is a read-only field.

Discovering routers

To discover a router on a port:

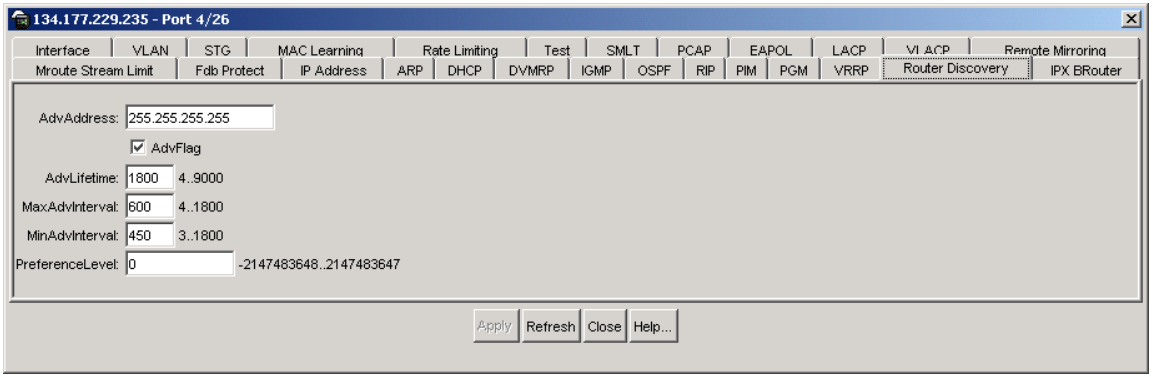
1 From the Device Manager menu bar, choose Edit > Port.

The Port dialog box opens with the Interface tab displayed.

2 Click the Router Discovery tab.

The Router Discovery tab opens (Figure 47).

Figure 47 Port dialog box—Router Discovery tab



3 Enter the Adv IP address.

4 Click Apply. The router is enabled.

Table 29 describes the Test tab fields.

Table 29 Router Discovery tab fields

Field	Description
AdvAddress	The IP destination address to be used for broadcast or multicast router advertisements sent from the interface. The accepted values are the all-systems multicast address, 224.0.0.1, or the limited-broadcast address, 255.255.255.255. The default value is 255.255.255.255.
AdvFlag	A flag indicating whether (True) or not (False) the address is to be advertised on the interface. The default value is TRUE (advertise address).
AdvLifetime	A flag indicating whether (True) or not (False) the address is to be advertised on the interface. The default value is TRUE (advertise address).

Table 29 Router Discovery tab fields

Field	Description
MaxAdvInterval	The maximum time (in seconds) allowed between sending unsolicited broadcast or multicast router advertisements from the interface. The accepted values are no less than 4 seconds and no greater than 1800 seconds. The default value is 600 seconds.
MinAdvInterval	The minimum time (in seconds) allowed between sending unsolicited broadcast or multicast router advertisements from the interface. The accepted values are no less than 3 seconds and no greater than the MaxAdvInterval. The default value is 450 seconds.
PreferenceLevel	Specifies the preference value (a higher number indicates more preferred) of the address as a default router address, relative to other router addresses on the same subnet. The accepted values are -2147483648 to 2147483647. The default value is 0.

Inserting an IPX BRouter

To insert an IPX BRouter on a port:

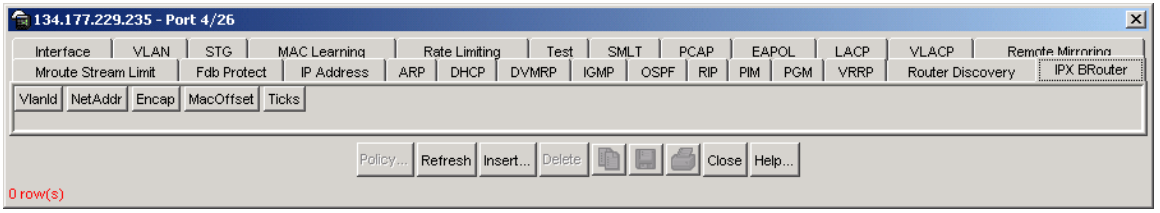
1 From the Device Manager menu bar, choose Edit > Port.

The Port dialog box opens with the Interface tab displayed.

2 Click the IPX BRouter tab.

The IPX BRouter tab opens (Figure 48).

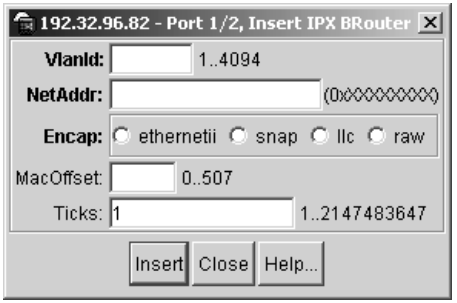
Figure 48 Port dialog box—IPX BRouter tab



3 Click Insert.

The Insert IPX BRouter dialog box opens (Figure 49).

Figure 49 Port, Insert IPX BRouter dialog box



4 Enter a VlanId for the IPX BRouter.

5 Enter a NetAddress.

6 Select an Encap.

7 Enter a Mac offset value.

8 Enter a tick value.

9 Click Insert.

The IPX BRouter is enabled.

Table 30 describes the Insert IPX BRouter dialog box fields.

Table 30 Insert IPX BRouter dialog box fields

Field	Description
VlanId	The VLAN id.
NetAddr	The IPX network address value.
Encap	The encapsulation method.
MacOffset	The mac_offset is a optional parameter that allows you to manually change the default MAC address for a logical or physical interface. Value is an integer from 0 to 507. The default is the next available value.
Ticks	The value that determines the best route for the IPX routed VLAN. The lower the tick value the better the route. Enter a tick value with the range of 1 to 32767. If you enter a value larger than 32767, an error message will display alerting you that the value has been changed to 32767, and a log message is generated.

Configuring Link Aggregation Control Protocol (LACP)

LACP allows you to manage link aggregation trunk groups. To configure LACP on a port:

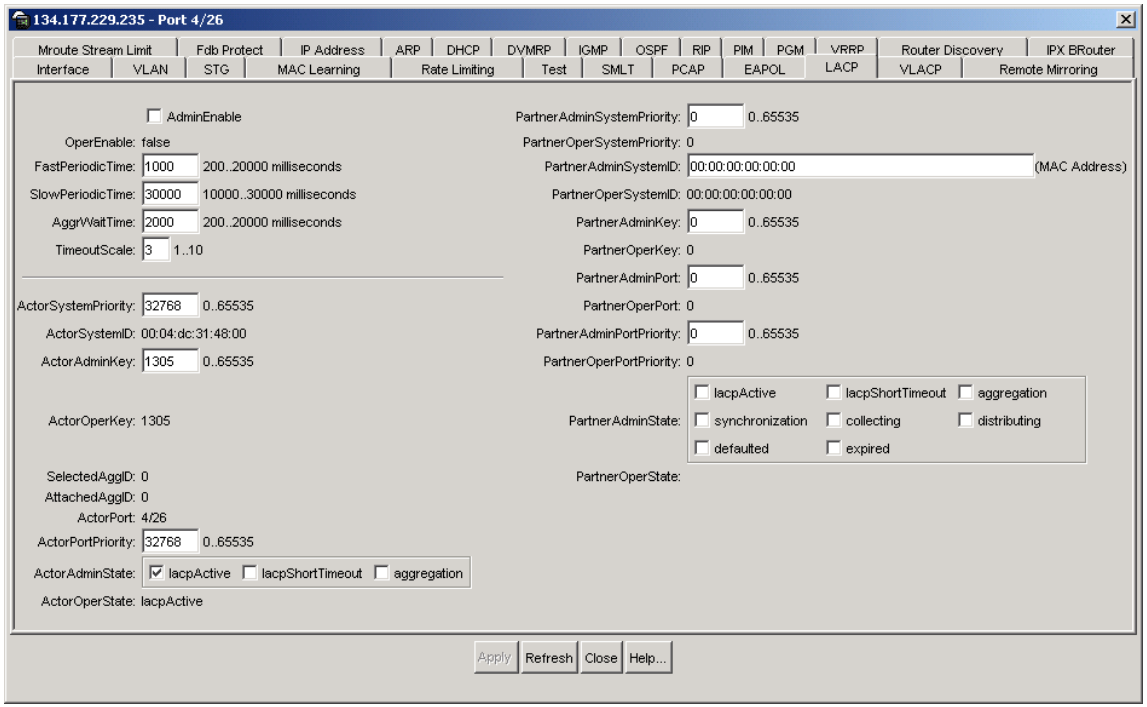
1. Select a port.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.

3. Click the LACP tab.

   The LACP tab opens (Figure 50).

Figure 50 Port dialog box—LACP tab



4. Click the AdminEnable check box to select LACP on the port.
5. Enter data in the remaining fields as necessary.
6. Click Apply.

7 Click Close.

Table 31 describes the LACP tab fields.

Table 31 LACP tab fields

Field	Description
AdminEnable	Enables or disables LACP on a port. The default value is False.
OperEnable	Indicates whether LACP is operationally enabled or disabled. This is a read-only field.
FastPeriodic Time	Specifies the number of milliseconds between periodic transmissions using short timeouts. Valid values range from 200- 20000 with a default of 1000.
SlowPeriodic Time	Specifies the number of milliseconds between periodic transmissions using long timeouts. Valid values range from 10000- 30000 with a default of 30000.
AggrWait Time	Specifies the number of milliseconds to delay aggregation to allow multiple links to aggregate simultaneously. Valid values range from 200- 20000 with a default of 2000.
Timeout Scale	Specifies a value used to calculate timeout time from periodic time. For example: Timeout = PeriodicTime * TimeoutScale Valid values range from 1- 10 with a default of 3.
ActorSystemPriority	Specifies a value used to define the priority value associated with the Actor's system ID. Valid values range from 0- 65535.
ActorSystemID	Specifies a read-only MAC address value that defines the value of the system ID for the system containing this aggregation port.
ActorAdminKey	Specifies the current administrative value of the key for the aggregation port. The meaning of particular key values is of local significance.
ActorOperKey	Specifies the current operational value of the key for the aggregation port. This is a read-only value. The meaning of particular key values is of local significance.
SelectedAggID	Specifies the identifier value of the aggregator that this aggregation port has currently selected. Zero indicates that the aggregation port has not selected an aggregator, either because it is in the process of detaching from an aggregator, or because there is no suitable aggregator available for it to select. This is a read-only field.
AttachedAggID	Specifies the identifier value of the aggregator that this aggregation port is currently attached to. Zero indicates that the aggregation port is not currently attached to an aggregator. This is a read-only field.

Table 31 LACP tab fields

Field	Description
ActorPort	Specifies the port number locally assigned to the aggregation port. The port number is communicated in LACPDUs as the actor port. This is a read-only field.
ActorPortPriority	Specifies the priority value assigned to this aggregation port. Valid values range from 0- 65535.
ActorAdminState	Identifies a string of 8 bits corresponding to the administrative values of actor state as transmitted by the actor in LACPDUs. The bit correspondence is as follows: • The first bit corresponds to bit 0 of actor state (lacpActive) • The second bit corresponds to bit 1 (lacpShortTimeout) • The third bit corresponds to bit 2 (Aggregation) • The fourth bit corresponds to bit 3 (Synchronization) • The fifth bit corresponds to bit 4 (Collecting) • The sixth bit corresponds to bit 5 (Distributing) • The seventh bit corresponds to bit 6 (Defaulted) • The eighth bit corresponds to bit 7 (Expired) Only lacpActive, lacpShortTimeout and aggregation are supported in the Passport 8000 Series switch. Thus, the user can only configure bits 0, 1, and 2.
ActorOperState	Identifies a string of 8 bits corresponding to the current operational values of actor state as transmitted by the actor in LACPDUs. This is a read-only field.
PartnerAdminSystemPriority	Identifies a value used to define the administrative priority value associated with the partner's system ID. The assigned value is used, along with the value of the PartnerAdminSystemID, PartnerAdminKey, PartnerAdminPort, and PartnerAdminPortPriority parameters, to manually configure aggregation. Valid values here range from 0- 65535.
PartnerOperSystemPriority	Specifies a value indicating the operational priority value associated with the partner's system ID. It may contain the manually configured value carried in the PartnerAdminSystemPriority field if there is no protocol partner. This is a read-only field.
PartnerAdminSystemID	Specifies a MAC address representing the administrative value of the aggregation port protocol partner's system ID. The assigned value is used, along with the value of the PartnerAdminSystemPriority, PartnerAdminKey, PartnerAdminPort, and PartnerAdminPortPriority parameters, to manually configure aggregation.
PartnerOperSystemID	Specifies a MAC address representing the current value of the aggregation port's protocol partner's system ID. A value of zero indicates that there is no known protocol partner. The value of this attribute may contain the manually configured value carried in the PartnerAdminSystemID field if there is no protocol partner. This is a read-only field.

Table 31 LACP tab fields

Field	Description
PartnerAdminKey	Specifies the current administrative value of the key for the protocol partner. The assigned value is used, along with the value of the PartnerAdminSystemPriority, PartnerAdminSystemID, PartnerAdminPort, and PartnerAdminPortPriority parameters, to manually configure aggregation. Valid values here range from 0- 65535.
PartnerOperKey	Specifies the current operational value of the key for the protocol partner. The value of this attribute may contain the manually configured value carried in the PartnerAdminKey parameter if there is no protocol partner. This is a read-only field.
PartnerAdminPort	Specifies the current administrative value of the port number for the protocol partner. The assigned value is used, along with the value of the PartnerAdminSystemPriority, PartnerAdminSystemID, PartnerAdminKey, and PartnerAdminPortPriority parameters, to manually configure aggregation. Valid values here range from 0- 65535.
PartnerOperPort	Specifies the operational port number assigned to this aggregation port by the aggregation port's protocol partner. This value may contain the manually-configured value carried in the PartnerAdminPort parameter if there is no protocol partner. This is a read-only field.
PartnerAdminPortPriority	Specifies the current administrative value of the port priority for the protocol partner. The assigned value is used, along with the value of the PartnerAdminSystemPriority, PartnerAdminSystemID, PartnerAdminKey, and PartnerAdminPort parameters, to manually configure aggregation. Valid values here range from 0- 65535.
PartnerOperPortPriority	Specifies the priority value assigned to this aggregation port by the partner. This value may contain the manually-configured value carried in the PartnerAdminPortPriority parameter if there is no protocol Partner. This is a read-only field.

Table 31 LACP tab fields

Field	Description
PartnerAdminState	Identifies a string of 8 bits corresponding to the administrative values of actor state as transmitted by the actor in LACPDUs. The bit correspondence is as follows: • The first bit corresponds to bit 0 of actor state (lacpActive) • The second bit corresponds to bit 1 (lacpShortTimeout) • The third bit corresponds to bit 2 (Aggregation) • The fourth bit corresponds to bit 3 (Synchronization) • The fifth bit corresponds to bit 4 (Collecting) • The sixth bit corresponds to bit 5 (Distributing) • The seventh bit corresponds to bit 6 (Defaulted) • The eighth bit corresponds to bit 7 (Expired) Only lacpActive, lacpShortTimeout and aggregation are supported in the Passport 8000 Series switch. Thus, the user can only configure bits 0, 1, and 2.
PartnerOperState	Identifies a string of 8 bits corresponding to the current operational values of actor state as transmitted by the actor in LACPDUs. This is a read-only field

Configuring Virtual LACP

VLACP is an extension to LACP used to detect end-to-end failure. To configure VLACP on a port:

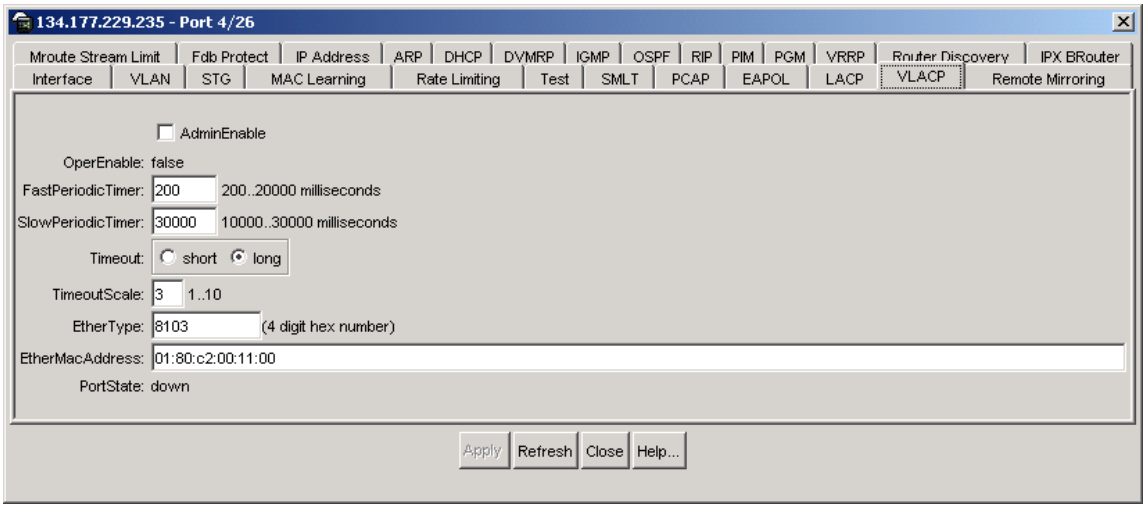
1. Select a port.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.

3. Click the VLACP tab.

   The VLACP tab opens (Figure 51).

Figure 51 Port dialog box—VLACP tab



4 Click the AdminEnable check box to select VLACP on the port.

5 Enter data in the remaining fields as necessary.

6 Click Apply.

7 Click Close.

Table 32 describes the VLACP tab fields.

Table 32 VLACP tab fields

Field	Description
AdminEnable	Enables or disables VLACP on a port. The default value is False.
OperEnable	Indicates whether VLACP is operationally enabled or disabled. This is a read-only field.
FastPeriodic Timer	Specifies the number of milliseconds between periodic transmissions using short timeouts. Valid values range from 200- 20000 with a default of 250
SlowPeriodic Timer	Specifies the number of milliseconds between periodic transmissions using long timeouts. Valid values range from 10000- 30000 with a default of 30000.
Timeout	Specifies whether the timeout control value is a short or long timeout.

Table 32 VLACP tab fields

Field	Description
TimeoutScale	Specifies a value used to calculate timeout time from periodic time. For example: Timeout = PeriodicTime * TimeoutScale Valid values range from 1- 10 with a default of 3.
EtherType	Specifies VLACP protocol identification. The ID value is a 4-digit Hex number, with a default of 8103.
EtherMacAddress	Identifies a multicast MAC address used exclusively for VLACPDUs.
PortState	Identifies whether the VLACP port state is up or down. This is a read-only field.

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: The Clear Counter function in Device Manager does not affect the AbsoluteValue counter in the switch. Instead, the Clear Counter function clears all cached data in Device Manager (except AbsoluteValue). To reset AbsoluteValue(s), use the Reset Counter function (Edit > Chassis > System).

To graph port statistics for a single or multiple ports:

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

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 52).

Figure 52 GraphPort dialog box—Interface tab

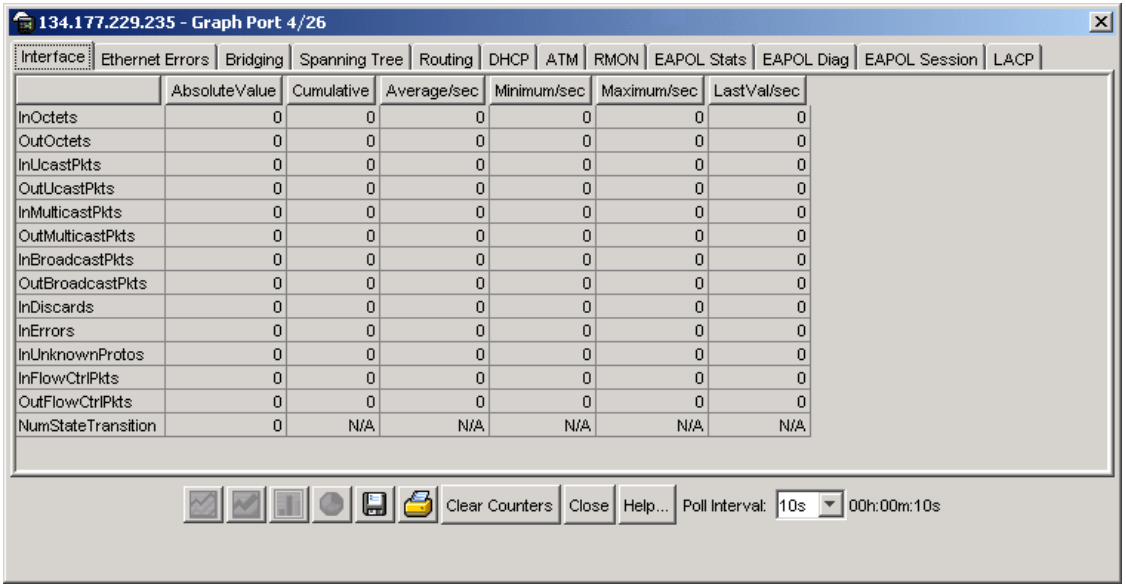


Table 33 describes the Interface tab fields in the graphPort dialog box.

Table 33 Graph 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 33 Graph 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 53).

Figure 53 GraphPort dialog box—Ethernet Errors tab

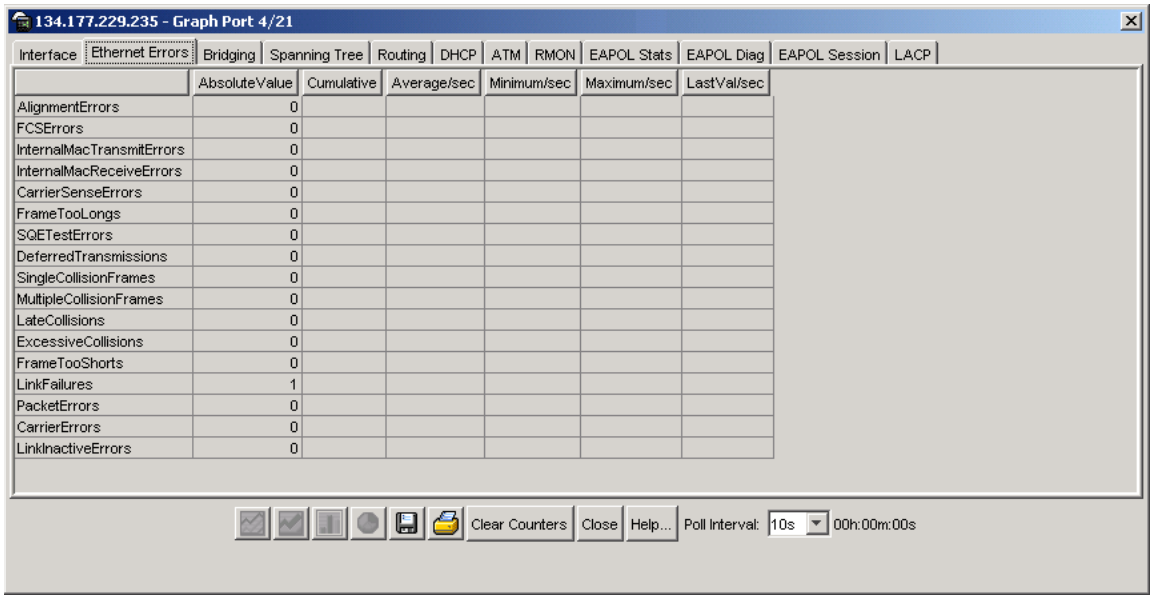


Table 34 describes the Ethernet Errors tab fields.

Table 34 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.

Table 34 Ethernet Errors tab fields (continued)

Field	Description
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.
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.

Table 34 Ethernet Errors tab fields (continued)

Field	Description
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.
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 54).

Figure 54 GraphPort dialog box—Bridging tab

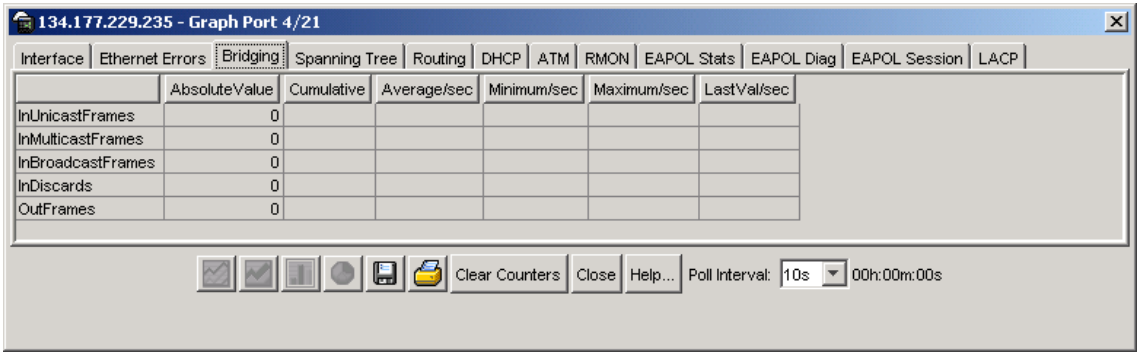


Table 35 describes the Bridging tab fields.

Table 35 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.

Table 35 Bridging tab fields (continued)

Field	Description
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 55).

Figure 55 GraphPort dialog box—Spanning Tree tab

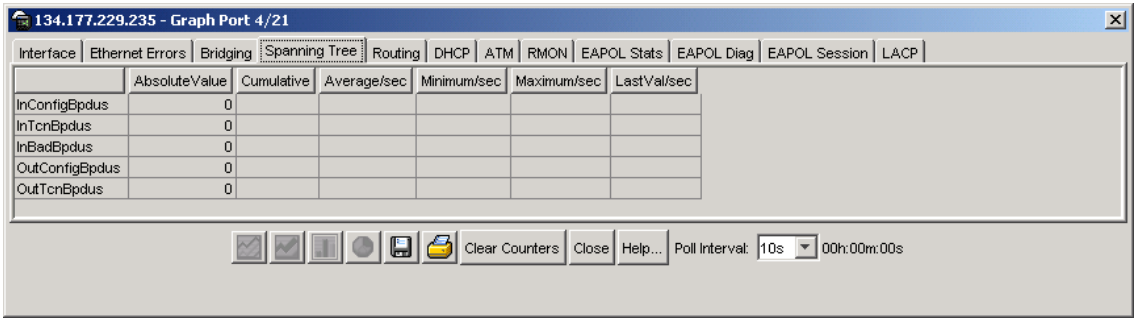


Table 36 describes the Spanning Tree tab fields.

Table 36 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:

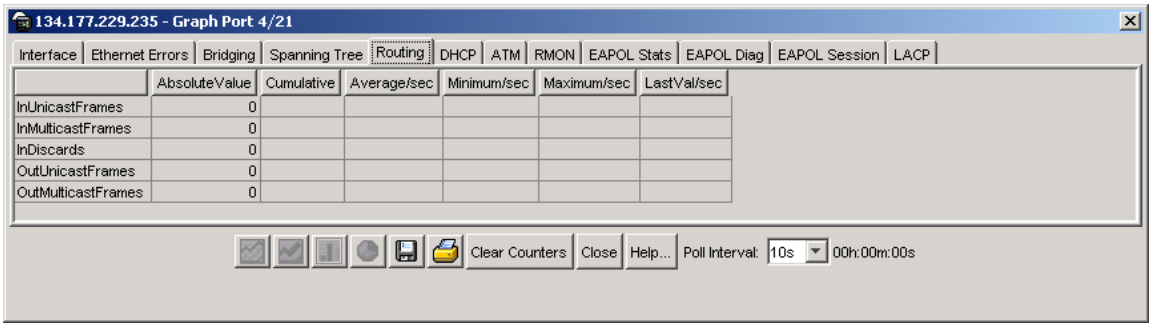
1. On the device view, select a port or multiple ports.
2. From the Device Manager menu bar, choose Graph > Port.

   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 56).

Figure 56 GraphPort dialog box—Routing tab



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).

Table 37 describes the Routing tab fields.

Table 37 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 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 Edit > Port.

The Port dialog box opens with the Interface tab displayed (Figure 22 on page 79).

3 Click the OSPF tab.

The OSPF tab opens (Figure 41 on page 111).

4 Click Enable to select the OSPF option.

5 Click Apply.

6 Click Close.

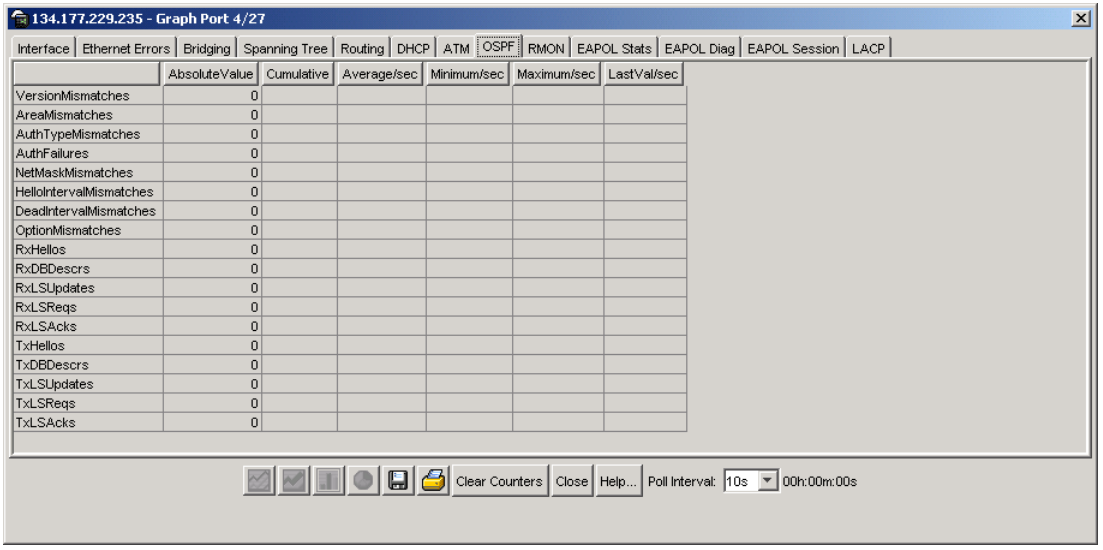
7 From the Device Manager menu bar, choose Graph > Port.

The graphPort dialog box opens with the Interface tab displayed.

8 Click the OSPF tab.

The OSPF tab opens (Figure 57).

Figure 57 GraphPort dialog box—OSPF tab



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

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

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

Table 38 describes the OSPF tab fields.

Table 38 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.

Table 38 OSPF tab fields

Field	Description
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.
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 LACP statistics

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

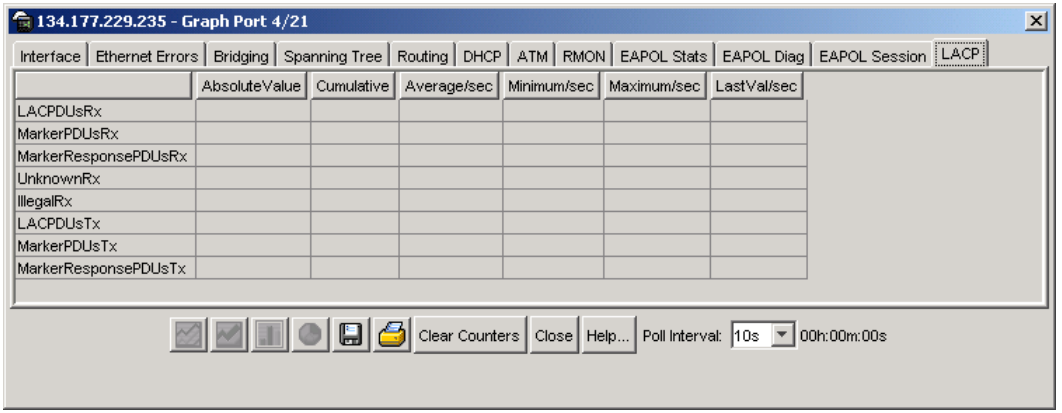
1. On the device view, select a port or multiple ports.
2. From the Device Manager menu bar, choose Graph > Port.

   The graphPort dialog box opens with the Interface tab displayed.

3. Click the LACP tab.

   The LACP tab opens (Figure 58).

Figure 58 GraphPort dialog box—LACP tab



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).

Table 39 describes the LACP tab fields.

Table 39 LACP tab fields

Field	Description
LACPDUsRX	Identifies the number of valid LACPDUs received on this aggregation port. This is a read-only field.
MarkerPDUsRX	Identifies the number of valid marker PDUs received on this aggregation port. This is a read-only field.
MarkerResponsePDUsRX	Identifies the number of valid marker response PDUs received on this aggregation port. This is a read-only field.
UnknownRX	Identifies the number of received frames that either: • carry the slow protocols Ethernet type value, but contain an unknown PDU or • are addressed to the slow protocols group MAC address, but do not carry the slow protocols Ethernet type. This is a read-only field.

Table 39 LACP tab fields

Field	Description
IllegalRX	Identifies the number of received frames that carry the slow protocols Ethernet type value, but contain a badly formed PDU or an illegal protocol subtype value. This is a read-only field.
LACPDUsTX	Identifies the number of LACPDUs transmitted on this aggregation port. This is a read-only field.
MarkerPDUsRX	Identifies the number of marker PDUs transmitted on this aggregation port. This is a read-only field.
MarkerResponsePDUsTX	Identifies the number of marker response PDUs transmitted on this aggregation port. This is a read-only field.

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:

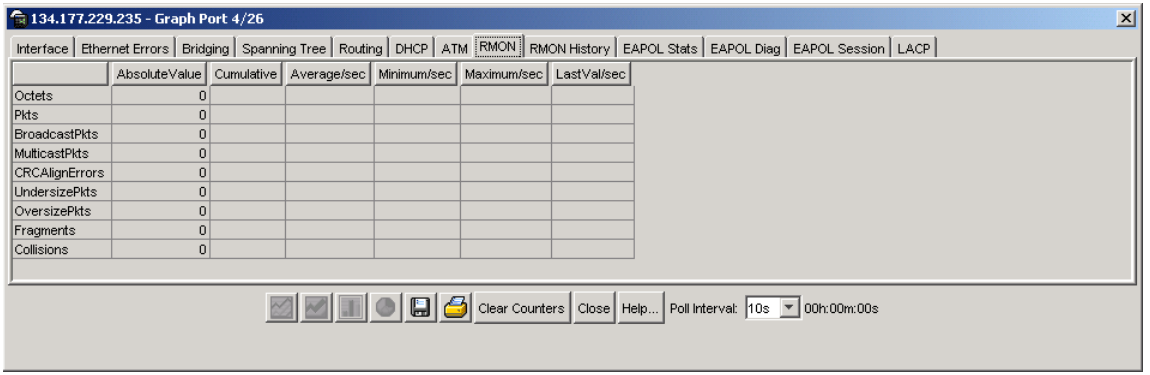
1. From the Device Manager menu bar, choose RMON > Options.
2. Click Enable.
3. Click Apply and then Close.
4. Right click on the port you want to graph.
5. Select Enable Rmon Stats.
6. From the Device Manager menu bar, choose Graph > Port.

   The graphPort dialog box opens with the Interface tab displayed.

7. Click the RMON tab.

   The RMON tab opens (Figure 59).

Figure 59 GraphPort dialog box—RMON tab



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

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

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

Table 40 describes the fields in the RMON tab.

Table 40 RMON tab fields

Field	Description
Octets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). You can use this object as a reasonable estimate of Ethernet utilization. For greater precision, sample the etherStatsPkts and etherStatsOctets objects before and after a common interval.
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).

Table 40 RMON tab fields (continued)

Field	Description
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:

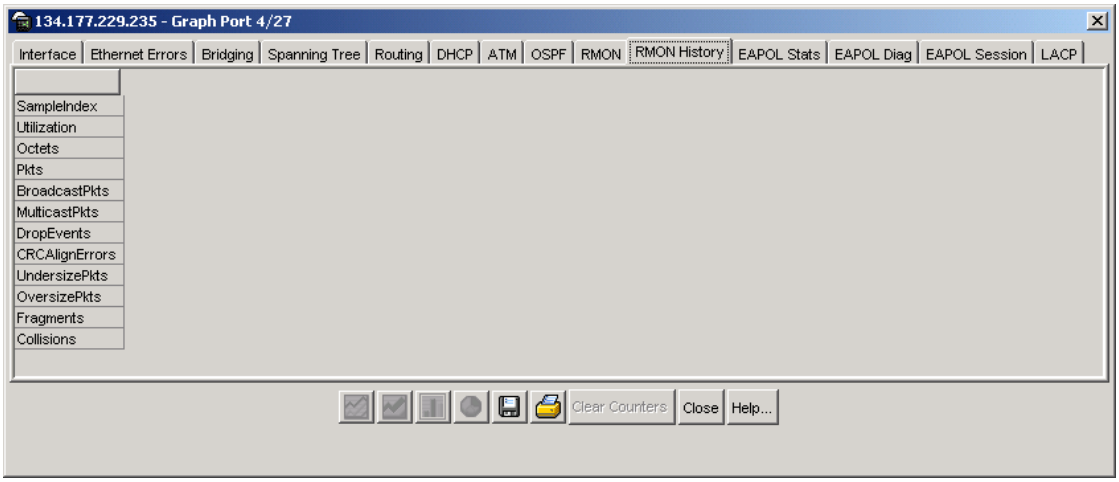
1. If you haven't already done so, enable RMON by choosing RMON > Options from the Device Manager menu bar.
2. Right click on the port you want to graph.
3. Select Enable Rmon History.
4. From the Device Manager menu bar, choose Graph > Port.

   The graphPort dialog box opens with the Interface tab displayed.

5. Click the RMON History tab.

The RMON History tab opens (Figure 60).

Figure 60 GraphPort dialog box—RMON History tab



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

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

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

Table 41 describes the fields in the RMON History tab.

Table 41 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 etherStststPkts 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: $Utilization = \frac{Pkts \times (9.6 + 6.4) + (Octets \times 0.8)}{Interval \times 10000}$ 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.

Table 41 RMON History tab fields (continued)

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 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.
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 38 on page 105).

4 Click Enable to select the DHCP option.

5 Click Apply.

6 Click Close.

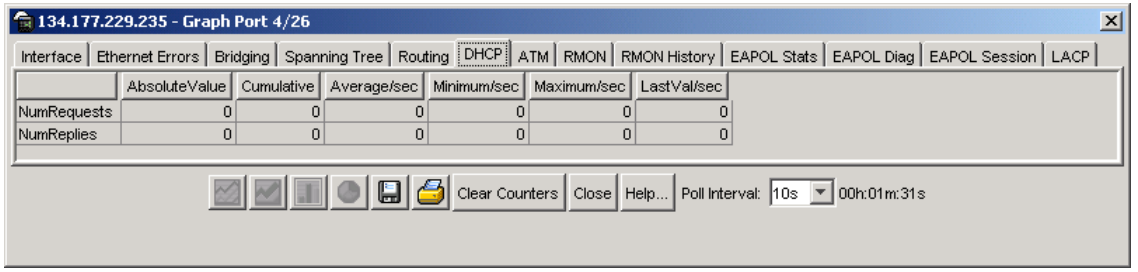
7 From the Device Manager menu bar, choose Graph > Port.

The graphPort dialog box opens with the Interface tab displayed.

8 Click the DHCP tab.

The DHCP tab opens (Figure 61).

Figure 61 GraphPort dialog box—DHCP tab



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

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

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

Table 42 describes the fields in the DHCP tab.

Table 42 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 VRRP statistics

To graph VRRP statistics:

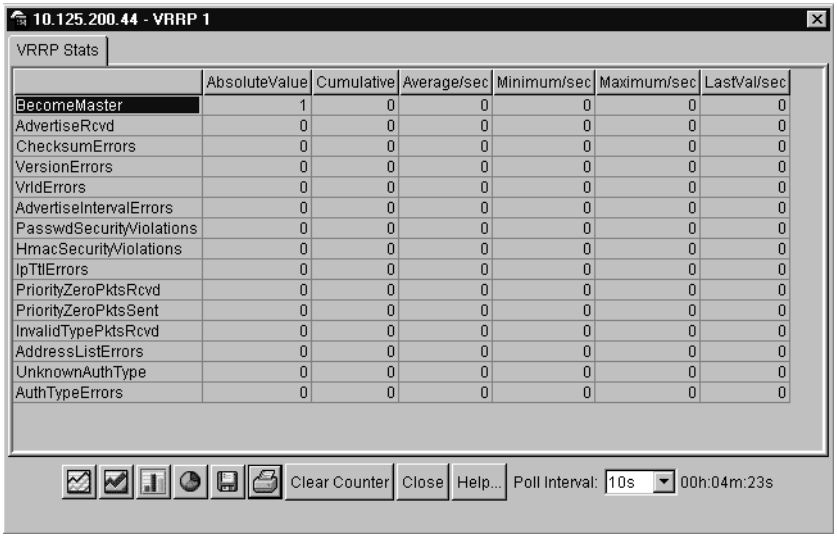
1. On the device view, select a port.
2. From the Device Manager menu bar, choose VLAN > VLANs.

   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 62).

Figure 62 VRRP dialog box—VRRP Stats tab



6 Select the statistics that you want to graph.

7 Click Graph.

Table 43 describes the fields in the VRRP Stats tab.

Table 43 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 43 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.

Graphing EAPoL statistics

The Passport 8000 Series switch allows you to monitor and troubleshoot your switch using the EAPoL Authentication, Diagnostic, and Session statistics graphing tools.

Note: For more information, see *Configuring and Managing Security* in the Passport 8000 Series Software Release 3.7.

Chapter 5
Configuring and graphing chassis information

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.

This chapter includes the following topics:

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 63).

Figure 63 Chassis dialog box—System tab

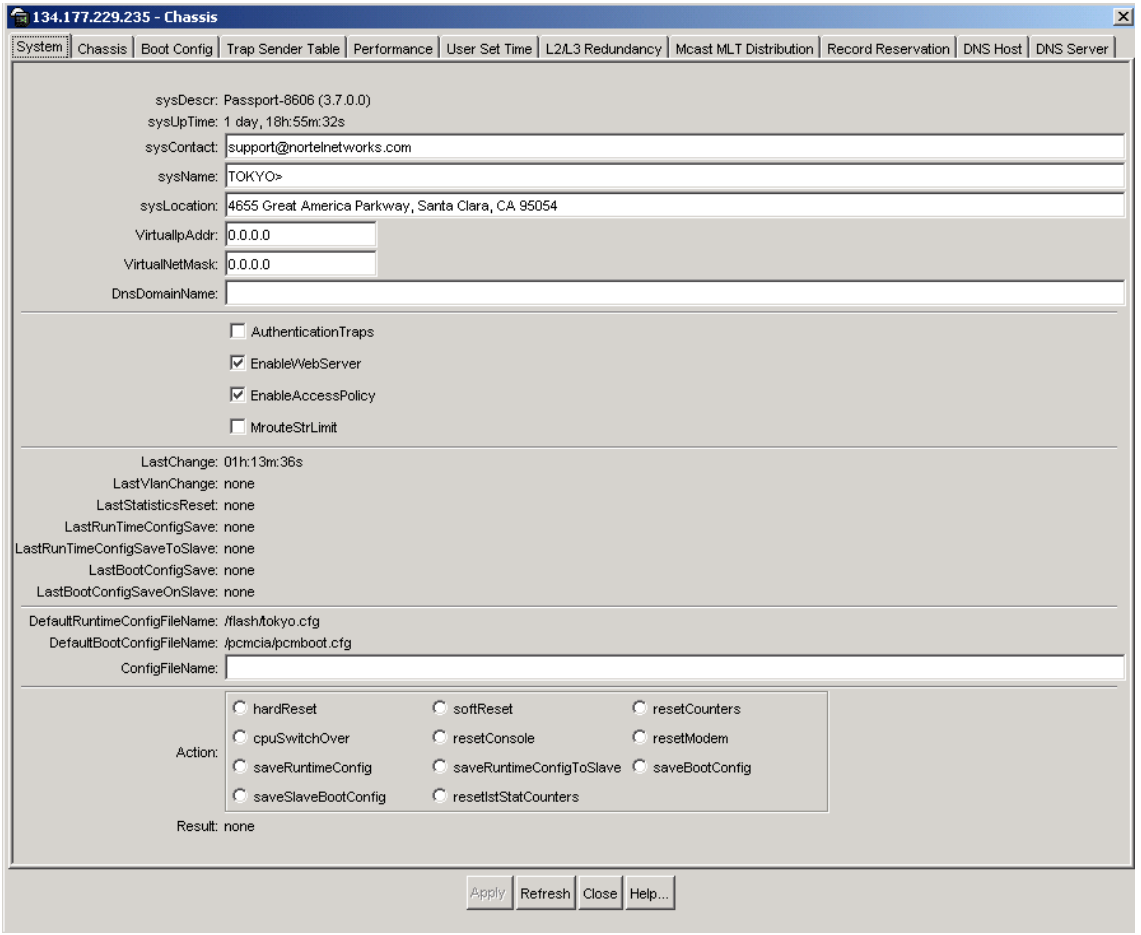


Table 44 describes the System tab fields.

Table 44 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.
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.
DnsDomainName	The default domain for querying the DNS server.
AuthenticationTraps	Enables or disables authentication traps. When you enable, SNMP traps are sent to trap receivers for all SNMP access authentication. To view traps, click the Trap Log button on the Device Manager toolbar.
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.
MrouteStrLimit	Enables or disables the mroute stream limit in the system.
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.

Table 44 System tab fields (continued)

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

Editing chassis information

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 64).

Figure 64 Chassis dialog box—Chassis tab

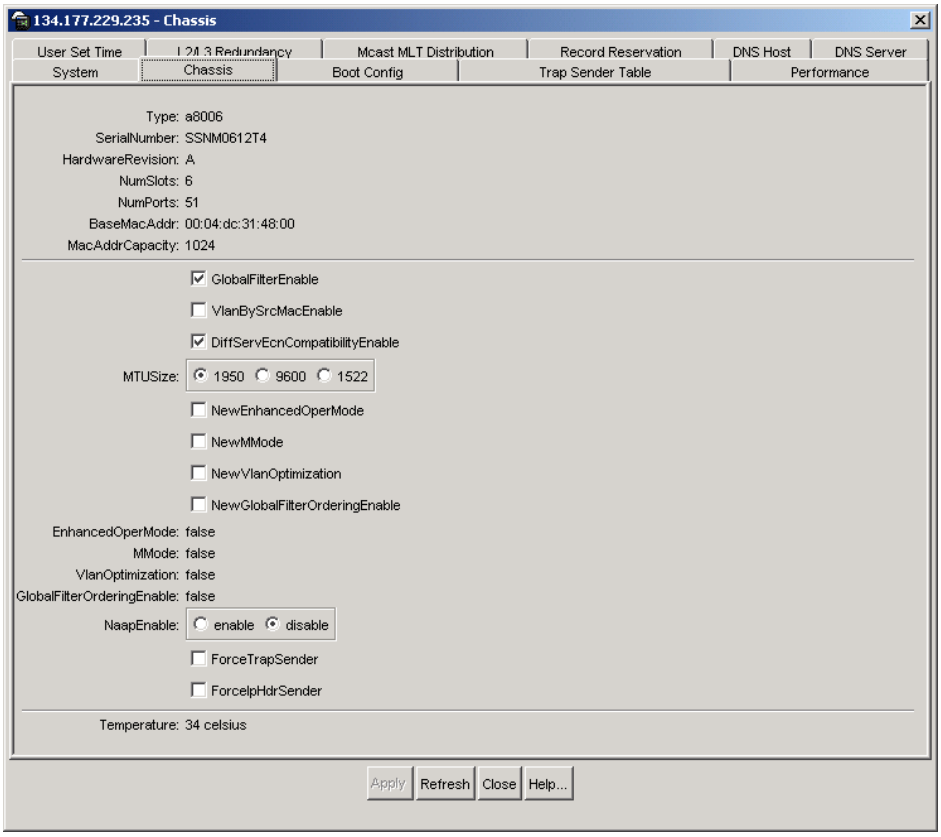


Table 45 describes the Chassis tab fields.

Table 45 Chassis tab fields

Field	Description
Type	The Passport 8000 Series module type.
SerialNumber	A unique chassis serial number.
HardwareRevision	The current hardware revision of the device chassis.

Table 45 Chassis tab fields (continued)

Field	Description
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.
MacAddrCapacity	Specifies a MAC address capacity.
GlobalFilterEnable	Used to enable/disable global filters in the system.
VlanBySrcMacEnable	Used to enable/disable source MAC based VLANs in the system.
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.
MTUSize	Specifies the maximum transmission unit size.
NewEnhancedOperMode	Enables enhanced operation mode.
NewMMode	Enables extended memory mode.
NewVlanOptimization	Enables VLAN optimization mode.
NewGlobalFilterOrderingEnable	Enables global filter ordering. The change will take effect on reboot.
EnhancedOperMode	Displays the current EnhancedOperMode status, enabled (true) or disabled (false).
MMode	Displays the current MMode status, enabled (true) or disabled (false).
VlanOptimization	Indicates whether or not VLAN Optimization is enabled on the system. This is a read-only field.
GlobalFilterOrderingEnable	Indicates whether or not GlobalFilterOrdering is enabled on the system. This is a read-only field.
NaapEnable	Enables or disables the NAAP feature.
ForceTrapSender	Turns on a flag that configures CLIP (CircuitLess IP) as the trap originator.

Table 45 Chassis tab fields (continued)

Field	Description
ForceIpHdrSender	Turns on a flag that decides whether the IP header source address is matched with the SNMP header sender networks.
Temperature	The current temperature of the chassis.

Enabling L2/L3 static routes

Note: After you enable or disable the high availability feature, the bootconfig is saved onto the master and the standby CPU and the standby CPU is reset automatically. However, you need to manually reset the master CPU.

To enable static routes:

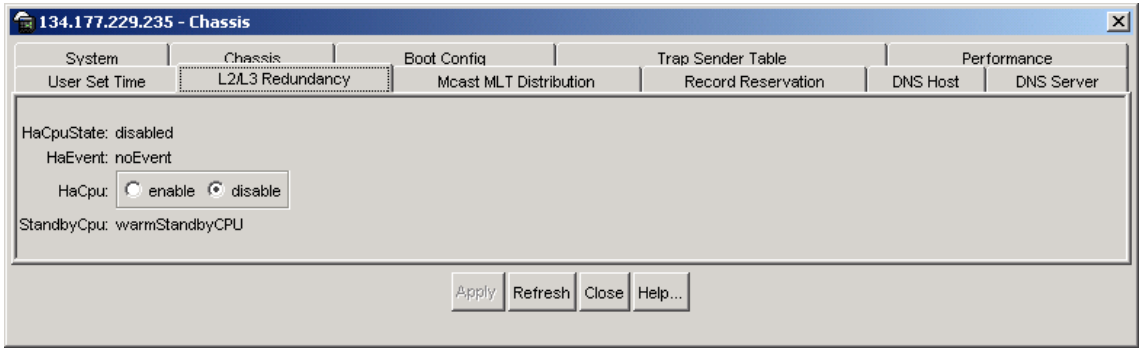
1. From the Device Manager menu bar, choose Edit > Chassis.

   The Chassis dialog box opens with the System tab displayed.

2. Click on the L2/L3 Redundancy tab.

   The L2/L3 Redundancy tab opens (Figure 65).

Figure 65 Chassis dialog box—L2/L3 Redundancy tab

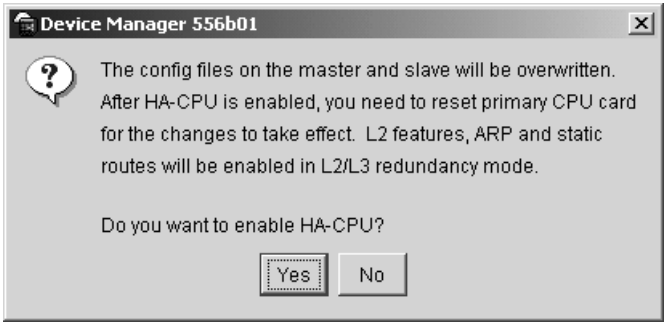


3. Click Enable.

4 Click Apply.

The enable HA-CPU message box opens (Figure 66).

Figure 66 Enable HA-CPU message box



5 Click Yes.

6 Click Close.

Disabling L2/L3 static routes

To disable static routes:

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

The Chassis dialog box opens with the System tab displayed.

2 Click on the L2/L3 Redundancy tab.

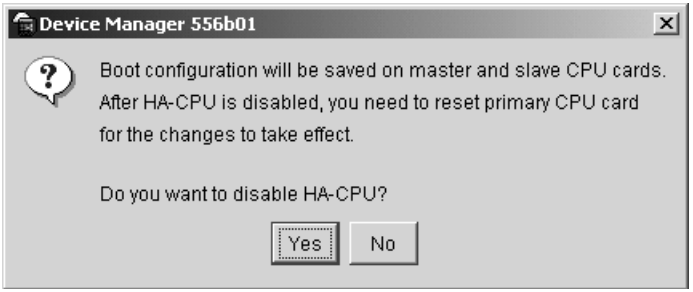
The L2/L3 Redundancy tab opens (Figure 65 on page 161).

3 Click Disable.

4 Click Apply.

The disable HA-CPU message box opens (Figure 67).

Figure 67 Disable HA-CPU message box



5 Click Yes.

6 Click Close.

Viewing L2/L3 Redundancy status

To view the L2/L3 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/L3 Redundancy tab.

The L2/L3 Redundancy tab opens (Figure 65 on page 161).

Table 46 describes the L2/L3 Redundancy tab fields.

Table 46 L2 Redundancy tab fields

Field	Description
HaCpuState	This field indicates the state of the CPUs. The possible CPU states area: • initialization - The two CPUs establish a connection and exchange version information. • oneWayActive - modules that need to be synchronized have been registered. • twoWayActive - modules that need to be synchronized have registered with the redundancy framework on both CPUs. • synchronized - table based synchronization was completed on the current CPU. • remote incompatible - the CPUs software versions are incompatible. • error - If an invalid event is generated in a given state the CPU displays the error state. • disabled - HA is not enabled on the CPU.
Ha Event	This field displays the event status. The possible event status values are: • Restart. • Transfer to a One Way or Two Way Active state. • Transfer to a synchronized state. • Transfer go to a remote incompatible state. • No event has occurred.
Enable	Allows you to enable or disable L2/L3 redundancy on the master CPU.
StandbyCpu	This field indicates if the L2/L3 Redundancy is enabled on the standby CPU. The possible states are: • hotStandbyCPU • warmStandbyCPU • standbyCPUNotPresent

Reserving records

To reserve records:

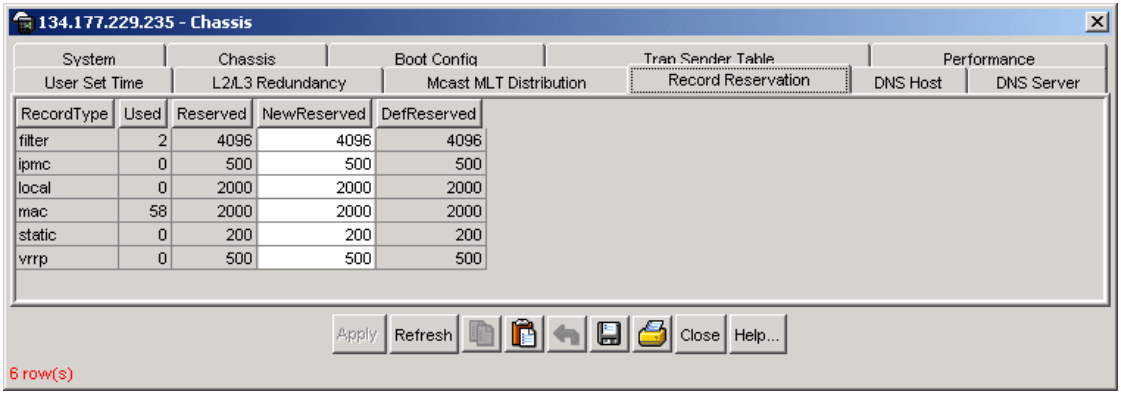
1 From the Device Manager menu bar, choose Edit > Chassis.

The chassis dialog box opens with the System tab displayed.

2 Click on the Record Reservation tab.

The Record Reservation tab opens (Figure 68). Each record type has number of reserved records shown in the Reserved column.

Figure 68 Chassis dialog box—Record Reservation tab



3 Select the amount in the NewReserved column for the record type you want to modify.

4 Click Apply.

The Reserved column displays the new number of reserved records.

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 69).

Figure 69 Chassis dialog box—Boot Config tab

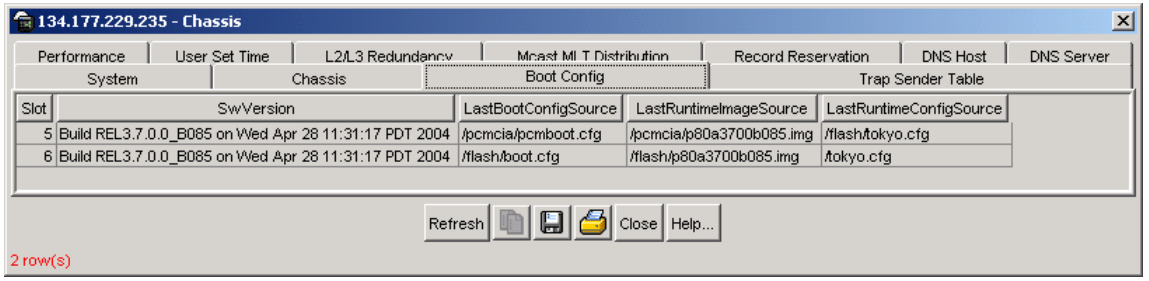


Table 47 describes the Boot Config tab fields.

Table 47 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.

Viewing the trap sender table

You can use the trap sender table to view source and receiving addresses as follows:

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 Sender Table tab.

The Trap Sender Table tab opens (Figure 70).

Figure 70 Chassis dialog box—Trap Sender Table tab

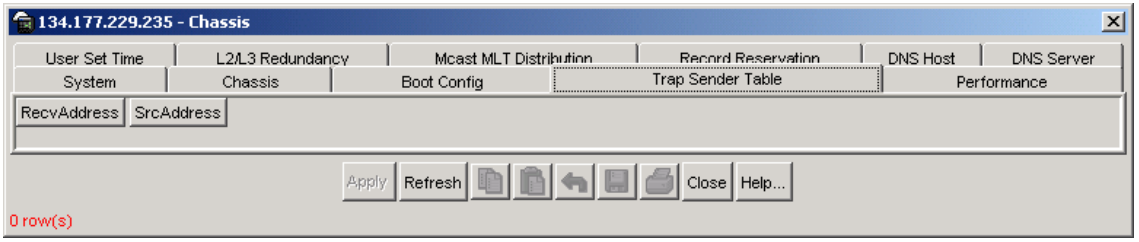


Table 48 describes the Trap Sender Table tab fields.

Table 48 Trap Sender Table tab fields

Field	Description
RecvAddress	Specifies the IP address for the trap receiver. This is a read-only parameter containing the IP address configured in the TAddress field in the TargetTable.
SrcAddress	Identifies the IP address for the trap sender.

Checking system performance

You can check system performance with the Performance tab. Note that the Performance tab displays the same data as the Graph > Chassis > System menu, with the exception of the DramSize field. For further information, see "Graphing system statistics" on page 197.

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 71).

Figure 71 Chassis dialog box—Performance tab

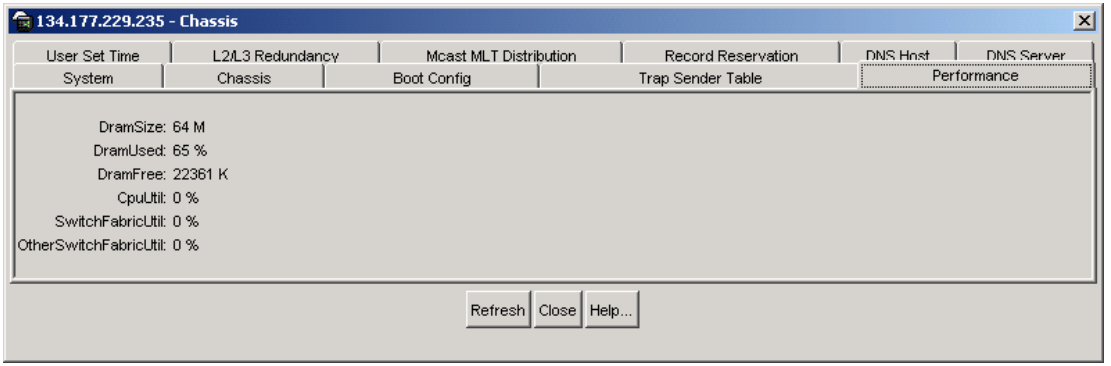


Table 49 describes the Performance tab fields.

Table 49 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 72).

Figure 72 Chassis dialog box—User Set Time tab

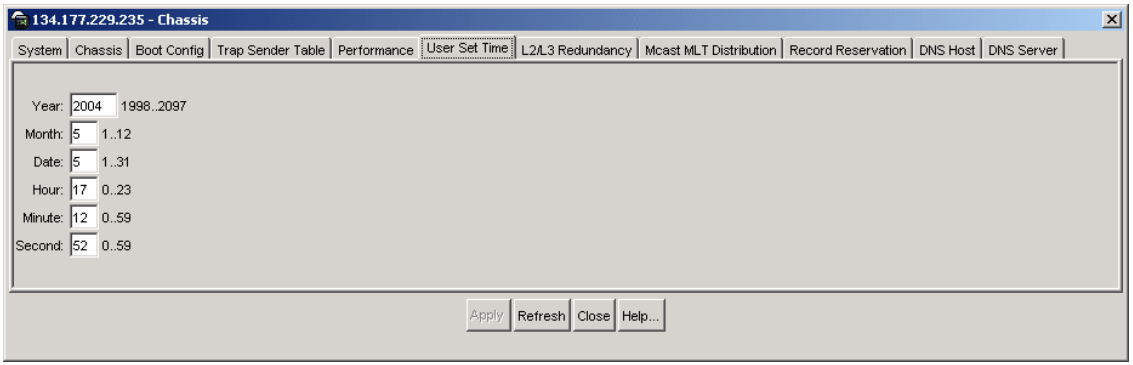


Table 50 describes the User Set Time tab fields.

Table 50 User Set Time tab fields

Field	Description
Year	The year (integer 1998...2097).
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).

Viewing the DNS host table

You can view the DNS host table as follows:

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

The chassis dialog box opens with the System tab displayed.

2 Click on the DNS Host tab.

The DNS Host tab opens (Figure 73).

Figure 73 Chassis dialog box—DNS Host tab

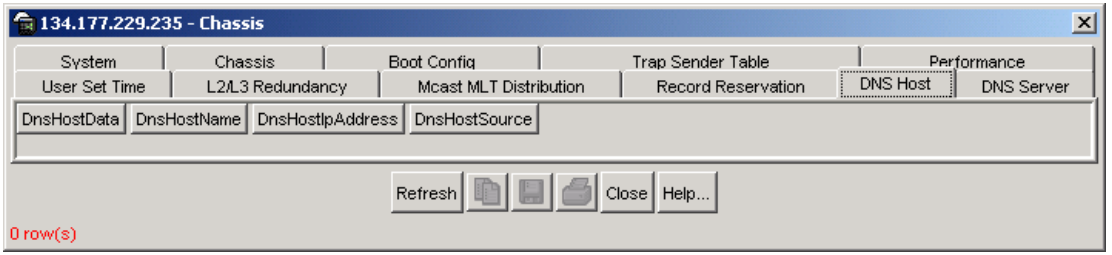


Table 51 describes the DNS Host tab fields.

Table 51 DNS Host tab fields

Field	Description
DnsHostData	Identifies the host name or host IP address. This is a read-only field.
DnsHostName	Identifies the host name. This is a read-only field.
DnsHostIpAddress	Identifies the host IP address. This is a read-only field.
DnsHostSource	Identifies the DNS server IP or host file. This is a read-only field.

Configuring the DNS server

You can configure the DNS server as follows:

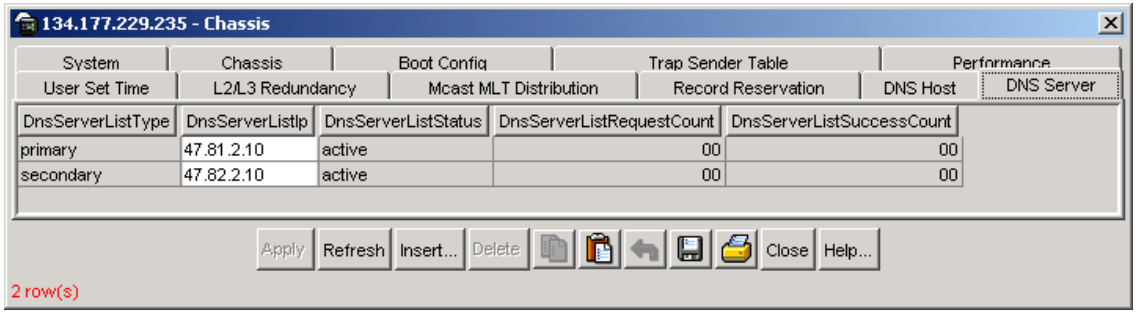
1 From the Device Manager menu bar, choose Edit > Chassis.

The chassis dialog box opens with the System tab displayed.

2 Click on the DNS Server tab.

The DNS Server tab opens (Figure 74).

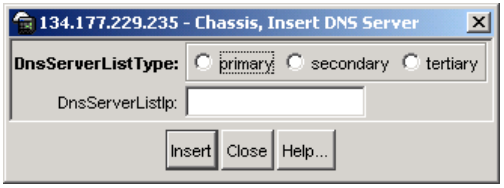
Figure 74 Chassis dialog box—DNS Server tab



3 Click on the DNS Server tab.

The DNS Server tab opens (Figure 75).

Figure 75 Insert DNS Server dialog box



4 Select a DNS server list type.

5 Enter a DNA server list IP address.

6 Click Insert.

7 Click Close.

Table 52 describes the Insert DNS Server dialog box fields.

Table 52 Insert DNS Server dialog box fields

Field	Description
ListType	Specifies whether the DNS server type is primary, secondary, or tertiary.
ListIp	Identifies the IP address of the DNS server.

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 76).

Figure 76 Card dialog box—Card tab

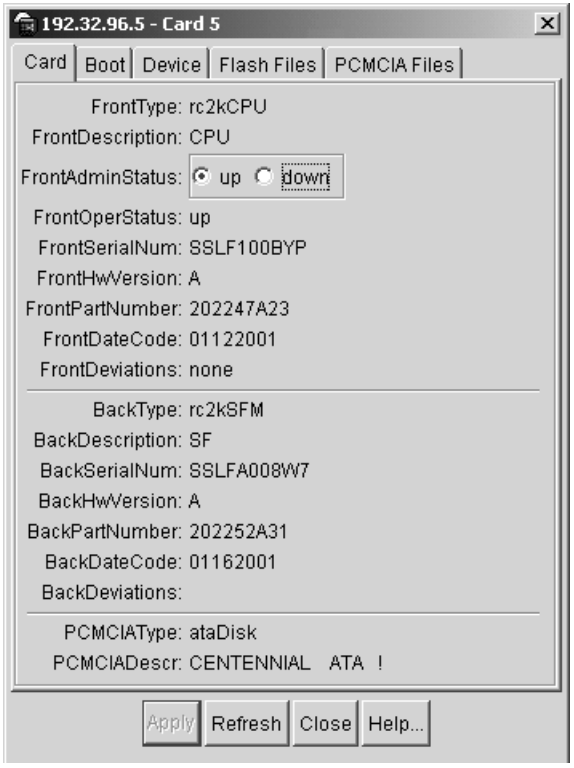


Table 53 describes the Card tab fields.

Table 53 Card tab fields

Field	Description
FrontType 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 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 BackSerialNum	Serial number of the I/O card.

Table 53 Card tab fields

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

Editing the 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 77).

Figure 77 Card dialog box—Boot tab

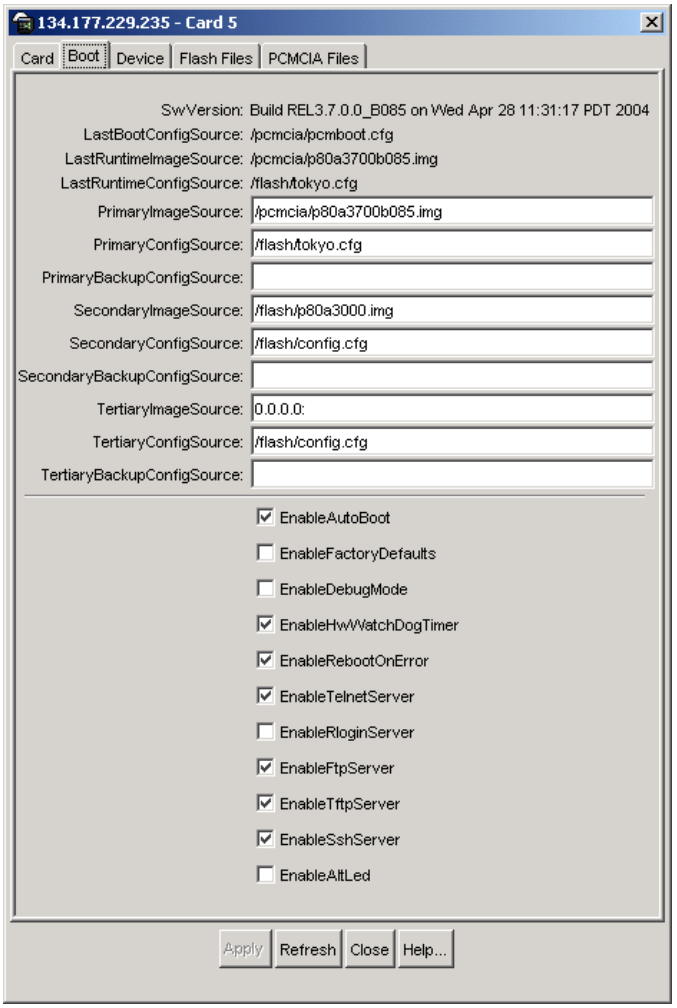


Table 54 describes the Boot tab fields.

Table 54 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.
PrimaryConfigSource	The primary configuration source file.
PrimaryBackupConfigSource	The primary backup configuration source (safeconfig).
SecondaryImageSource	The secondary image source file.
SecondaryConfigSource	The secondary configuration source file.
SecondaryBackupConfigSource	The secondary backup configuration source (safeconfig).
TertiaryImageSource	The tertiary image source file.
TertiaryConfigSource	The tertiary configuration source file.
TertiaryBackupConfigSource	The tertiary backup configuration source (safeconfig).
EnableAutoBoot	Enables the autoboot option. 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.

Table 54 Boot tab fields (continued)

Field	Description
EnableSshServer	Enables SSH server option.
EnableAltLed	Enables the alternate LED.

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 78).

Figure 78 Card dialog box—Device tab

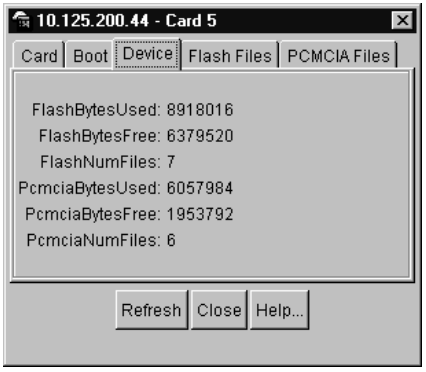


Table 55 describes the Device tab fields.

Table 55 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 79).

Figure 79 Card dialog box—Flash Files tab

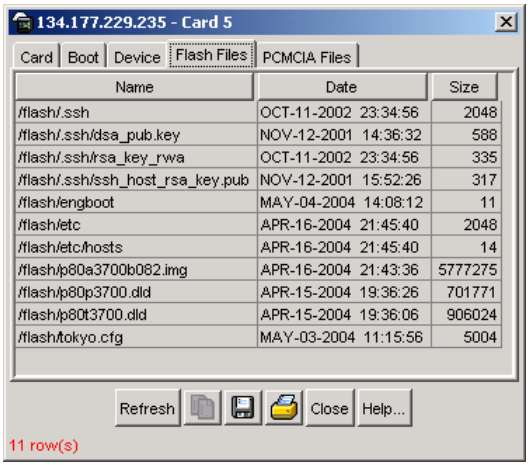


Table 56 describes the Flash Files tab fields.

Table 56 Flash Files tab fields

Field	Description
Name	Directory name of the flash file.
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 80).

Figure 80 Card dialog box—PCMCIA Files tab

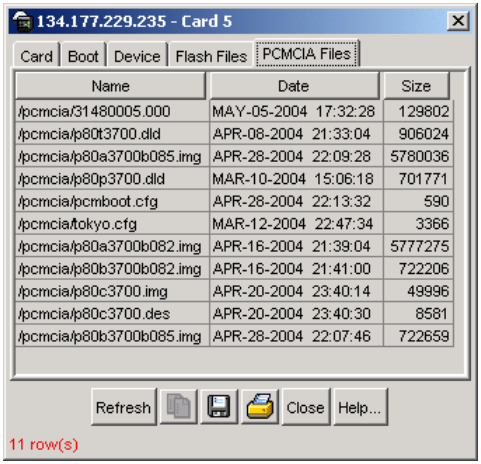


Table 57 describes the PCMCIA Files tab fields.

Table 57 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 the 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 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 81).

Figure 81 Mgmt Port dialog box

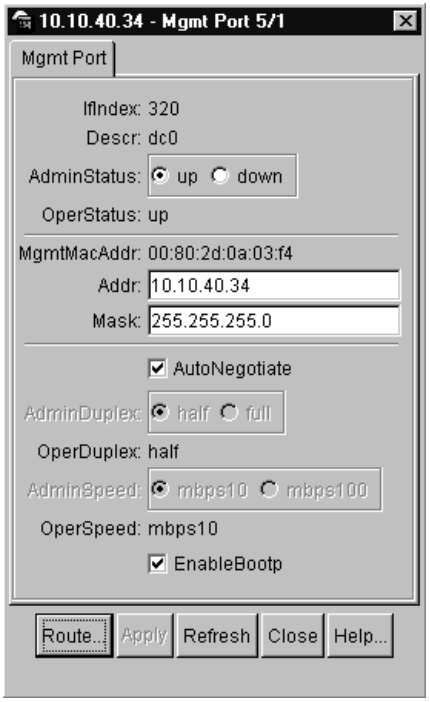


Table 58 describes the Mgmt Port dialog box fields.

Table 58 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 58 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:

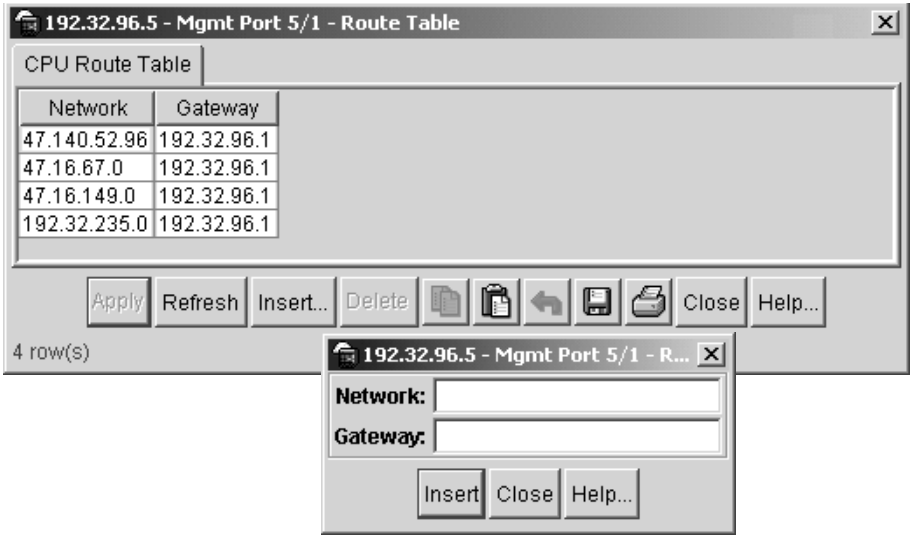
1. Select the management port object.
2. From the Device Manager menu bar, choose Edit > Mgmt Port.

   The Mgmt Port dialog box opens (Figure 81 on page 182).

3. On the Mgmt Port dialog box, click Route.

   The Mgmt Port Route Table dialog box opens (Figure 82).

Figure 82 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 82).

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

Table 59 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 83).

Figure 83 Serial Port dialog box

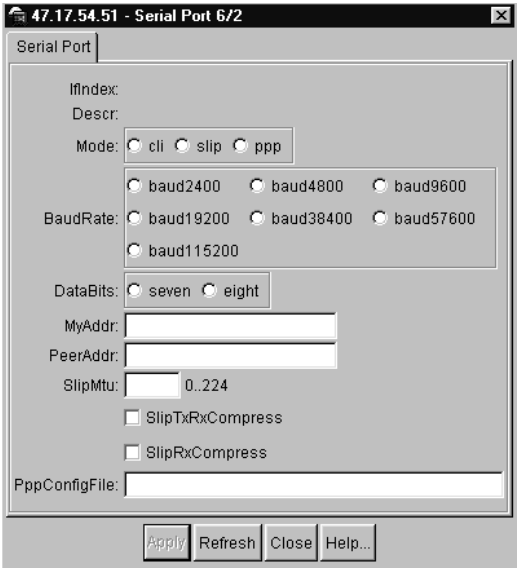


Table 60 describes the Serial Port dialog box fields.

Table 60 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.

Table 60 Serial Port dialog box fields (continued)

Field	Description
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 84).

Figure 84 Fan dialog box

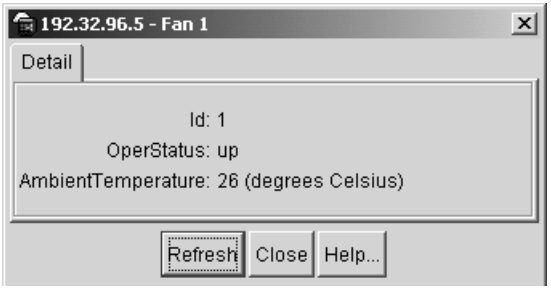


Table 61 describes the Fan dialog box fields.

Table 61 Fan dialog box fields

Field	Description
Id	The fan ID.
OperStatus	Actual status of the Fan: • unknown(1) - status cannot be determined. • up(2) - present and supplying power. • 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 85).

Figure 85 MDA dialog box

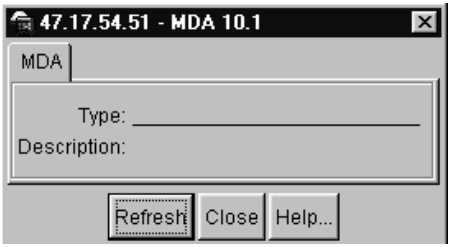


Table 62 describes the MDA fields.

Table 62 MDA dialog box fields

Field	Description
Type	This field displays the media type of the MDA, either: • OC-3 SMF MDA • OC-3 MMF MDA • OC-12 SMF MDA • OC-12 MMF MDA—rc2klx0c12cBaseMM
Description	This field displays a description of the MDA, either: • OC-3 SMFMDA—Quad OC-3 SM • OC-3 MMFMDA—Quad OC-3 MM • OC-12 SMF MDA—Single Port OC-12 SM • 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 86).

Figure 86 PowerSupply dialog box

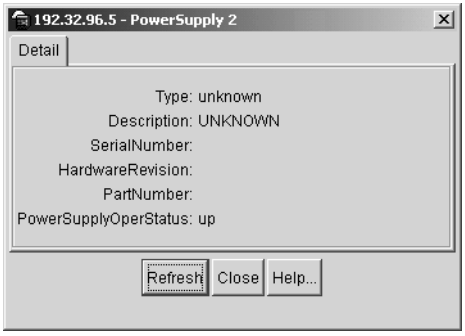


Table 63 describes the PowerSupply Detail tab fields.

Table 63 PowerSupply Detail tab fields

Field	Description
Type	Describes the type of power used— AC or DC.
Description	Provides a description of the power supply.
SerialNumber	Defines the serial number of the power supply.
HardwareRevision	Displays the hardware revision number.
PartNumber	Displays the part number of the power supply.
PowerSupplyOperStatus	Displays the status of the power supply, on (up) or off (down).

Editing the 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.

Copying a PCMCIA or flash file

To copy files between the flash and the PCMCIA:

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

  The FileSystem dialog box opens with the Copy File tab active (Figure 87).

Figure 87 FileSystem dialog box—Copy File tab

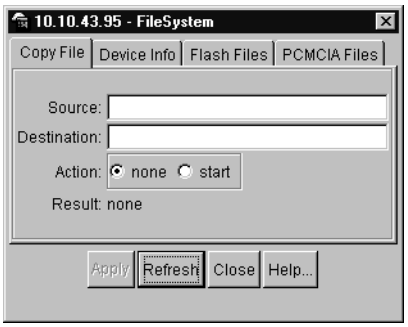


Table 64 describes the Copy File tab fields.

Table 64 Copy File tab fields

Field	Description
Source	The source file to copy from the flash/PCMCIA or the config file on the NVRAM or trace file.
Destination	The device and the file name (optional) to which the source file is to be copied. The destination can be flash, PCMCIA or the NVRAM. Trace files are not a valid destination.
Action	Select **start** to begin the copy process or **none** to cancel the copy process.
Result	Displays the result of the copy process: • none • inProgress • success • fail • invalidSource • invalidDestination • outOfMemory • outOfSpace • fileNotFound

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 88).

Figure 88 FileSystem dialog box—Device Info tab

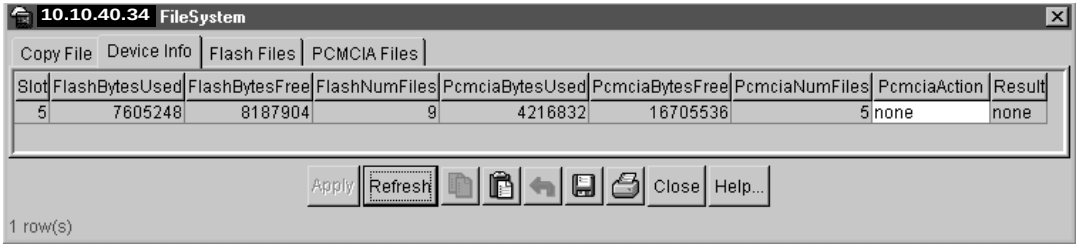


Table 65 describes the Device Info tab fields.

Table 65 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 89).

Figure 89 FileSystem dialog box—Flash Files tab

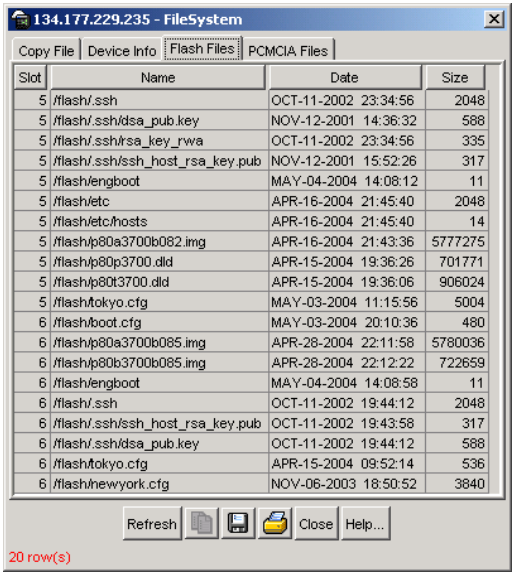


Table 66 describes the Flash Files tab fields.

Table 66 Flash Files tab fields

Field	Description
Slot	The slot number of the CPU module.
Name	The name of the Flash file.

Table 66 Flash Files tab fields

Field	Description
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 90).

Figure 90 FileSystem dialog box—PCMCIA Files tab

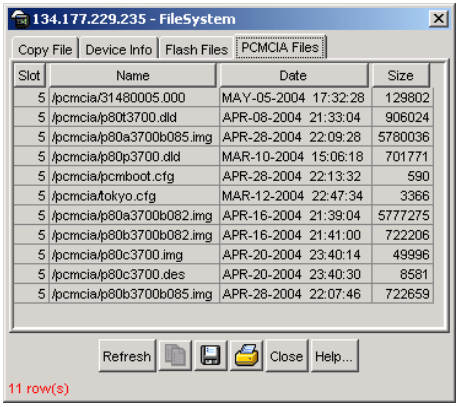


Table 67 describes the Flash Files tab fields.

Table 67 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 *Using the 8672ATME/ATMM Modules*.

Graphing chassis statistics

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

- "Graphing system statistics," next
- "Graphing SNMP statistics" on page 198
- "Graphing IP statistics" on page 201
- "Graphing ICMP In statistics" on page 204
- "Graphing ICMP Out statistics" on page 205
- "Graphing OSPF statistics" on page 207

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: The Clear Counter function in Device Manager does not affect the AbsoluteValue counter in the switch. Instead, the Clear Counter function clears all cached data in Device Manager (except AbsoluteValue). To reset AbsoluteValue(s), use the Reset Counter function (Edit > Chassis > System).

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 system statistics

You can graph system statistics by using the Graph > Chassis > System menu. Note that the System tab displays the same data as the Edit > Chassis > Performance menu, with the exception of the DramSize field. For further information, see “Checking system performance” on page 167.

To graph system statistics:

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

The Graph Chassis dialog box opens with the System tab displayed (Figure 91).

Figure 91 Graph Chassis dialog box—System tab

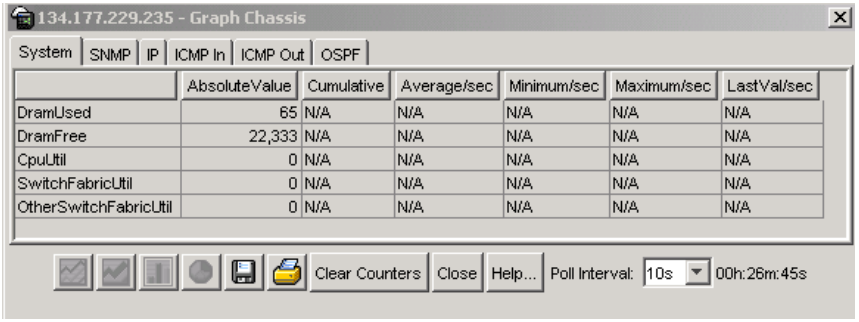


Table 68 describes the System tab fields.

Table 68 System tab fields

Field	Description
DramUsed	The percentage of DRAM space used. **Note:** Only the AbsoluteValue column is valid in the System tab. All other columns display as N/A since they are percentages and not actual memory counters.
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.

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 System tab displayed (Figure 91 on page 198).

2 Click SNMP.

The SNMP tab opens (Figure 92)

Figure 92 Graph Chassis dialog box—SNMP tab

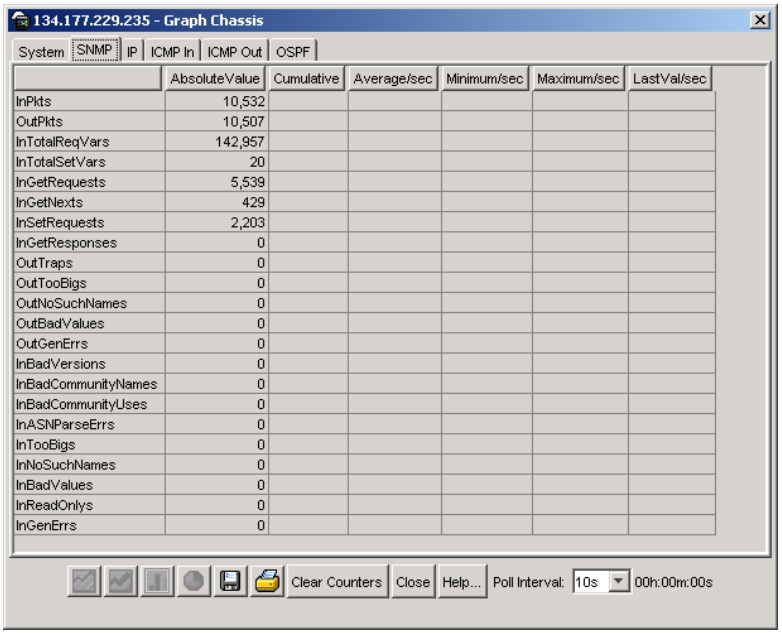


Table 69 describes the SNMP tab fields.

Table 69 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 69 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 System tab displayed (Figure 91 on page 198).

2. Click the IP tab.

The IP tab opens (Figure 93).

Figure 93 GraphChassis dialog box—IP tab

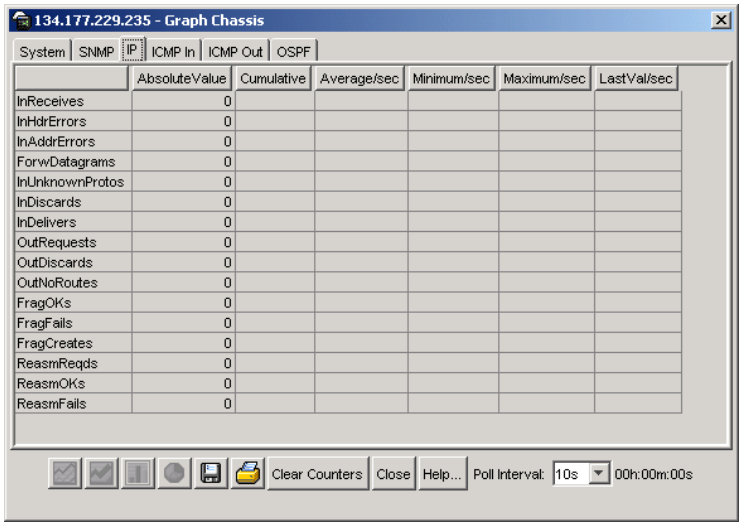


Table 70 describes the IP tab fields.

Table 70 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 70 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 70 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 Graph Chassis dialog box opens with the System tab displayed (Figure 91 on page 198).

2 Click the ICMP In tab.

The ICMP In tab opens (Figure 94).

Figure 94 GraphChassis dialog box—ICMP In tab

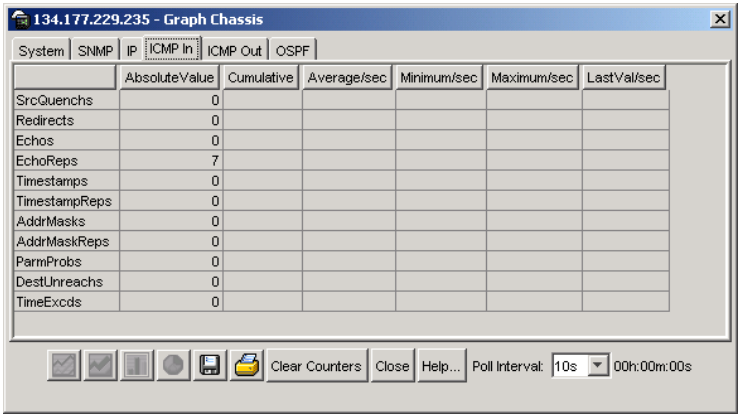


Table 71 describes the ICMP In tab fields.

Table 71 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 Graph Chassis dialog box opens with the System tab displayed Figure 91 on page 198.

2. Click the ICMP Out tab.

   The ICMP Out tab opens (Figure 95).

Figure 95 GraphChassis—ICMP Out tab

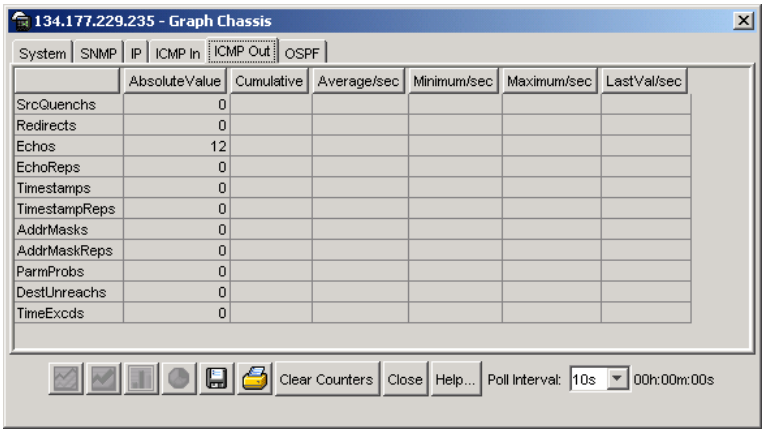


Table 72 describes the ICMP Out tab fields.

Table 72 ICMP Out tab fields

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

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 Graph Chassis dialog box opens with the System tab displayed (Figure 91 on page 198).

2 Click the OSPF tab.

The OSPF tab opens (Figure 96).

Figure 96 GraphChassis dialog box—OSPF tab

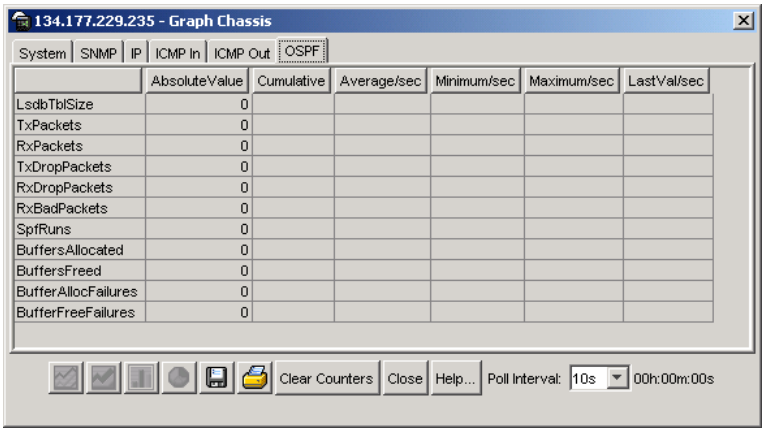


Table 73 describes the OSPF tab fields.

Table 73 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.

Table 73 OSPF tab fields (continued)

Field	Description
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.

Appendix A
RMON alarm variables

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

Table 74 lists the alarm variable categories and provides a brief variable description.

Table 74 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 74 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 74 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. 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 74 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. 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 74 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 74 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. 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 74 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 74 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). **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 74 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 74 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 74 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 74 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 74 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 74 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 74 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