Part No. 210245-C
April 2001

4401 Great America Parkway
Santa Clara, CA 95054

Reference for the BayStack 350/410/450 Management Software Operations Version 5.0

NORTEL NETWORKS™

Copyright © 2001 Nortel Networks

Trademarks

Restricted rights legend

Statement of conditions

Nortel Networks NA Inc. software license agreement

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

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

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

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

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

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

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

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

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

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

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

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Figures

Tables

Preface

Welcome to the Nortel Networks™ Device Manager software, a set of graphical network management applications you can use to configure and manage the BayStack™ 350/410/450 switches.

This guide provides information about using the features and capabilities of the Device Manager graphical user interface (GUI) to perform network management operations for the BayStack switches.

Before you begin

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

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

Text conventions

This guide uses the following text conventions:

`screen text`	indicates text you enter and system output, for example, prompts and system messages. Example: `Rmon is currently disabled. Do you want to enable it now?`
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.

Related publications

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

- *Using the BayStack 350 Series 10/100 Autosense Switch* (part number: 309979-D)
- *Using the BayStack 410-24T 10BASE-T Switch* (part number: 309985-D)
- *Using the BayStack 450 10/100/1000 Series Switch* (part number: 309978-D)

These documents provide information about BayStack family of switches including installation instructions and configuration settings.

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

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

How to get help

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

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

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

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

Chapter 1
Device Manager basics

The Device Manager application manages network devices using the simple network management protocol (SNMP). Device Manager is a graphical user interface (GUI) between your BayStack switch and the other devices that make up your network. Device Manager allows you to remotely manage a single device and makes retrieval of configuration information for a device a point-and-click operation.

Device Manager displays a real-time physical view of the front panel of a device. From the front panel view, you can view fault, configuration, and performance information for the device, a module, or a single port.

This chapter describes the basic features of the Device Manager when used with BayStack switches.

Note: In this document, BayStack 350, BayStack 410, and BayStack 450 switches are collectively known as the "BayStack switch." For installation information about a specific BayStack switch, refer to the respective switch user's manual.

Note: Device Manager 5.0 supports BayStack 350, BayStack 410, and BayStack 450 switch software version 3.1.

Starting Device Manager

To start Device Manager:

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

- In a Microsoft® Windows® environment, from the Windows Start menu, choose Programs > Nortel Frame Switch Management Software > Device Manager.
- In a UNIX environment, verify that the Device Manager installation directory */usr/lnms/dm* is in your search path; then type:

  ```
  dm>
  ```

The initial Device Manager window opens (Figure 1).

Figure 1 Initial Device Manager window

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

Setting the Device Manager properties

Device Manager communicates with a Device Manager switch using SNMP. The Device Manager Properties dialog box allows you to configure important communication parameters such as the polling interval, time out, and retry count. You can set these parameters before you open a device to manage. You can also access the Properties dialog box at any other time while Device Manager is running.

To open the Properties dialog box:

➔ From the initial Device Manager window, choose Device > Properties.

The Properties dialog box (Figure 2) opens.

Figure 2 Properties dialog box

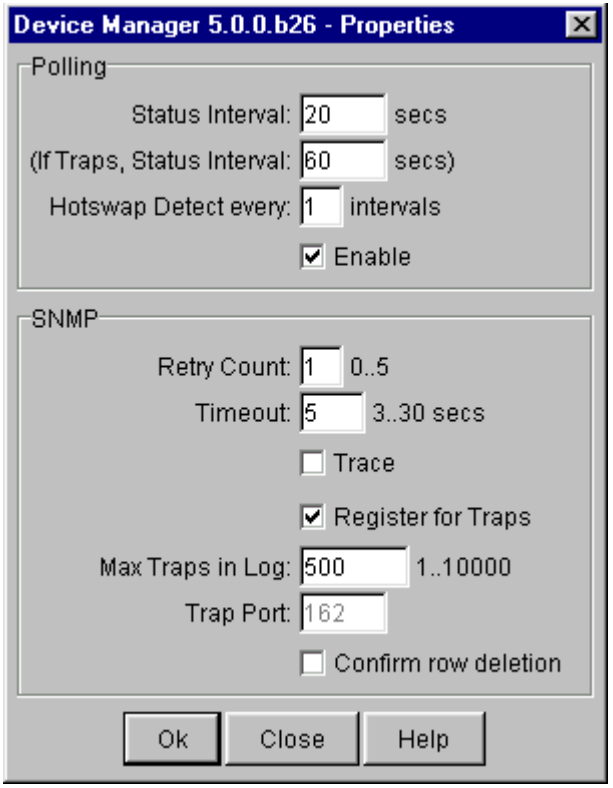


Table 1 describes the Properties dialog box items.

Table 1 Properties dialog box items

Area	Item	Description
Polling	Status Interval	Intervals at which status information is gathered (default is 20 seconds). For a full stack, set this to 60 seconds.
	(If IP traps, Status Interval secs)	Intervals at which status information is gathered (default is 60 seconds) if a trap is detected.
	Hotswap Detect every	Intervals at which Device Manager polls for module information. The default is 60 seconds.
	Enable	Enables or disables periodic polling of the device for updated status. If this is disabled (not checked), the chassis status is updated only when you click the Refresh button.
SNMP	Retry Count	Number of times Device Manager sends the same polling request if a response is not returned to Device Manager.
	Timeout	Length of each retry of each polling waiting period. When you access the device through a slow link, you may want to increase the time out interval and then decrease the Retry count value.
	Trace	Enables or disables SNMP tracing. When selected (checked), SNMP PDU trace messages are displayed in the Device > Log dialog box.
	Register for Traps	Configures whether Device Manager should automatically register to receive traps when Device Manager is launched against a switch.
	Max Traps in Log	Number of traps that may exist in the trap log. Default is 500.
	Trap Port	Configures the UDP port that the Device Manager listens on to receive SNMP traps.
	Confirm row deletion	If this is checked, Device Manager displays a confirmation dialog box before deleting a row.

Opening a device

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

To display the device view:

➔ Do one of the following:

- Choose Device > Open.
- Click the folder icon in the Device Manager.
- Press [Ctrl]+O.

The Open Device dialog box opens (Figure 3).

Figure 3 Open Device dialog box

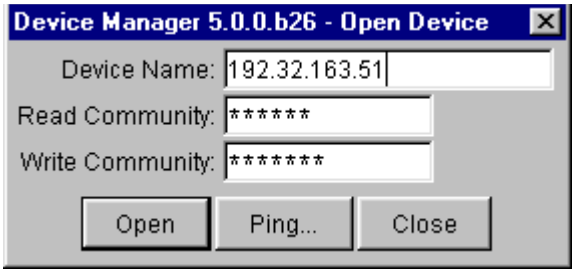


Table 2 describes the Open Device dialog box items.

Table 2 Open Device dialog box items

Item	Description
Device Name	Enter either an IP address or a DNS name for the device.
Read Community	SNMP read community string for the device. Default is `public` (displayed as ******). The entry is case-sensitive.
Write Community	SNMP write community string for the device. Default is `private` (displayed as *******).The entry is case-sensitive.

To open and identify a device:

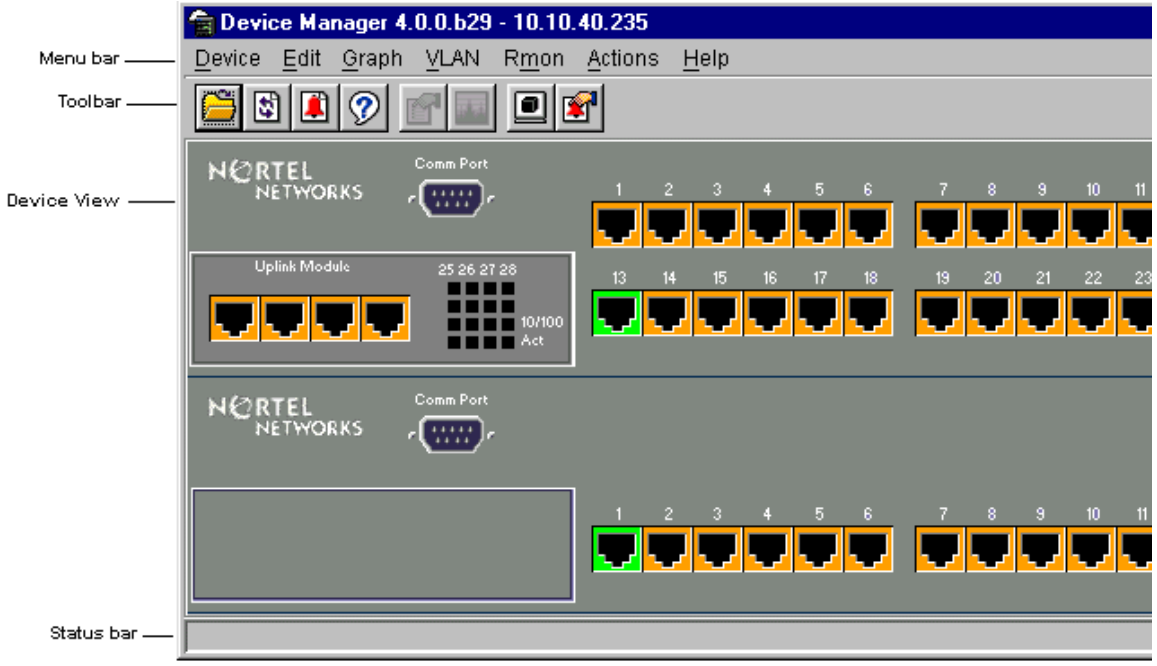
1. Type the DNS name or IP address of the device in the Device Name field.
2. Type the proper community strings in the Read Community and Write Community fields.
3. Click Open.

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

Device Manager window

The Device Manager Window has four parts as shown in Figure 4.

Figure 4 Device Manager main window



Note: If you need information about integrating Device Manager with HP OpenView (compiling MIBs), refer to "HP OpenView" on page 159.

Menu bar

The menu bar contains commands for operating Device Manager.

The commands are described in Table 3.

Table 3 Menu bar commands

Command	Description
Device	Opens a device, where you can view and edit parameters for managing the chassis and system.
Edit	Displays and allows you to edit parameters for the selected MDA, I/O module, and selected port, as well as set FileSystem, Bridge, Security and Diagnostic parameters.
Graph	Displays Device Manager statistics in graph mode.
VLAN	Displays and configures VLANs, Snooping, MLTs, and STGs parameters.
Rmon	Configures alarms and view events monitoring network devices, as well as control the means and mode of event notification.
Actions	Opens a Telnet session.
Help	Views online Help topics for Device Manager.

Toolbar

Below the menu bar is a toolbar. The toolbar provides quick access to commonly used Device Manager commands as described in Table 4.

Table 4 Toolbar buttons

Toolbar button	Command	Description
	Open Device	Opens a device. You can also use Device > Open.
	Refresh Display	Refreshes the graphical representation of the switch.
	Trap Log	Opens the trap log.
	Help	Opens Help.[1] You can also use Help.
	Edit Component	Makes changes to a port, MDA, or chassis. You can also use Edit > port.
	Graph Component	Graphs statistics. You can also use: Graph > Port Graph > Chassis
	Telnet	Opens a Telnet session.
	Alarm Manager	Sets Rmon alarms. You can also use Rmon > Alarm Manager.

1 If online Help does not open, refer to "Online Help" on page 48.

Device view

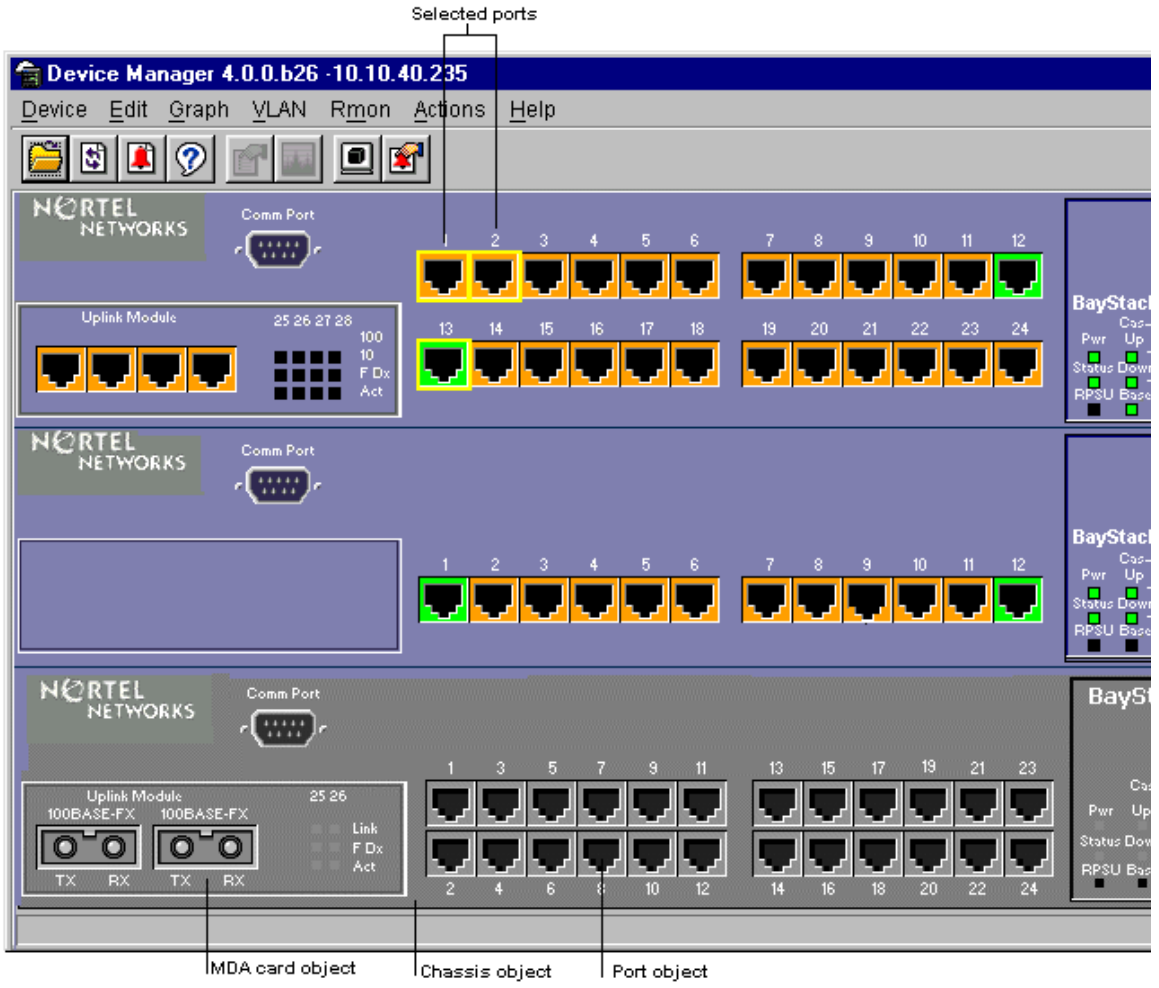
The device view, a graphical representation of the switch, is displayed below the toolbar. From this graphic, you can determine the operating status of the ports and MDAs in your configuration. You also use the device view to perform management tasks on specific objects.

The types of objects contained in the device view are:

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

Figure 5 illustrates a stack of BayStack switches.

Figure 5 Device view



Although the BayStack 450 switch is physically installed as the base switch in this stack, Device Manager displays the switch in the top position.

Selecting a switch

To select a single switch or unit, click on the edge of the device and the edge of the switch is outlined in yellow.

Selecting the chassis

A chassis is a stack of switches. To select a chassis, click on the edge of the graphical representation of the chassis. The edge of the chassis is outlined in yellow in the device view. To select the chassis in a stack, choose Edit > Chassis.

Selecting the MDA

The MDA is an independent module located at the bottom left of a switch. You can select the media dependent adapter (MDA) by clicking inside the graphical representation of the MDA. The edge of the MDA is outlined in the device view.

Selecting ports

To select a port, click on the graphical representation of the port. The edge of the port is outlined in yellow on the graphical representation of the switch.

To select multiple ports:

➔ Do one of the following:

- For a block of multiple ports, drag and select the port group.
- For multiple ports anywhere on the chassis, click on a port, then [Ctrl]+click on successive ports anywhere on the chassis.

Selected ports are outlined in yellow.

Conventions of the switch graphic

The conventions of the graphical representation of the switch are different from the actual switch. This section explains these conventions and how information is visually displayed in different colors on the MDA and/or port.

Table 5 describes the colors in the graphic of the ports in the MDA and in the chassis.

Table 5 MDA and port colors

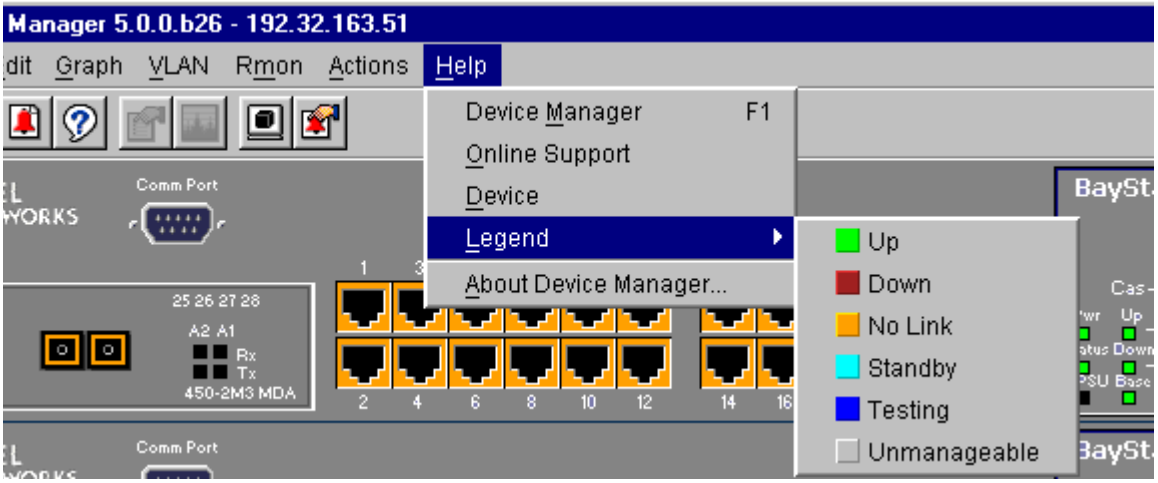
Color	Description
Green (Up)	Module/port is operating.
Red (Down)	Module/port is present, but is not operating.
Orange (No Link)	Port has no link.
Light blue (StandBy)	Port is on standby.
Dark blue (Testing)	Port is being tested.
Gray (Unmanageable)	Port has been disabled manually or unmanageable.

Refer to the Legend in the Help menu for a quick reference of these conventions.

To view the Legend in Help:

➔ From the Device Manager main menu, choose Help > Legend (Figure 6).

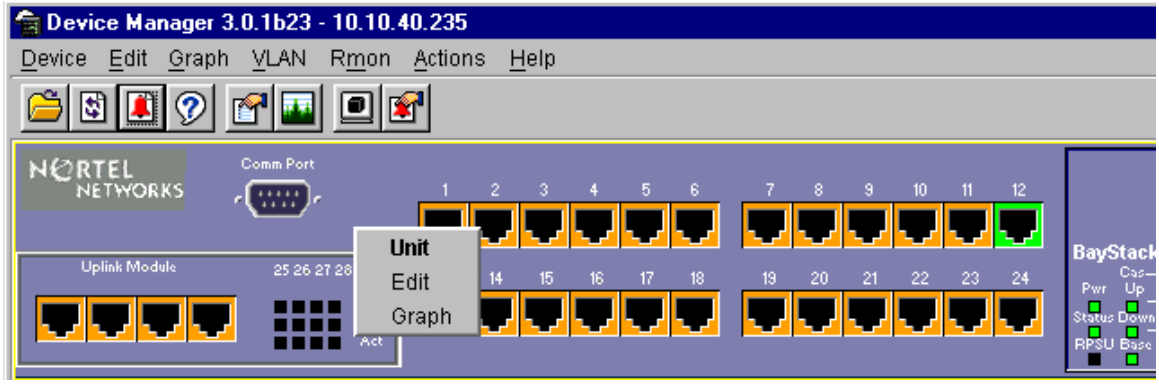
Figure 6 Legend



Shortcut menus

Each object (unit, port, and MDA) has a shortcut menu that opens when you right-click a selected object or group of objects. These shortcut menus are shown respectively in Figure 7, Figure 8, and Figure 9 on page 37. The shortcut menus provide a faster path for editing objects and applying changes; however, you can access the same options using the menu bar or the toolbar.

Figure 7 Unit shortcut menu



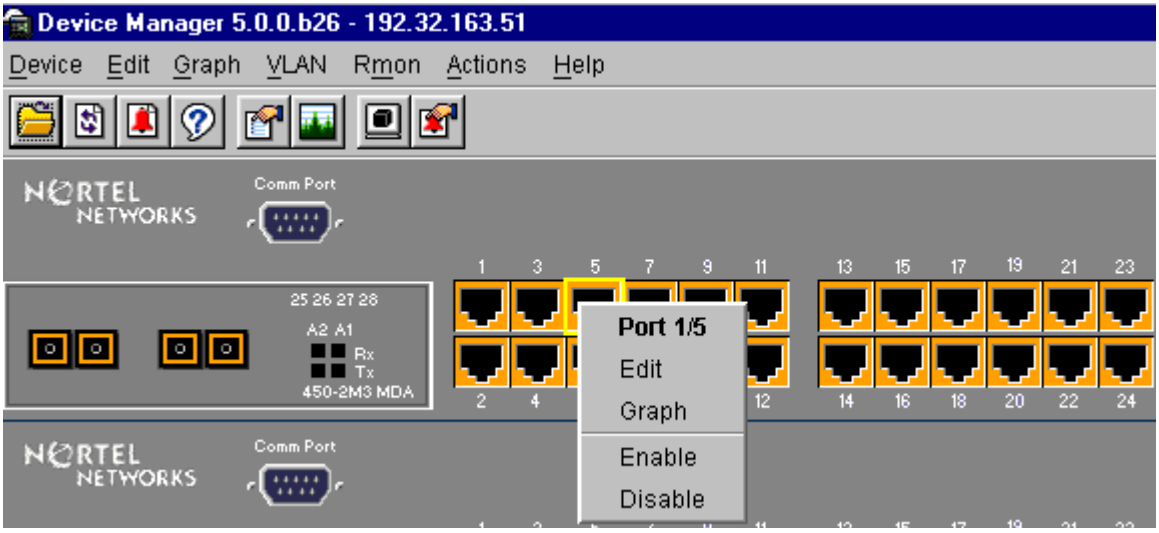
The unit shortcut menu commands are described in Table 6.

Table 6 Unit shortcut menu commands

Command	Description
Unit	Indicates that you have selected the chassis.
Edit	Edits chassis parameters.
Graph	Graphs chassis statistics (base switch only).

The port shortcut menu is shown in Figure 8.

Figure 8 Port shortcut menu



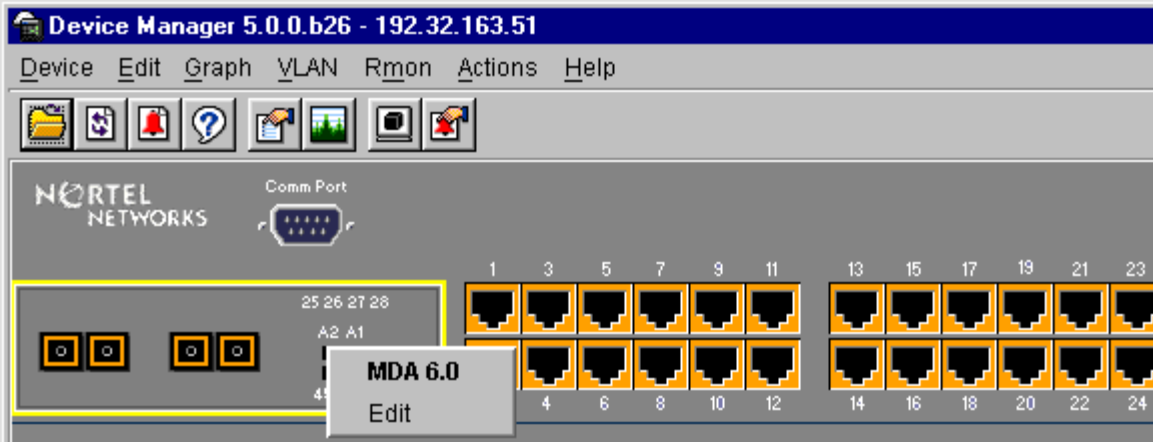
The port shortcut menu commands are described in Table 7.

Table 7 Port shortcut menu commands

Command	Description
Port	Indicates that you have selected a specific port.
Edit	Edits port parameters.
Graph	Graphs port statistics.
Enable	Administratively brings a port up.
Disable	Administratively shuts down a port.

The MDA shortcut menu (Figure 9) provides a way to quickly view the MDA parameters.

Figure 9 MDA shortcut menu



The MDA shortcut menu commands are described in Table 8.

Table 8 MDA shortcut menu commands

Command	Description
MDA x.x	Indicates that you have selected an MDA.
Edit	Edits MDA parameters.

Command buttons

Table 9 describes command buttons that may appear in various Device Manager windows, tabs and dialog boxes.

Table 9 Device Manager command buttons

Button	Description
Apply	Applies the changes entered in the field in a window, tab or dialog box. Changes are displayed as bold (UNIX) or underlined (PC) text or numbers.
Insert	Inserts or creates a new group, such as a Spanning Tree group.
Delete	Deletes a setting for a port, MDA, or IP address from a parameter.

Table 9 Device Manager command buttons (continued)

Button	Description
Refresh	Refreshes the information. Every time you click Refresh, new information is polled from the switch and displayed.
Close	Closes the tab or dialog box and disregards changes made to the field.
Help	Displays context-sensitive Help. Typically, when this button is clicked, a shortcut menu opens with the Stop, Export, and Replicate commands.
Export	Exports information to a file specified by the user. This file can then be imported into a text editor or spreadsheet for further analysis.

Accessing dialog boxes and objects

This section describes some general conventions that apply to accessing dialog boxes and objects in the Device Manager.

Basic conventions

Some basic conventions govern how you use the Device Manager. Table 10 contains information about those conventions.

Table 10 Basic conventions

Usage for	Description
Columns	Columns are resized automatically to fit the information contained in them. To resize the columns manually, click and hold the resize tabs between columns and move the column divider left or right.
Editable fields	Editable fields are displayed in “white.”
Read-only fields	Read-only fields are displayed in “gray.”
Ports	Select a port in one of two ways: • When you create an alarm in Rmon, click the down arrow to display a list of ports. • Enter the port location as an expression. For example, 1/2 is equivalent to port 2 on Unit 1).
Values	Values for IP addresses, MAC addresses, and time includes: • Enter an IP address in decimal format: <xxx>.<xxx>.<xxx>.<xxx> • Enter a MAC address in hexadecimal format: xx-xx-xx • Time is based on the delta from the computer system clock.

Editing objects

Depending on the object selected, you can edit objects and values in the Device Manager in several ways. To edit an object, do one of the following:

- Choose an object on the graphical representation, and then click the Edit component on the toolbar button. The Edit window opens for that object.
- In a dialog box, click Edit button.
- From a chassis, MDA, or port shortcut menu, choose Edit. The Edit dialog box opens for that object.

When you change values in a field, you can see fields that have been changed but not applied. Changed fields have the following characteristics:

- In a Windows environment, the value is underlined.
- In a UNIX environment, the value is displayed in **bold.**

Note: To make permanent changes in the configuration, click Apply. Changes are not applied to Device Manager until you click Apply.

Note: After you apply changes to fields, many windows contain a Refresh button. Click Refresh to display new information in the window.

Graphing

To make performance monitoring fast and easy, Device Manager tracks and graphs a wide range of statistics for the Device Manager objects. Statistics are maintained for the chassis and each port. For information about the statistics tracked for the chassis and ports, refer to "Graphing chassis statistics" on page 69 and "Single object statistics" on page 40.

The remainder of this section describes the general procedure for graphing objects, the graph screens, and the types of graphs available.

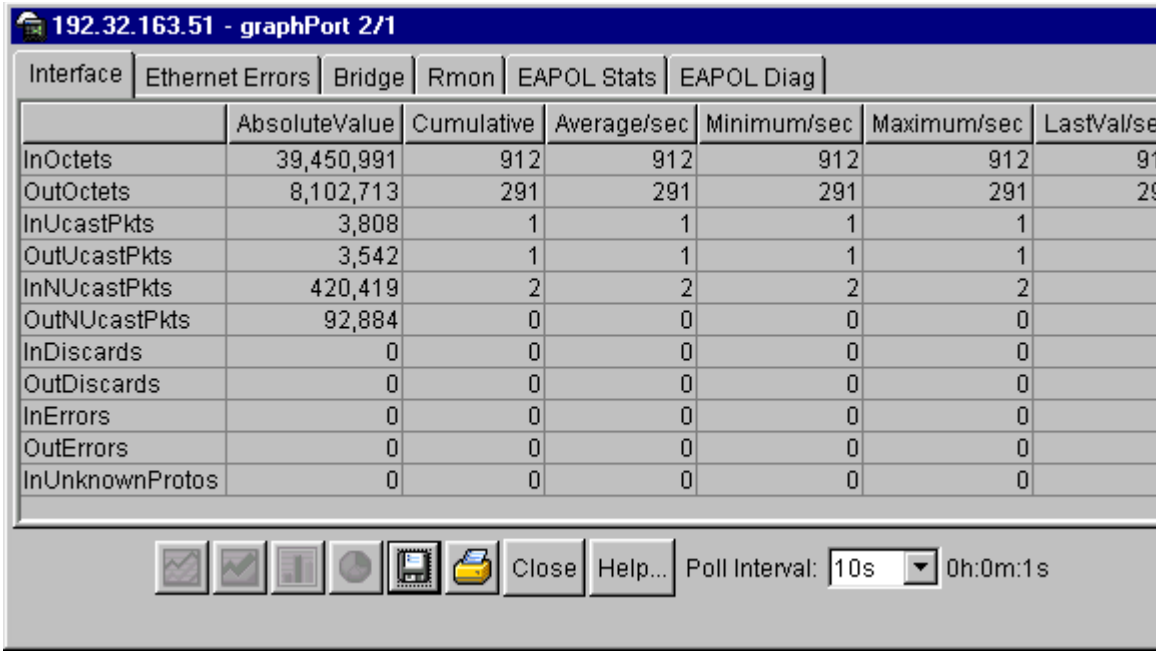
You can graph a port in the Device Manager window. To open the Graph dialog box:

1. Select the port you want to graph.
2. Do one of the following:
   - From the main menu, choose Graph > Port.
   - From the shortcut menu, choose Graph.
   - On the toolbar, click Graph.

Single object statistics

When you graph a single object, the statistics for a single port are displayed (Figure 10).

Figure 10 Single port statistics tabs



Statistics are organized into groups. Select from the tabs in the Graph Port window for the group of statistics you want to view.

The statistics are updated based on the poll interval that you can set at the bottom of the window. Click the down arrow at the side of the Poll Interval field to select a different polling interval.

As many as six statistics can be associated with a given counter. A counter is the type of information collected.

Table 11 describes the types of statistics collected for a given counter.

Table 11 Types of statistics

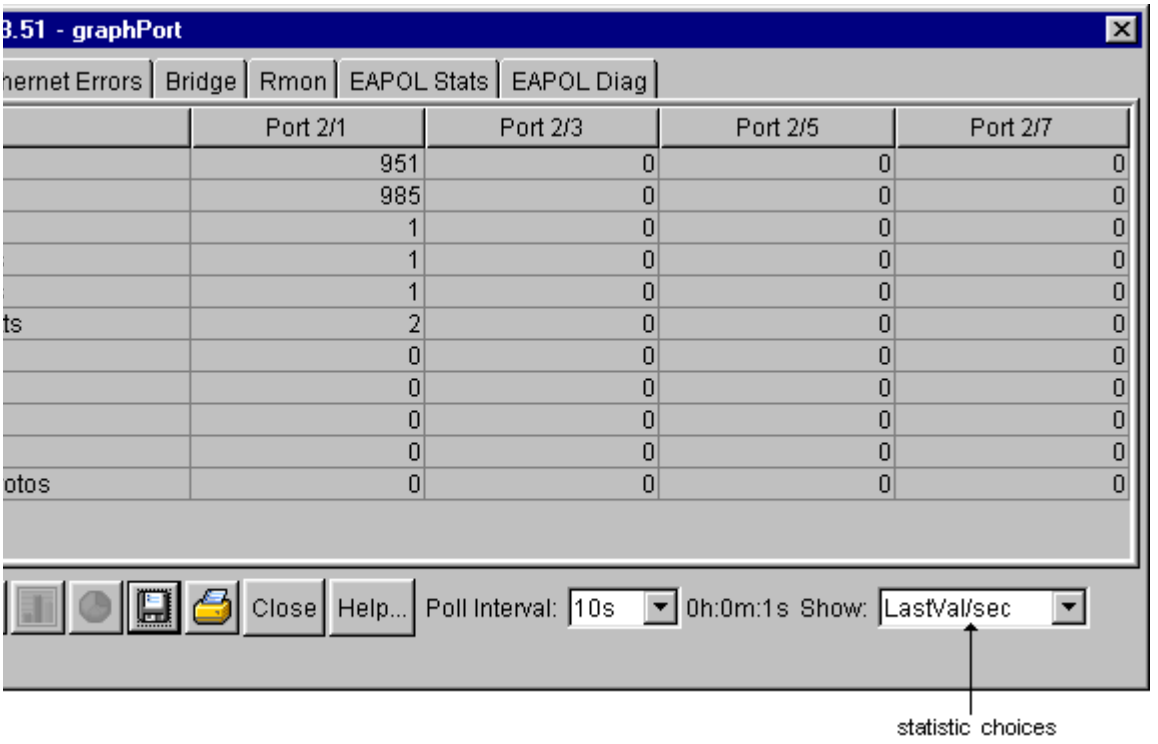
Statistic	Description
AbsoluteValue	Total count since the last time counters were reset. A system reboot resets all counters.
Cumulative	Total count since the statistics tab was first opened. The elapsed time for the cumulative counter is displayed at the bottom of the graph window.
Average	Cumulative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

You can export the on-screen statistics to a tab-separated file format and import the file into other applications.

Multiple object statistics

When you graph multiple objects, statistics for several ports are displayed (Figure 11).

Figure 11 Multiple-port statistics tabs



Not all statistics available for a single object are available when you graph multiple objects. The layout is similar to a single object graph except that the statistics choices are at the bottom of the screen.

The buttons for bar, pie, and line graphs are located at the bottom of the graphic. The Save button is located next to the graph buttons.

Creating a graph

Device Manager can graph a single cell or multiple cells, in a row or column on a tab. To create a graph:

1. Select the cells that you want to graph.
2. Click the button at the bottom of the window for the type of graph you want.

Device Manager supports line graphs, area charts, bar charts, and pie charts; respectively. Figure 12, Figure 13 on page 44, and Figure 14 on page 45, and Figure 15 on page 46 illustrate the different graph styles.

Figure 12 Line graph

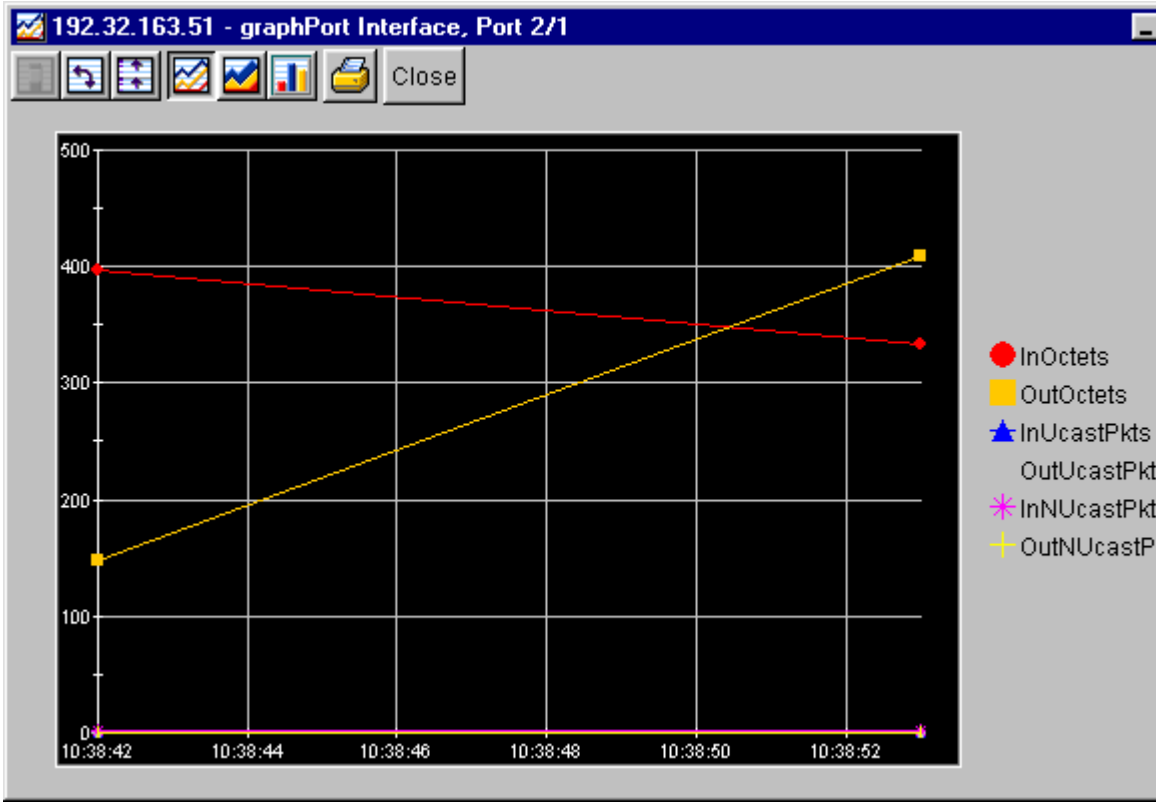


Figure 13 Area chart

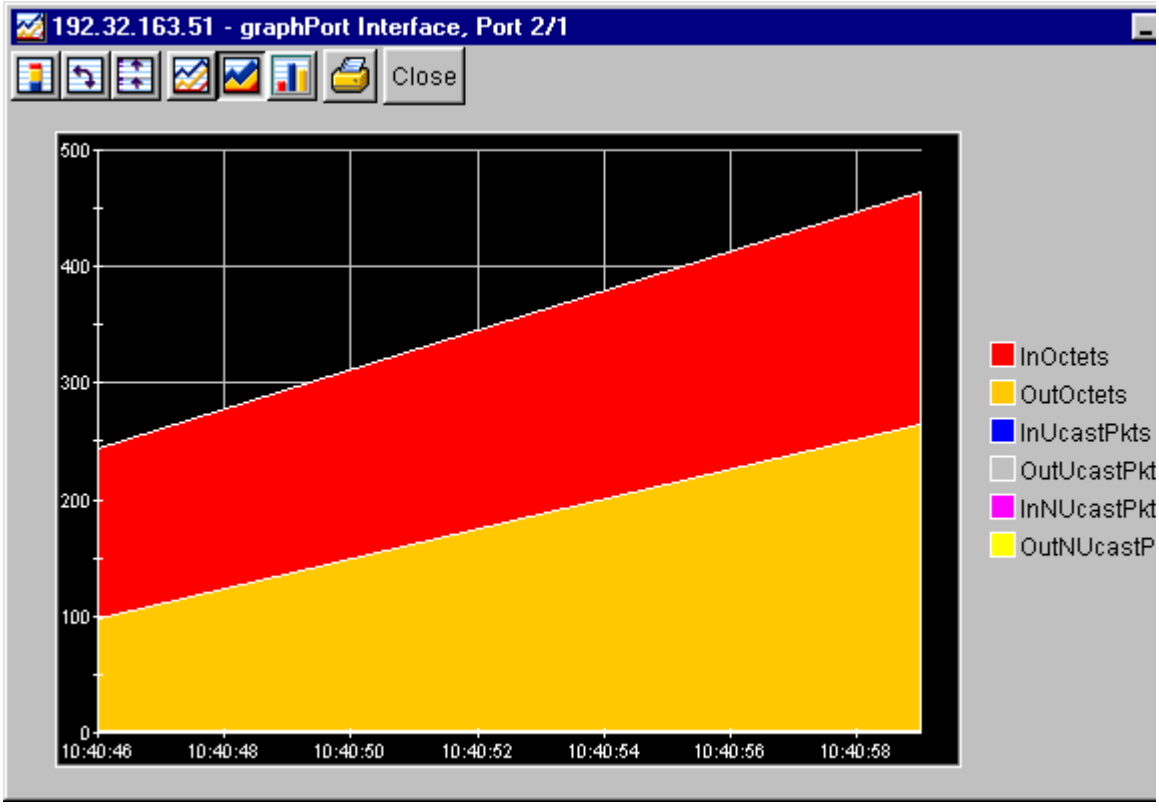


Figure 14 Bar graph

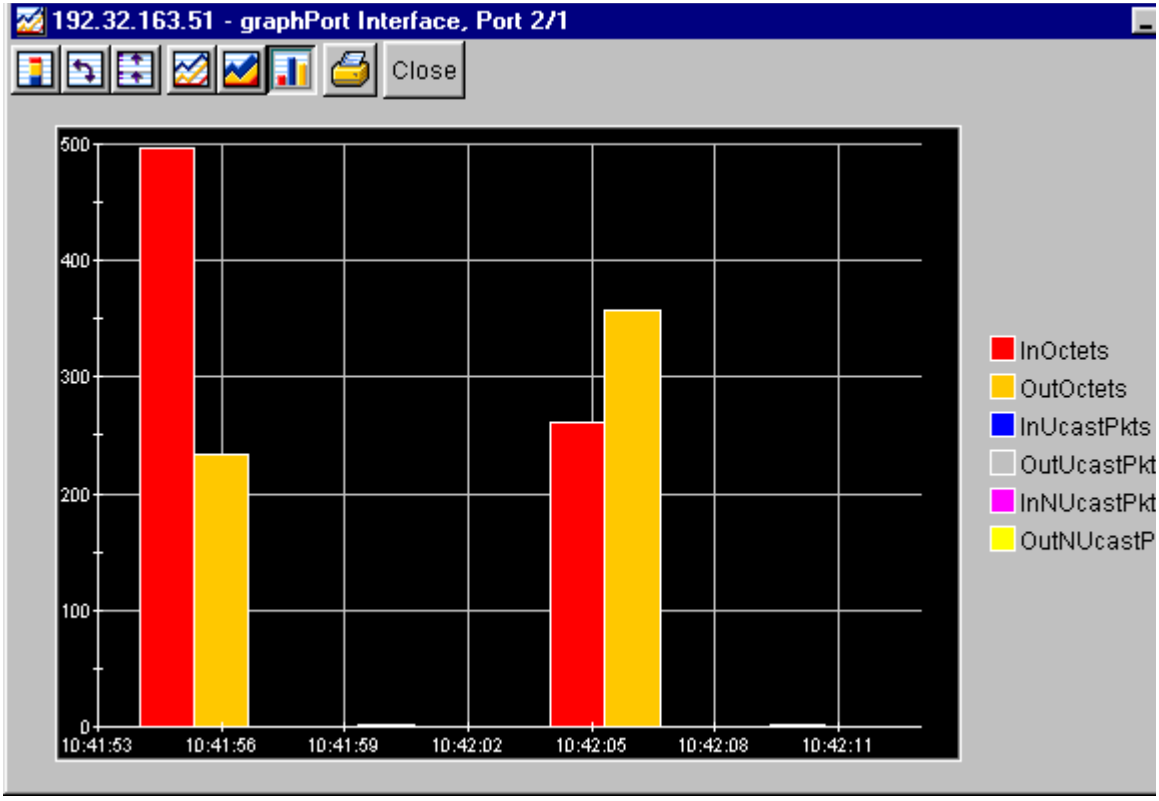
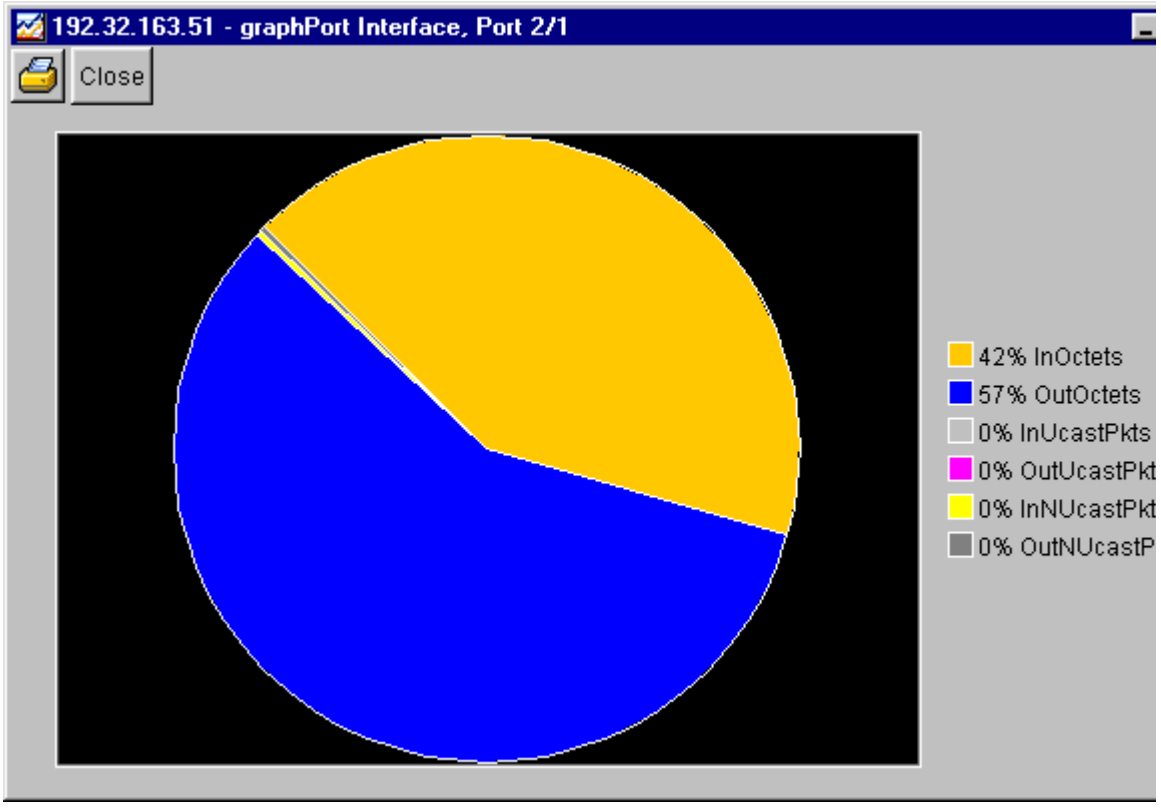


Figure 15 Pie graph



Device Manager trap log

You can configure a BayStack switch to send out SNMP traps. When Device Manager is running, any traps received are recorded in the Trap Log.

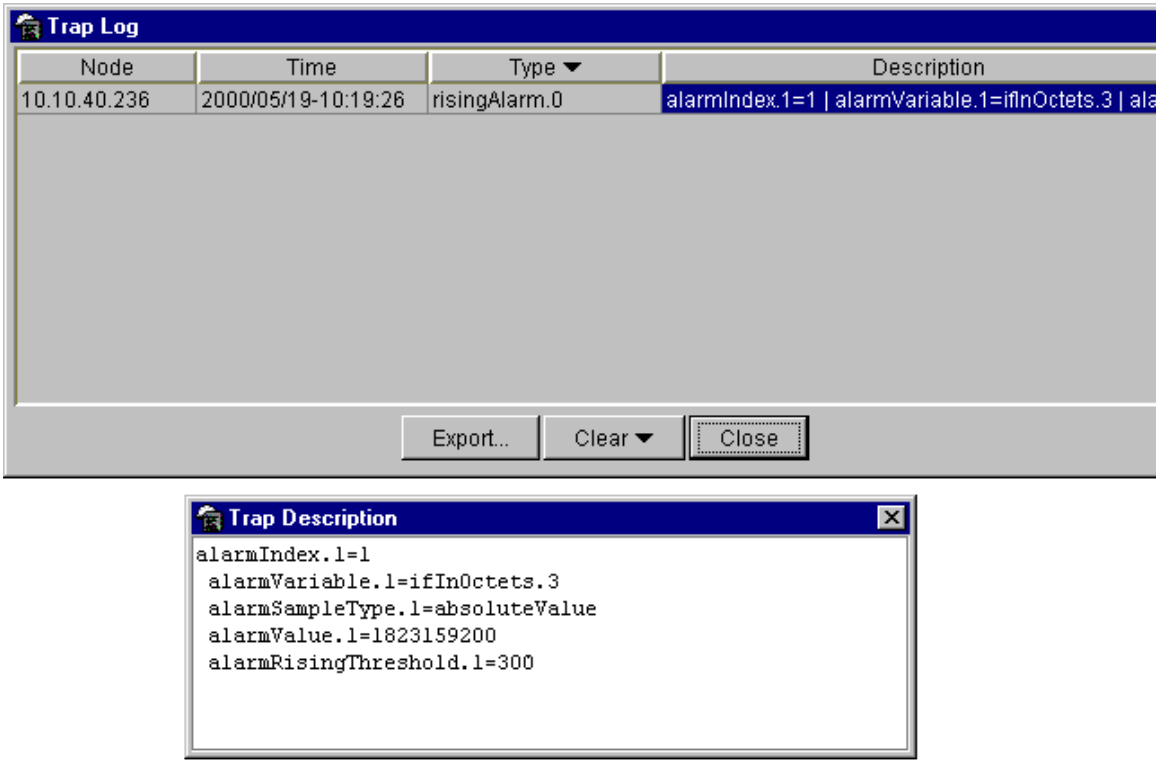
To view the trap log:

➔ Do one of the following:

- From the Device Manager main menu, choose Device > Trap Log.
- On the toolbar, click Trap.

The Trap Log dialog box opens displaying the trap log (Figure 16).

Figure 16 Trap Log dialog box



By default, the Device Manager assumes that traps are sent in SNMP V1 format.

Management stations operating with Device Manager are automatically added to trap receivers. If you want to edit trap receivers, refer to the "Trap Receivers tab" on page 62.

Telneting to a switch

You can Telnet to the BayStack switch or stack you are configuring.

To Telnet to a switch:

➔ From the Device Manager main menu, choose Actions > Telnet.

A Telnet window to the switch opens.

Online Help

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

Chapter 2
Configuring and graphing a switch

Device Manager allows you to configure and graph a stack of BayStack switches. You can also view the IP and the MAC addresses of a switch.

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

Viewing individual switches in a stack

You can view information about each individual switch, unit or card within a stack.

To view information for a specific switch, unit or card:

1. Point and click the switch, unit or card to select.
2. From the shortcut menu, choose Edit > Unit.

   The Unit dialog box opens (Figure 17).

Figure 17 Unit dialog box

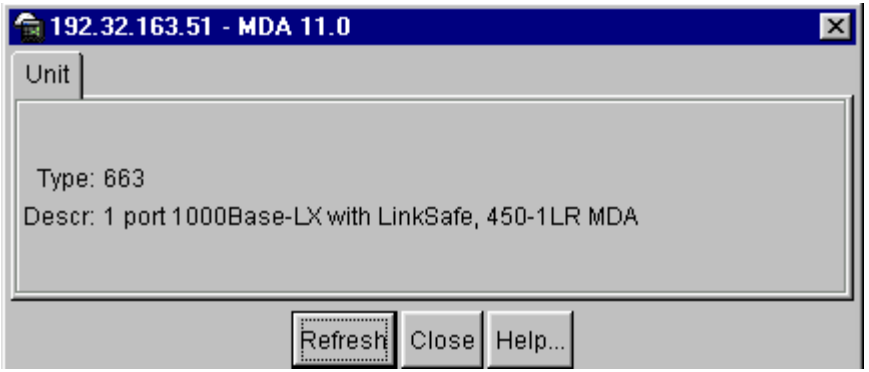


Table 12 describes the Unit dialog box fields.

Table 12 Unit dialog box fields

Field	Description
Type	The type of component or subcomponent. The values are defined under s5ChasComTypeVal in the Registration MIB.
Description	A description of the component/sub-component. If not available, the value is a zero length string.
Ver	The version number of the component/sub-component. If not available, the value is a zero length string.
SerialNumber	The serial number of the component/sub-component. If not available, the value is a zero length string.

Viewing switch IP information

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

To open the IP dialog box:

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

The IP dialog box opens (Figure 18 on page 51) with the Globals tab displayed.

Globals tab

To open the Globals tab:

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

The IP dialog box opens (Figure 18) with the Globals tab displayed.

Figure 18 Globals tab

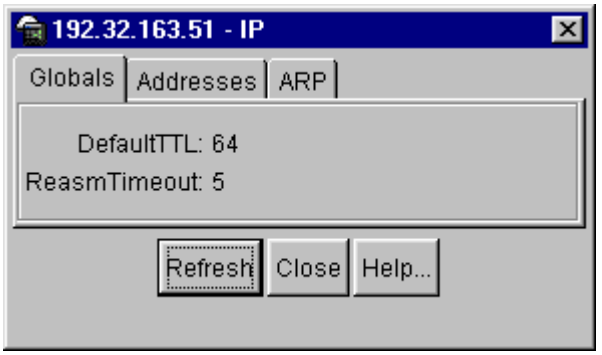


Table 13 describes the Globals tab fields.

Table 13 Globals tab fields

Field	Description
DefaultTTL	Default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol. Default value is 64.
ReasmTimeout	Maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity. Default value is 5.

Addresses tab

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

To open the Addresses tab:

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

The IP dialog box opens (Figure 18) with the Globals tab displayed.

2 Click the Addresses tab.

The Addresses tab opens (Figure 19).

Figure 19 Addresses tab

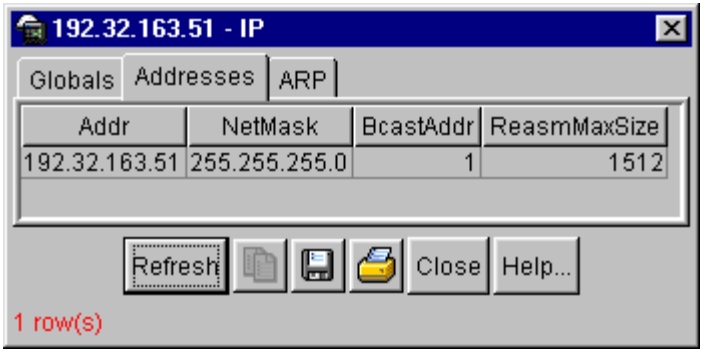


Table 14 describes the Addresses tab fields.

Table 14 Addresses tab fields

Field	Description
Addr	IP address of a device.
NetMask	Subnet mask address.
BcastAddr	IP broadcast address used.
ReasmMaxSize	Size of the largest IP datagram that this entity can reassemble from incoming IP fragmented datagrams received on this interface.

ARP tab

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

To open the ARP tab:

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

The IP dialog box opens (Figure 18) with the Globals tab displayed.

2 Click the ARP tab.

The ARP tab opens (Figure 20).

Figure 20 ARP tab

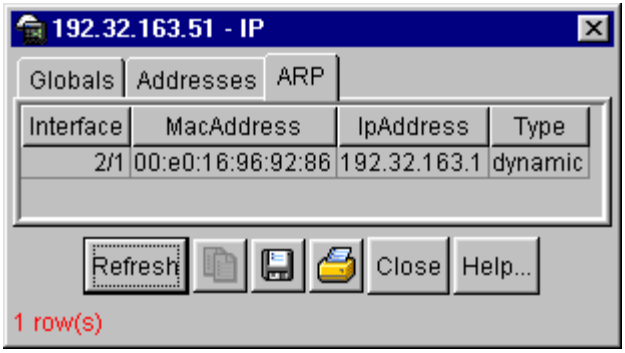


Table 15 describes the ARP tab fields.

Table 15 ARP tab fields

Field	Description
Interface	Port number of the device.
MacAddress	Unique hardware address of the device.
IpAddress	IP address of the device used to represent a point of attachment in a TCP/IP internetwork.
Type	Type of mapping.

Editing the chassis configuration

You can edit a chassis configuration from the Chassis dialog box. To open this dialog box:

To open the Chassis dialog box:

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

   The Chassis dialog box opens (Figure 21 on page 54) with the System tab displayed.

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

System tab

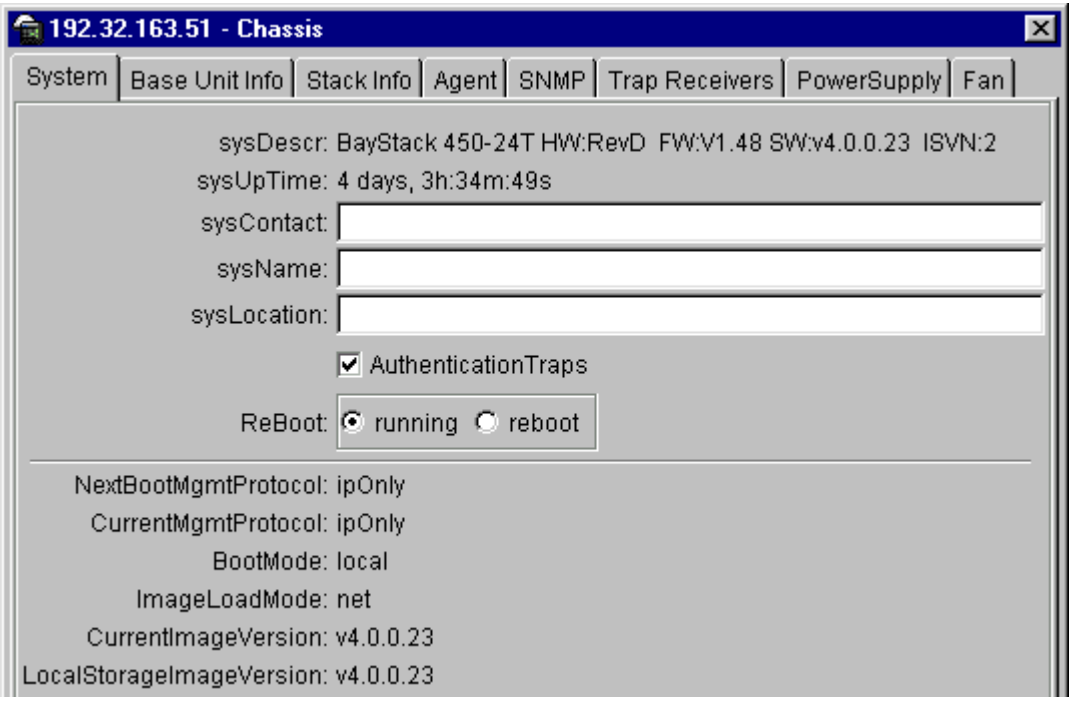
Use the System tab to specify, among other things, tracking information for a device and device descriptions.

To open the System tab:

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

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

Figure 21 System tab



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

Table 16 describes the System tab items.

Table 16 System tab fields

Field	Description
sysDescr	Assigned system name.
sysUpTime	Time since the system was last booted.
sysContact	Contact information (in this case, an e-mail address) for the system administrator.
sysName	Name of the device.
sysLocation	Physical location of this device.
AuthenticationTraps	If selected (checked), SNMP traps are sent to trap receivers for all SNMP access authentication. If not selected (not checked), traps are not received.
Reboot	Reboot the switch or the stack
NextBootMgmtProtocol	Transport protocol(s) to use after the next boot of the agent.
CurrentMgmtProtocol	Current transport protocol(s) that the agent supports.
BootMode	Source from which to load the initial protocol configuration information to boot the switch the next time, local (from the switch), or net (over the network), or none.
ImageLoadMode	Source from which to load the agent image at the next boot.
CurrentImageVersion	Version number of the agent image that is currently used on the switch.
LocalStorageImageVersion	Version number of the agent image that is stored in flash memory on the switch.
NextBootDefaultGateway	IP address of the default gateway for the agent to use after the next time the switch is booted.
CurrentDefaultGateway	IP address of the default gateway that is currently in use.
NextBootLoadProtocol	Transport protocol to be used by the agent to load the configuration information and the image at the next boot.
LastLoadProtocol	Transport protocol last used to load the image and configuration information on the switch.
SystemAuthControl	The administrative state of the EAP.

Base Unit Info tab

The Base Unit Info tab contains information about the unit. The Base Unit Info tab also includes read-only information on the operating status of the hardware, the admin state, and the location of the base unit.

To open the Base Unit Info tab:

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

   The Chassis dialog box opens (Figure 21 on page 54) with the System tab displayed.
3. Click the Base Unit Info tab.

   The Base Unit Info tab opens (Figure 22).

Figure 22 Base Unit Info tab

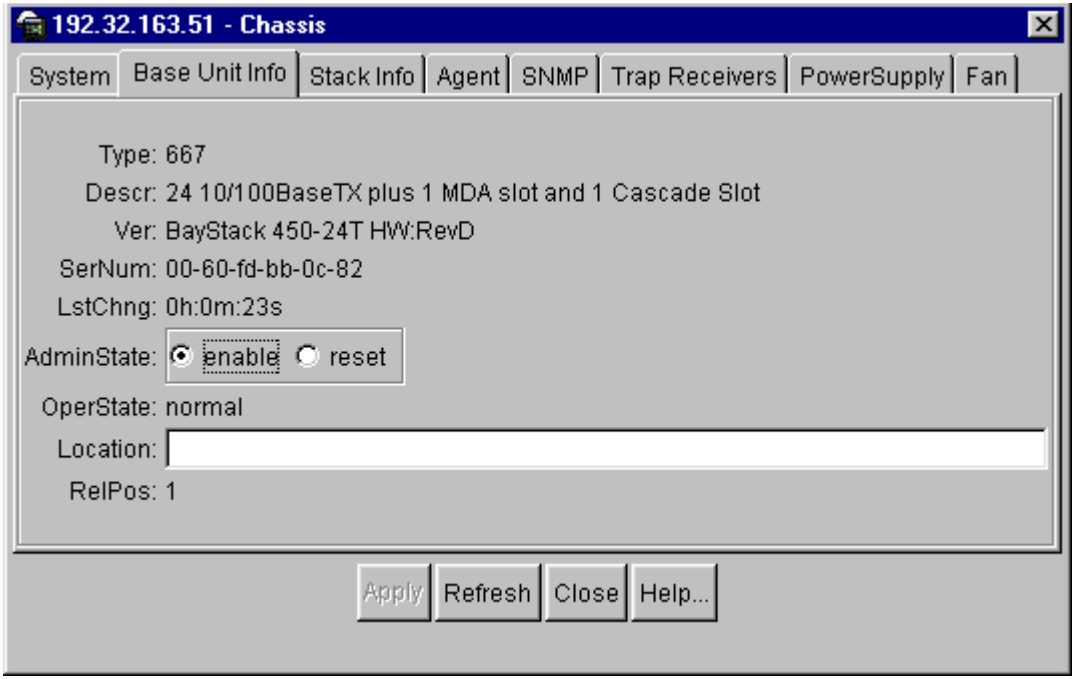


Table 17 describes the Base Unit Info tab items.

Table 17 Base Unit Info tab fields

Fields	Description
Type	Switch type.
Descr	Description of the switch hardware, including number of ports and transmission speed.
Ver	Switch hardware version number.
SerNum	Switch serial number.
LstChng	Value of sysUpTime (system up time) 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 system, the value is zero.
AdminState	Administrative state of the switch. Select either `enable` or `reset`. **Note**: In a stack configuration, `Reset` only resets the base unit.
OperState	Operational state of the switch.
Location	Physical location of the switch.
RelPos	The position of the base unit relative to the other components in a stack. Components in the unit group are numbered in the ascending order with the uppermost component being numbered one. The value of this object should never be greated than the value of s5ChasGrpMaxEnts. If not available, a value of zero is returned. **Note**: This object is only implemented in agents that support virtual chassis.

Stack Info tab

The Stack Info tab provides information about the operating status of the stacked switches. This tab is enabled for a stack of BayStack switches only.

To open the Stack Info tab:

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

   The Chassis dialog box opens (Figure 21 on page 54) with the System tab displayed.
3. Click the Stack Info tab.

   The Stack Info tab opens (Figure 23).

Figure 23 Stack Info tab

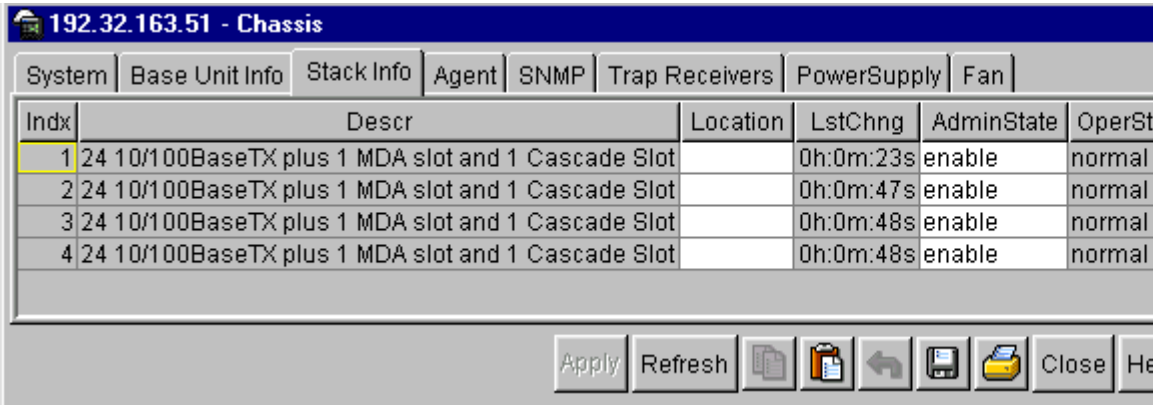


Table 18 describes the Stack Info tab fields.

Table 18 Stack Info tab fields

Field	Description
Descr	Description of the component or subcomponent. If not available, the value is a zero length string.
Location	Geographic location of a component in a system modeled as a chassis, but possibly physically implemented with geographically separate devices connected together to exchange management information. Chassis modeled in this manner are sometimes referred to as virtual chassis. An example value is: “4th flr wiring closet in blg A.” Notes: 1. This object is applicable only to components that can be found in either the Board or Unit groups. If the information is unavailable, for example, the chassis is not modeling a virtual chassis or component is not in Board or Unit group, the value is a zero length string. 2. If this object is applicable and is not assigned a value through a SNMP SET PDU when the row is created, the value will default to the value of the object s5ChasComSerNum.
LstChng	Value of sysUpTime when it was detected that the component/ sub-component was added to the chassis. If this has not occurred since the cold/warm start of the agent, then the value is zero.
AdminState	The state of the component or subcomponent. The values that are read-only are: • enable — unit in the stack is in operation state • reset — resets that unit in the stack

Table 18 Stack Info tab fields (continued)

Field	Description
OperState	Current operational state of the component. The possible values are: • other — some other state • notAvail — state not available • removed — component removed • disabled — operation disabled • normal — normal operation • resetInProg — reset in progress • testing — doing a self test • warning — operating at warning level • nonFatalErr — operating at error level • fatalErr — error stopped operation The allowable values are determined by the component type.
Ver	Hardware type and software version number.
SerNum	Serial number of the component or subcomponent. If not available, the value is a zero length string.

Agent tab

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

To open the Agent tab:

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

   The Chassis dialog box opens (Figure 21 on page 54) with the System tab displayed.
3. Click the Agent tab.

   The Agent tab opens (Figure 24).

Figure 24 Agent tab

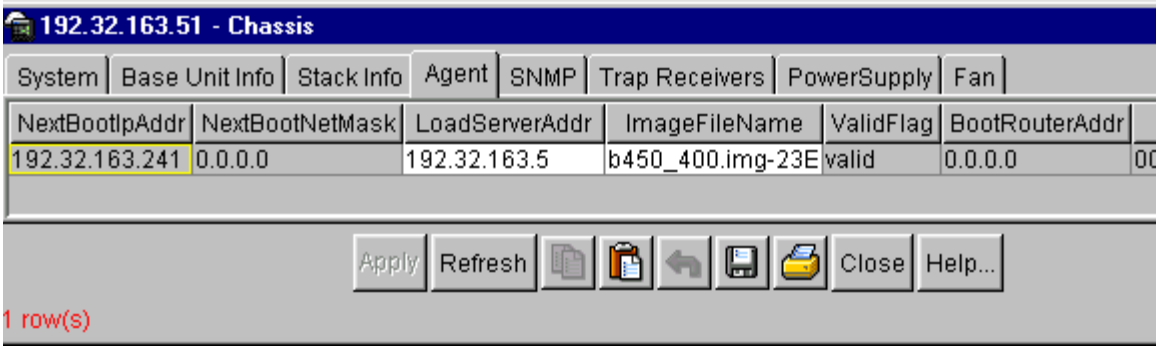


Table 19 describes the Agent tab fields.

Table 19 Agent tab fields

Field	Description
NextBootIpAddr	IP address of the BootP server to be used the next time the switch is booted.
NextBootNetMask	Subnet mask to be used the next time the switch is booted.
LoadServerAddr	IP address of the load server for the configuration file and/or the image file. The value is `0.0.0.0` if it is not used.
ImageFileName	Name of the images associated with the interface. Some agents in may support a value that contains multiple file names instead of a single file name. Multiple names are specified as a list of filenames separated by semicolons. The value is a zero length string when not used.
ValidFlag	Indicates if the configuration and/or image file(s) were downloaded from this interface and if the file names have not been changed.
BootRouterAddr	IP address of the boot router for the configuration file and/or the image file.
MacAddr	MAC address of the switch.

SNMP tab

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

To open the SNMP tab:

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

   The Chassis dialog box opens (Figure 21 on page 54) with the System tab displayed.
3. Click the SNMP tab.

   The SNMP tab opens (Figure 25).

Figure 25 SNMP tab for agent software addresses

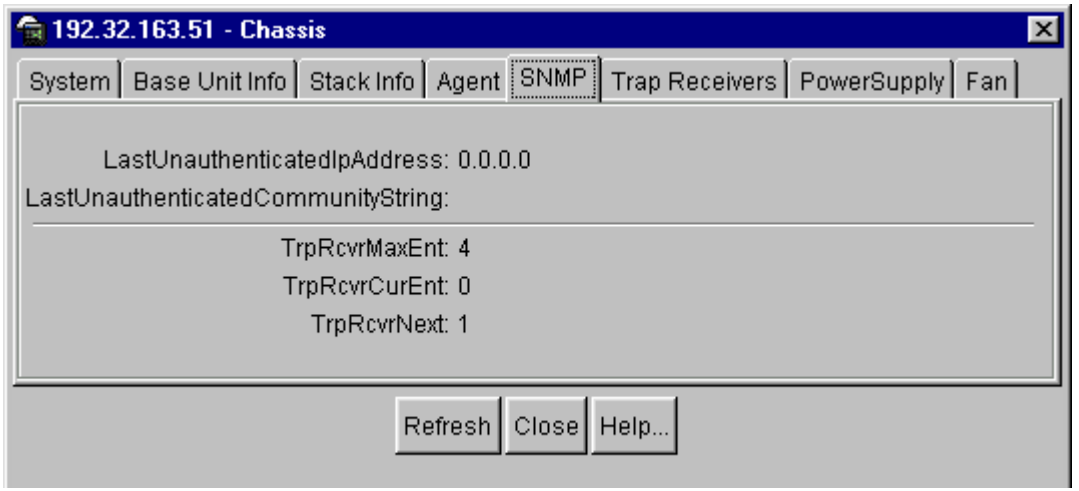


Table 20 describes the SNMP tab fields.

Table 20 SNMP tab fields

Field	Description
LastUnauthenticatedIpAddress	Last IP address that was not authenticated by the device.
LastUnauthenticatedCommunityString	Last community string that was not authenticated by the device.
TrpRcvrMaxEnt	Maximum number of trap receiver entries.
TrpRcvrCurEnt	Current number of trap receiver entries.
TrpRcvrNext	Next trap receiver entry to be created.

Trap Receivers tab

The Trap Receivers tab lists the devices that will receive SNMP traps from a Device Manager switch. When Device Manager opens a device, it automatically adds the device on which Device Manager is running to the Trap Receivers list.

To open the Trap Receivers tab:

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

   The Chassis dialog box opens (Figure 21 on page 54) with the System tab displayed.
3. Click the Trap Receivers tab.

   The Trap Receivers tab opens (Figure 26).

Figure 26 Trap Receivers tab

Table 21 describes the Trap Receivers tab items.

Table 21 Trap Receivers tab items

Item	Description
Indx	Index of the row in the tab.
NetAddr	Address (or DNS hostname) for the trap receiver.
Community	Community string used for trap messages to this trap receiver.

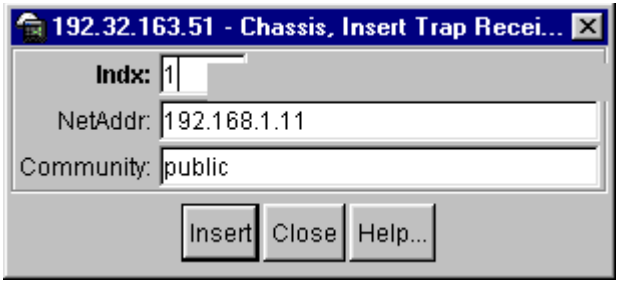
Editing network traps

To edit the network traps table:

1 In the Trap Receivers tab (Figure 26 on page 63), click Insert.

The Chassis, Insert Trap Receive dialog box opens (Figure 27).

Figure 27 Chassis, Insert Trap Receive dialog box



2 Add the Index, NetAddr, and the Community information.

Note: Refer to Table 21 for description of the Chassis, Insert Trap Receivers dialog box items

3 Click Insert.

PowerSupply tab

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

To open the PowerSupply tab:

1 Select the chassis.

2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens (Figure 21 on page 54) with the System tab displayed.

3 Click the PowerSupply tab.

The PowerSupply tab opens (Figure 28).

Figure 28 PowerSupply tab

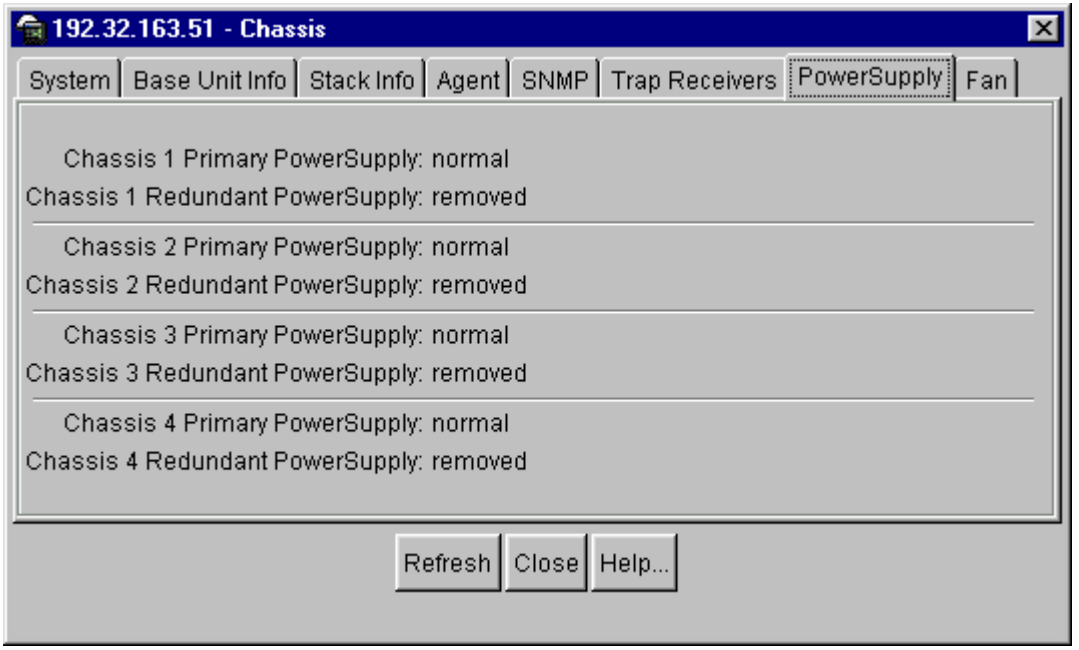


Table 22 describes the PowerSupply tab fields.

Table 22 PowerSupply tab fields

Field	Description
Chassis # Primary/Redundant PowerSupply	Operational state of the BayStack. Possible values include: • other: Some other state. • notAvail: State not available. • removed: Component was removed. • disabled: Operation disabled. • normal: State is in normal operation. • resetInProg: There is a reset in progress. • testing: System is doing a self test. • warning: System is operating at a warning level. • nonFatalErr: System is operating at error level. • fatalErr: A fatal error stopped operation. • notConfig: A module needs to be configured. The allowable values are determined by the component type.

Fan tab

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

To open the Fan tab:

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

   The Chassis dialog box opens (Figure 21 on page 54) with the System tab displayed.
3. Click the Fan tab.

   The Fan tab opens (Figure 29).

Figure 29 Fan tab

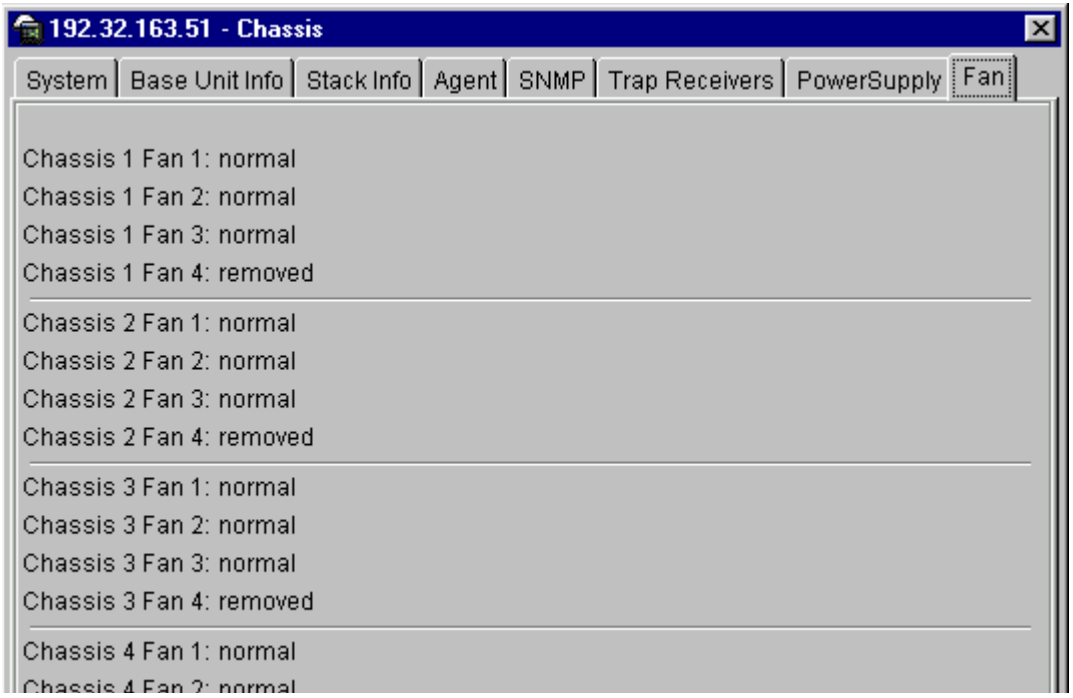


Table 23 describes the Fan tab fields.

Table 23 Fan tab fields

Field	Description
Chassis # Fan #	The current operational state of the fan. Values include: • other: Some other state. • notAvail: This state is not available. • removed: Fan was removed. • disabled: Fan is disabled. • normal: Fan is operating in normal operation. • resetInProg: A reset of the fan is in progress. • testing: Fan is doing a self test. • warning: Fan is operating at a warning level. • nonFatalErr: Fan is operating at error level. • fatalErr: An error stopped the fan operation • notConfig: Fan needs to be configured. The allowable values are determined by the component type.

FileSystem dialog box

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

To open the FileSystem dialog box:

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

The FileSystem dialog box opens (Figure 30).

Figure 30 FileSystem dialog box

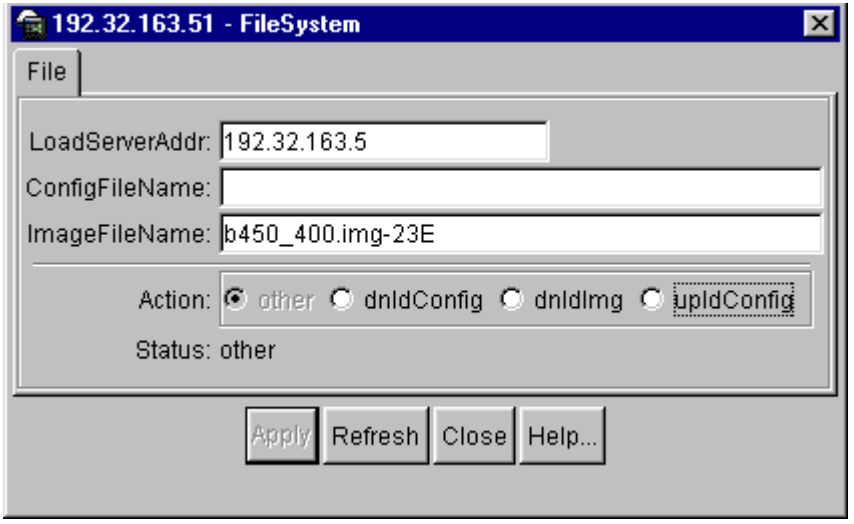


Table 24 describes the FileSystem dialog box items.

Table 24 FileSystem dialog box items

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

Table 24 FileSystem dialog box items (continued)

Item	Description
Action	This is used to download or upload a config file or an image file. In read operation, if there is no action taken since the boot up, it will return with a value of other. Otherwise, it will return the latest action. Actions include: • other — if no action taken since the boot up • dnldConfig — download a config file to a device. • dnldImg — download an image to a device. • upldConfig — upload a config file to a server from a device. Config file contain the current MIB object values of the unit. • upldImg — upload an image from a device to a server.
Status	This is used to get the status of the latest action as shown by s5AgInfoFileAction. The values that can be read are: • other — if no action taken since the boot up. • inProgress — the operation is in progress. • success — the operation succeeds. • fail — the operation failed.

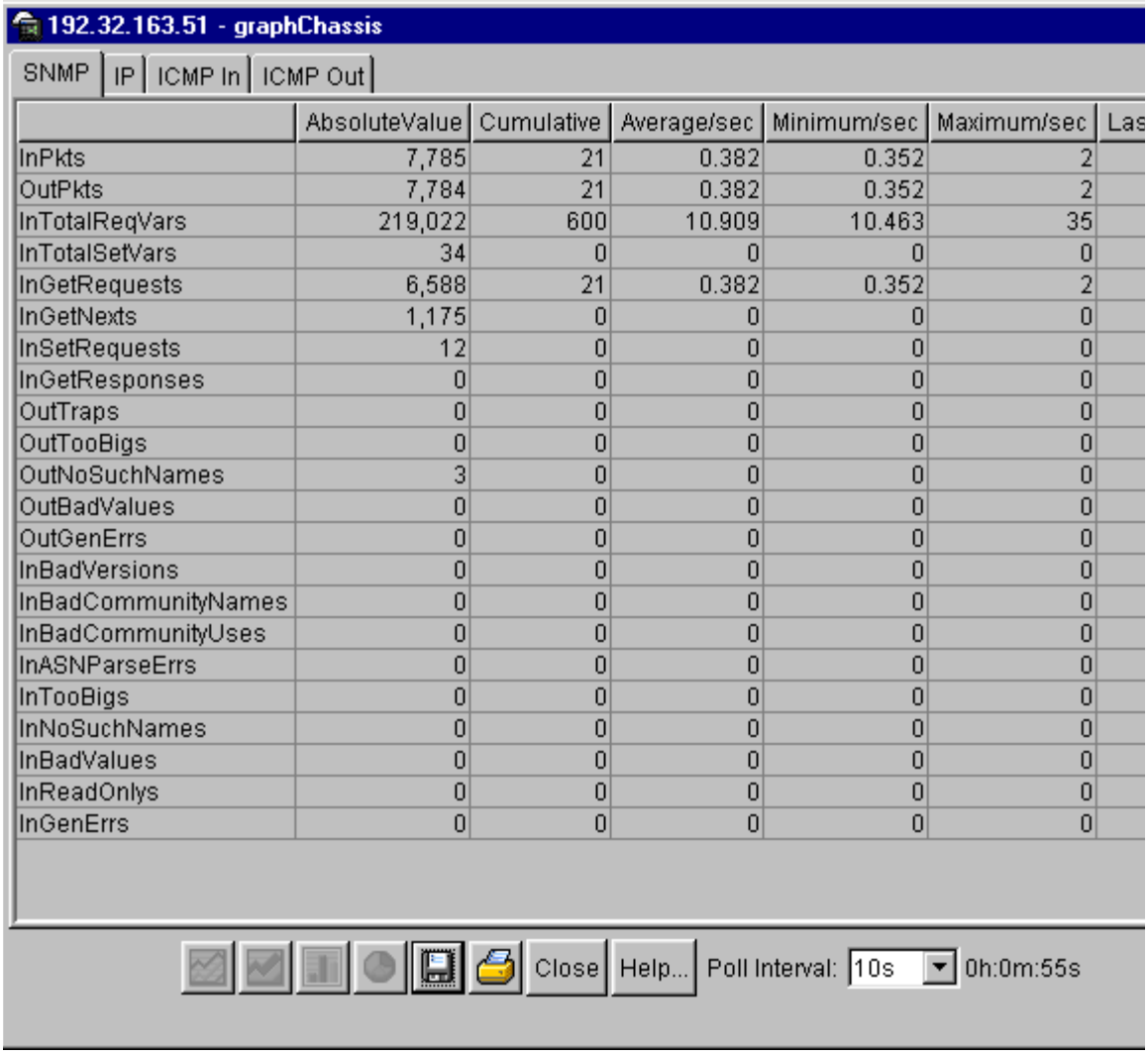
Graphing chassis statistics

To graph chassis statistics:

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

   The Chassis dialog box opens (Figure 31) with the SNMP tab displayed.

Figure 31 SNMP tab for chassis statistics



	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	Las
InPkts	7,785	21	0.382	0.352	2	
OutPkts	7,784	21	0.382	0.352	2	
InTotalReqVars	219,022	600	10.909	10.463	35	
InTotalSetVars	34	0	0	0	0	
InGetRequests	6,588	21	0.382	0.352	2	
InGetNexts	1,175	0	0	0	0	
InSetRequests	12	0	0	0	0	
InGetResponses	0	0	0	0	0	
OutTraps	0	0	0	0	0	
OutTooBigs	0	0	0	0	0	
OutNoSuchNames	3	0	0	0	0	
OutBadValues	0	0	0	0	0	
OutGenErrs	0	0	0	0	0	
InBadVersions	0	0	0	0	0	
InBadCommunityNames	0	0	0	0	0	
InBadCommunityUses	0	0	0	0	0	
InASNParseErrs	0	0	0	0	0	
InTooBigs	0	0	0	0	0	
InNoSuchNames	0	0	0	0	0	
InBadValues	0	0	0	0	0	
InReadOnlys	0	0	0	0	0	
InGenErrs	0	0	0	0	0	

The following sections describe the Chassis dialog box tabs with descriptions of the statistics on each tab. Six columns provide the statistics for the counters that are listed on the tab.

SNMP tab

The SNMP tab lists chassis statistics.

To open the SNMP tab:

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

   The Chassis dialog box opens (Figure 31 on page 70) with the SNMP tab displayed.

   Table 25 describes the SNMP tab fields.

Table 25 SNMP tab fields

Field	Description
InPkts	Number of messages delivered to the SNMP from the transport service.
OutPkts	Number of SNMP messages passed from the SNMP protocol to the transport service.
InTotalReqVars	Number of MIB objects retrieved successfully by the SNMP protocol as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
InTotalSetVars	Number of MIB objects altered successfully by the SNMP protocol as the result of receiving valid SNMP Set-Request PDUs.
InGetRequests	Number of SNMP Get-Request PDUs that have been accepted and processed by the SNMP protocol.
InGetNexts	Number of SNMP Get-Next PDUs accepted and processed by the SNMP protocol.
InSetRequests	Number of SNMP Set-Request PDUs accepted and processed by the SNMP protocol.
InGetResponses	Number of SNMP Get-Response PDUs accepted and processed by the SNMP protocol.
OutTraps	Number of SNMP Trap PDUs generated by the SNMP protocol.
OutTooBigs	Number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is TooBig.

Table 25 SNMP tab fields (continued)

Field	Description
OutNoSuchNames	Number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is NoSuchName.
OutBadValues	Number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is BadValue.
OutGenErrs	Number of SNMP PDUs generated by the SNMP protocol for which the value of the error-status field is GenErr.
InBadVersions	Number of SNMP messages delivered to the SNMP protocol for an unsupported SNMP version.
InBadCommunityNames	Number of SNMP messages delivered to the SNMP protocol that used an unknown SNMP community name.
InBadCommunityUses	Number of SNMP messages delivered to the SNMP protocol that represented an SNMP operation not allowed by the SNMP community named in the message.
InASNParseErrs	Number of ASN.1 or BER errors encountered by the SNMP protocol when decoding received SNMP messages.
InTooBigs	Number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is TooBig.
InNoSuchNames	Number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is NoSuchName.
InBadValues	Number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is BadValue.
InReadOnlys	Number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is ReadOnly. It is a protocol error to generate an SNMP PDU containing the value “readOnly” in the error-status field. This object is provided to detect incorrect implementations of the SNMP.
InGenErrs	Number of SNMP PDUs delivered to the SNMP protocol for which the value of the error-status field is GenErr.

IP tab

The IP tab shows IP information for the chassis.

To open the IP tab:

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

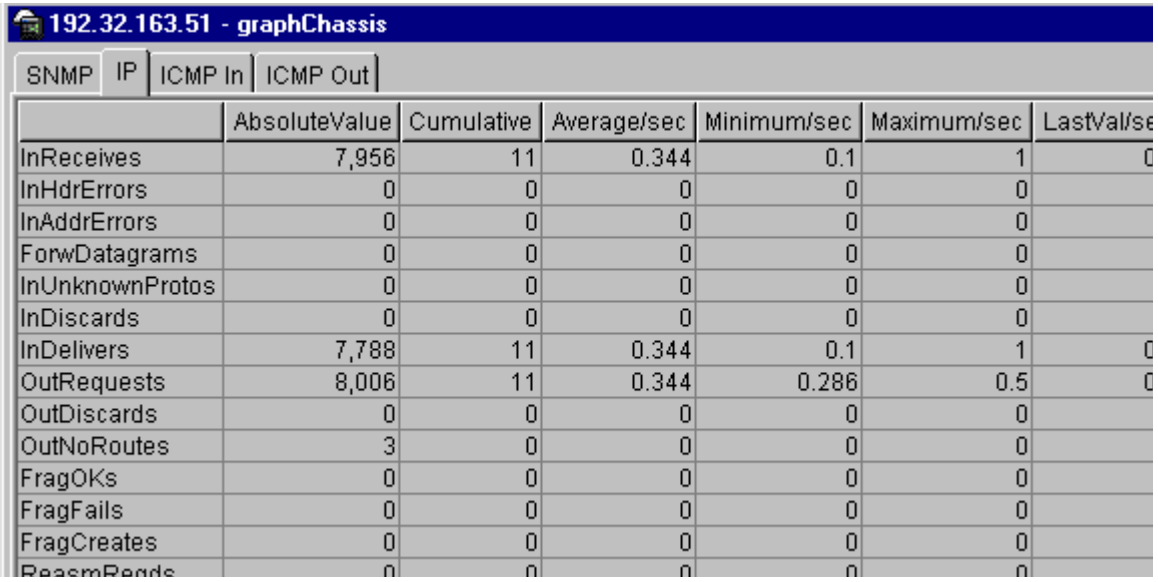
- On the toolbar, click Graph.

The Chassis dialog box opens (Figure 31 on page 70) with the SNMP tab displayed.

3 Click the IP tab.

The IP tab opens (Figure 32).

Figure 32 IP tab



	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/se
InReceives	7,956	11	0.344	0.1	1	0
InHdrErrors	0	0	0	0	0	
InAddrErrors	0	0	0	0	0	
ForwDatagrams	0	0	0	0	0	
InUnknownProtos	0	0	0	0	0	
InDiscards	0	0	0	0	0	
InDelivers	7,788	11	0.344	0.1	1	0
OutRequests	8,006	11	0.344	0.286	0.5	0
OutDiscards	0	0	0	0	0	
OutNoRoutes	3	0	0	0	0	
FragOKs	0	0	0	0	0	
FragFails	0	0	0	0	0	
FragCreates	0	0	0	0	0	
ReasmReqds	0	0	0	0	0	

Table 26 describes the IP tab fields.

Table 26 IP tab fields

Field	Description
InReceives	Number of input datagrams received from interfaces, including those received in error.
InHdrErrors	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.

Table 26 IP tab fields (continued)

Field	Description
InAddrErrors	Number of input datagrams discarded because the IP address in the IP header destination field was not a valid address. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For addresses that are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ForwDatagrams	Number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. For addresses that do not act as IP Gateways, this counter will include only those packets that were Source-Routed by way of this address and had successful Source-Route option processing.
InUnknownProtos	Number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
InDiscards	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	Number of input datagrams successfully delivered to IP user-protocols (including ICMP).
OutRequests	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	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	Number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams that meet this no-route criterion. Note that this includes any datagrams a host cannot route because all of its default gateways are down.
FragOKs	Number of IP datagrams that have been successfully fragmented at this entity.

Table 26 IP tab fields (continued)

Field	Description
FragFails	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	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
ReasmReqds	Number of IP fragments received that needed to be reassembled at this entity.
ReasmOKs	Number of IP datagrams successfully reassembled.
ReasmFails	Number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.

ICMP In tab

The ICMP In tab shows ICMP In information for the chassis.

To open the ICMP In tab:

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

   The Chassis dialog box opens (Figure 31 on page 70) with the SNMP tab displayed.
3. Click the ICMP In tab.

   The ICMP In tab opens (Figure 33).

Figure 33 ICMP In tab

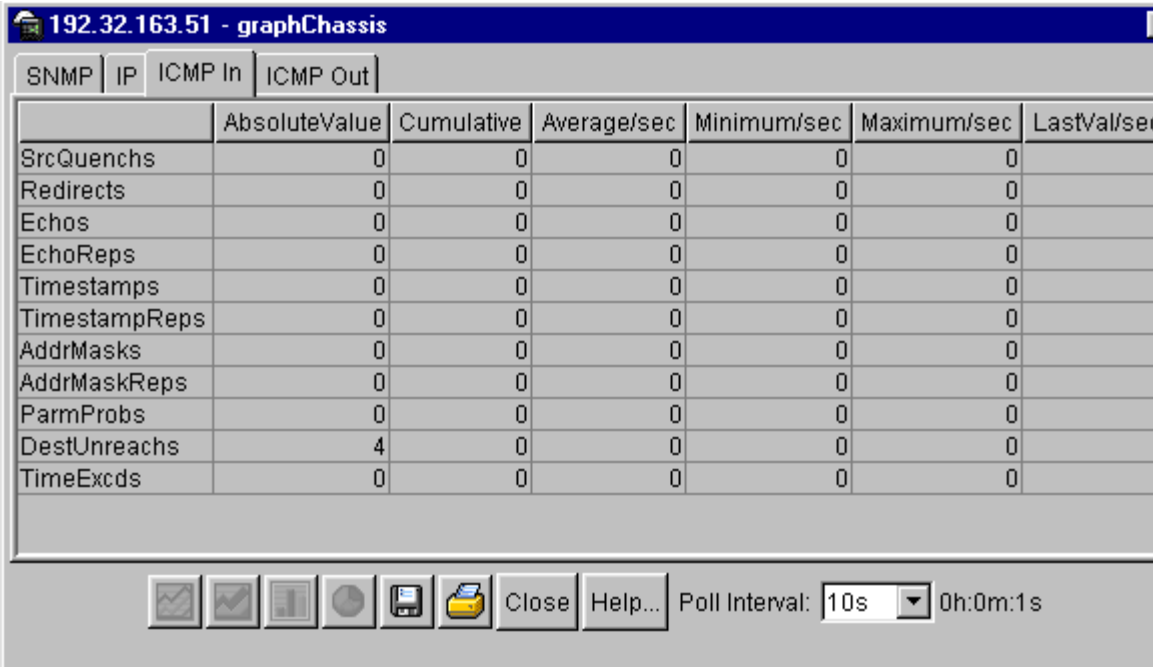


Table 27 describes the ICMP In tab fields.

Table 27 ICMP In tab fields

Fields	Description
SrcQuenchs	Number of ICMP Source Quench messages received.
Redirects	Number of ICMP Redirect messages received.
Echos	Number of ICMP Echo (request) messages received.
EchoReps	Number of ICMP Echo Reply messages received.
Timestamps	Number of ICMP Timestamp (request) messages received.
TimestampReps	Number of ICMP Timestamp Reply messages received.
AddrMasks	Number of ICMP Address Mask Request messages received.
AddrMaskReps	Number of ICMP Address Mask Reply messages received.
ParmProbs	Number of ICMP Parameter Problem messages received.
DestUnreachs	Number of ICMP Destination Unreachable messages received.
TimeExcds	Number of ICMP Time Exceeded messages received.

ICMP Out tab

The ICMP Out tab shows ICMP Out information for the chassis.

To open the ICMP Out tab:

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

   The Chassis dialog box opens (Figure 31 on page 70) with the SNMP tab displayed.
3. Click the ICMP Out tab.

   The ICMP Out tab opens (Figure 34).

Figure 34 ICMP Out tab

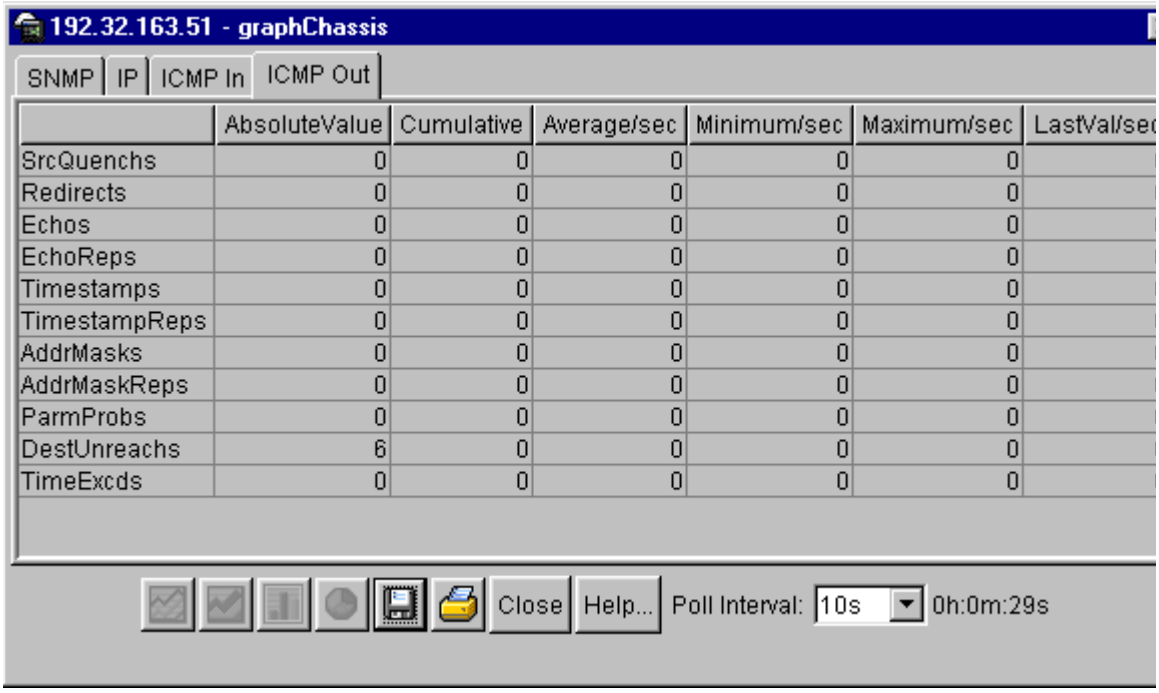


Table 28 describes the ICMP Out tab fields.

Table 28 ICMP Out tab fields

Fields	Description
SrcQuenchs	Number of ICMP Source Quench messages received.
Redirects	Number of ICMP Redirect messages received.
Echos	Number of ICMP Echo (request) messages received.
EchoReps	Number of ICMP Echo Reply messages received.
Timestamps	Number of ICMP Timestamp (request) messages received.
TimestampReps	Number of ICMP Timestamp Reply messages received.
AddrMasks	Number of ICMP Address Mask Request messages received.
AddrMaskReps	Number of ICMP Address Mask Reply messages received.
ParmProbs	Number of ICMP Parameter Problem messages received.
DestUnreachs	Number of ICMP Destination Unreachable messages received.
TimeExcds	Number of ICMP Time Exceeded messages received.

Chapter 3
Configuring and graphing ports

Device Manager allows you to configure and graph the ports on a BayStack switch and the ports on an MDA installed in the switch. You can configure multiple ports or a single port.

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

This chapter describes how you use Device Manager to configure and graph ports on a BayStack switch.

Configuring a single port

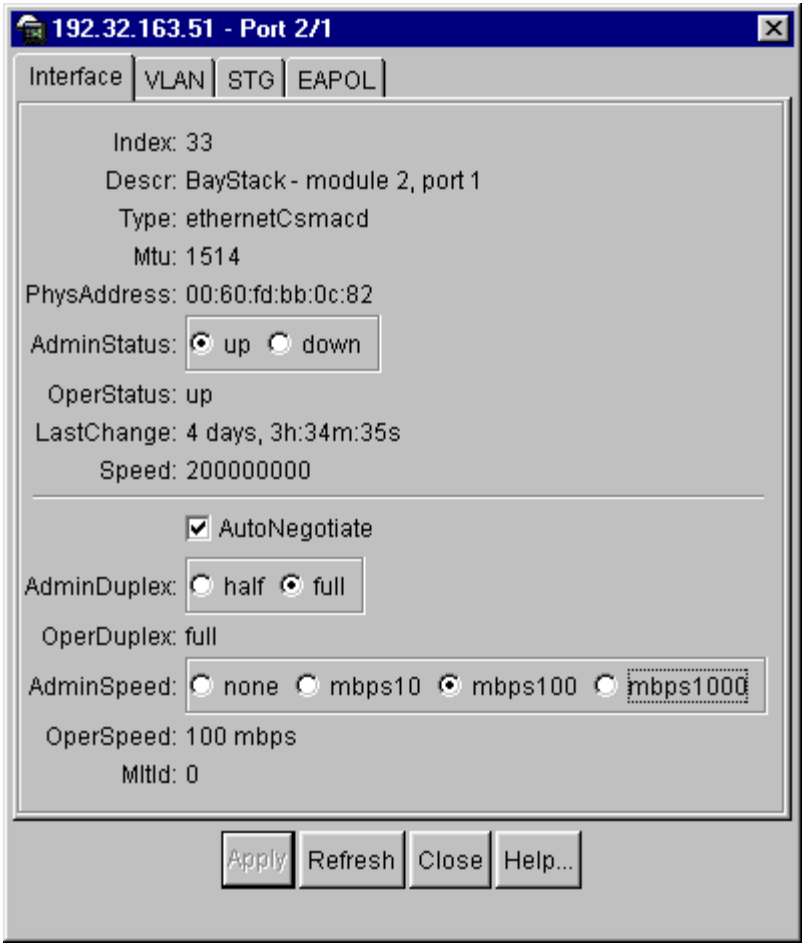
After selecting the single port that you want to view or edit, there are four ways to open the configuration dialog box for a port.

To view or edit a single port:

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

   The Port dialog box for a single port opens (Figure 35) with the Interface tab displayed.

Figure 35 Interface tab for a single port



Port dialog box tabs for a single port

The Port dialog box tabs for a single port contains three tabs:

- "Interface tab for a single port" (next)
- "VLAN tab for a single port" on page 83
- "STG tab for a single port" on page 84
- "EAPOL tab for a single port" on page 86

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

Interface tab for a single port

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

To view the Interface tab:

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

   The Port dialog box for a single port opens (Figure 35 on page 80) with the Interface tab displayed.

Table 29 describes the Interface tab items for a single port.

Table 29 Interface tab items for a single port

Item	Description
Index	A unique value assigned to each interface. The value ranges between 1 and 255.
Descr	Type of switch followed by Unit (module) #, port #.
Type	Media type for this interface.
Mtu	Size of the largest packet, in octets, that can be sent or received on the interface.
PhysAddress	MAC address assigned to a particular interface.
AdminStatus	Current administrative state of the interface, which can be one of the following: • up • down When a managed system is initialized, all interfaces start with AdminStatus in the down state. AdminStatus changes to the up state (or remains in the down state) as a result of either management action or the configuration information available to the managed system.

Table 29 Interface tab items for a single port (continued)

Item	Description
OperStatus	Current operational state of the interface, which can be one of the following: • up • down • testing If AdminStatus is up, then OperStatus should be up if the interface is ready to transmit and receive network traffic. If AdminStatus is down, then OperStatus should be down. It should remain in the down state if and only if there is a fault that prevents it from going to the up state. The testing state indicates that no operational packets can be passed.
LastChange	Value of the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero.
Speed	The estimate bandwidth of the interface in bits per second (bps). For interfaces that do not vary in bandwidth or have no way to estimate the bandwidth, this object should contain the nominal bandwidth. If the bandwidth of the interface is greater than the maximum value reported by the object, then the object displays its maximum value (4,294,967,295). For a sub-layer that has no concept of bandwidth, the object should be zero.
AutoNegotiate	Indicates whether the port is enabled (checked) for autonegotiation or not.
AdminDuplex	The current administrative duplex mode of the port (half or full).
OperDuplex	Indicate current duplex value of the port.
AdminSpeed	Set the speed of a port: none, mbps10, and mbps100 (or mbps 1000)
OperSpeed	The current operating speed of the port.
MltId	The MultiLink Trunk to which the port is assigned (if any).

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

VLAN tab for a single port

The VLAN tab shows the VLAN membership for a single port.

To view the VLAN tab:

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

   The Port dialog box for a single port opens (Figure 35 on page 80) with the Interface tab displayed.
3. Click the VLAN tab.

   The VLAN tab opens (Figure 36).

Figure 36 VLAN tab for a single port

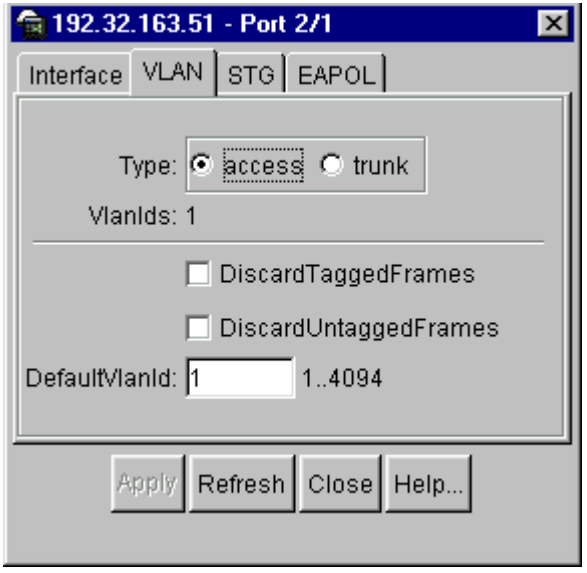


Table 30 describes the VLAN tab items for a single port

Table 30 VLAN tab items for a single port

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

STG tab for a single port

The STG tab shows the STG information for a single port.

To view the STG tab:

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

   The Port dialog box for a single port opens (Figure 35 on page 80) with the Interface tab displayed.

3 Click the STG tab.

The STG tab opens (Figure 37).

Figure 37 STG tab for a single port

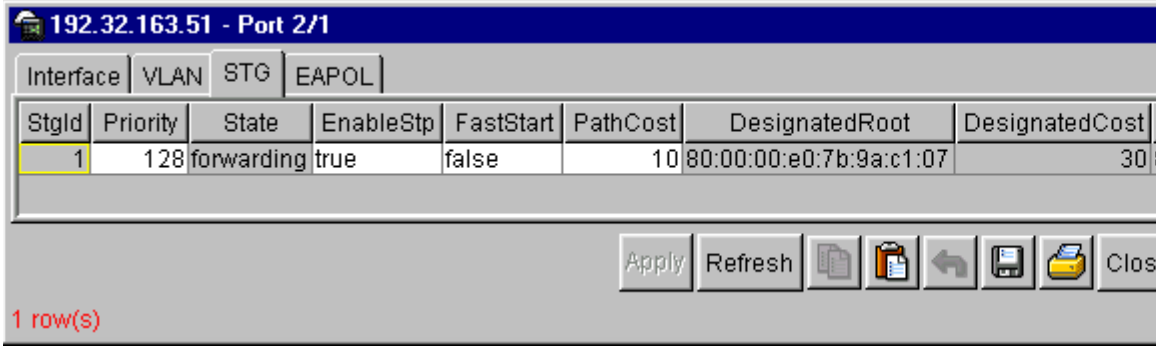


Table 31 describes the STG tab items for a single port.

Table 31 STG tab items for a single port

Item	Description
StgId	STG identifier assigned to this port.
Priority	Value of the priority field contained in the first octet of the port ID. The other octet is given by the value of the “rcStgPort.”
State	The current state of the port as defined by application of the “Spanning Tree Protocol.” These are the instructions the port takes on a frame when it is received. If the bridge detects a port is malfunctioning, it will list it as “broken(6).” For ports that are disabled, the value is “disabled(1).”
EnableStp	Enables (True) or disables (False) spanning tree of the port.
FastStart	When this is enabled (True), spanning tree of the port resolves in 4 seconds.
PathCost	Contribution of the port to the pathcost of paths towards the spanning tree root, including the current port. 802.1D-1990 specifications recommends that the default of this parameter be in inverse proportion to the speed of the attached LAN.
DesignatedRoot	The unique “Bridge Identifier.” This is recorded as Root in the configuration bridge PDUs transmitted by the Designated Bridge for the segment to that the port is attached.
DesignatedCost	Path cost of the Designated Port of the segment connected to the port. The value is compared to the Root Path Cost field in received bridge PDUs.

Table 31 STG tab items for a single port (continued)

Item	Description
DesignatedBridge	Bridge Identifier of the bridge that this port considers to be the Designated Bridge for this port's segment.
DesignatedPort	Port Identifier of the port on the Designated Bridge for this port's segment.
ForwardTransitions	Number of times this port has transitioned from the learning state to the forwarding state.

EAPOL tab for a single port

The EAPOL-based security feature uses the Extensible Authentication Protocol (EAP), as described in the IEEE Draft P802.1X, to allow you to set up network access control on internal LANs.

To view the EAPOL tab:

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

   The Port dialog box for a single port opens (Figure 35 on page 80) with the Interface tab displayed.
3. Click the EAPOL tab.

   The EAPOL tab opens (Figure 38).

Figure 38 EAPOL tab for a single port

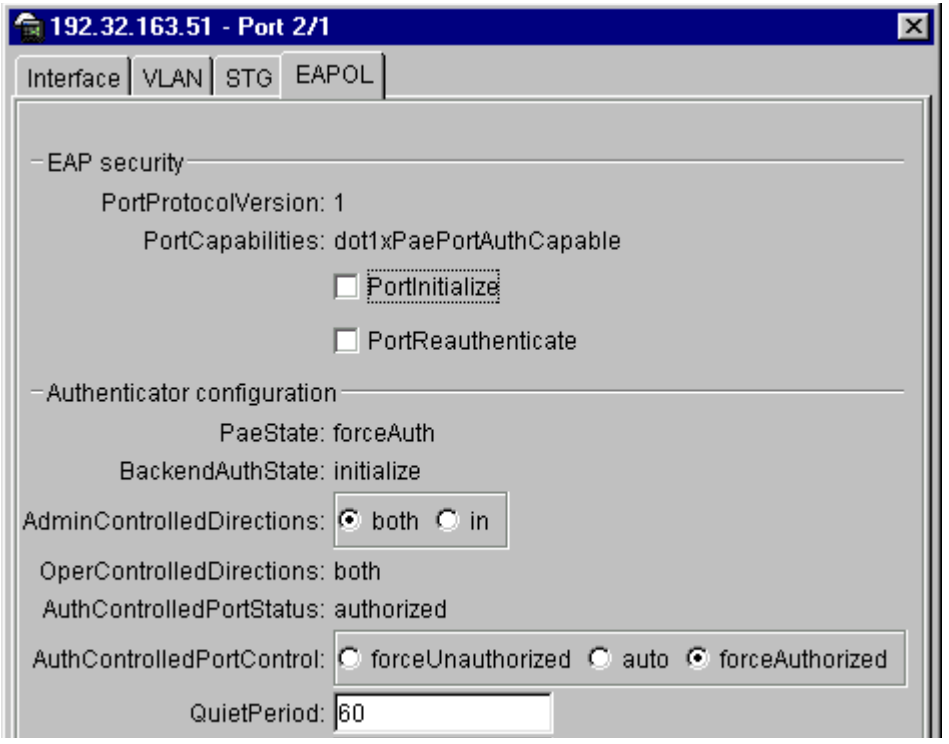


Table 32 describes the EAPOL tab items for a single port.

Table 32 EAPOL tab items for a single port

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

Table 32 EAPOL tab items for a single port (continued)

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

Configuring multiple ports

After selecting the ports that you want to view or edit, there are three ways to open the configuration window for multiple ports. The configuration dialog box for multiple ports has two tabs.

To view or edit multiple ports:

1. Select the ports that you want to edit.

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

2. Do one of the following:

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

   The Port dialog box for multiple ports opens with the Interface tab displayed.

Port dialog box tabs for multiple ports

The Port dialog box for multiple ports contains three tabs:

- "Interface tab for multiple ports" (next)
- "VLAN tab for multiple ports" on page 92
- "EAPOL tab for multiple ports" on page 94

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

Interface tab for multiple ports

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

To view or edit the Interface tab for multiple ports:

1. Select the ports that you want to edit.

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

2. Do one of the following:

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

   The Port dialog box for a multiple port (Figure 39) opens with the Interface tab displayed.

Figure 39 Interface tab for multiple ports

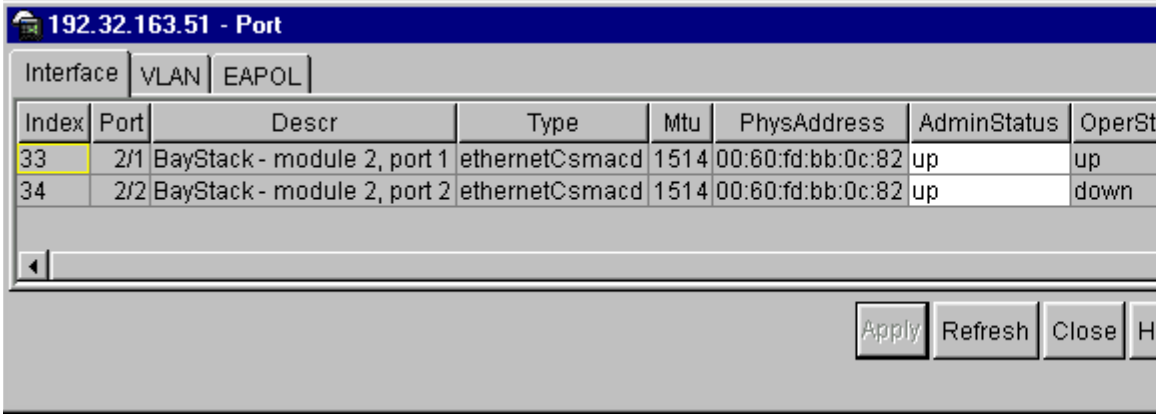


Table 33 describes the Interface tab fields for multiple ports.

Table 33 Interface tab fields for multiple ports

Field	Description
Index	A unique value assigned to each interface. The value ranges between 1 and 255.
Descr	Type of switch followed by Unit (module) #, port #.
Type	Media type for this interface.
Mtu	Size of the largest packet, in octets, that can be sent or received on the interface.
PhysAddress	MAC address assigned to a particular interface.
AdminStatus	Current administrative state of the interface, which can be one of the following: • up • down When a managed system is initialized, all interfaces start with AdminStatus in the down state. AdminStatus changes to the up state (or remains in the down state) as a result of either management action or the configuration information available to the managed system.
OperStatus	Current operational state of the interface, which can be one of the following: • up • down • testing If AdminStatus is up, then OperStatus should be up if the interface is ready to transmit and receive network traffic. If AdminStatus is down, then OperStatus should be down. It should remain in the down state if and only if there is a fault that prevents it from going to the up state. The testing state indicates that no operational packets can be passed.
LastChange	Value of the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero.
Speed	The estimate bandwidth of the interface in bits per second (bps). For interfaces that do not vary in bandwidth or have no way to estimate the bandwidth, this object should contain the nominal bandwidth. If the bandwidth of the interface is greater than the maximum value reported by the object, then the object displays its maximum value (4,294,967,295). For a sub-layer that has no concept of bandwidth, the object should be zero.
AutoNegotiate	Indicates whether the port is enabled (checked) for autonegotiation or not.
AdminDuplex	The current administrative duplex mode of the port (half or full).

Table 33 Interface tab fields for multiple ports (continued)

Field	Description
OperDuplex	Indicate current duplex value of the port.
AdminSpeed	Set the speed of a port: none, mbps10, and mbps100, and mbps 1000
OperSpeed	The current operating speed of the port.
MltId	The MultiLink Trunk to which the port is assigned (if any).

VLAN tab for multiple ports

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

To view or edit the Interface tab for multiple ports:

1. Select the ports that you want to edit.

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

2. Do one of the following:

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

   The Port dialog box for a multiple port (Figure 39 on page 90) opens with the Interface tab displayed.

3. Click the VLAN tab.

   The VLAN tab opens (Figure 40).

Figure 40 VLAN tab for multiple ports

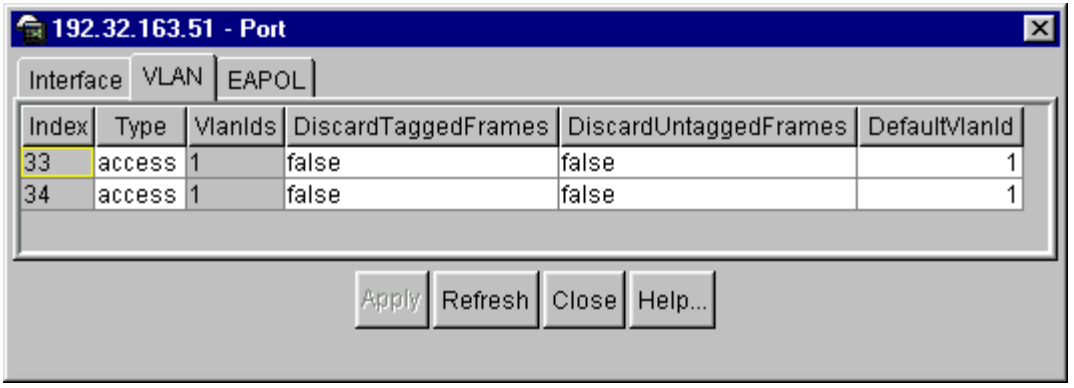


Table 34 describes the VLAN tab fields for multiple ports.

Table 34 VLAN tab items for multiple ports

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

EAPOL tab for multiple ports

The EAPOL-based security feature uses the Extensible Authentication Protocol (EAP), as described in the IEEE Draft P802.1X, to allow you to set up network access control on internal LANs.

To view the EAPOL tab:

1. Select the ports that you want to edit.

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

2. Do one of the following:

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

     The Port dialog box for a single port opens (Figure 35 on page 80) with the Interface tab displayed.

3. Click the EAPOL tab.

   The EAPOL tab opens (Figure 41).

Figure 41 EAPOL tab for multiple ports

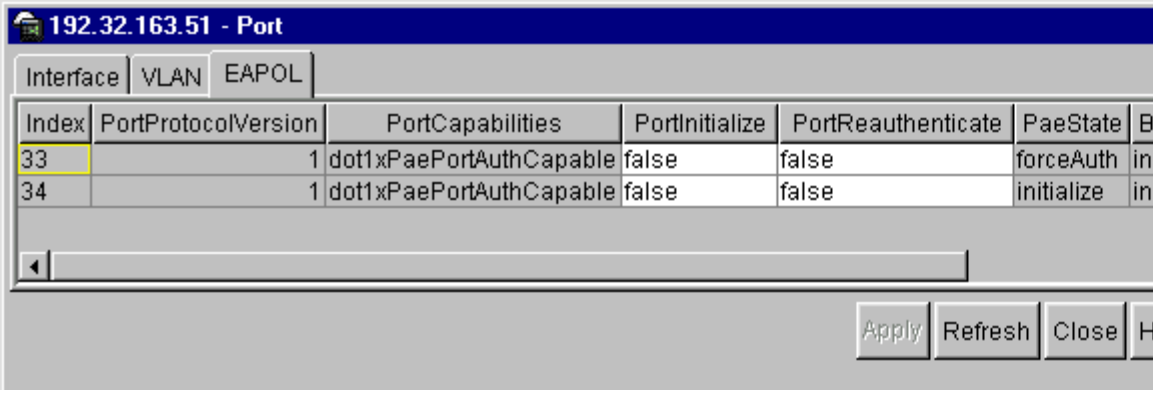


Table 35 describes the EAPOL tab items for a single port.

Table 35 EAPOL tab items for a single port

Item	Description
PortProtocolVersion	The EAP Protocol version that is running on this port.
PortCapabilities	The PAE functionality that is implemented on this port. Always returns dot1xPaePortAuthCapable(0).
PortInitialize	Setting this attribute to True initializes this port's EAPOL state.
PortReauthenticate	Setting this attribute to True reauthenticates the client.
PaeState	The current authenticator PAE state machine stat value.
BackendAuthState	The current state of the Backend Authentication state machine.
AdminControlledDirections	The current value of the administrative controlled directions parameter for the port.
OperControlledDirections	The current value of the operational controlled directions parameter for the port.
AuthControlledPortStatus	The current value of the controlled port status parameter for the port.
AuthControlledPortControl	The current value of the controlled port control parameter for the port.
QuietPeriod	The current value of the time interval between authentication failure and the start of a new authentication.
TxPeriod	Time to wait for response from supplicant for EAP requests/Identity packets.
SuppTimeout	Time to wait for response from supplicant for all EAP packets except EAP Request/Identity.
ServerTimeout	Time to wait for a response from the RADIUS server
MaxReq	Number of times to retry sending packets to the supplicant.
ReAuthPeriod	Time interval between successive re-authentications.
ReAuthEnabled	Whether to re-authenticate or not. Setting this object to Enabled reauthenticates the existing supplicant at the time interval specified in the Re-authentication Period field.
KeyTxEnabled	The value of the KeyTranmissionEnabled constant currently in use by the Authenticator PAE state machine. This always returns false as key transmission is irrelevant.

Table 35 EAPOL tab items for a single port (continued)

Item	Description
LastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

Graphing port statistics

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

To open the graphPort dialog box for graphing:

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

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

2. Do one of the following:

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

   The graphPort dialog box for a single port (Figure 35 on page 80) or for multiple ports opens with the Interface tab displayed.

GraphPort dialog box tabs for multiple ports

The graphPort dialog box contains four tabs:

- "EAPOL Diag tab for graphing ports" on page 109

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

Interface tab for graphing ports

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

To open the Interface tab for graphing:

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

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

2. Do one of the following:

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

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

Figure 42 Interface tab for graphing ports

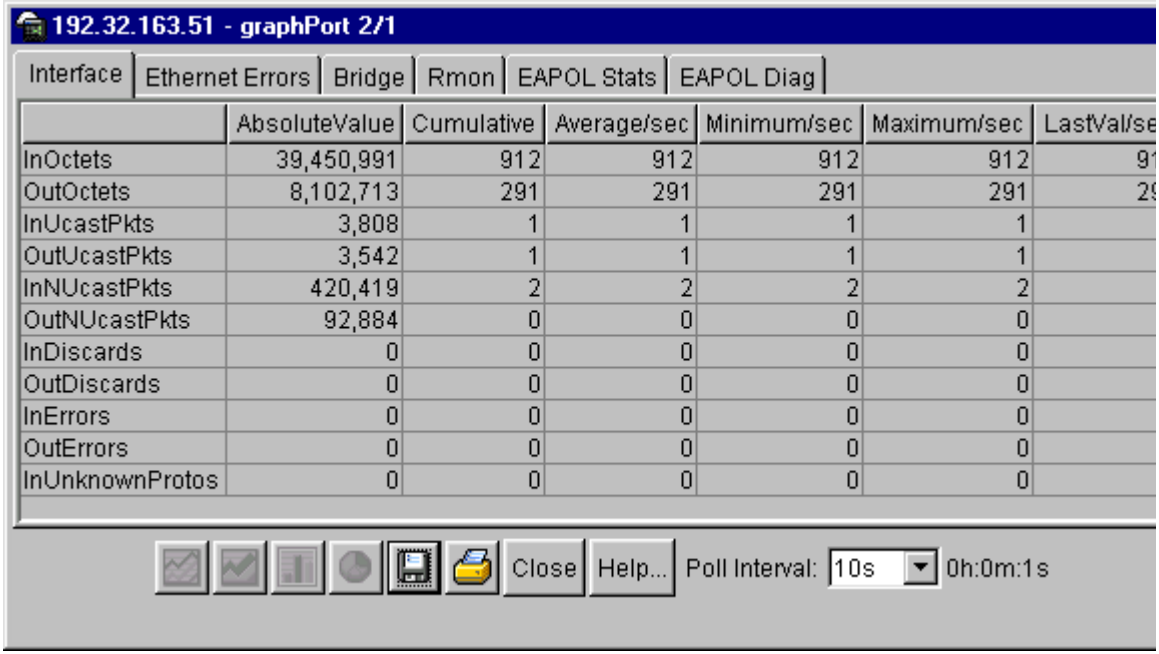


Table 36 describes the Interface tab fields for graphing ports.

Table 36 Interface tab fields for graphing ports

Fields	Description
InOctets	Number of octets received on the interface, including framing characters.
OutOctets	Number of octets transmitted out of the interface, including framing characters.
InUcastPkts	Number of packets delivered by this sub-layer to a higher sub-layer that were not addressed to a multicast or broadcast address at this sub-layer.
OutUcastPkts	Number of packets that higher-level protocols requested be transmitted that were not addressed to a multicast address at this sub-layer. This number includes those packets discarded or unsent.
InNUcastPkts	Number of packets delivered by this sub-layer to a higher sub-layer, which were addressed to a broadcast address at this sub-layer.

Table 36 Interface tab fields for graphing ports (continued)

Fields	Description
OutNUcastPkts	Number of packets that higher-level protocols requested be transmitted, and were addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
InDiscards	Number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
OutDiscards	Number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
InErrors	For packet-oriented interfaces: Number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
OutErrors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character- oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

Ethernet Errors tab for graphing ports

The Ethernet Errors tab shows Ethernet errors for graphing a port or ports.

To open the Ethernet Errors tab for graphing:

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

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

2. Do one of the following:

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

   The graphPort dialog box for a single port (Figure 35 on page 80) or for multiple ports opens with the Interface tab displayed.

3 Click the Ethernet Errors tab.

The Ethernet Errors tab opens (Figure 43).

Figure 43 Ethernet Errors tab for graphing ports

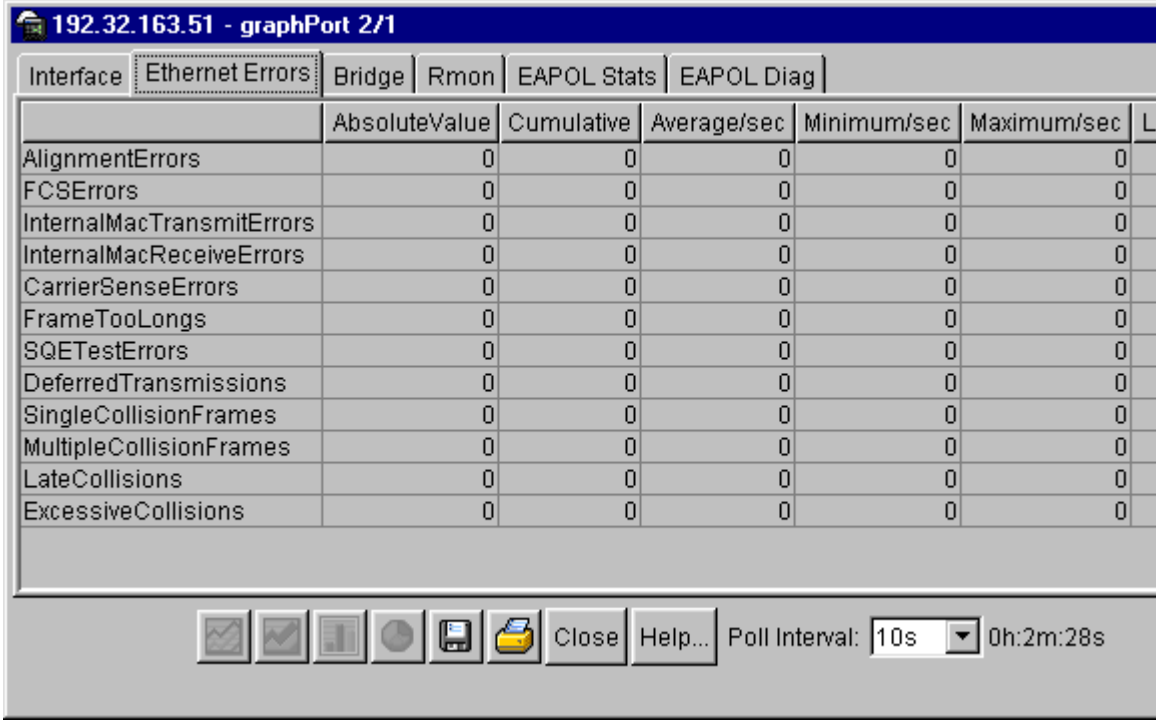


Table 37 describes the Ethernet Errors tab fields for graphing ports.

Table 37 Ethernet Errors tab fields for graphing ports

Field	Description
AlignmentErrors	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
FCSErrors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
InternalMacTransmitErrors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the LateCollisions object, the ExcessiveCollisions object, or the CarrierSenseErrors object.
InternalMacReceiveErrors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the FrameTooLongs object, the AlignmentErrors object, or the FCSErrors object. The precise meaning of the count represented by an instance of this object is implementation specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted.
CarrierSenseErrors	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 37 Ethernet Errors tab fields for graphing ports (continued)

Field	Description
FrameTooLongs	A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
SQETestErrors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
DeferredTransmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
SingleCollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the MultipleCollisionFrames object.
MultipleCollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object.
LateCollisions	Number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
ExcessiveCollisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.

Bridge tab for graphing ports

The Bridge tab shows bridge information for graphing a port or ports.

To open the Bridge tab for graphing:

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

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

2. Do one of the following:

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

   The graphPort dialog box for a single port (Figure 35 on page 80) or for multiple ports opens with the Interface tab displayed.

3. Click the Bridge tab.

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

Figure 44 Bridge tab for graphing ports

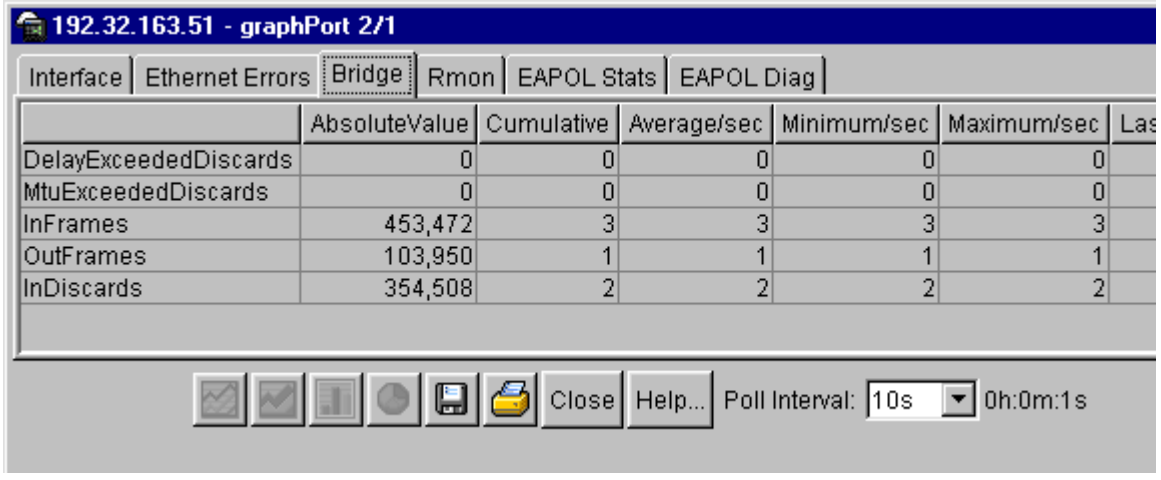


Table 38 describes the Bridge tab fields for graphing ports.

Table 38 Bridge tab fields for graphing ports

Fields	Description
DelayExceededDiscards	Number of frames discarded by the port due to excessive transit delays through the bridge. It is incremented by both transparent and source route bridges.
MtuExceededDiscards	Number of frames discarded by the port due to an excessive size. It is incremented by both transparent and source route bridges.
InFrames	Number of frames that have been received by this port from its segment. Note: A frame received on the interface corresponding to this port is only counted by this object if it is for a protocol being processed by the local bridging function, including bridge management frames.
OutFrames	Number of frames that have been transmitted by the port to its segment. Note: A frame transmitted on the interface corresponding to the port is only counted by this object if it is for a protocol being processed by the local bridging function, including bridge management frames.
InDiscards	Count of valid frames received which were discarded (that is, filtered) by the forwarding process.

Rmon tab for graphing ports

The Rmon tab shows Ethernet statistics for graphing a port or ports.

To open the Rmon tab for graphing:

1 Select the port or ports you want to graph.

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

2 Do one of the following:

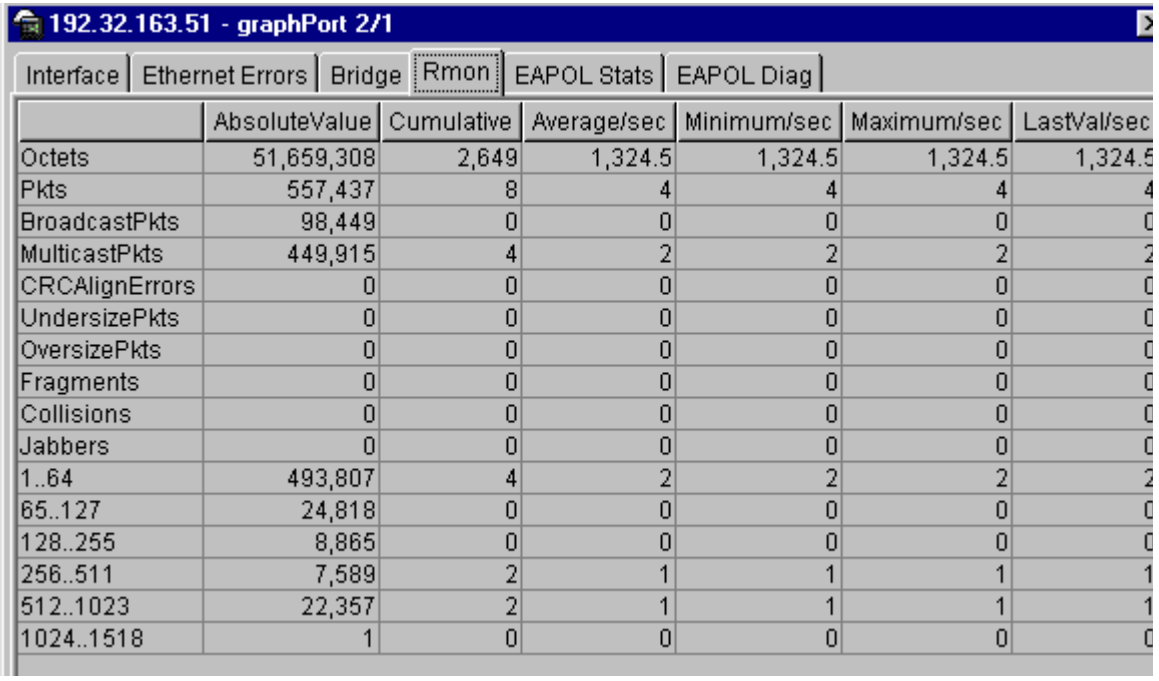
- From the Device Manager main menu, choose Graph > Port.
- From the shortcut menu, choose Graph.
- On the toolbar, click Graph.

The graphPort dialog box for a single port (Figure 35 on page 80) or for multiple ports opens with the Interface tab displayed.

3 Click the Rmon tab.

The Rmon tab for graphing ports opens (Figure 45).

Figure 45 Rmon tab for graphing ports



	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
Octets	51,659,308	2,649	1,324.5	1,324.5	1,324.5	1,324.5
Pkts	557,437	8	4	4	4	4
BroadcastPkts	98,449	0	0	0	0	0
MulticastPkts	449,915	4	2	2	2	2
CRCAlignErrors	0	0	0	0	0	0
UndersizePkts	0	0	0	0	0	0
OversizePkts	0	0	0	0	0	0
Fragments	0	0	0	0	0	0
Collisions	0	0	0	0	0	0
Jabbers	0	0	0	0	0	0
1..64	493,807	4	2	2	2	2
65..127	24,818	0	0	0	0	0
128..255	8,865	0	0	0	0	0
256..511	7,589	2	1	1	1	1
512..1023	22,357	2	1	1	1	1
1024..1518	1	0	0	0	0	0

Table 39 describes the Rmon tab fields for graphing ports.

Table 39 Rmon tab fields for graphing ports

Field	Description
Octets	Number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). You can use this object as a reasonable estimate of Ethernet utilization. For greater precision, sample the etherStatsPkts and etherStatsOctets objects before and after a common interval.
Pkts	Number of packets (including bad packets, broadcast packets, and multicast packets) received.
BroadcastPkts	Number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
MulticastPkts	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.
CRCAlignErrors	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 non-integral number of octets (Alignment Error).
UndersizePkts	Number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
OversizePkts	Number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed.
Fragments	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 non-integral 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	Best estimate of the number of collisions on this Ethernet segment.
Jabbers	Number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Jabber is defined as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.

Table 39 Rmon tab fields for graphing ports (continued)

Field	Description
1..64	Number of packets (including bad packets) received that were less than or equal to 64 octets in length (excluding framing bits but including FCS octets).
65..127	Number of packets (including bad packets) received that were greater than 65 octets in length inclusive (excluding framing bits but including FCS octets).
128..255	Number of packets (including bad packets) received that were greater than 128 octets in length inclusive (excluding framing bits but including FCS octets).
256..511	Number of packets (including bad packets) received that were greater than 256 octets in length inclusive (excluding framing bits but including FCSoctets).
512..1023	Number of packets (including bad) received that were greater than 512 octets in length inclusive (excluding framing bits but including FCS octets).
1024..1518	Number of packets (including bad) received that were greater than 1024 octets in length inclusive (excluding framing bits but including FCS octets).

EAPOL Stats tab for graphing ports

EAP allows the exchange of authentication information between any end station or server connected to the switch and an authentication server (such as a RADIUS server).

The EAPOL Stats tab shows EAPOL statistics for graphing ports.

To open the EAPOL Stats tab for graphing:

1 Select the port or ports you want to graph.

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

2 Do one of the following:

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

The graphPort dialog box for a single port (Figure 35 on page 80) or for multiple ports opens with the Interface tab displayed.

3 Click the EAPOL Stats tab.

The EAPOL Stats tab for graphing ports opens (Figure 46).

Figure 46 EAPOL Stats tab for graphing ports

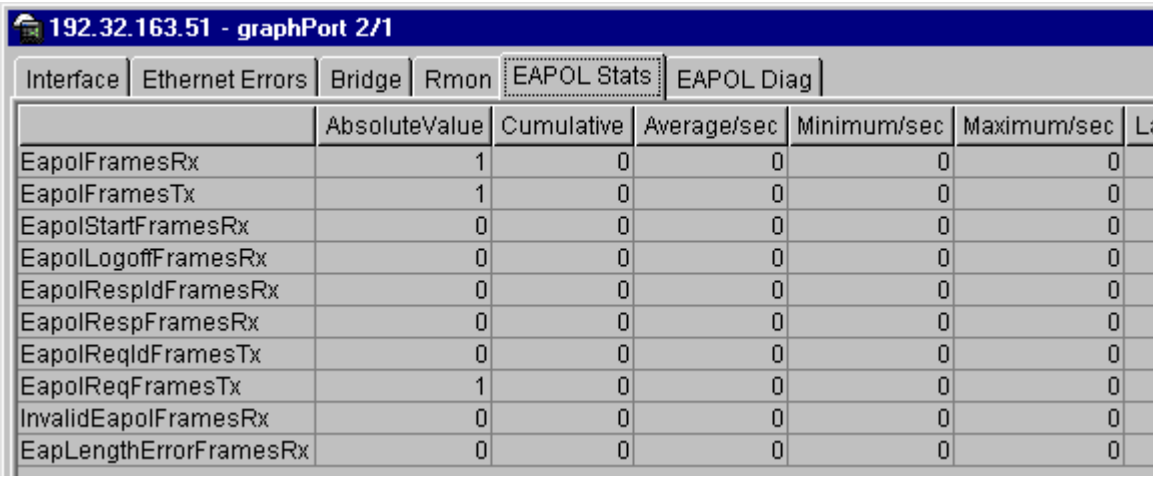


Table 40 describes the EAPOL Stats tab fields for graphing ports.

Table 40 EAPOL Stats tab fields for graphing ports

Field	Description
EapolFramesRx	The number of valid EAPOL frames of any type that have been received by this authenticator.
EapolFramesTx	The number of EAPOL frame types of any type that have been transmitted by this authenticator.
EapolStartFramesRx	The number of EAPOL start frames that have been received by this authenticator.
EapolLogoffFramesRx	The number of EAPOL Logoff frames that have been received by this authenticator.

Table 40 EAPOL Stats tab fields for graphing ports (continued)

Field	Description
EapolRespIdFramesRx	The number of EAPOL Resp/Id frames that have been received by this authenticator.
EapolRespFramesRx	The number of valid EAP Response frames (Other than Resp/Id frames) that have been received by this authenticator.
EapolReqIdFramesTx	The number of EAPOL Req/Id frames that have been transmitted by this authenticator.
EapolReqFramesTx	The number of EAP Req/Id frames (Other than Rq/Id frames) that have been transmitted by this authenticator.
InvalidEapolFramesRx	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EapLengthErrorFramesRx	The number of EAPOL frames that have been received by this authenticator in which the packet body length field is not valid.

EAPOL Diag tab for graphing ports

The EAPOL Diag tab shows EAPOL diagnostic information for graphing ports.

To open the EAPOL Diag tab for graphing:

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

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

2. Do one of the following:

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

   The graphPort dialog box for a single port (Figure 35 on page 80) or for multiple ports opens with the Interface tab displayed.

3. Click the EAPOL Diag tab.

   The EAPOL Diag tab for graphing ports opens (Figure 47).

Figure 47 EAPOL Diag tab for graphing ports

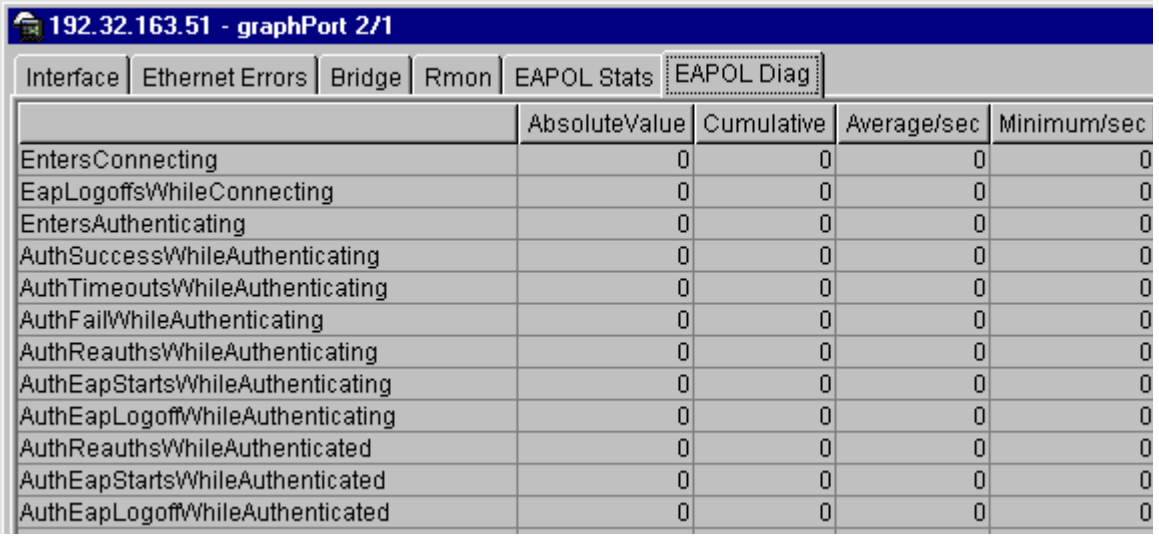


Table 41 describes the EAPOL Diag tab fields for graphing ports.

Table 41 EAPOL Diag tab fields for graphing ports

Field	Description
EntersConnecting	Counts the number of times that the Authenticator PAE state machine transitions to the Connecting state from any other state.
EapLogoffsWhileConnecting	Counts the number of times that the Authenticator PAE state machine transitions from Connected to Disconnected as a result of receiving an EAPOL-Logoff message.
EntersAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Connecting to Authenticating as a result of receiving an EAP-Response/ Identity message being received from the supplicant.
AuthSuccessWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Authenticated as a result of the Backend authentication state machine indicating successful authentication of the supplicant.
AuthTimeoutsWhile Authenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of the Backend authentication state machine indicating authentication timeout.

Table 41 EAPOL Diag tab fields for graphing ports (continued)

Field	Description
AuthFailWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Held as a result of the Backend authentication state machine indicating authentication failure.
AuthReauthsWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of a reauthentication request.
AuthEapStartsWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of an EAPOL-Start message being received from the supplicant.
AuthEapLogoffWhileAuthenticating	Counts the number of times that the Authenticator PAE state machine transitions from Authenticating to Aborting as a result of an EAPOL-Logoff message being received from the supplicant.
AuthReauthsWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Connecting as a result of a reauthentication request.
AuthEapStartsWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Connecting as a result of an EAPOL-Start message being received from the supplicant.
AuthEapLogoffWhileAuthenticated	Counts the number of times that the Authenticator PAE state machine transitions from Authenticated to Disconnected as a result of an EAPOL-Logoff message being received from the supplicant.
BackendResponses	Counts the number of times that the Backend Authentication state machine sends an Initial-Access request packet to the Authentication server.
BackendAccessChallenges	Counts the number of times that the Backend Authentication state machine receives an Initial-Access challenge packet from the Authentication server.
BackendOtherRequestsToSupplicant	Counts the number of times that the Backend Authentication state machine sends an EAP request packet (other than an Identity, Notification, failure, or success message) to the supplicant.
BackendNonNakResponsesFromSupplicant	Counts the number of times that the Backend Authentication state machine receives a response from the supplicant to an initial EAP request and the response is something other than EAP-NAK.

Table 41 EAPOL Diag tab fields for graphing ports (continued)

Field	Description
BackendAuthSuccesses	Counts the number of times that the Backend Authentication state machine receives an EAP-success message from the Authentication server.
BackendAuthFails	Counts the number of times that the Backend Authentication state machine receives an EAP-failure message from the Authentication server.

Chapter 4
Working with MultiLink Trunk ports

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

MultiLink Trunking (MLT) features

For the BayStack switches, MultiLink Trunking has the following general features and requirements:

- A unit can have up to 6 MultiLink Trunks (MLTs).
- Up to four ports can belong to a MultiLink Trunk.
- Ports in a MultiLink Trunk can be on different units in the stack.
- MultiLink Trunking is supported on 10BASE-T, 100BASE-TX, 100BASE-FX, and Gigabit Ethernet ports.
- MultiLink Trunking is compatible with the Spanning Tree Protocol.
- IEEE 802.1Q tagging is supported on a MultiLink Trunk.
- For bridge traffic, the algorithm that distributes traffic across a MultiLink Trunk is based on the source and destination MAC addresses.

Setting up MLTs

To set up MultiLink Trunks:

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

The MLT dialog box opens (Figure 48).

Figure 48 MLT dialog box

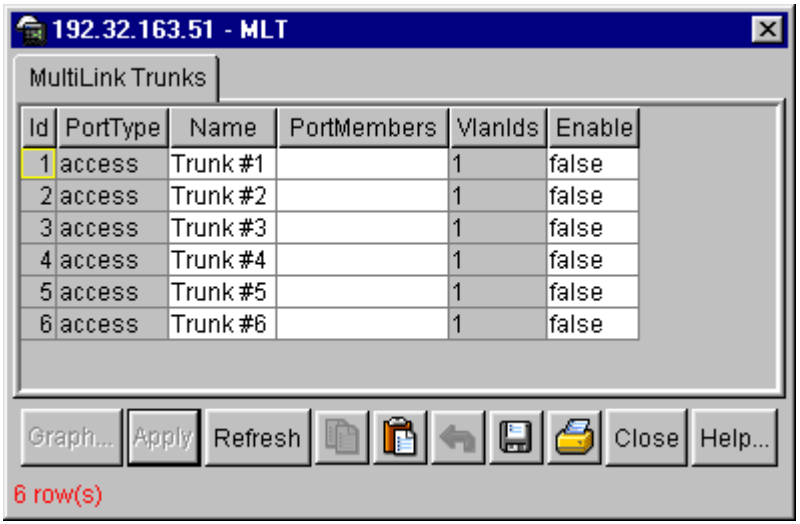


Table 42 describes the active MLT dialog box fields.

Table 42 MLT dialog box fields

Field	Description
ID	Number of the MLT (assigned consecutively).
Name	Name given to the MultiLink Trunk.
PortType	Access or trunk port.
PortMembers	Ports assigned to the MLT.
VlanIds	The VLANIDs of which this port trunk is a member.
Enable	Select True if the MLT is enabled or False is MLT is disabled.

Adding ports to a MultiLink Trunk

To add ports to an existing MultiLink Trunk:

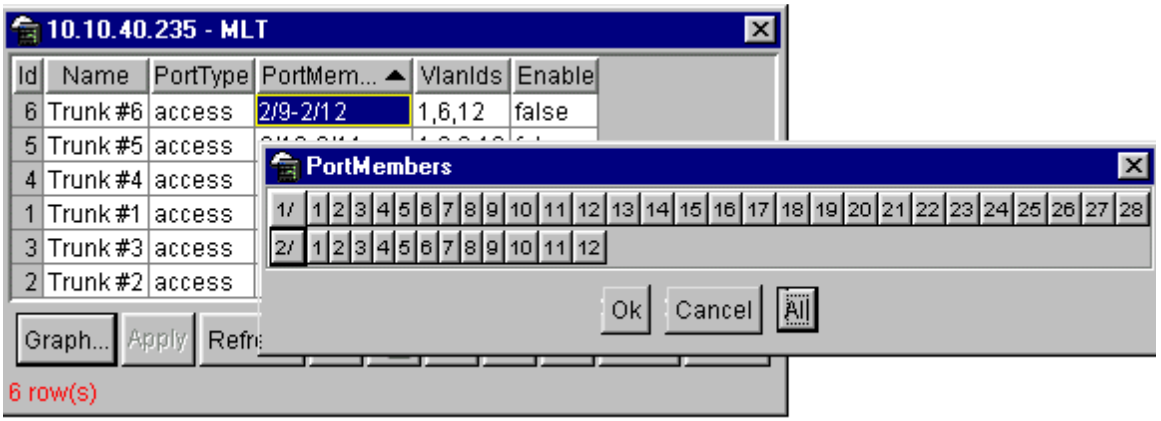
1. From the Device Manager menu bar, choose VLAN > MLT.

   The MLT dialog box opens (Figure 48 on page 114).

2. Double-click in the PortMembers field.

   The PortMembers dialog box opens (Figure 49).

Figure 49 PortMembers dialog box



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

Note: The first enabled distributed MLT causes the stack to reset. Please refer to the BayStack 450 manual for more details on MLT rules.

MultiLink Trunk statistics

To view MultiLink Trunk interface statistics:

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

   The MLT dialog box opens (Figure 48 on page 114).

2. Select an MLT row and then click Graph.

   The Statistics, MLT dialog box (Figure 50) opens with the Interface tab displayed.

Figure 50 Statistics, MLT dialog box

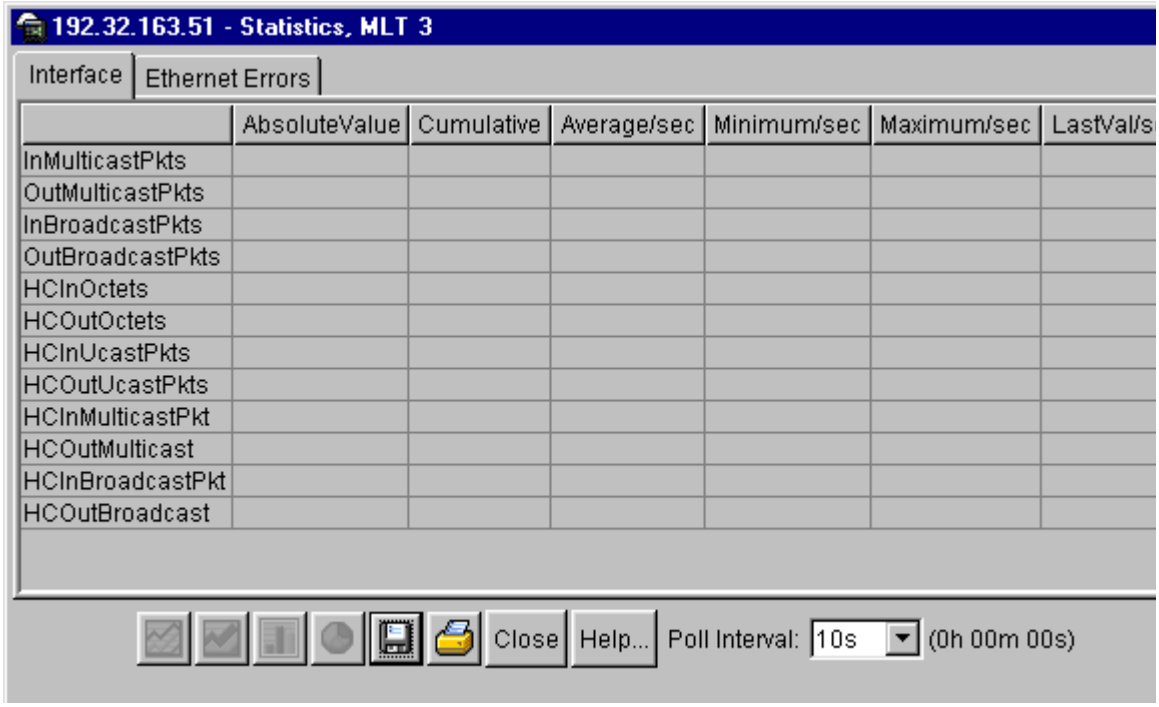


Table 43 describes in the Interface tab fields.

Table 43 Interface tab fields

Field	Description
InMulticastPkt	Number of packets delivered to this MLT that were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this number includes both Group and Functional addresses.
OutMulticastPkts	Number of packets that higher-level protocols requested be transmitted, and that were addressed to a multicast address at this MLT, including those that were discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses.
InBroadcastPkts	Number of packets delivered to this MLT that were addressed to a broadcast address at this sub-layer.
OutBroadcastPkts	Number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this MLT, including those that were discarded or not sent.
HCInOctets	Number of octets received on the MLT interface, including framing characters.
HCOutOctets	Number of octets transmitted out of the MLT interface, including framing characters.
HCInUcastPkts	Number of packets delivered by this MLT to higher level protocols that were not addressed to a multicast or broadcast address at this sub-layer.
HCOutUcastPkts	Number of packets that higher-level protocols requested be transmitted that were not addressed to a multicast address at this MLT.This total number includes those packets discarded or unsent.
HCInMulticastPkt	Number of packets delivered to this MLT that were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this number includes both Group and Functional addresses.
HCOutMulticast	Number of packets that higher-level protocols requested be transmitted, and that were addressed to a multicast address at this MLT, including those that were discarded or not sent. For a MAC layer protocol, this number includes both Group and Functional addresses.
HCInBroadcastPkt	Number of packets delivered to this MLT that were addressed to a broadcast address at this sub-layer.
HCOutBroadcast	Number of packets that higher-level protocols requested be transmitted, and that were addressed to a broadcast address at this MLT, including those that were discarded or not sent.

MultiLink Trunk Ethernet errors statistics

To view MultiLink Trunk Ethernet error statistics:

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

   The MLT dialog box opens (Figure 48 on page 114).

2. Select an MLT (a row) by clicking inside a field of an appropriate MLT.

3. Click Graph.

   The Statistics, MLT dialog box opens (Figure 50 on page 116) with the Interface tab displayed.

4. Click the Ethernet Errors tab.

   The Ethernet Errors tab opens (Figure 51).

Figure 51 Ethernet Errors tab for MLT

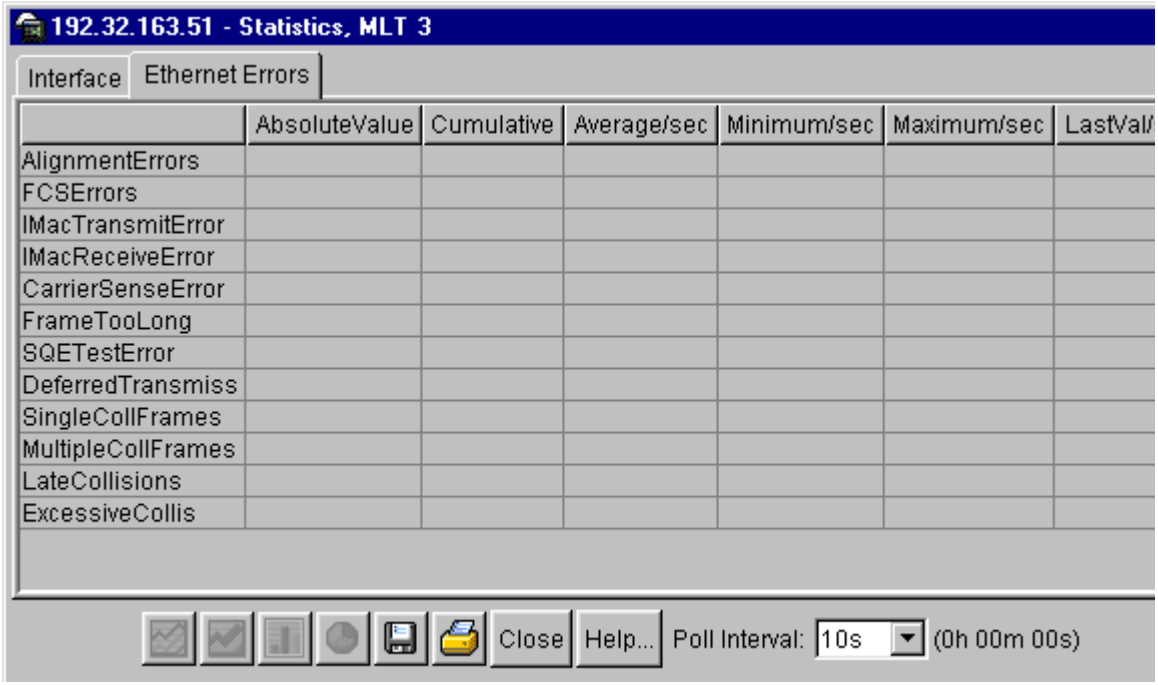


Table 44 describes the Ethernet Errors tab for MLT fields.

Table 44 Ethernet Errors tab for MLT fields

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

Table 44 Ethernet Errors tab for MLT fields (continued)

Field	Description
FrameTooLong	A count of frames received on a particular MLT that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions occur are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
SQETestError	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular MLT. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document.
DeferredTransmiss	A count of frames for which the first transmission attempt on a particular MLT is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions.
SingleCollFrames	A count of successfully transmitted frames on a particular MLT for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the MultipleCollisionFrames object.
MultipleCollFrames	A count of successfully transmitted frames on a particular MLT for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the SingleCollisionFrames object.
LateCollisions	The number of times that a collision is detected on a particular MLT later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
ExcessiveColls	A count of frames for which transmission on a particular MLT fails due to excessive collisions.

Chapter 5
Creating and managing VLANs

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

BayStack switch VLANs

A VLAN is a collection of ports on one or more switches that define a broadcast domain. BayStack support two types of VLANs:

- Port-based VLAN
- Protocol-based VLAN

For further information about VLANs on specific models, refer to *Using the BayStack 350 10/100/1000 Switch* (part number 309979-*x*), *Using the BayStack 410-24T 10BASE-T Switch* (part number 309985-*x*), and *Using the BayStack 450 10/100/1000 Series Switch* (part number 309978-*x*).

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

- VLANs must have unique VLAN IDs (VIDs) and names.
- An access port can belong to multiple protocol-based VLANs with a unique protocol in each VLAN. Access port can only belong to one of the protocol-based VLANS with the same protocol. However, a tagged trunk can belong to multiple-based VLANs with the same protocol.
- A port (access or tagged trunk) can belong to multiple port-based VLANs.

- A port (access or tagged trunk) can belong to a port *and* protocol-based VLAN.
- 410 and gigabyte MDA ports must be tagged trunks for a protocol-based VLAN.

Creating VLANs

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

VLAN Information

To open the VLAN dialog box:

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

The VLAN dialog box opens with the Basic tab displayed (Figure 52).

Figure 52 Basic tab

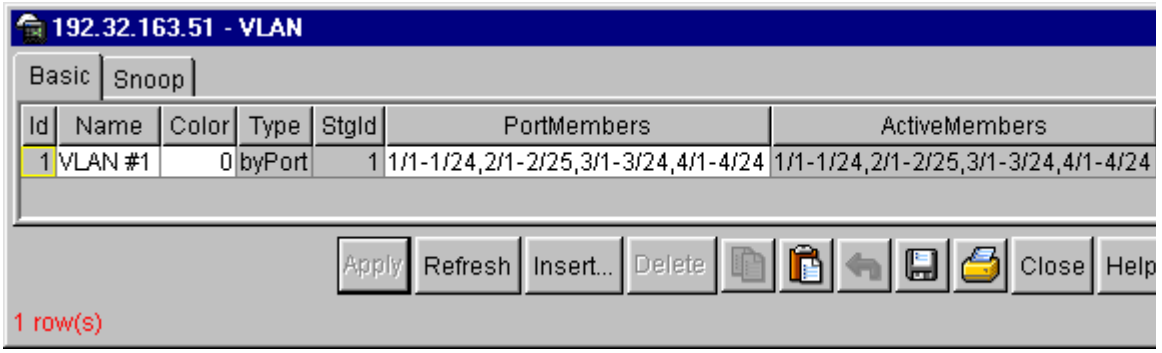


Table 45 describes the Basic tab fields.

Table 45 Basic tab fields

Field	Description
Name	Name of the VLAN.
Color	An administratively-assigned color code for the VLAN. The value of this object is used by the VLAN Manager GUI tool to select a color when it draws this VLAN on the screen.

Table 45 Basic tab fields (continued)

Field	Description
Type	Indicates the type of VLAN: byPort or byProtocolId.
StgId	Spanning tree group ID to which the VLAN belongs.
PortMembers	Ports that are members of the VLAN.
ActiveMember	Set of ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met.
ProtocolId	Protocol for protocol-based VLANs. This value is taken from the Assigned Numbers RFC. For port-based VLANs, none is the displayed value.
UserDefinedPid	When rcVlanProtocolId is set to usrDefined(15) in a protocol-based VLAN, this field represents the 16-bit user defined protocol identifier.

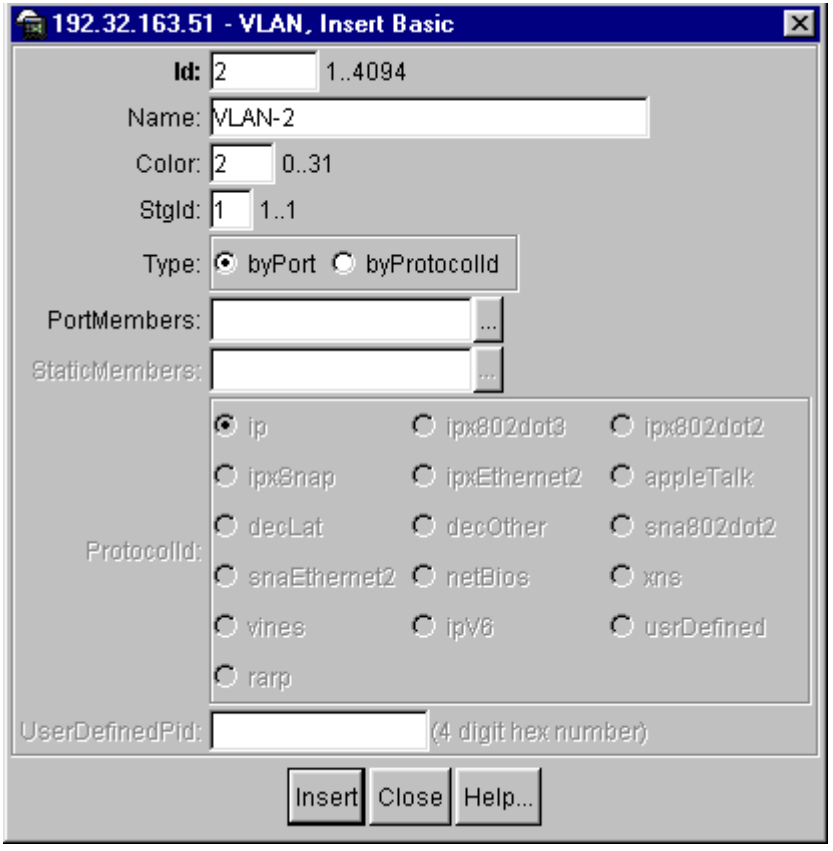
Creating a port-based VLAN

To create a port-based VLAN:

1 In the Basic tab (Figure 52 on page 122), click Insert.

The VLAN, Insert Basic dialog box for creating VLANs opens (Figure 53). This dialog box opens with the Type field set to byPort.

Figure 53 VLAN, Insert Basic dialog box for port-based VLANs



2 Type the (VLAN) ID.

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

3 Type the VLAN name (optional).

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

4 In the Type field, click byPort (if not already selected).

5 Specify the port membership by clicking the PortMembers text box.

6 Click Insert.

Creating a protocol-based VLAN

To create a protocol-based VLAN:

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

   The VLAN dialog box opens (Figure 52 on page 122) with the Basic tab displayed.

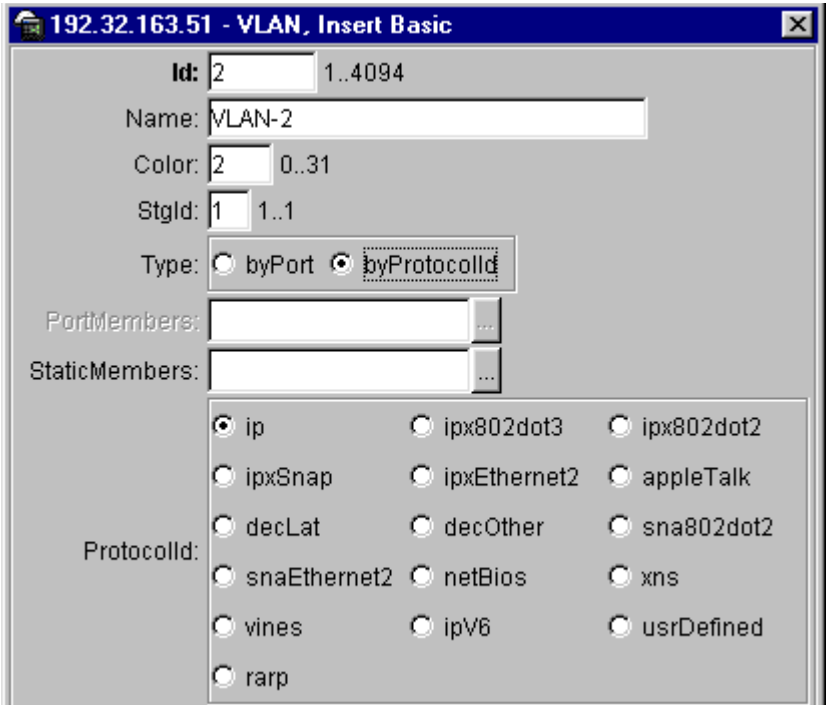
2. Click Insert.

   The VLAN, Insert Basic dialog box opens (Figure 53 on page 124).

3. Change the Type field to byProtocolID.

   The dialog box changes to display additional fields you need to set up protocol-based VLANs (Figure 54).

Figure 54 VLAN, Insert Basic dialog box for protocol-based VLANs



4. Type the unique VLAN ID in the Id field.

5 Type the VLAN name (optional).

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

6 In the Type field, click byProtocolID (if not already selected).

7 Click Insert.

Note: To assign BayStack 410 switches and gigabit MDA ports to a protocol-based VLAN, tag the port and select the port and choose Edit Port > VLAN.

Accepting tagged and untagged frames

In the switches, you can configure whether or not tagged frames are sent or received to the port level. Refer to "VLAN tab for a single port" on page 83 for VLAN tab field descriptions. Tagging is set as true or false for the port and applied to all VLANs on that port. You can select whether or not to discard:

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

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

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

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

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

To set a port to discard tagged frames it receives:

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

   The Port dialog box opens with the Interface tab displayed (Figure 35 on page 80).
3. Click the VLAN tab.

   The VLAN tab (Figure 36 on page 83) opens.
4. Check the DiscardTaggedFrames and the DiscardUntaggedFrames check boxes.
5. Click Apply.

Snoop tab

You can use the Snoop tab in the VLAN menu option to enable or disable the IGMP snooping on a BayStack switch.

To open the port-based VLAN:

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

   The VLAN dialog box opens with the Basic tab displayed (Figure 52 on page 122).

2. Click the Snoop tab.

   The Snoop tab opens (Figure 55).

Figure 55 Snoop tab

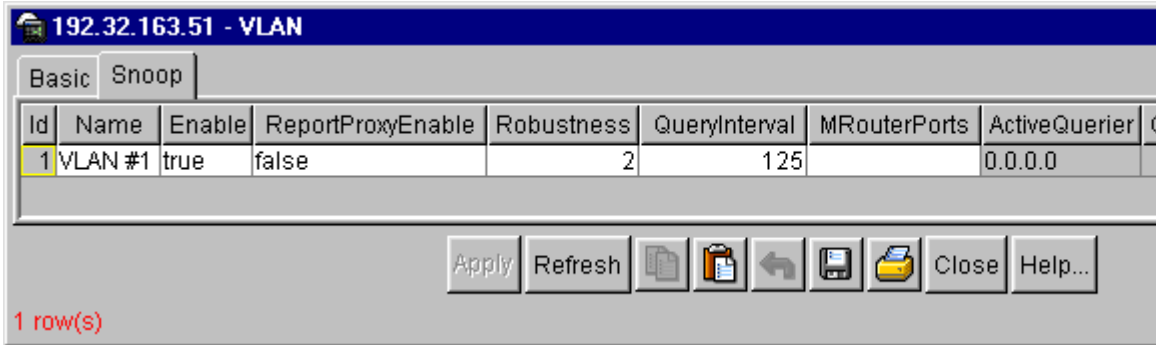


Table 46 describes the Snoop tab fields.

Table 46 Snoop tab fields

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

Note: Enable and ReportProxyEnable apply to ALL Vlans. Enabling (or disabling) for any active Vlan will enable (or disable) for all active Vlans.

Chapter 6
Troubleshooting with Device Manager

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

- Topology tab (next)
- Topology Table tab (page 132)

Topology tab

To view topology information:

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

The Diagnostics dialog box opens with the Topology tab displayed (Figure 56).

Figure 56 Topology tab

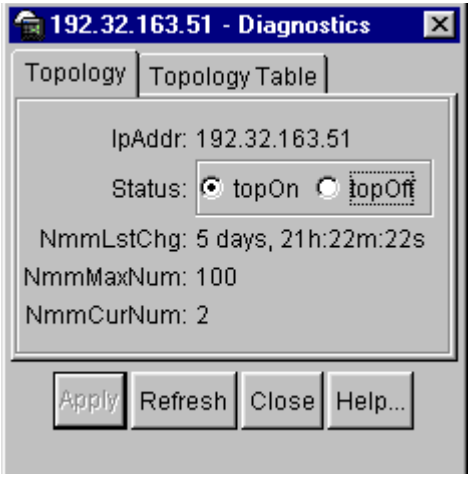


Table 47 describes the Topology tab items.

Table 47 Topology tab items

Item	Description
IpAddr	IP address of the device.
Status	Sets whether Nortel Networks topology is topOn or topOff for the device. The default value is On.
NmmLstChg	This is the value of sysUpTime the last time an entry in the network management MIB (NMM) topology table was added, deleted, or modified. If the table has not changed since the last cold or warm start of the agent, then the value is zero.
NmmMaxNum	Maximum number of entries in the NMM topology table.
NmmCurNum	Current number of entries in the NMM topology table.

Topology Table tab

To view more topology information:

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

   The Diagnostics dialog box opens with the Topology tab displayed (Figure 56 on page 131).

2. Click the Topology Table tab.

   The Topology Table tab opens (Figure 57).

Figure 57 Topology Table tab

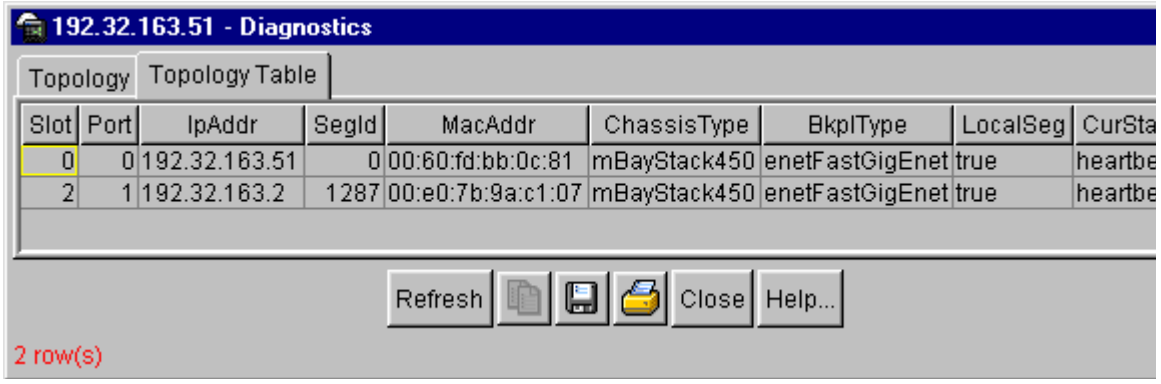


Table 48 describes the Topology Table tab fields.

Table 48 Topology Table tab fields

Field	Description
Slot	Slot number in the chassis in which the topology message was received.
Port	Port on which the topology message was received.
IpAddr	IP address of the sender of the topology message.
SegId	Segment identifier of the segment from which the remote agent sent the topology message. This value is extracted from the message.
MacAddr	MAC address of the sender of the topology message.
ChassisType	Chassis type of the device that sent the topology message.
BkplType	Backplane type of the device that sent the topology message.
LocalSeg	Indicates if the sender of the topology message is on the same Ethernet segment as the reporting agent.
CurState	Current state of the sender of the topology message. The choices are: • topChanged — Topology information has recently changed. • heartbeat — Topology information is unchanged. • new — The sending agent is in a new state.

Chapter 7
Monitoring switch performance

The Remote Network Monitoring (RMON) MIB is an interface between the RMON agent on a BayStack 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 especially suitable for Ethernet networks. The RMON agent continuously collects statistics and proactively monitors switch performance. You can view this data using the Device Manager.

RMON has three major functions:

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

Working with RMON information

You can view RMON information by looking at the Graph information associated with the port or chassis, or by using the Rmon menu option on the menu bar.

Rmon Ethernet statistics tab

Device Manager gathers Ethernet statistics that you can have graphed in a variety of formats, or you can save the statistics to a file and export them to a presentation or graphing application. To view RMON Ethernet statistics using the Graph information:

1 Select a port.

2 On the toolbar, click Graph.

The Port dialog box opens with the Interface tab displayed (Figure 35 on page 80).

3 Click the Rmon tab.

The Rmon tab opens (Figure 45 on page 105).

For descriptions of the Rmon tab fields, refer to Table 39 on page 106. For descriptions of the statistics columns, refer to Table 11 on page 41.

Viewing history

Ethernet History records periodic statistical samples from a network. A sample is called a history and is gathered in time intervals referred to as “buckets.” Histories establish a time-dependent method for gathering RMON statistics on a port. The value of these history records reflects what will be created if you use JDM to create new history control records. Control records and buckets are stored on the unit with the port they are monitoring. The default values for history are:

- Buckets are gathered for each port at 30-second and at 30-minute intervals.
- Number of buckets gathered is 6, 3 for each 30 second, and 3 for each 30 minute interval.

The BayStack 450 limits the number of history control records per unit to 85 and the number of actual stored buckets per unit to 255.

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.

RmonControl dialog box

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

To open the RmonControl dialog box:

➔ From the Device Manager main menu, choose Rmon > Control.

The RmonControl dialog box opens with the History tab displayed (Figure 58).

Figure 58 RmonControl dialog box

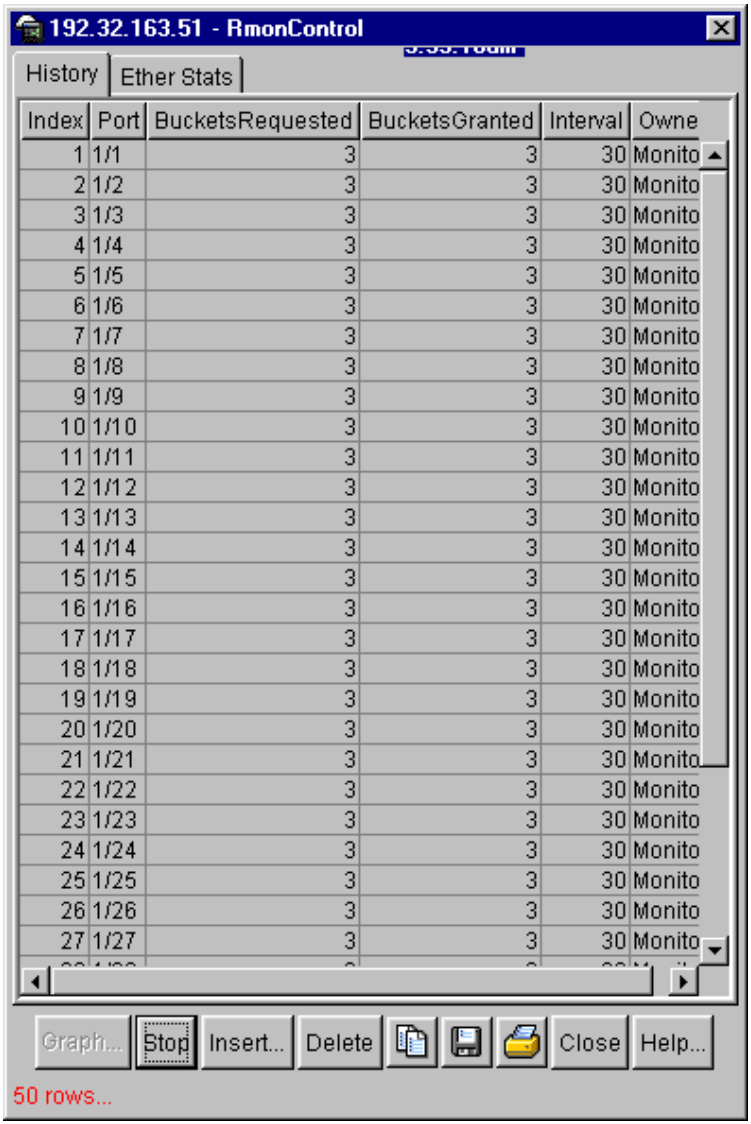


Table 49 describes the History tab fields.

Table 49 History tab fields

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

Creating a history

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

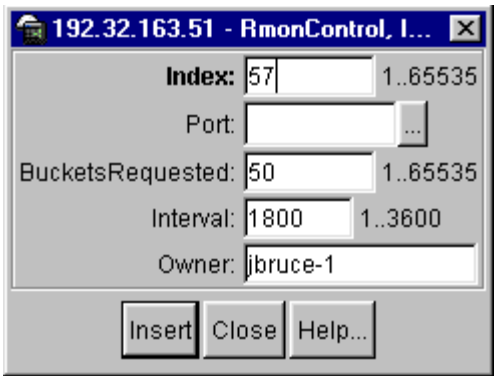
1. From the Device Manager main menu, choose Rmon > Control.

   The RmonControl dialog box opens with the History tab displayed (Figure 58 on page 137).

2. Click Insert.

   The RmonControl, Insert History dialog box opens (Figure 59).

Figure 59 RmonControl, Insert History dialog box



Refer to Table 49 on page 138 for a description of the RmonControl, Insert History dialog box fields.

3 Select the port from the port list or type the port number.

4 Set the number of buckets in the BucketsRequested field.

The default is 50.

5 Set the interval.

The default is 1800 seconds.

6 Type the owner, the network management system that created this entry.

7 Click Insert.

Disabling history

To disable RMON history on a port:

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

The RmonControl dialog box opens with the History tab displayed (Figure 58 on page 137).

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

3 Click Delete.

The entry is removed from the table.

Viewing a detailed history

To view a detailed history of a particular port in the history table:

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

   The RmonControl dialog box opens with the History tab displayed (Figure 58 on page 137).

2. Click on a port in the history table to highlight that port.

3. Click Graph.

   The RmonHistory Port number dialog box opens (Figure 60).

Figure 60 RmonHistory Port number dialog box

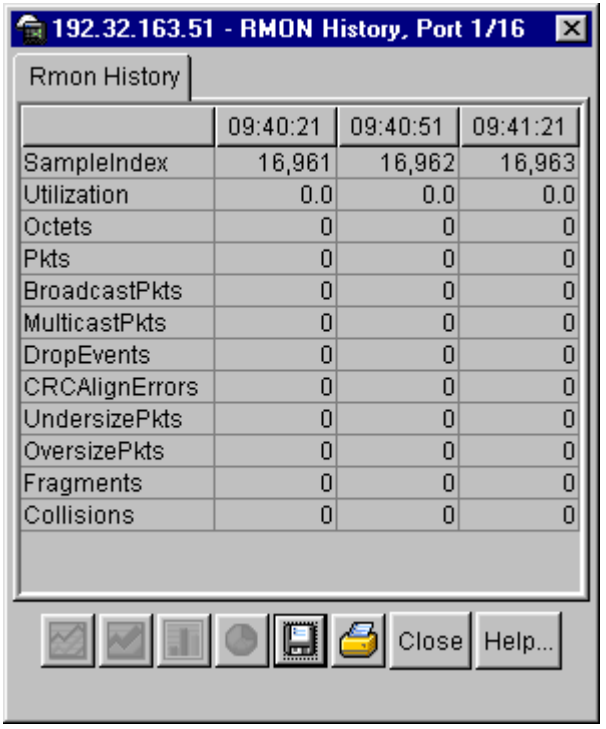


Table 50 describes the RMONHistory Port number tab fields.

Table 50 RMONHistory Port number tab fields

Field	Description
etherHistoryIndex	The history of which this entry is a part. The history identified by a particular value of this index is the same history as identified by the same value of historyControlIndex.
etherHistorySampleIndex	An index that uniquely identifies the particular sample this entry represents among all samples associated with the same historyControlEntry. This index starts at 1 and increases by one as each new sample is taken.
etherHistoryIntervalStart	The value of sysUpTime at the start of the interval over which this sample was measured. If the probe keeps track of the time of day, it should start the first sample of the history at a time such that when the next hour of the day begins, a sample is started at that instant. Note: Following this rule may require the probe to delay collecting the first sample of the history, as each sample must be of the same interval. The sample which is currently being collected is not accessible in this table until the end of its interval.
etherHistoryDropEvents	The total number of events in which packets were dropped by the probe due to lack of resources during this sampling 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.
etherHistoryOctets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
etherHistoryPkts	The number of packets (including bad packets) received during this sampling interval.
etherHistoryBroadcastPkts	The number of good packets received during this sampling interval that were directed to the broadcast address.
etherHistoryMulticastPkts	The number of good packets received during this sampling interval that were directed to a multicast address. Note that this number does not include packets addressed to the broadcast address.

Table 50 RMONHistory Port number tab fields (continued)

Field	Description
etherHistoryCRCAlignErrors	The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) 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 non-integral number of octets (Alignment Error).
etherHistoryUndersizePkts	The number of packets received during this sampling that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
etherHistoryOversizePkts	The number of packets received during this sampling that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
etherHistoryFragments	The total number of packets received during this sampling interval that were less than 64 octets in length (excluding graming bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherHistoryJabbers	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). The allowed range to detect jabber is between 20 ms and 150 ms.
etherHistoryCollisions	The best estimate of the total number of collisions on this Ethernet segment during this sampling interval. The value returned depends on the location of the RMON probe. Note: an RMON probe inside a repeater should ideally report collisions between the repeater and one or more other hosts as well as receiver collisions observed on any coax segments to which the repeater is connected.
etherHistoryUtilization	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Rmon Ether Stats tab

To use RMON to gather Ethernet statistics:

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

   The RmonControl dialog box opens with the History tab displayed (Figure 58 on page 137).

2. Click the Ether Stats tab.

   The Ether Stat tab opens (Figure 61).

Figure 61 Ether Stats tab

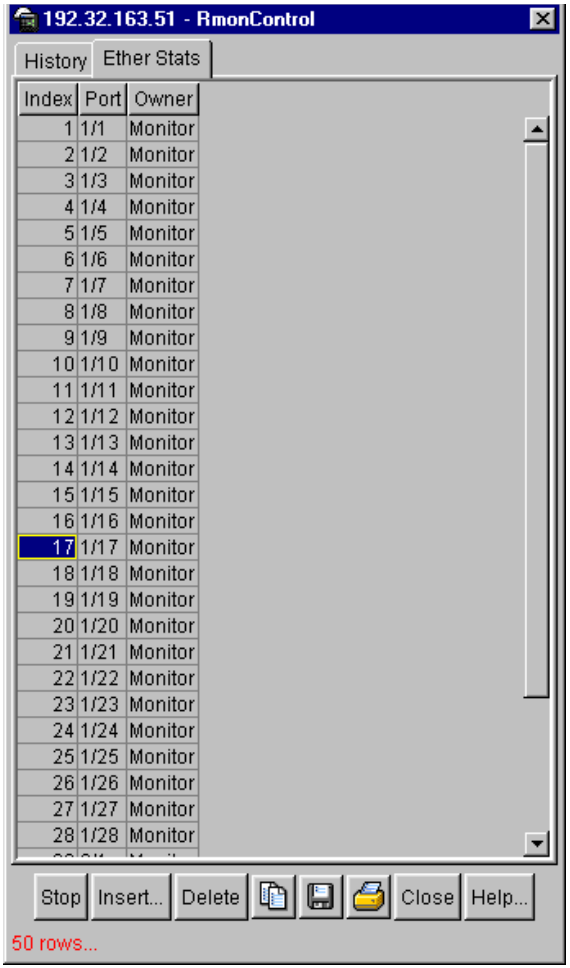


Table 51 describes the Ether Stats tab fields.

Table 51 Ether Stats tab fields

Field	Description
Port	Any Ethernet interface on the device.
Owner	The network management system that created this entry.

Gathering Ethernet statistics

To gather Ethernet statistics:

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

   The RmonControl dialog box opens with the History tab displayed (Figure 58 on page 137).

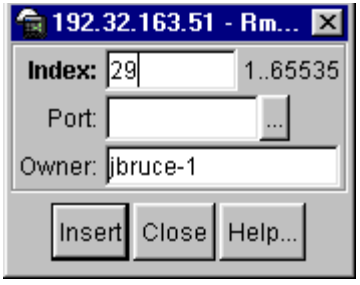
2. Click the Ether Stats tab.

   The Ether Stat tab opens (Figure 61 on page 143).

3. Click Insert.

   The RmonControl, Insert EtherStats dialog box opens (Figure 62).

Figure 62 RmonControl, Insert Ether Stats dialog box



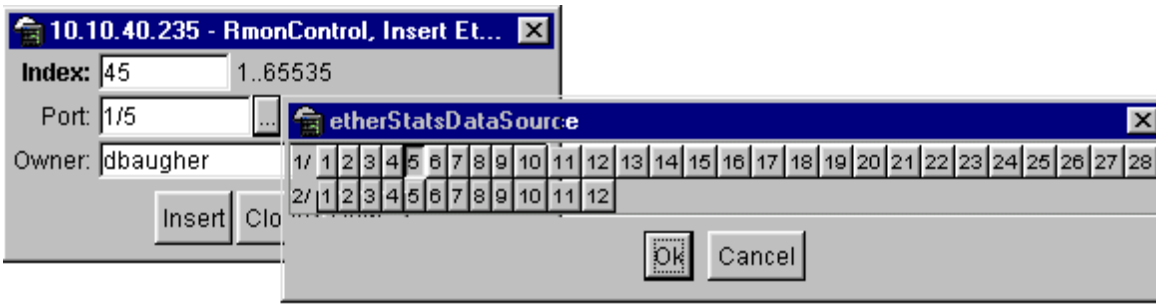
4. Enter the port number you want or select the port from the list menu

   Device Manager assigns the index.

5. Click Insert.

   The etherStatsDataSource dialog box opens with the port identified. (Figure 63).

Figure 63 etherStatsDataSource dialog box



6 Click Ok.

Disabling Ethernet statistics gathering

To disable Ethernet Statistics that you have set:

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

The RmonControl dialog box opens with the History tab displayed (Figure 58 on page 137).

2 Click the Ether Stats tab.

The Ether Stat tab opens (Figure 61 on page 143).

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

4 Click Delete.

Using alarms

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

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

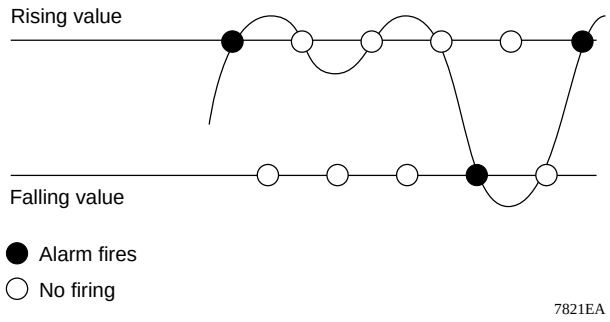
When alarms are activated, you can view the activity in a log or a trap log, or you can create a script to notify you by beeping a console, sending e-mail, or calling a pager.

How RMON alarms work

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

The alarm's upper limit is called the *rising value*, and its lower limit is called the *falling value*. RMON periodically samples the data based upon the alarm interval. During the *first* interval that the data passes above the rising value, the alarm fires as a rising event. During the first interval that the data drops below the falling value, the alarm fires as a falling event (Figure 64).

Figure 64 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.

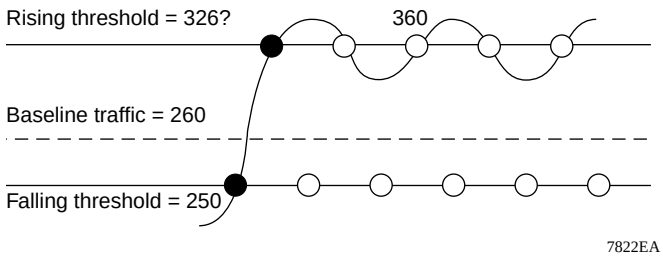
A general guideline is to define one of the threshold values to an expected, baseline value, then define the opposite threshold as the out-of-bounds limit. Because of sample averaging, the value may be equal to ±1 of the baseline units. For example, assume an alarm is defined on octets going out of a 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 64 octets are transmitted out of the port every 2 seconds, which is equivalent to baseline traffic of 320 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 320 and the upper limit is defined at 400 (or at any value greater than 320 + 64 = 384).

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 non baseline outbound traffic.

If the alarm is defined with a falling threshold less than 260 (assuming the alarm polling interval is 10 seconds), for example 250, then the rising alarm can fire only once (Figure 65). For the rising alarm to fire a second time, the falling alarm (the opposite threshold) must fire. Unless the port becomes inactive or spanning tree is disabled (which would cause the value for outbound octets to drop to zero), the falling alarm cannot fire because the baseline traffic is always greater than the value of the falling threshold. By definition, the failure of the falling alarm to fire prevents the rising alarm from firing a second time.

Figure 65 Alarm example — threshold less than 260



Creating alarms

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

When you create an alarm, you also select a sample type, which can be either absolute or delta. *Absolute* alarms are defined on the cumulative value of the alarm variable. An example of an alarm defined with absolute value is card operating status. Because this value is not cumulative, but instead represents states, such as card up (value 1) and card down (value 2), you set it for absolute value. Therefore, an alarm could be created with a rising value of 2 and a falling value of 1 to alert a user to whether the card is up or down.

Most alarm variables related to Ethernet traffic are set to *delta* value. Delta alarms are defined based on the difference in the value of the alarm variable between the start of the polling period and the end of the polling period. Delta alarms are sampled twice per polling period. For each sample, the last two values are added together and compared to the threshold values. This process increases precision and allows for the detection of threshold crossings that span the sampling boundary. If you track the current values of a given delta-valued alarm and add them together, therefore, the result is twice the actual value. (This result is not an error in the software.)

Alarm Manager dialog box

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

1. On the main menu of the Device Manager, select a port on the stack where you created an alarm.
2. On the toolbar, click Alarm Manager.

   The Alarm Manager dialog box opens (Figure 66) and displays the statistics for the chosen port.

Figure 66 Alarm Manager dialog box

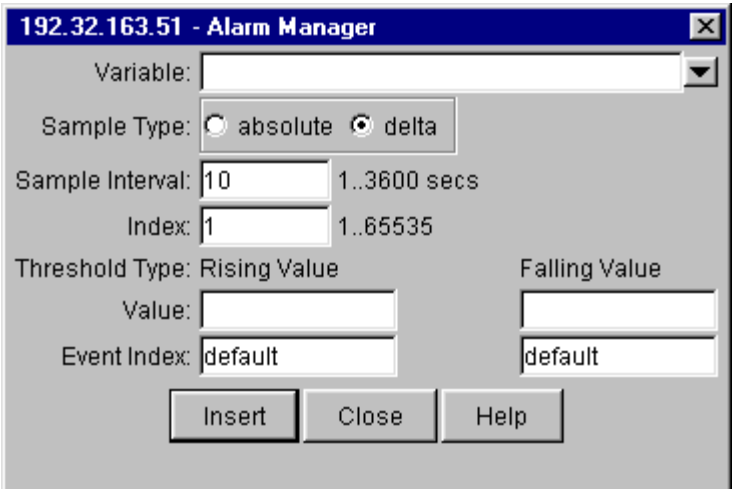


Table 52 describes the Alarm Manager dialog box items.

Table 52 Alarm Manager dialog box items (1 of 2)

Item	Description
Variable	Name and type of alarm—indicated by the format: *alarmname.x* where x=0 indicates a chassis alarm. *alarmname.* where the user must specify the index. This will be a card number for module-related alarms, an STG ID for spanning tree group alarms (the default STG is 1, other STG IDs are user-configured), or the Ether Statistics Control Index for Rmon Stats alarms *alarmname* with no dot or index is a port-related alarm and results in display of the port selection tool.
Sample Type	Select either absolute or delta. For more information about sample types, refer to "Creating alarms" on page 147.
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.

Table 53 Alarm Manager dialog box items (2 of 2)

Item	Description	
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.)

Example alarm

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

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

1 Do one of the following:

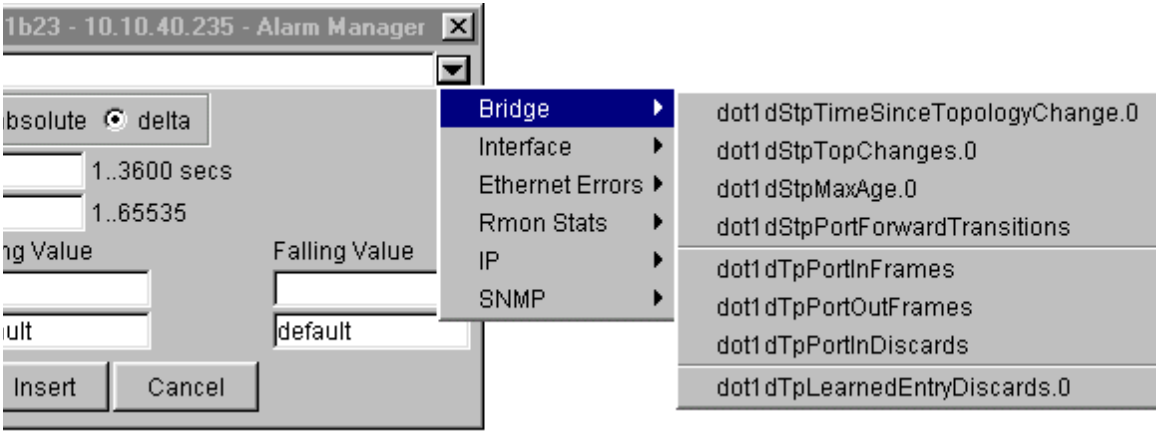
- From the Device Manager main menu, choose Rmon > Alarm Manager.
- On the toolbar, click Alarm Manager.

The Alarm Manager dialog box opens (Figure 66 on page 149).

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

Refer to the Alarm variables list (Figure 67).

Figure 67 Alarm variables list



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

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

3. For this example, select Bridge > dot1dStpTopChanges.0 from the variable list. (Refer to Appendix B, “RMON alarm variables,” on page 215 for a definition of the variable). The example is a chassis alarm, indicated by the “.0” in the variable.
4. For this example, select a rising value of 4 and a falling value of 0.
5. Leave the remaining fields at their default values, including a sample type of Delta.
6. Click Insert.

Alarms tab

You can define or delete an alarm for any MIB that resolves to an integer value. Do not use string variables (such as system description) as alarm variables.

To open the Alarms tab:

➔ From the Device Manager main menu, choose Rmon >Alarms.

The RmonAlarms dialog box opens with the Alarms tab (Figure 68) displayed.

Figure 68 Alarms tab

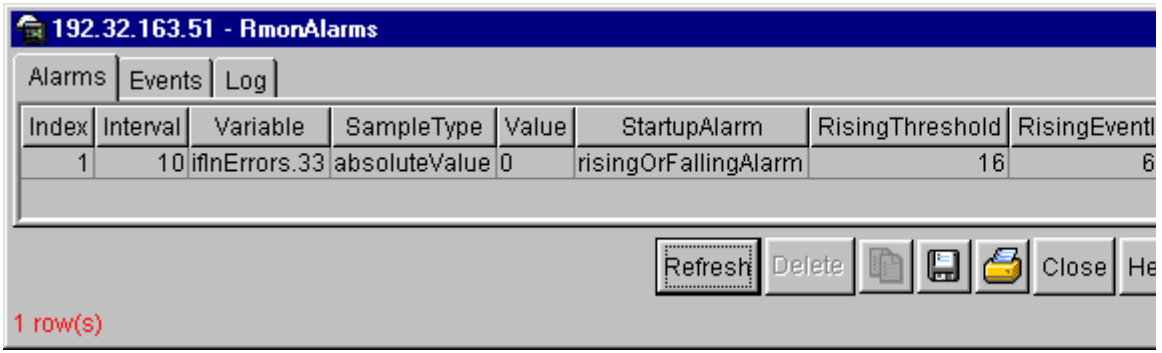


Table 54 describes the Alarms tab fields.

Table 54 Alarms tab fields

Field	Description
Interval	The interval in seconds over which data is sampled and compared with the rising and falling thresholds. When setting this variable, note that in the case of deltaValue sampling, you should set the interval short enough so that the sampled variable is very unlikely to increase or decrease by more than 2^31 - 1 during a single sampling interval.
Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Counter, Gauge, or TimeTicks) may be sampled.

Table 54 Alarms tab fields (continued)

Field	Description
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue(1), the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue(2), the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.
Value	The value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value is the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value is the sampled value at the end of the period. This is the value that is compared with the rising and falling thresholds. The value during the current sampling period is not made available until the period is completed and remains available until the next period completes.
StartupAlarm	The alarm that may be sent when this entry is first set to valid. If the first sample after this entry becomes valid is greater than or equal to the risingThreshold and alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3), then a single rising alarm is generated. If the first sample after this entry becomes valid is less than or equal to the fallingThreshold and alarmStartupAlarm is equal to fallingAlarm(2) or risingOrFallingAlarm(3), then a single falling alarm is generated.
RisingThreshold	A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal to this threshold and the associated alarmStartupAlarm is equal to risingAlarm(1) or risingOrFallingAlarm(3). After a rising event is generated, another such event is not generated until the sampled value falls below this threshold and reaches the alarmFallingThreshold.
RisingEventIndex	The index of the eventEntry that is used when a rising threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of the eventIndex object. If there is no corresponding entry in the eventTable, then no association exists. In particular, if this value is zero, no associated event is generated, because zero is not a valid event index.

Table 54 Alarms tab fields (continued)

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

Deleting an alarm

To delete an alarm:

1. From the Device Manager main menu, choose Rmon >Alarms.

   The RmonAlarms dialog box opens with the Alarms tab displayed (Figure 68 on page 152).

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

Working with events

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

When RMON is globally enabled, two default events are generated:

- RisingEvent
- FallingEvent

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

Events tab

Items in the Events tab specify whether a trap, a log, or a trap and a log is generated to view alarm activity.

To view the Events tab:

1. From the Device Manager main menu, choose Rmon > Alarm.

   The RmonAlarm dialog box opens with the Alarms tab displayed (Figure 68 on page 152).

2. Click the Events tab.

   The Events tab opens (Figure 69).

Figure 69 Events tab

Table 55 describes the Events tab fields.

Table 55 Events tab fields

Field	Description
Index	Uniquely identifies an entry in the event table. Each entry defines one event that is to be generated when the appropriate conditions occur.
Description	Specifies whether the event is a rising or falling event.
Type	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	The network management system that created this entry.
Status	Normally valid. A not-valid field indicates that an SNMP agent other than the Device Manager has tried to modify an RMON parameter or that network conditions have corrupted an SNMP packet sent by the Device Manager. The status would temporarily appear as “under creation” and then the status would become either “valid” or the field would be deleted.

Creating an alarm event

To create an alarm event:

1. From the Device Manager main menu, choose Rmon > Alarms.

   The RmonAlarm dialog box opens with the Alarms tab displayed (Figure 68 on page 152).

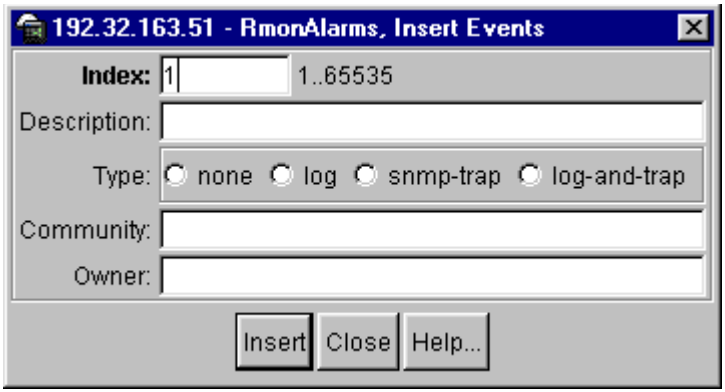
2. Click the Events tab.

   The Events tab opens (Figure 69 on page 155).

3 Click Insert.

The RmonAlarms, Insert Events dialog box opens (Figure 70).

Figure 70 RmonAlarms, Insert Events dialog box



4 In the Description field, enter a name for the event.

5 Select the type of event you want.

Default is log-and-trap. You can set the event type to log to reduce traffic from the switch or to snmp-trap to save memory or for better CPU utilization. If you select snmp-trap or log-and-trap, you must set trap receivers.

6 Click Insert.

The new event is displayed in the Events dialog box.

Table 56 describes the RmonAlarms, Insert Events dialog box items.

Table 56 RmonAlarms, Insert Events dialog box items

Item	Description
Index	Uniquely identifies an entry in the event table. Each entry defines one event that is to be generated when the appropriate conditions occur.
Description	Specifies whether the event is a rising or falling event.

Table 56 RmonAlarms, Insert Events dialog box items (continued)

Item	Description
Type	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.
Owner	The network management system that created this entry.

Deleting events

To delete an event:

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

   The event is removed from the table.

Log tab

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

To view the Log tab:

1. From the Device Manager main menu, choose Rmon > Alarm.

   The RmonAlarm dialog box opens with the Alarms tab displayed (Figure 68 on page 152).
2. Click the Log tab.

   The Log tab opens (Figure 71).

Figure 71 Log tab

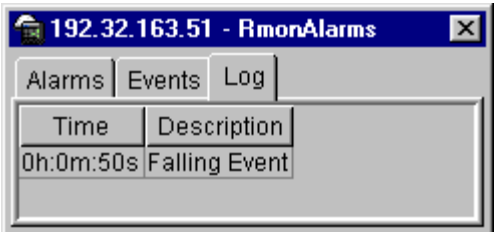


Table 57 describes the Log tab fields.

Table 57 Log tab fields

Field	Description
Time	The value of sysUpTime when this entry was created.
Description	Specifies whether the event is a rising or falling event.

HP OpenView

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

To integrate RMON into HP openView:

1. To see the path, enter the following:

   ```
   setenv | grep PATH
   ```

2. 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:.
   ```

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

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

   `dm/hpov/baystack_mibs`

4. Load each of the MIB files in the following order:

   bayAgent.mib

   bayChas.mib

   bayChasTraps.mib

   bayEMTmib

   baylfex.mib

   bayS5Reg.mib

   bayS5Rt.mib

   bayS5Tcs.mib

   baySRoot.mib

   rc_vlan.mib

   rfc1213.mib

   rfc1215.mib

   rfc1447.mib

   rfc1450.mib

   rfc1493.mib

   rfc1573_bs.mib

   rfc1573_rcc.mib

   rfc1643.mib

   rfc1757.mib

   rfc1757_rcc.mib

   rfc1907.mib

Now you can start HP OpenView.

Log only event bug

HP OpenView versions 4.0 and 5.0 contain bugs that do not affect the integrity of the product when it stands alone. However, when combined with Device Manager, unexpected results occur. The “Log only” event categorization bug in HP OpenView 4.0 causes traps to be written to the ASCII trap log file and to be displayed in the event browser.

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

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

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

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

To display a standard SNMP traps in the event browser for HP OpenView 5.0:

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

   Your choices are Error Events, Threshold Events (normally used for RMON alarms), Status Events, Configuration Events, or Application Alert Events.
5. Click OK.
6. Choose File > Save.

Chapter 8
Setting up bridging

The Bridge parameters allow you to configure the global Spanning Tree and to view MAC address table for a BayStack 350/410/450 switch. Bridge information also includes Spanning Tree Group (STG) information.

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

Base tab

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

To view the Base tab:

➔ From the Device Manager menu bar, select Edit > Bridge.

The Bridge dialog box opens with the Base tab displayed (Figure 72).

Figure 72 Base tab

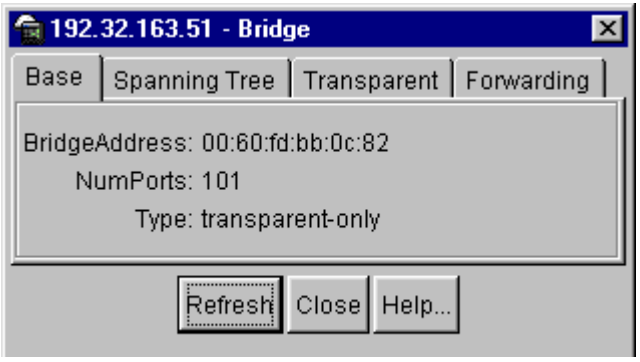


Table 58 describes the Base tab fields.

Table 58 Base tab fields

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

Spanning Tree tab

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

To view the Spanning Tree tab:

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

   The Bridge dialog box opens, with the Base tab displayed.

2. Click the Spanning Tree tab.

   The Spanning Tree tab opens (Figure 73).

Figure 73 Spanning Tree tab

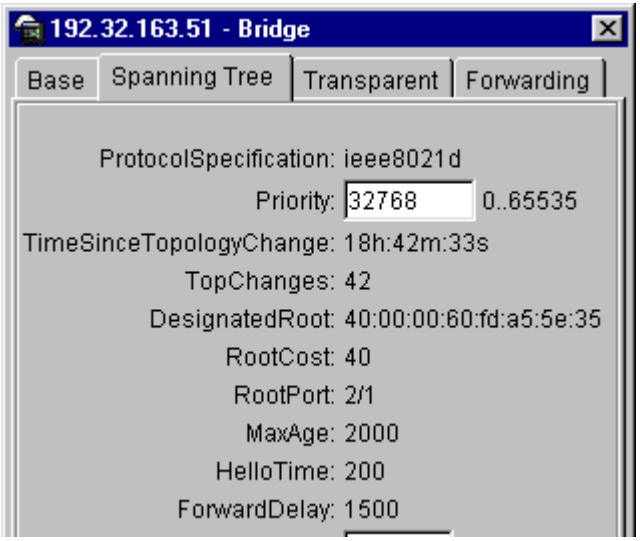


Table 59 describes the Spanning Tree tab fields.

Table 59 Spanning Tree tab fields

Field	Description
ProtocolSpecification	Version of the spanning tree protocol being run. Values include: • decLb100: Indicates the DEC LANbridge 100 spanning tree protocol. • ieee8021d: IEEE 802.1d implementations will return this entry. When future versions of the IEEE spanning tree protocol are released that are incompatible with the current version, a new value will be defined.
Priority	Value of the writable portion of the bridge ID. That is, the first two octets of the (8-octet long) bridge ID. The last six octets of the bridge ID are given by the value of BridgeAddress.
TimeSinceTopologyChange	Time (in hundredths of a second) since the last time a topology change was detected by the bridge entity.
TopChanges	Number of topology changes detected by this bridge since the management entity was reset or initialized.

Table 59 Spanning Tree tab fields (continued)

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

Table 59 Spanning Tree tab fields (continued)

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

Transparent tab

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

To view the Transparent tab:

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

   The Bridge dialog box opens, with the Base tab displayed (Figure 72 on page 164).

2. Click the Transparent tab.

   The Transparent tab opens (Figure 74).

Figure 74 Transparent tab

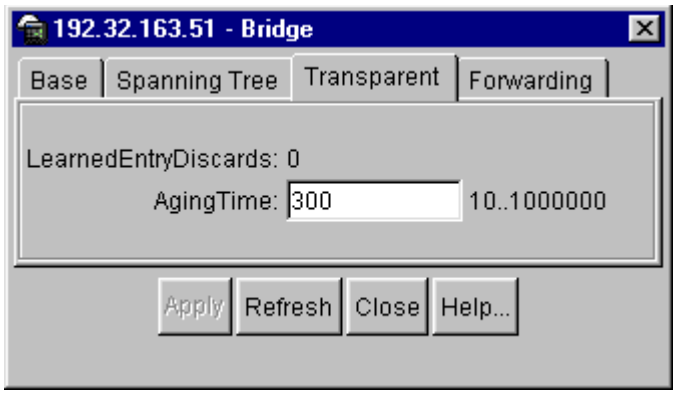


Table 60 describes the Transparent tab items.

Table 60 Transparent tab items

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

Forwarding tab

The Forwarding tab displays the MAC forwarding database.

To view the Forwarding tab:

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

The Bridge dialog box opens, with the Base tab displayed (Figure 72 on page 164).

2 Click the Forwarding tab.

The Forwarding tab opens (Figure 75).

Figure 75 Forwarding tab

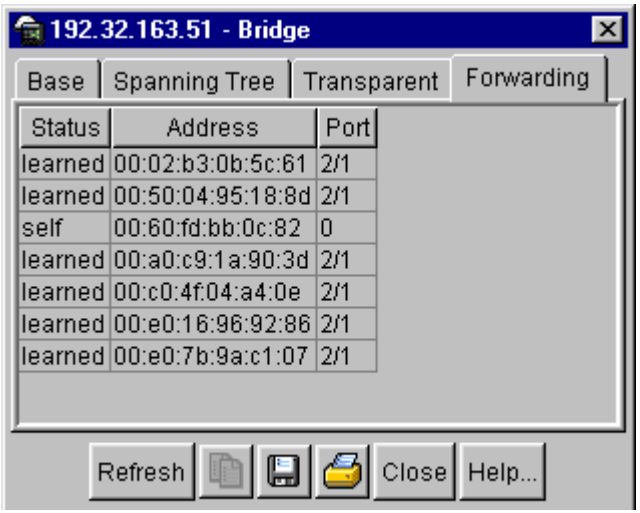


Table 61 describes the Forwarding tab fields.

Table 61 Forwarding tab fields

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

Spanning tree group (STG)

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

Configuration tab

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

To view the Configuration tab:

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

The STG dialog box opens, with the Configuration tab displayed (Figure 76).

Figure 76 Configuration tab

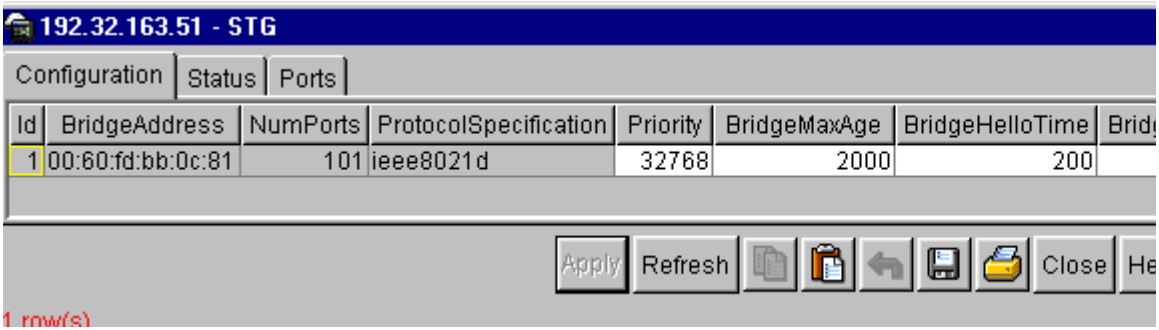


Table 62 describes the Configuration tab items.

Table 62 Configuration tab items

Item	Description
ID	An identifier used to identify a STG in the device.
BridgeAddress	MAC address used by a bridge when it is referred to in a unique fashion. It is recommended that the number be the smallest MAC address of all ports belonging to the bridge. However, it is only required to be unique. When concatenated with Priority, a unique bridge identifier is formed that is used in the spanning tree protocol.
NumPorts	Number of ports controlled by this bridging entity.

Table 62 Configuration tab items (continued)

Item	Description
ProtocolSpecification	Version of the spanning tree protocol being run. Values include: • decLb100: Indicates the DEC LANbridge 100 spanning tree protocol. • ieee8021d: IEEE 802.1d implementations will return this entry. When future versions of the IEEE spanning tree protocol are released that are incompatible with the current version, a new value will be defined.
Priority	Value of the writable portion of the bridge ID. That is, the first two octets of the (8-octet long) bridge ID. The last six octets of the bridge ID are given by the value of BridgeAddress.
BridgeMaxAge	Value that all bridges use for the maximum age of this bridge when it is acting as the root. **Note**: 802.1D-1990 specifies that the range is related to the value of BridgeHelloTime. The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error may be returned if the value set is not a whole number.
BridgeHelloTime	Value that all bridges use for HelloTime when this bridge is acting as the root. **Note**: The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error may be returned if the value set is not a whole number.
BridgeForwardDelay	Value that all bridges use for ForwardDelay when this bridge is acting as the root. **Note**: 802.1D-1990 specifies that the range is related to the value of BridgeHelloTime. The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error may be returned if the value set is not a whole number.
PortMembers	Bit-field used to identify the ports in the system that are members this STG. The bit-field is 32 octets long representing ports 0 to 255 (inclusive).

Status tab

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

To view the Status tab:

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

   The STG dialog box opens, with the Configuration tab displayed (Figure 76 on page 171).

2. Click the Status tab.

   The Status tab opens (Figure 77).

Figure 77 Status tab

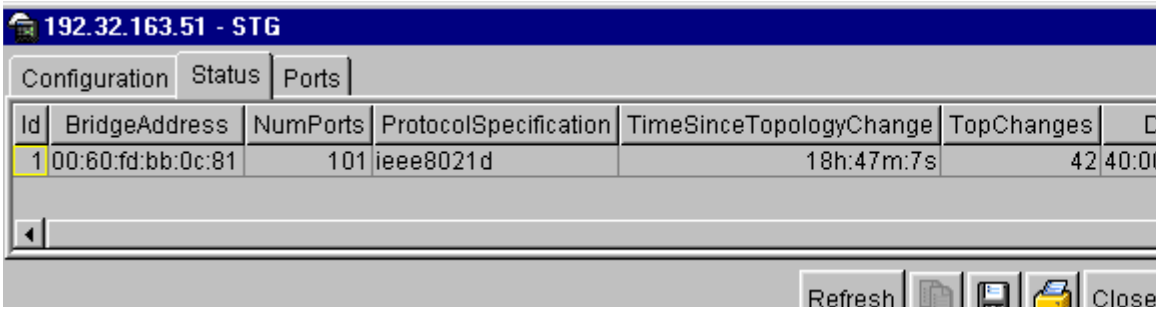


Table 63 describes the Status tab fields.

Table 63 Status tab fields

Field	Description
ID	An identifier used to identify a STG in the device.
BridgeAddress	MAC address used by a bridge when it is referred to in a unique fashion. It is recommended that the number be the smallest MAC address of all ports belonging to the bridge. However, it is only required to be unique. When concatenated with Priority, a unique bridge identifier is formed that is used in the spanning tree protocol.
NumPorts	Number of ports controlled by this bridging entity.

Table 63 Status tab fields (continued)

Field	Description
ProtocolSpecification	Version of the spanning tree protocol being run. Values include: • decLb100: Indicates the DEC LANbridge 100 spanning tree protocol. • ieee8021d: IEEE 802.1d implementations will return this entry. When future versions of the IEEE spanning tree protocol are released that are incompatible with the current version, a new value will be defined.
TimeSinceTopologyChange	Time (in hundredths of seconds) since the last topology change was detected by the bridge entity.
TopChange	Number of topology changes detected by the bridge since the management entity was last reset or initialized.
DesignatedRoot	Bridge identifier of the root of the spanning tree as determined by the spanning tree protocol. The value is used as the root identifier parameter in all configuration bridge PDUs originated by this node.
RootCost	Cost of the path to the root as seen from the bridge.
RootPort	Port that has the lowest cost path from the bridge to the root bridge.
MaxAge	Maximum age of spanning tree protocol information learned from the network on any port before it is discarded, in units of hundredths of a second. This is the actual value that this bridge is currently using.
HelloTime	Amount of time between the transmission of configuration bridge PDUs by this node on any port when it is the root of the spanning tree (in hundredths of a seconds). This is the actual value that this bridge is currently using.

Table 63 Status tab fields (continued)

Field	Description
HoldTime	Value of the interval length during which no more than two configuration bridge PDUs shall be transmitted by this node (in hundredths of a second).
ForwardDelay	This time value (in hundredths of a seconds) that controls how fast a port changes its spanning state when moving towards the forwarding state. Value determines how long the port stays in each of the listening and learning states, which precede the forwarding state. This is also used when a topology change has been detected and is underway, to age all dynamic entries in the forwarding database. **Note**: This value is the one that this bridge is currently using, in contrast to BridgeForwardDelay which is the value that this bridge and all others would start using if/when this bridge were to become the root.

Ports tab

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

To view the Ports tab:

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

   The STG dialog box opens, with the Configuration tab displayed (Figure 76 on page 171).

2. Click the Ports tab.

   The Ports tab opens (Figure 78).

Figure 78 Ports tab

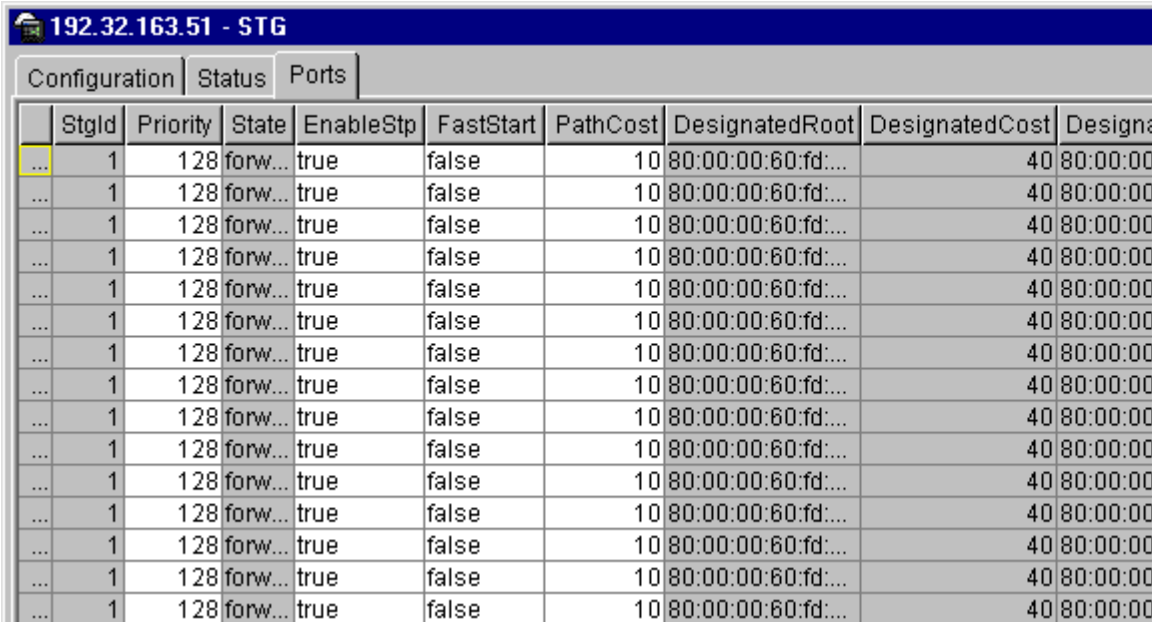


Table 64 describes the Ports tab fields.

Table 64 Ports tab fields

Field	Description
StgId	STG identifier assigned to this port.
Priority	Value of the priority field contained in the first octet of the port ID. The other octet is given by the value of the “rcStgPort.”
State	The current state of the port as defined by application of the “Spanning Tree Protocol.” These are the instructions the port takes on a frame when it is received. If the bridge detects a port is malfunctioning, it will list it as “broken(6).” For ports that are disabled, the value is “disabled(1).”
EnableStp	Enables (True) or disables (False) the spanning tree of the port.
FastStart	When this is enabled (True), the port is move to forwarding or blocking state in 4 seconds.
PathCost	Contribution of the port to the pathcost of paths towards the spanning tree root, including the current port. 802.1D-1990 specifications recommends that the default of this parameter be in inverse proportion to the speed of the attached LAN.

Table 64 Ports tab fields (continued)

Field	Description
DesignatedRoot	The unique “Bridge Identifier.” This is recorded as Root in the configuration bridge PDUs transmitted by the Designated Bridge for the segment to which the port is attached.
DesignatedCost	Path cost of the Designated Port of the segment connected to the port. The value is compared to the Root Path Cost field in received bridge PDUs.
DesignatedBridge	Bridge identifier of the bridge that this port considers to be the Designated Bridge for this port's segment.
DesignatedPort	Port identifier of the port on the Designated Bridge for this port's segment.
ForwardTransitions	Number of times this port has transitioned from the learning state to the forwarding state.

Chapter 9
Setting up ATM

The ATM options provide information about the portion of the management information base (MIB) that manages ATM LAN emulation client (LEC) nodes and the Media dependant adapter (MDA).

From the Edit submenu, you can select two ATM parameters:

- "Atm LEC" (next)
- "Atm MDA" on page 197

Note: The ATM option is supported only in rev D or higher of the BayStack 350 and the BayStack 450.

Atm LEC

The Atm LEC allows applications to flow across an ATM network just as they would on an Ethernet network. The Atm LEC is an Ethernet port in a virtual LAN network that has its own ATM address.

This section describes the ATM information available in Device Manager on the following tabs:

- Ports tab (page 180)
- Status tab (page 181)
- Basic tab (page 184)
- Timers tab (page 188)

- Others tab (page 190)
- Server VCCs tab (page 192)
- MacAddress tab (page 194)
- ARP tab (page 195)

Ports tab

You use the Ports tab to manage Atm LEC specific options.

To view the Ports tab:

➔ From the Device Manager menu bar, select Edit > Atm LEC.

The AtmLec dialog box opens with the Ports tab displayed (Figure 79).

Figure 79 Ports tab

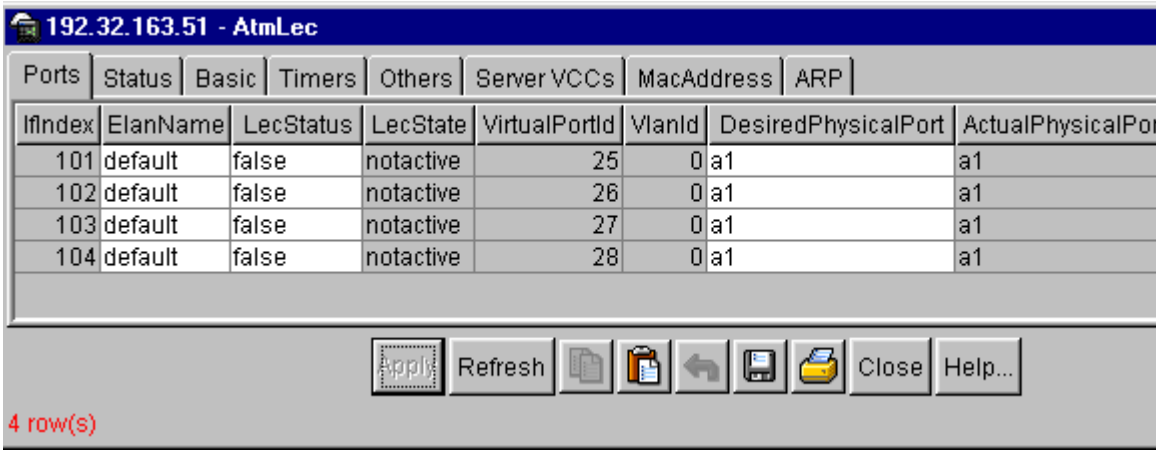


Table 65 describes the Ports tab fields.

Table 65 Ports tab fields

Field	Description
IfIndex	An index value used to identify a LAN emulation client (LEC) instance. Each LEC is treated as a logical port; therefore, each LEC has a unique row in the “ifTable” and “rcPort” tables.
ElanName	The ELAN Name this client uses the next time it returns to the its initial state.
LecStatus	A read/write value used to enable(true)/disable(false) the LEC.
LecState	Indicates the current state of the LEC.
VirtualPortId	Indicates the virtual port mapping of the LEC.
VlanId	Indicates the VLAN Id membership of the LEC. A values of zero (0) indicates no membership.
DesiredPhysicalPort	The entry is used to configure the desired physical port the LEC instance should associate with. Each LEC can only be associated with one physical port, which then can support one or more LEC instances. This object can only be written when the status of the LEC is disabled.
ActualPhysicalPort	This entry is used to display the actual port the LEC instance should associate with. Each LEC can only be associated with one physical port, which can then support one or more LEC instances.
FailoverEnable	This entry is used enable or disable the failover feature for the LEC instance. Failover allows traffic to be moved from a failing port to the another available port. Use the ActualPhysicalPort to identify the port currently carrying the traffic. Use the DesiredPhysicalPort to select a preferred port.

Status tab

The Status tab is a read-only table containing identification, status, and operational information about the LAN emulation clients this agent manages.

To view the Status tab:

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

The AtmLec dialog box opens with the Ports tab displayed (Figure 79 on page 180).

2 Click the Status tab.

The Status tab opens (Figure 80).

Figure 80 Status tab

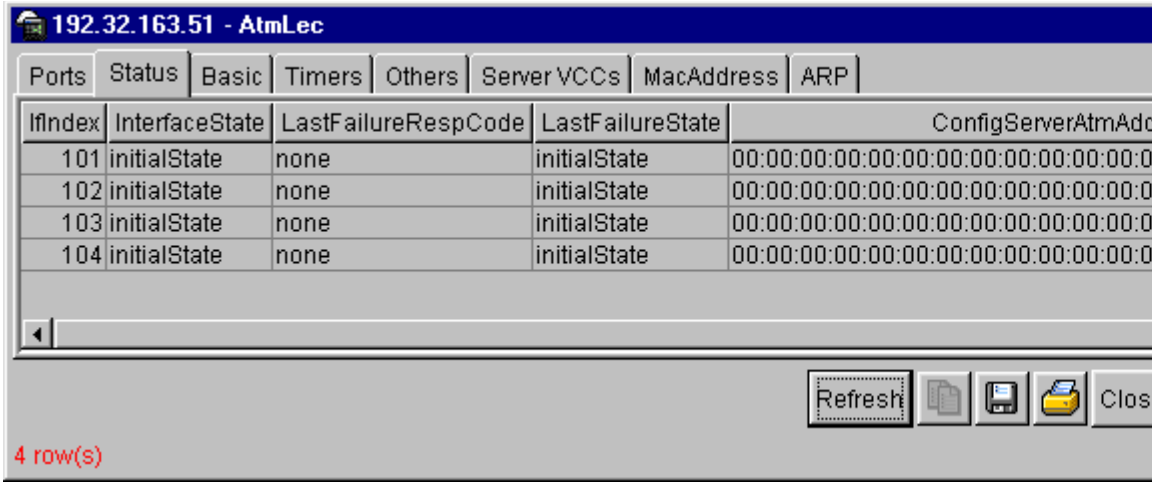


Table 66 describes the Status tab fields.

Table 66 Status tab fields

Field	Description
IfIndex	Identifies the logical interface number assigned to the client, and is used to identify corresponding rows in the interfaces MIB. **Note**: Re-initialization of the management agent may cause the `IfIndex` of a client to change.
InterfaceState	Current state of the LAN emulation client.
LastFailureRespCode	Status code from the last failed configure response or join response. Failed responses are those that the configure response / join response frame contains a non-zero code, or fails to arrive within a time-out period. If none of this client's requests have failed, this object has the value none. If the failed response contained a status code that is not defined in the LAN emulation specification, this object has the value of `undefinedError`. The value `timeout` is self-explanatory. Other failure codes correspond to those defined in the specification, although they may have different numeric values.

Table 66 Status tab fields (continued)

Field	Description
LastFailureState	State the client was in when updated by the LastFailureRespCode. If LastFailureRespCode is none, then this object has the value initialState.
ConfigServerAtmAddress	The ATM address of the LAN emulation configuration server (if known) or the empty string.
ConfigSource	Indicates whether the LAN emulation client used the LAN emulation configuration server, and, if so, what method it used to establish the configuration direct VCC. The value `configInProgress` indicates configuration is in progress, and may be used to troubleshoot LECs in the configuration phase.
ActualLanType	Data frame format that this LAN Emulation Client is using right now. This may come from • ConfigLanType • LAN Emulation Configuration Server • LAN Emulation Server This value is related to `ifMtu` and `ifType`. See the LEC management specification for more details.
ActualMaxDataFrameSize	Maximum Data Frame Size. The maximum data frame size that this LAN Emulation client is using right now. This may come from • ConfigMaxDataFrameSize • LAN emulation configuration server • LAN emulation server
ActualLanName	The identity of the emulated LAN (ELAN) that this client last joined or wants to join. This may come from: • ConfigLanName • LAN emulation configuration server • LAN emulation server
ActualLesAtmAddress	LE Server ATM Address. The LAN Emulation Server address currently in use or most recently attempted. If no LAN Emulation Server attachment has been tried, this object's value is the zero-length string.

Basic tab

The Basic tab describes the LECs executed by the host. Each LEC has a row in the MIB-II/RFC interface table that describes the emulated packet interface it displays to higher layers. Each LEC also has a row in this and other LLEC MIB tables that describes its interface with other LAN emulation components. This table contains configuration variables, three extension tables contain client status, performance statistics, and information about control/multicast VCCs.

LECs are created by management. However, the Basic tab does not directly support row creation.

To view the Basic tab:

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

   The AtmLec dialog box opens with the Ports tab displayed (Figure 79 on page 180).

2. Click the Basic tab.

   The Basic tab opens (Figure 81).

Figure 81 Basic tab

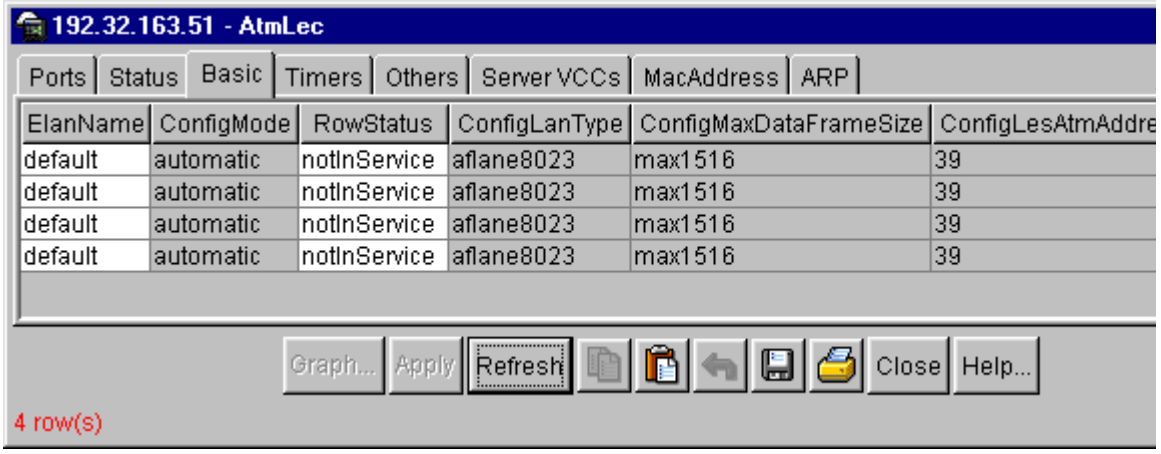


Table 67 describes the Basic tab fields.

Table 67 Basic tab fields

Field	Description
ElanName	The ELAN Name this client uses the next time that it returns to the Initial State.
ConfigMode	Indicates how the LEC configures ATM when the device is restarted. Entries include: Automatic: Client uses a LAN emulation configuration server (LECS) to find out the ATM address of the LAN emulation server (LES). It also obtains other parameters, including: • ConfigLanType • ConfigMaxDataFrameSize • ConfigLanName. **Note**: ConfigLessAtmAddress is ignored. Manual: Management tells the client the ATM address of its LES and the values of other parameters, including: • ConfigLanType • ConfigMaxDataFrameSize • ConfigLanName ConfigLessAtmAddress tells the client which LES to call.
RowStatus	This entry is used to create and delete rows in the Basic tab. The management station cannot change the status of a primary ATM address to “notInService” or “destroy” unless ifAdminStatus on the client is set to `down` and lecInterfaceState also on the client is set to `initialState`. Secondary ATM addresses may be deleted at any time if permitted by the agent.
ConfigLanType	The data frame format that the client uses the next time it returns to its initial state. • Auto-configuring clients use this parameter when configuring requests. • Manually-configured clients use it in their join requests. This MIB will not be overwritten with the new value. Instead, ActualLanType in the Status tab is updated.

Table 67 Basic tab fields (continued)

Field	Description
ConfigMaxDataFrameSize	Maximum data frame size that the client uses the next time it returns to the initial state. • Auto-configuring clients use this parameter when configuring requests. • Manually-configured clients use it in their join requests. This MIB will not be overwritten with the new value. Instead, ActualMaxDataFrameSize in the Status tab is updated.
ConfigLesAtmAddress	This is the LAN emulation server that the client uses the next time it is started in manual configuration mode. • There is no need to set this address if the ConfigMode is set to automatic. • The client uses LECS to find a LES. It then places the auto-configured address in ActualLesAtmAddress in the Status tab.
Owner	The device that configured this entry and is using the resources assigned to it.

LECs are created by management. However, the Basic tab does not directly support row creation.

LecStatistics dialog box

LecStatistics dialog box has traffic statistics for all the LAN emulation clients this host implements. Each row in this dialog box has traffic statistics for one LAN Emulation client.

To make performance monitoring fast and easy, LecStatistics dialog box tracks and graphs a wide range of statistics. Statistics are maintained for the ATM.

To view the LecStatistics dialog box:

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

The AtmLec dialog box opens with the Ports tab displayed (Figure 79 on page 180).

2 Click the Basic tab.

The Basic tab opens (Figure 81 on page 184).

3 Click an item to graph.

4 Click Graph.

The lecStatistics dialog box opens (Figure 82).

Figure 82 lecStatistics dialog box

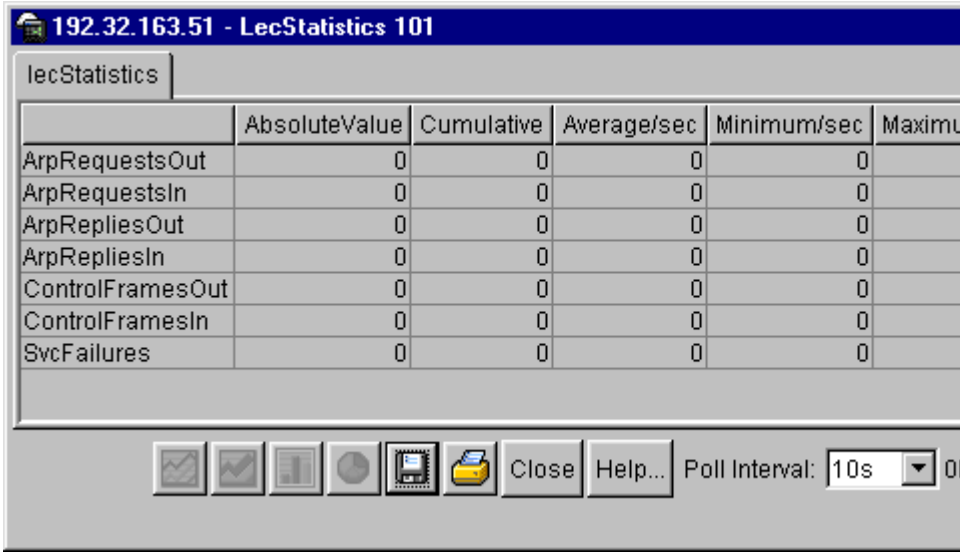


Table 68 describes the lecStatistics dialog box fields.

Table 68 lecStatistics dialog box fields

Field	Description
ArpRequestsOut	Number of LE ARP requests sent over the LANE user-network interface (LUNI) by this LANE client.
ArpRequestsIn	The number of LE ARP requests received over the LUNI by this LANE client. Requests may arrive on the Control Direct VCC or on the Control Distribute VCC, depending upon how the LES is implemented and the chances it has had for learning. This covers both VCCs.
ArpRepliesOut	Number of LE ARP responses sent over the LUNI by this LANE client.

Table 68 lecStatistics dialog box fields (continued)

Field	Description
ArpRepliesIn	Number of LE ARP responses received over the LUNI by this LANE client. This includes all such replies, whether solicited or not. Replies may arrive on the Control Direct VCC or on the Control Distribute VCC, depending upon how the LES is implemented. This counter covers both VCCs.
ControlFramesOut	Number of control packets sent by this LANE client over the LUNI.
ControlFramesIn	Number of control packets received by this LANE client over the LUNI.
SvcFailures	Number of: • Outgoing LLC-multiplexed LANE flows that this client tried, but failed, to open • Incoming LLC-multiplexed LANE flows that client did not accept or establish. Only failures that the LEC is aware and that are clearly LANE-related are counted.

Timers tab

The Timers tab is a read-only table containing Timers information about the LAN emulation clients this agent manages.

To view the Timers tab:

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

The AtmLec dialog box opens with the Ports tab displayed (Figure 79 on page 180).

2 Click the Timers tab.

The Timers tab opens (Figure 83).

Figure 83 Timers tab

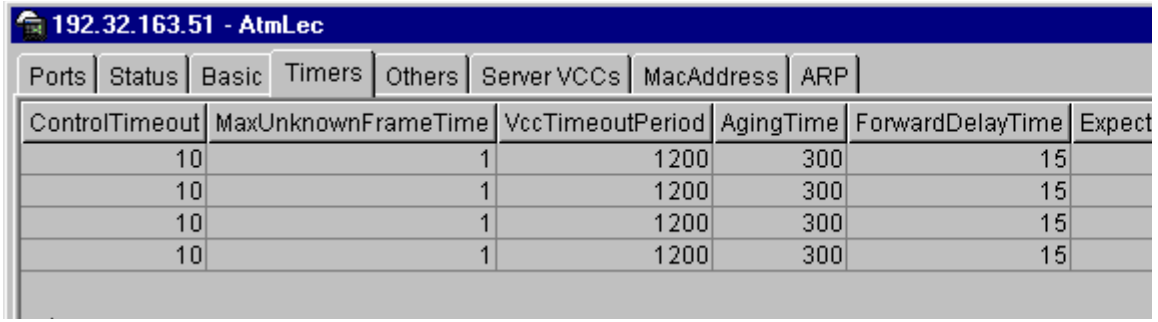


Table 69 describes the Timers tab fields.

Table 69 Timers tab fields

Field	Description
ControlTimeout	Time out period used for most request/response control frame interactions (as specified elsewhere in the LAN emulation specification). In LAN emulation V2.0 (LANE V2.0), this value is the maximum cumulative time-out for an exponential back-off algorithm.
MaxUnknownFrameTime	This is the period of time that a LEC can send no more than maximum unknown frame count frames to the broadcast and unknown server (BUS) for a given unicast LAN destination. It must also initiate the address resolution protocol to resolve that LAN destination. This time value is expressed in seconds.
VccTimeoutPeriod	A LEC must release any data direct VCC that it has not used to transmit or receive any data frames for the length of the VCC time-out period. This parameter is only useful for SVC data direct VCCs signalled. It should not be used for any SVC signalled. This time value is expressed in seconds. Items to consider when setting this parameter: • A default value is 20 minutes • A value of 0 seconds sets the time-out period as infinite • Negative values are rejected by the agent.
AgingTime	Maximum time that a LEC maintains an entry for a unicast LAN destination in the ARP cache. This time value is expressed in seconds.

Table 69 Timers tab fields (continued)

Field	Description
ForwardDelayTime	Maximum time that a LEC maintains an entry for a non-local MAC address in its ARP cache. Items to consider when setting this parameter: • Topology change flag is true. • ForwardDelayTime should be less than AgingTime • This time value is expressed in seconds
ExpectedArpResponseTime	Maximum time that the LEC expects an ARP request ARP response cycle to take. This is used for retries and verifies. This time value is expressed in seconds.
FlushTimeOut	Time limit to wait to receive a flush response after the flush request has been sent and before taking recovery action. This time value is expressed in seconds.
PathSwitchingDelay	Time since sending a frame to the BUS after which the LEC assumes that the frame has been either discarded or delivered. May be used to bypass the flush protocol. This time value is expressed in seconds.
ConnectionCompleteTimer	For connection establishment this is the time period in which data is expected from a calling party. This time value is expressed in seconds. This parameter is optional.

Others tab

The Others tab has miscellaneous parameters that may be changed either by the network manager or by the LECS.

To view the Others tab:

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

The AtmLec dialog box opens with the Ports tab displayed (Figure 79 on page 180).

2 Click the Others tab.

The Others tab opens (Figure 84).

Figure 84 Others tab

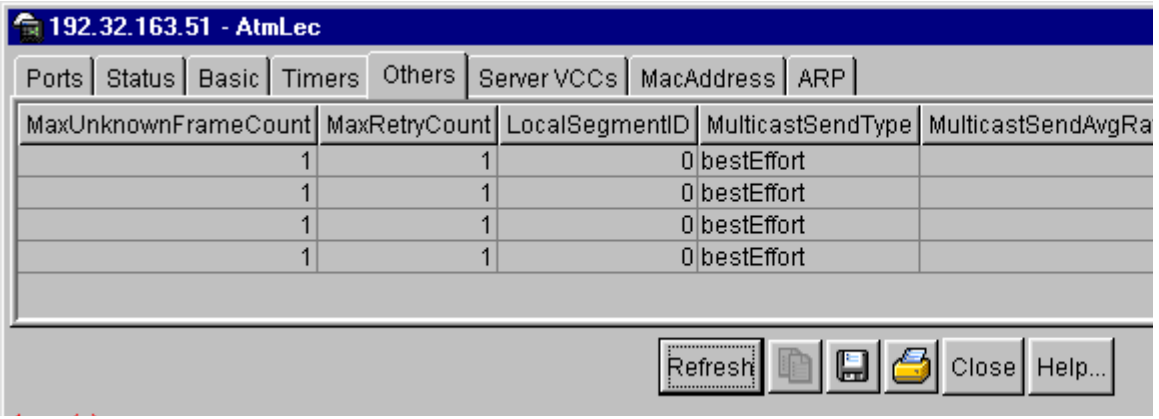


Table 70 describes the Others tab fields.

Table 70 Others tab fields

Item	Description
MaxUnknownFrameCount	This is for LANE V1.0 versions only, and should not be used except as required for backwards compatibility.
MaxRetryCount	Maximum retry count.
LocalSegmentID	Local Segment ID. The segment ID of the emulated LAN. Only required for IEEE 802.5 clients that are source routing bridges. **Note**: Do not implement except as required for backwards compatibility.
MulticastSendType	Signalling parameter used by the LEC to specify traffic parameters when establishing the multicast send VCC for an emulated LAN.
MulticastSendAvgRate	Signalling parameter that is used by the LEC when establishing the multicast send VCC. Forward and backward sustained cell rate are requested by LEC when setting up multicast send VCC (if using variable bit rate codings).
MulticastSendPeakRate	Signalling parameter that is used by the LEC when establishing the multicast send VCC. Forward and backward peak cell rate are requested by LEC when setting up the multicast send VCC when using either variable or constant bit rate codings.
ConfigLecsAtmAddress	Manually configured LECS address that a client may use in its attempts at auto-configuration.

Server VCCs tab

The Server VCCs tab identifies the control VCCs and multicast VCCs for each LECs that the host implements. Each row in this tab describes the control VCCs and Multicast VCCs for one LEC.

To view the Server VCCs tab:

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

The AtmLec dialog box opens with the Ports tab displayed (Figure 79 on page 180).

2 Click the Server VCCs tab.

The Server VCCs opens (Figure 85).

Figure 85 Server VCCs tab

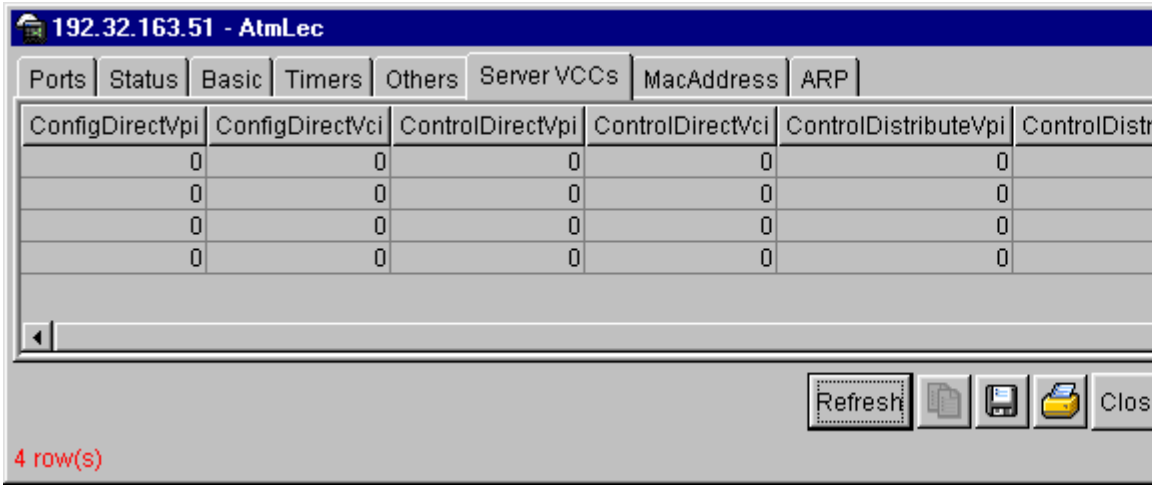


Table 71 describes the Server VCCs tab fields.

Table 71 Server VCCs tab fields

Field	Description
ConfigDirectVpi	If a configuration direct VCC exists, the object contains the VPI that identifies that VCC at the point where it connects to the LEC. Otherwise, the value is 0.
ConfigDirectVci	If a configuration direct VCC exists, the object contains the VCI that identifies that VCC at the point where it connects to this LEC. Otherwise, this object has the value is 0.
ControlDirectVpi	If the Control Direct VCC exists, the object contains the VPI that identifies that VCC at the point where it connects to this LEC. Otherwise, this object has the value is 0.
ControlDirectVci	If the Control Direct VCC exists, the object contains the VCI that identifies that VCC at the point where it connects to this LEC. Otherwise, this object has the value is 0.
ControlDistributeVpi	If the Control Distribute VCC exists, the object contains the VPI that identifies that VCC at the point where it connects to this LEC. Otherwise, this object has the value is 0.
ControlDistributeVci	If the Control Distribute VCC exists, the object contains the VCI that identifies that VCC at the point where it connects to this LEC. Otherwise, this object contains the value is 0.
MulticastSendVpi	If the Multicast Send VCC exists, the object contains the VPI that identifies that VCC at the point where it connects to this LEC. Otherwise, this object has the value is 0.
MulticastSendVci	If the Multicast Send VCC exists, the object contains the VCI which identifies that VCC at the point where it connects to this LEC. Otherwise, this object has the value is 0.
MulticastForwardVpi	For LANE V1.0 clients: If there is a multicast forward VCC, this contains the VPI that identifies that VCC at the point where it connects to this LEC. Otherwise, and for a LANE V2.0 clients: The value is 0.
MulticastForwardVci	For a LANE V1.0 client: If the multicast forward VCC exists, this object contains the VCI that identifies that VCC at the point where it connects to this LEC. Otherwise, and for a LANE V2.0 clients: The value is 0.

MacAddress tab

The MacAddress tab contains entries for all of the registered MAC addresses belonging to LECs for the agent. The MacAddress features include:

- For LANE clients, the entries includes the local unicast MAC address(es). Each LEC has zero or more local unicast MAC addresses.
- For operational LEC, every address in this variable must have been registered with the LE server.
- Two LECs joined to the same emulated LAN must not have the same local unicast MAC address.
- The MAC addresses for an LEC may change during normal operations.
- When answering an ARP request for any address in this list, the remote address bit in the flags field of the ARP response must be clear.
- Each table row describes a MAC address and/or ATM address pair registered for a particular client.

To view the MacAddress tab:

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

The AtmLec dialog box opens with the Ports tab displayed (Figure 79 on page 180).

2 Click the MacAddress tab.

The MacAddress tab opens (Figure 86).

Figure 86 MacAddress tab

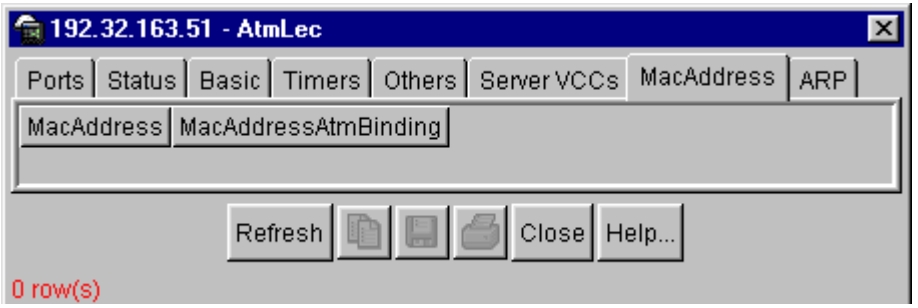


Table 72 describes the MacAddress tab fields.

Table 72 MacAddress tab fields

Item	Description
MacAddress	This entry contains all of the registered MAC addresses belonging to LECs for his agent. For LANE clients, this includes local unicast MAC Address(es). Each LEC has zero or more local unicast MAC addresses. In an operational LEC, every address in this variable must have been registered with the LE server. Two LECs joined to the same emulated LAN cannot have the same local unicast MAC address. The MAC addresses for a A LEC may change during normal operations. When answering an ARP request for any address in this list, the remote address bit in the Flag field of the ARP response must be clear. For a LANE V2.0 client, this includes multicast MAC addresses
MacAddressAtmBinding	The non-multiplexed ATM address registered for MacAddress.

ARP tab

The ARP tab provides access to MAC-to-ATM ARP cache for the ATM LECS. The tab also contains entries for unicast addresses and for the broadcast address.

For LANE V2.0 clients whose selective multicast flag is set, this tab also contains multicast address entries.

Each entry establishes a relationship between a LAN destination (external to the LEC) and the ATM address for that LAN destination. The ATM LAN emulation ARP cache entry also contains information about the binding of one MAC address to one ATM address.

To view the ARP tab:

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

The AtmLec dialog box opens with the Ports tab displayed (Figure 79 on page 180).

2 Click the ARP tab.

The ARP tab opens (Figure 87).

Figure 87 ARP tab

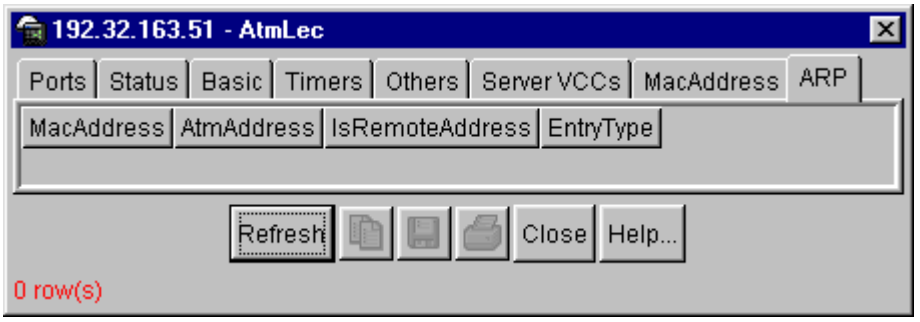


Table 73 describes the ARP tab fields.

Table 73 ARP tab fields

Field	Description
MacAddress	The MAC address that this cache entry provides a translation. Since ATM LAN Emulation uses an ARP protocol to locate the broadcast/unknown server, the value may be the broadcast MAC address. The value could also be a multicast or group MAC address. Unicast MAC addresses should be unique within any given ATM emulated LAN. However, there is no requirement that they be unique across disjointed emulated LANs.
AtmAddress	The non-multiplexed, LEC or broadcast/multicast service ATM address that corresponds to the MacAddress. This value may be determined using the ARP procedure, through source address learning, or through some other mechanisms. **Note**: Some agents may provide write access to this object. The effect of attempting to write an ATM address to a learned row is undefined. Agents may disallow the write, accept the write and change the row's type, or even accept the write as-is.

Table 73 ARP tab fields (continued)

Field	Description
IsRemoteAddress	Indicates whether the entry is for a local or remote MAC address. Entries include: Local: This is a MAC address that is local to the remote client. True: Address is believed to be remote or its status is unknown. For an entry created using ARP, this represents the remote address flag being set in the ARP response. During a topology change period, remote ARP entries generally age-out faster than others. That is, they are subject to ForwardDelayTime and AgingTime. False: Address is believed to be local. That is, it was registered with the LES by the client whose ATM address is AtmAddress. For an entry created using ARP, this represents the remote address flag being set in the ARP response.
EntryType	Indicates how the ARP table entry was created and whether it is aged.

Atm MDA

Atm MDA provides port and server information for your media dependent adaptor. Atm MDA supports dual OC-3 fiber optic network speed. For more information on the available models, see *Installing Media Dependent Adapters* or *Using the BayStack 450 10/100/1000 Series Switch*.

The AtmMDA dialog box contains the following tabs:

- Ports tab (next)
- Server tab (page 198)

Ports tab

You use the Ports tab to manage Atm MDA specific options.

To view the Ports tab:

➔ From the Device Manager menu bar, select Edit > Atm MDA.

The AtmMDA dialog box opens with the Ports tab displayed (Figure 88).

Figure 88 AtmMDA dialog box

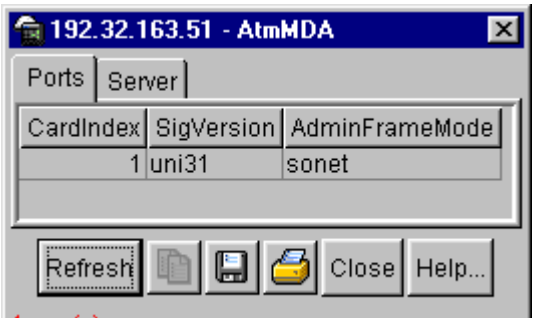


Table 74 describes the Ports tab fields.

Table 74 Ports tab fields

Field	Description
CardIndex	This indicates the ATM card identification.
SigVersion	This indicates the version of the signalling entity that is associated with the ATM port, including: • uni30: Version is UNI 3.0. • uni31: Version is UNI 3.1.
AdminFrameMode	When read, this returns the configured ATM frame mode. When set, only modes “sonet” and “sdh” are supported.

Server tab

The Server tab provides ATM MDA hardware server information.

To view the Server tab:

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

The AtmMDA dialog box opens with the Ports tab displayed (Figure 79 on page 180).

2 Click the Server tab.

The Server tab opens (Figure 89).

Figure 89 Server tab

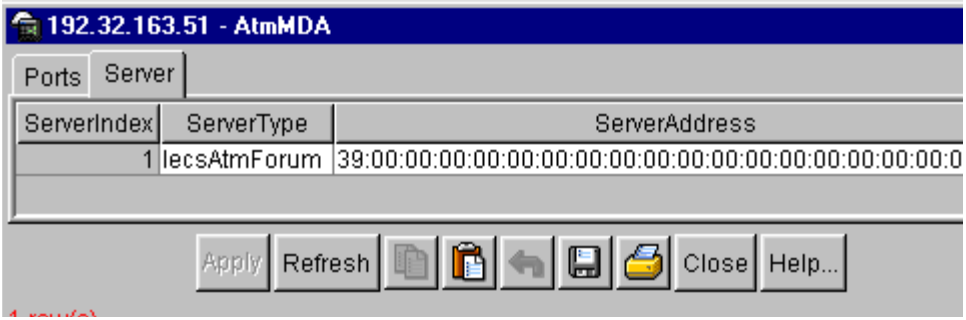


Table 75 describes the Server tab fields.

Table 75 Server tab fields

Field	Description
ServerIndex	An index to the LEC server table.
ServerType	The field specifies how the LEC can get to the server and the server type (LES or LECS). The LEC can connect to either the LECS using ATM Forum/ILMI/Direct LECS address or the LES using ATM address.
ServerAddress	The field specifies the ATM address (20 octets) of the server when an ATM address is needed. If an ATM address is not needed, zero is returned when read. The ATM address must start with a 39, 45, or 47.

Chapter 10
Configuring security parameters

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

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

General tab

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

To view the General tab:

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

The Security dialog box opens with the General tab displayed (Figure 90).

Figure 90 General tab

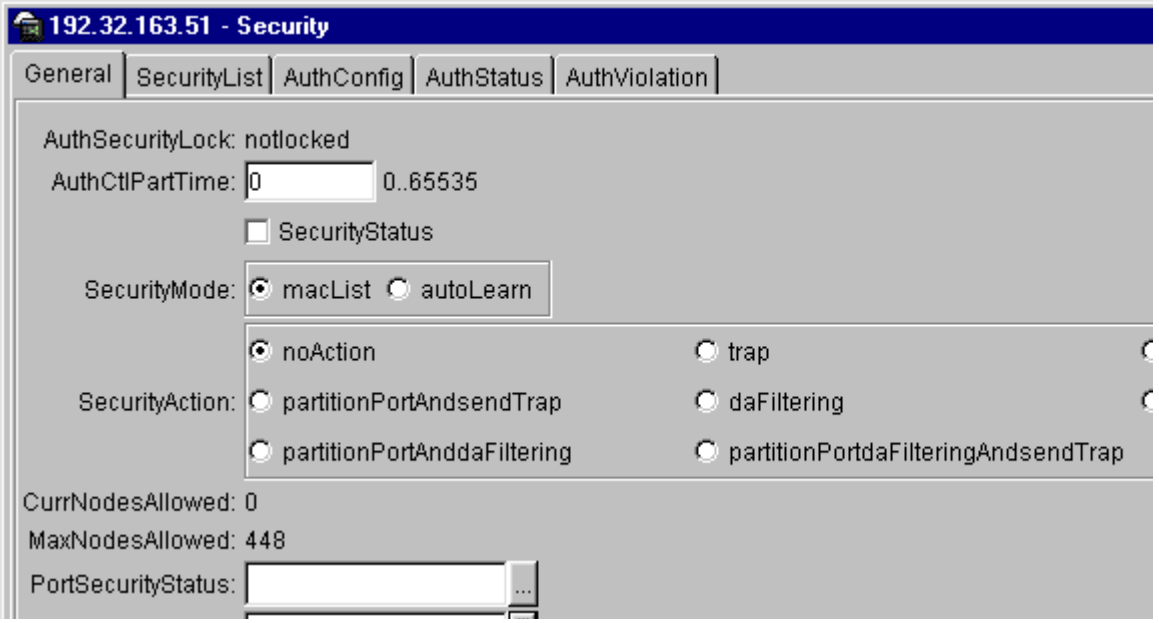


Table 76 describes the General tab items.

Table 76 General tab items

Items	Description
AuthSecurityLock	If this parameter is listed as “locked,” the agent refuses all requests to modify the security configuration. Entries also include: • other • notlocked
AuthCtlPartTime	This value indicates the duration of the time for port partitioning in seconds. Default: 0 (zero). When the value is zero, port remains partitioned until it is manually re-enabled.
SecurityStatus	Indicates whether or not the switch security feature is enabled.
SecurityMode	Mode of switch security. Entries include: • macList: Indicates that the switch is in the MAC-list mode. You can configure more than one MAC address per port. • autoLearn: Indicates that the switch learns the first MAC address on each port as an allowed address of that port.

Table 76 General tab items (continued)

Items	Description
SecurityAction	Actions performed by the software when a violation occurs (when SecurityStatus is enabled). The security action specified here applies to all ports of the switch. A blocked address causes the port to be partitioned when unauthorized access is attempted. Selections include: • noAction: Port does not have any security assigned to it, or the security feature is turned off. • trap: Listed trap. • partitionPort: Port is partitioned. • partitionPortAndsendTrap: Port is partitioned and traps are sent to the trap receive station. • daFiltering: Port filters out the frames where the destination address field is the MAC address of unauthorized Station. • daFilteringAndsendTrap: Port filters out the frames where the desitnation address field is the MAC address of unauthorized station. Traps are sent to trap receive station(s). • partitionPortAnddaFiltering: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. • partitionPortdaFilteringAndsendTrap: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. Traps are sent to trap receive station(s). **Note**: “da” means destination address.
CurrNodesAllowed	Current number of entries of the nodes allowed in the AuthConfig tab.
MaxNodesAllowed	Maximum number of entries of the nodes allowed in the AuthConfig tab.
PortSecurityStatus	Set of ports that security has enabled. The bit-wise of the PortSecurityStatus and the PortLearnStatus must be an empty set.
PortLearnStatus	Set of ports where auto-learning is enabled.
CurrSecurityLists	Current number of entries of the Security listed in the SecurityList tab
MaxSecurityLists	Maximum entries of the Security listed in the SecurityList tab.

SecurityList tab

The SecurityList tab contains a list of Security port items.

To view the SecurityList tab:

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

   The Security window opens with the General tab displayed (Figure 90 on page 202).

2. Click the SecurityList tab.

   The SecurityList tab opens (Figure 91).

Figure 91 SecurityList tab

Table 77 describes the SecurityList tab fields.

Table 77 SecurityList tab fields

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

Security, Insert SecurityList dialog box

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

To view the Security, Insert AuthConfig dialog box:

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

   The Security window opens with the General tab displayed.

2. Click the SecurityList tab.

   The SecurityList tab opens (Figure 91 on page 204).

3. Click inside a row.

4. Click Insert.

   The Security, Insert SecurityList dialog box opens (Figure 92).

Figure 92 Security, Insert SecurityList dialog box

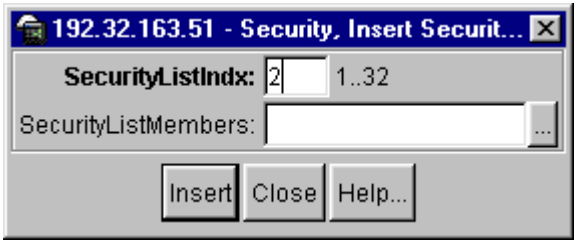


Table 78 describes the Security, Insert AuthConfig dialog box items.

Table 78 Security, Insert AuthConfig dialog box items

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

AuthConfig tab

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

To view the AuthConfig tab:

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

The Security window opens with the General tab displayed (Figure 90 on page 202).

2 Click the AuthConfig tab.

The AuthConfig tab opens (Figure 93).

Figure 93 AuthConfig tab

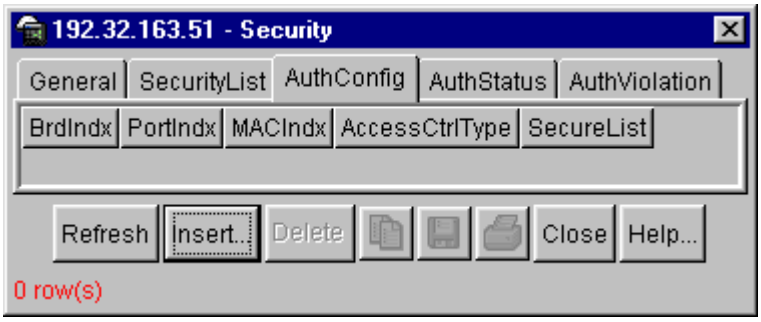


Table 79 describes the AuthConfig tab fields.

Table 79 AuthConfig tab fields

Field	Description
BrdIndx	Index of the slot containing the board on where the port is located. This value is meaningful only if SecureList value is zero. For other SecureList values, this parameter should have the value of zero.
PortIndx	Index of the port on the board. This value is meaningful only if SecureList value is zero. For other SecureList values, this parameter should have the value of zero.
MACIndx	An index of MAC addresses that are either designated as `allowed` (station) or `not-allowed` (station).

Table 79 AuthConfig tab fields (continued)

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

Security, Insert AuthConfig dialog box

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

To view the Security, Insert AuthConfig dialog box:

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

   The Security window opens with the General tab displayed (Figure 90 on page 202).

2. Click the AuthConfig tab.

   The AuthConfig tab opens (Figure 93 on page 206).

3. Click inside a row.

4. Click Insert.

   The Security, Insert AuthConfig dialog box opens (Figure 94).

Figure 94 Security, Insert AuthConfig dialog box

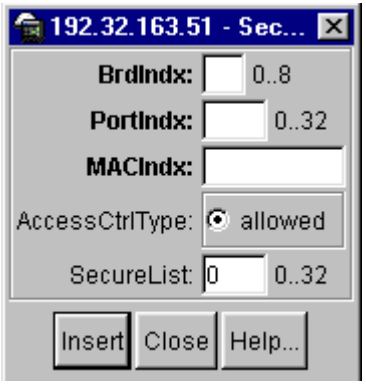


Table 80 describes the Security, Insert AuthConfig dialog box items.

Table 80 Security, Insert AuthConfig dialog box items

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

AuthStatus tab

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

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

To view the AuthStatus tab:

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

   The Security window opens with the General tab displayed (Figure 90 on page 202).

2. Click the AuthStatus tab.

   The AuthStatus tab opens (Figure 95).

Figure 95 AuthStatus tab

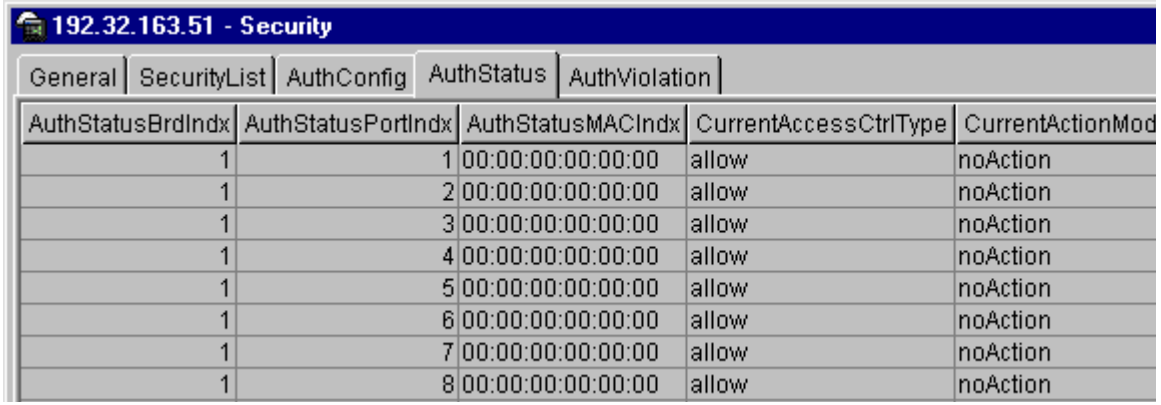


Table 81 describes the AuthStatus tab fields.

Table 81 AuthStatus tab fields

Field	Description
AuthStatusBrdIndx	The index of the board. This corresponds to the index of the slot containing the board if the index is greater than zero.
AuthStatusPortIndx	The index of the port on the board. This corresponds to the index of the last manageable port on the board if the index is greater than zero.
AuthStatusMACIndx	The index of MAC address on the port. This corresponds to the index of the MAC address on the port if the index is greater than zero.
CurrentAccessCtrlType	Displays whether the node entry is `node allowed` or `node blocked type`.
CurrentActionMode	A value representing the type of information contained, including: noAction: Port does not have any security assigned to it, or the security feature is turned off. partitionPort: Port is partitioned. partitionPortAndsendTrap: Port is partitioned and traps are sent to the trap receive station. Filtering: Port filters out the frames, where the destination address field is the MAC address of unauthorized station. FilteringAndsendTrap: Port filters out the frames, where the destination address field is the MAC address of unauthorized station. Trap are sent to trap receive station. sendTrap: A trap is sent to trap receive station(s). partitionPortAnddaFiltering: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. partitionPortdaFilteringAndsendTrap: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. Traps are sent to trap receive station(s).
CurrentPortSecurStatus	Displays the security status of the current port, including: • If the port is disabled, notApplicable is returned. • If the port is in a normal state, portSecure is returned. • If the port is partitioned, portPartition is returned.

AuthViolation tab

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

To view the AuthViolation tab:

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

   The Security window opens with the General tab displayed (Figure 90 on page 202).

2. Click the AuthViolation tab.

   The AuthViolation tab opens (Figure 96).

Figure 96 AuthViolation tab

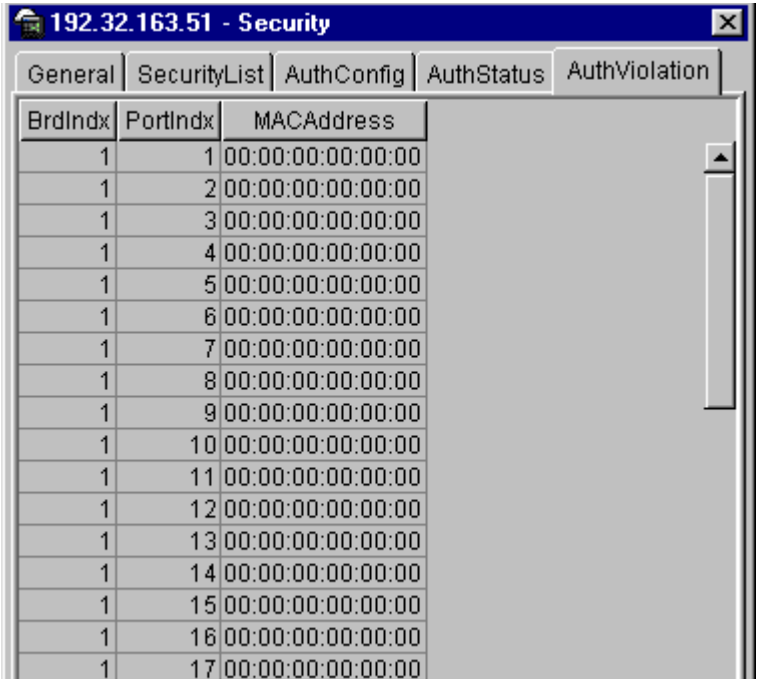


Table 82 describes the AuthViolation tab fields.

Table 82 AuthViolation tab fields

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

Appendix A
Reference documents

For more information about networking concepts, protocols, and topologies, you may want to consult the following sources:

- RFC 1213 (MIB-II)
- RFC 1493 (Bridge MIB)
- RFC 1573 (Interface MIB)
- RFC 1643 (Ethernet MIB)
- RFC 1757 (Rmon)
- RFC 1271 (Rmon)
- IEEE 802.1D (Standard for Spanning Tree Protocol)
- IEEE 802.3 (Ethernet)
- IEEE 802.1Q (VLAN Tagging)
- IEEE 802.1p (Prioritizing)

Appendix B
RMON alarm variables

Bridge alarm variables

Table 83 Bridge alarm variables

Variable	Definition
dot1dStpTimeSinceTopologyChange.0	Time (in hundredths of a second) since the last topology change was detected by the bridge entity.
dot1dStpTopChanges.0	Number of topology changes detected by this bridge since the management entity was last reset or initialized.
dot1dStpMaxAge.0	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.
dot1dStpPortForwardTransitions	Number of times this port has transitioned from the Learning state to the Forwarding state.
dot1dTpPortInFrames	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.
dot1dTpPortOutFrames	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.
dot1dTpPortInDiscards	Count of valid frames received that were discarded (that is, filtered) by the forwarding process.
dot1dTpLearnedEntryDiscards.0	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.

Interface alarm variables

Table 84 Interface alarm variables

Variable	Definition
ifInOctets	Number of octets received on the interface, including framing characters.
ifInDiscards	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.
ifInUnknownProtos	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	Number of octets transmitted out of the interface, including framing characters.
ifOutDiscards	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.
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.
ifOperStatus	The current operational state of the interface. The testing(3) state indicates that no operational packets can be passed. If ifAdminStatus is down (2), then ifOperStatus should be down (2). If ifAdminStatus is changed to up (1), then ifOperStatus should change to up (1) if the interface is ready to transmit and receive network traffic; it should change to dormant (5) if the interface is waiting for external actions (such as a serial line waiting for an incoming connection); it should remain in the down (2) state if and only if there is a fault that prevents it from going to the up (1) state.
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.

Ethernet errors alarm variables

Table 85 Ethernet errors alarm variables

Variable	Definition
dot3StatsAlignmentErrors	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 obtain 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 obtain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC.
dot3StatsSingleCollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsMultipleCollisionFrames object.
dot3StatsMultipleCollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsSingleCollisionFrames object.
dot3StatsSQETestErrors	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.
dot3StatsDeferredTransmissions	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.

Table 85 Ethernet errors alarm variables (continued)

Variable	Definition
dot3StatsLateCollisions	Number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet. Five hundred and twelve bit-times corresponds to 51.2 microseconds on a 10 Mb/s system. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics.
dot3StatsExcessiveCollisions	A count of frames for which transmission on a particular interface fails due to excessive collisions.
dot3StatsInternalMacTransmitErrors	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.
dot3StatsCarrierSenseErrors	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.
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.
dots3StatsInternalMacReceiveErrors	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.

Rmon alarm variables

Table 86 Rmon alarm variables

Variable	Definition
etherStatsOctets	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	Number of packets (including bad packets, broadcast packets, and multicast packets) received.
etherStatsBroadcastPkts	Number of good packets received that were directed to the broadcast address. Note that this number does not include multicast packets.
etherStatsMulticastPkts	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.
etherStatsCRCAlignErrors	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).
etherStatsUndersizePkts	Number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
etherStatsOversizePkts	Number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
etherStatsFragments	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	Best estimate of the number of collisions on this Ethernet segment.

IP alarm variables

Table 87 IP alarm variables

Variable	Definition
ipInReceives.0	Number of input datagrams received from interfaces, including those received in error.
ipInHdrErrors.0	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.
ipAddrErrors.0	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.
ipForwDatagrams.0	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 via this entity and the Source-Route option processing was successful.
ipUnknownProtos.0	Number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
ipInDiscards.0	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.
ipInDelivers.0	Number of input datagrams successfully delivered to IP user-protocols (including ICMP).
ipOutRequests	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.
ipOutDiscards.0	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.
ipOutNoRoutes.0	Number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams that meet this 'no-route' criterion. Note that this counter includes any datagrams that a host cannot route because all of its default gateways are down.

Table 87 IP alarm variables (continued)

Variable	Definition
ipFragOKs.0	Number of IP datagrams that have been successfully fragmented at this entity.
ipFragFails.0	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.
ipFragCreates.0	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
ipReasmReqds.0	Number of IP fragments received that needed to be reassembled at this entity.
ipReasmOks.0	Number of IP datagrams successfully reassembled.
ipReasmFails.0	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.
icmpInSrcQuenchs.0	Number of ICMP Source Quench messages received.
icmpInRedirects.0	Number of ICMP Redirect messages received.
icmpInEchos.0	Number of ICMP Echo (request) messages received.
icmpInEchoReps.0	Number of ICMP Echo Reply messages received.
icmpnTimestamps.0	Number of ICMP Timestamp (request) messages received.
icmpInTimestampReps.0	Number of ICMP Timestamp Reply messages received.
icmpInAddrMask.0	Number of ICMP Address Mask Request messages received.
icmpInAddrMaskReps.0	Number of ICMP Address Mask Reply messages received.
icmpInParmProbs.0	Number of ICMP Parameter Problem messages received.
icmpnDestUnreachs.0	Number of ICMP Destination Unreachable messages received.
icmpInTimeExcds.0	Number of ICMP Time Exceeded messages received.
icmpOutSrcQuenchs.0	Number of ICMP Source Quench messages sent.
icmpOutRedirects.0	Number of ICMP Redirect messages sent. For a host, this object will always be zero, because hosts do not send redirects.
icmpOutEchos.0	Number of ICMP Echo (request) messages sent.
icmpOutEchoReps.0	Number of ICMP Echo Reply messages sent.
icmpOutTimestamps.0	Number of ICMP Timestamp (request) messages sent.
icmpOutTimestampReps.0	Number of ICMP Timestamp Reply messages sent.
icmpOutAddrMasks.0	Number of ICMP Address Mask Request messages sent.

Table 87 IP alarm variables (continued)

Variable	Definition
icmpOutAddrMaskReps.0	Number of ICMP Address Mask Reply messages sent.
icmpOutParmProbs.0	Number of ICMP Parameter Problem messages sent.
icmpOutDestUnreachs.0	Number of ICMP Destination Unreachable messages sent.
icmpOutTimeExcds	Number of ICMP Time Exceeded messages sent.

SNMP alarm variables

Table 88 SNMP alarm variables

Variable	Definition
snmpInPkts.0	Number of messages delivered to the SNMP entity from the transport service.
snmpOutPkts.0	Number of SNMP messages that were passed from the SNMP protocol entity to the transport service.
snmpInBadVersions.0	Number of SNMP messages that were delivered to the SNMP protocol entity and were for an unsupported SNMP version.
snmpBadCommunityNames.0	Number of SNMP messages delivered to the SNMP protocol entity that used an SNMP community name not known to said entity.
snmpBadCommunityUses.0	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.
snmpInASNParseErrs.0	Number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding received SNMP messages.
snmpInTooBigs.0	Number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is tooBig.
snmpInNoSuchNames.0	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	Number of SNMP PDUs that were delivered to the SNMP protocol entity and for which the value of the error-status field is badValue.
snmpInReadOnlys.0	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 88 SNMP alarm variables (continued)

Variable	Definition
snmpInGenErrs.0	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	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	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	Number of SNMP Get-Request PDUs that have been accepted and processed by the SNMP protocol entity.
snmpInGetNexts.0	Number of SNMP Get-Next PDUs that have been accepted and processed by the SNMP protocol entity.
snmpInSetRequests.0	Number of SNMP Set-Request PDUs that have been accepted and processed by the SNMP protocol entity.
snmpInGetResponses.0	Number of SNMP Get-Response PDUs that have been accepted and processed by the SNMP protocol entity.
snmpInTraps.0	Number of SNMP Trap PDUs that have been accepted and processed by the SNMP protocol entity.
snmpOutTooBigs.0	Number of SNMP PDUs that were generated by the SNMP protocol entity and for which the value of the error-status field is tooBig.
snmpOutNoSuchNames.0	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	Number of SNMP PDUs that were generated by the SNMP protocol entity and for which the value of the error-status field is badValue.
snmpOutGenErrs.0	Number of SNMP PDUs that were generated by the SNMP protocol entity and for which the value of the error-status field is genErr.
snmpOutGetRequests.0	Number of SNMP Get-Request PDUs that have been generated by the SNMP protocol entity.
snmpOutGetNexts.0	Number of SNMP Get-Next PDUs that have been generated by the SNMP protocol entity.
snmpOutSetRequests.0	Number of SNMP Set-Request PDUs that have been generated by the SNMP protocol entity.
snmpOutGetResponses.0	Number of SNMP Get-Response PDUs that have been generated by the SNMP protocol entity.
snmpOutTraps.0	Number of SNMP Trap PDUs that have been generated by the SNMP protocol entity.

Index

A

B

C

D

E

F

G

H

I

L

M

O

P

R

S

T

U

V