Reference for the BayStack 380-24F Gigabit Switch Management Software

NORTEL NETWORKS™

Copyright © 2003 Nortel Networks

Trademarks

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

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

SPARC is a trademark of Sparc International, Inc.

Sun and Solaris are trademarks of Sun Microsystems, Inc.

HP is a trademark of Hewlett-Packard Corporation.

UNIX is a trademark of X/Open Company Limited.

IBM and AIX are trademarks of International Business Machines Corporation (IBM).

Netscape Navigator is a trademark of Netscape Communications Corporation.

Ethernet is a trademark of Xerox Corporation.

Intel and Pentium are trademarks of Intel Corporation.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Statement of conditions

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

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

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

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

Nortel Networks Inc. software license agreement

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

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

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

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

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

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

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

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

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

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

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

Should you have any questions concerning this Agreement, contact Nortel Networks Inc., 2375 N. Glenville Dr., Richardson, TX 75082.

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

Contents

Reference for the BayStack 380-24F Gigabit Switch Management Software

Reference for the BayStack 380-24F Gigabit Switch Management Software

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 Nortel Networks BayStack* 380-24F Gigabit Switch. This guide provides information about using the features and capabilities of the Java-based Device Manager graphical user interface (GUI) to perform network management operations for the switch.

> **Note:** This version of Device Manager supports BayStack 380-24F Gigabit Switch software version 2.1.

Before you begin

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

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

Text conventions

This guide uses the following text conventions:

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

Related publications

For more information about using the BayStack 380-24F Gigabit Switch, refer to the following publications:

- *Using the BayStack 380-24F Gigabit Switch* (part number 214391-A)

  Describes how to install and use the BayStack 380-24F Gigabit Switch; includes instructions to use the console interface to configure the switch.

- *Installing the BayStack 380-24F Gigabit Switch* (part number 214390-A)

  Provides installation instructions for the switch in English and five other languages.

- *Getting Started with the BayStack 380-24F Gigabit Switch Management Software* (part number 214392-A)

  Provides an introduction to the major features of the Device Manager software and how to use it to manage the BayStack 380-24F switch.

- *Using Web-Based Management for the BayStack 380-24F Gigabit Switch* (part number 214394-A)

  Describes how to use the Web-based management interface to configure and monitor switch operations.

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

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

How to get help

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

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

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

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

Chapter 1
Device Manager basics

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

- Instructions to start Device Manager, set the Device Manager properties, and open a device (next)
- A summary of the Device Manager user interface features and how to use them (starting on page 25)
- Instructions to view statistics and display graphs (page 33)
- Instructions to use Device Manager to Telnet to a switch (page 40)
- Information about the trap log (page 42)
- Information about online Help (page 43)

> → **Note:** This version of Device Manager supports BayStack 380-24F Gigabit Switch software version 2.1.

Starting Device Manager

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

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

  JDM

The initial Device Manager window opens (Figure 1).

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

Figure 1   Device Manager window

Setting the Device Manager properties

Device Manager communicates with the BayStack 380-24F switch using Simple Network Management Protocol (SNMP). The software is shipped with default values set for important communication parameters, such as the polling interval, timeout, and retry count. You may want to set the parameters before you open a device to manage.

To set the Device Manager properties:

1   Choose Device > Properties.

The Properties dialog box opens (Figure 2).

Figure 2 Properties dialog box

2 Type information and select check boxes.

3 Click OK.

Table 1 describes the Properties dialog box items.

Table 1 Properties dialog box items

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

Opening a device

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

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

Table 2   SNMP community string default values

Access level	Description
Read-only	public
Read/write	private

To display the device view:

1   Do one of the following:

- Choose Device > Open.
- Choose Device > Open Last, and select an IP address from the list.
- Click the folder icon in the Device Manager window.

- Press [Ctrl] + O.

The Open Device dialog box opens (Figure 3).

Figure 3 Open Device dialog box

Table 3 describes the Open Device dialog box fields.

Table 3 Open Device dialog box fields

Field	Description
Device Name	Either an IP address or a DNS name for the device, entered by the user.
Read Community	SNMP read community string for the device. Default is `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.
v3 Enabled	Specifies that v3 is enabled
User Name	Specifies the user name.
Authentication Protocol	Specifies the authentication protocol.
Authentication Password	Specifies the authentication password.
Privacy Protocol	Specifies a privacy protocol.
Privacy Password	Specifies the privacy password.

2 In the Device Name text box, type the DNS name or IP address of the device.

3   In the Read Community and Write Community text boxes, type the proper community strings.

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

4   Click Open.

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

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

Figure 4   Device view

Device Manager window

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

- Menu bar
- Toolbar
- Device view
- Status bar

Figure 5 Parts of the Device Manager window

Menu bar

Tool bar

Device view

Status bar

Menu bar

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

Table 4 Menu bar commands

Command	Description
Device	Opens the Open Device dialog box.
Edit	Opens edit dialog boxes for selected objects in the device view. This command also opens dialog boxes for managing files and running diagnostic tests.
Graph	Opens statistics dialog boxes for the selected object.
VLAN	Opens dialog boxes for managing VLANs, spanning tree groups (STGs), and Multi-Link Trunks.
Rmon	Opens RMON configuration and monitoring dialog boxes.
Actions	Provides quick opening of a Telnet session without going through other dialog boxes. It also provides quick opening of the Web Management Software Home page.
Help	Opens online Help topics for Device Manager and provides a legend for the port colors in the device view.

Toolbar

The toolbar contains buttons that provide quick access to commonly used commands and some additional actions.

Table 5   Toolbar buttons

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

Device view

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

Selecting objects

The types of objects contained in the device view are:

- A switch (called a unit in the menus and dialog boxes)
- Min-GBIC ports
- GBIC ports

Figure 6   Objects in the device view
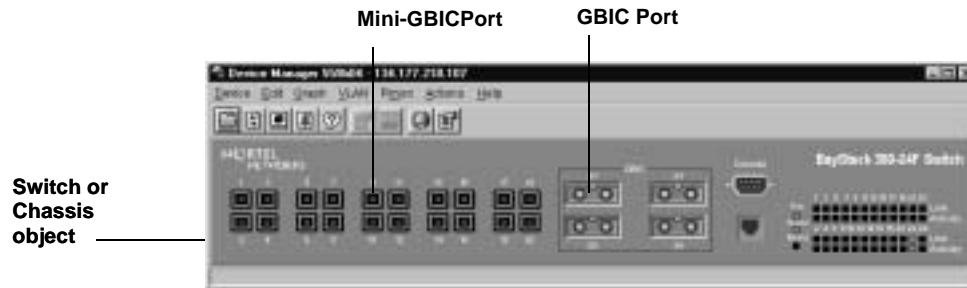
Selecting a single object

To select a single object:

➡ Click the edge of the object.

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

Selecting multiple objects

To select multiple objects of the same type (such as GBIC ports or or mini-GBIC ports):

➡ For a block of contiguous ports, drag to select the group of mini-GBIC ports.

To select all the ports in a switch:

➡ Choose Edit > Select > Ports.

LEDs and ports

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

For a full description of the LEDs for the Baystack 380, refer to *Using the BayStack 380-24F 1000 Switch*.

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

Table 6 shows the status assigned to each color.

Table 6 Port color codes

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

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

Figure 7   Color port legend
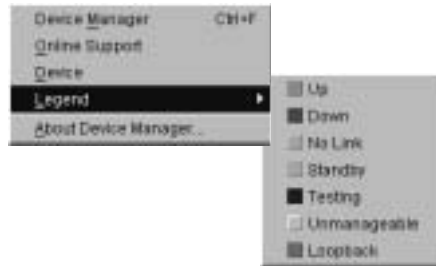
Shortcut menus

Each object in the device view has a shortcut menu that opens when you right-click a selected object. The switch unit shortcut menu (Figure 8) provides access to basic hardware information about the switch and to the graphing dialog boxes for the switch.

Figure 8   Switch unit shortcut menu
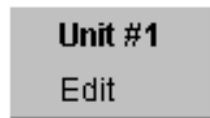
Table 7 describes the Edit command on the switch unit shortcut menu.

Table 7   Switch unit shortcut menu command

Command	Description
Edit	Opens a read-only dialog box that provides basic hardware information about the switch.

The port shortcut menu (Figure 9) provides a faster path for editing and graphing a single port; however, you can access the same options using the menu bar or the toolbar.

Figure 9   Port shortcut menu

```
Port 1/1
  Edit
  Graph
  Enable
  Disable
```
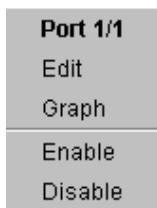
Table 8 describes the commands on the port shortcut menu.

Table 8   Port shortcut menu commands

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

Status bar

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

Using the buttons in Device Manager dialog boxes

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

Table 9   Device Manager buttons

Button	Name	Description
Insert	Insert	Opens a dialog box to create a new entry for a table; then from the dialog box, inserts the new entry in the table.
	Copy	Copies selected cells from a table.
	Paste	Pastes copied values to a currently selected table cell.
	Reset Changes	Causes changed (but not applied) fields to revert to their previous values.
	Print Table or Print Graph	Prints the table or graph that is displayed.
Stop	Stop/Refresh	Stops the current action (compiling, saving, and so forth). If you are updating or compiling a large data table, the Refresh button changes to a Stop button while this action is taking place. Clicking the Stop button interrupts the polling process.
	Export Data	Exports information to a file you specify. You can then import this file into a text editor or spreadsheet for further analysis.

Editing objects

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

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

The edit dialog box opens for that object.

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

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

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

Working with statistics and graphs

Device Manager tracks a wide range of statistics for each port. You can view and graph statistics for a single object or multiple objects. For information about the statistics tracked for the switch and ports, refer to "Statistics for single and multiple objects" on page 37 and "Graphing chassis statistics" on page 63.

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

Types of statistics

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

Table 10   Types of statistics

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

Types of graphs

With Device Manager, you can create line, area, bar, and pie graphs. Figure 10, Figure 11, Figure 12, and Figure 13 illustrate the different graph styles, respectively.

Figure 10 Line graph
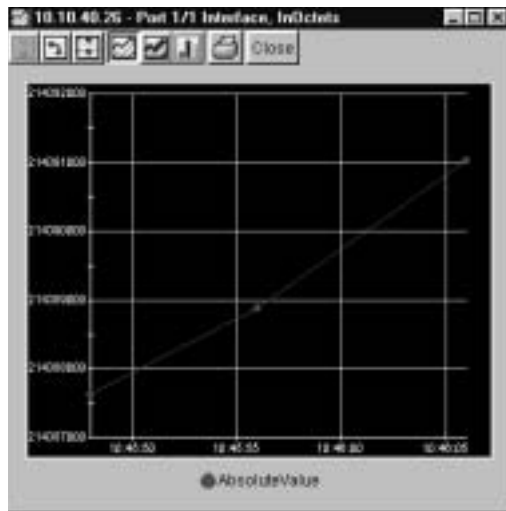
Figure 11 Area graph
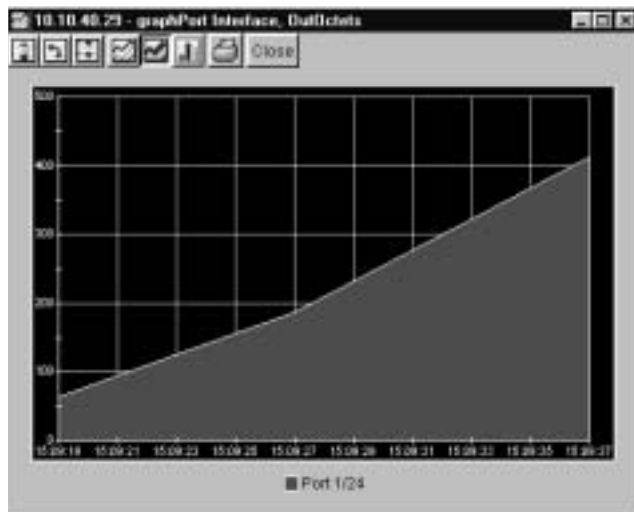
Figure 12 Bar graph
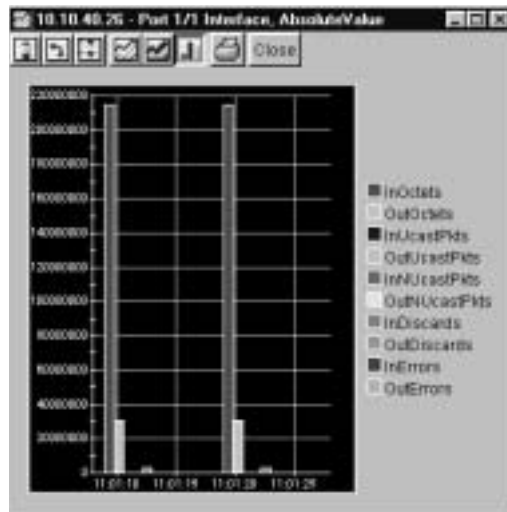
Figure 13 Pie graph

Statistics for single and multiple objects

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

The dialog box for a single object shows all six types of statistics for each counter (Figure 14).

Figure 14 Interface statistics for a single port

The statistics dialog box for multiple objects shows a single type of statistics (Table 10 on page 34) for the selected objects. For example, Figure 15 shows LastValue statistics for the selected ports.

Figure 15 Interface statistics for multiple ports

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

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

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

See the next section, "Viewing statistics as graphs," for instructions to use these buttons.

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

Viewing statistics as graphs

To create a graph for an object:

1 Select the object or objects to be graphed.

See "Selecting objects" on page 28.

2 Do one of the following:

- On the toolbar, click Graph Selected.

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

A statistics dialog box opens with tabs for different categories of statistics for the selected object (Figure 16).

Figure 16   Statistics dialog box for a port
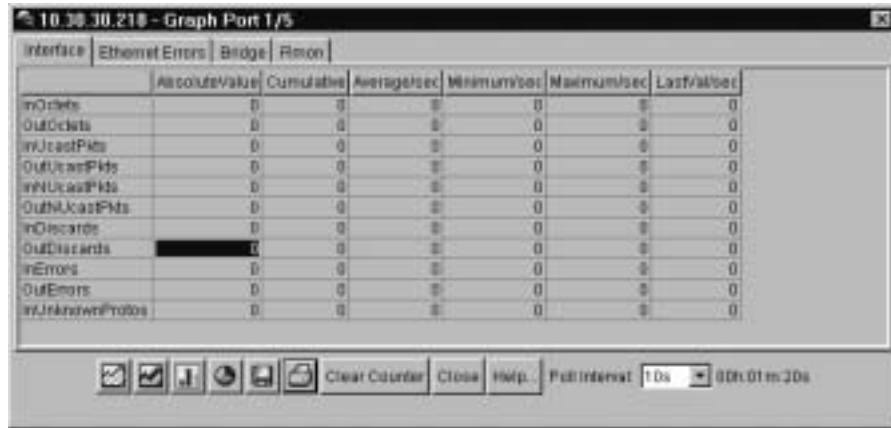
3   Select a tab for the group of statistics you want to view.

4   On the displayed data table, drag to select the cells you want to graph. (They must be in the same row or column.)

5   Click one of the graph buttons at the bottom of the dialog box

See "Types of graphs" on page 34.

A graph dialog box opens for the selected graph type.

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

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

Table 11 describes the buttons in the graph dialog boxes.

Table 11   Graph dialog box buttons

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

Telneting to a switch

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

To Telnet to a switch:

➡ Do one of the following:

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

A Telnet window to the switch opens.

Opening the Web-based management home page

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

To open the Web-based management home page:

➨ Do one of the following:

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

Figure 17   Open home page icon

The Web-based management home page opens (Figure 18).

Figure 18   Web-based management home page

Reference for the BayStack 380-24F Gigabit Switch Management Software
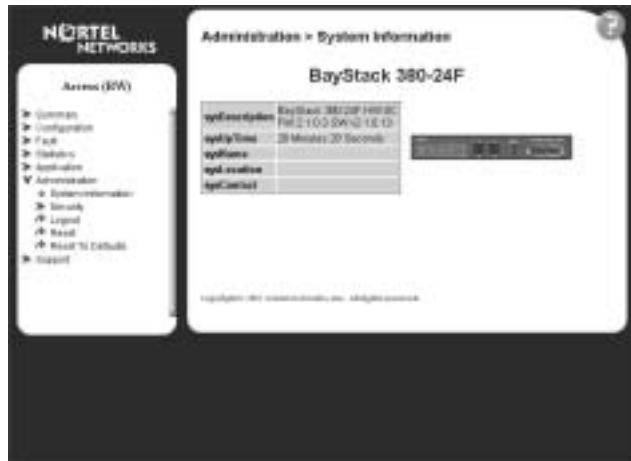
Trap log

You can configure a BayStack 380-24F Switch to send SNMP generic traps. When Device Manager is running, any traps received are recorded in the trap log. You set the maximum number of entries in the trap log using the Properties dialog box (Figure 2 on page 21). The default number of trap log entries is 500.

To view the trap log:

➡ Do one of the following:

• On the toolbar, click the Trap Log button.

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

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

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

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

For more information about traps and trap receivers, refer to *Using the BayStack 380-24F 1000 Switch*.

Online Help

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

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

Table 12   Help file locations

Platform	Default path
Windows 95, Windows 98, or Windows NT	JDM Directory\help\dmhelp.html
UNIX	DM-UNIX/DM/help

Chapter 2
Configuring and graphing the switch

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

Viewing switch IP information

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

To open the IP dialog box:

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

The Edit IP dialog box opens (Figure 19 on page 46) with the Globals tab displayed.

Globals tab

To open the Globals tab:

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

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

Figure 19 Globals tab
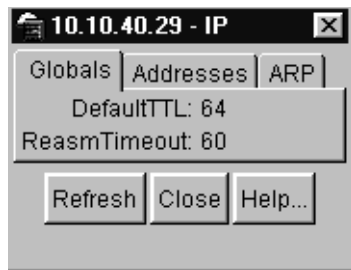
Table 13 describes the Globals tab items.

Table 13 Globals tab items

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

Addresses tab

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

To open the Addresses tab:

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

The IP dialog box opens with the Globals tab displayed (Figure 19 on page 46).

2 Click the Addresses tab.

The Addresses tab opens (Figure 20 on page 47).

Figure 20 Edit IP dialog box — IP Address tab

Table 14 describes the IP Address tab items.

Table 14 IP Addresses tab items

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

ARP tab

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

To open the ARP tab:

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

The IP dialog box opens with the Globals tab displayed (Figure 19 on page 46).

2 Click the ARP tab.

The ARP tab opens (Figure 21 on page 48).

Figure 21 Edit IP dialog box — ARP tab
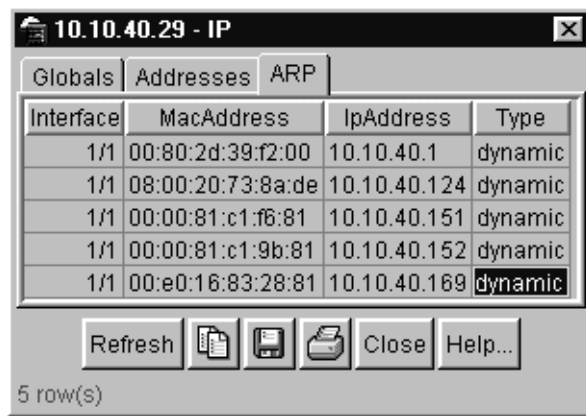
Table 15 describes the ARP tab items.

Table 15 ARP tab items

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

Editing the chassis configuration

You can edit a chassis configuration from the Edit Chassis dialog box (Figure 22 on page 50).

To open the Chassis dialog box:

1 Select the chassis.

2 Do *one* of the following:

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

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

System tab

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

To open the System tab:

1 Select the chassis.

2 From the shortcut menu, choose Edit > Chassis.

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

Figure 22   Edit Chassis dialog box — System tab

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

Table 16 describes the System tab items.

Table 16   System tab items

Item	Description
sysDescr	The assigned system name.
sysUpTime	The time since the system was last booted.
sysContact	Type the contact information (in this case, an e-mail address) for the system administrator.
sysName	Type the name of this device.
sysLocation	Type the physical location of this device.

Table 16 System tab items (continued)

Item	Description
AuthenticationTraps	Click enable or disable. When you select enabled, SNMP traps are sent to trap receivers for all SNMP access authentication. When you select disabled, no traps are received. To view traps, click the Trap toolbar button.
NextBootMgmtProtocol	The transport protocol(s) to use after the next boot of the agent.
CurrentMgmtProtocol	The current transport protocol(s) that the agent supports.
BootMode	The source from which to load the initial protocol configuration information to boot the switch the next time, local (from the switch), or net (over the network), or none.
ImageLoadMode	The source from which to load the agent image at the next boot.
CurrentImageVersion	The version number of the agent image that is currently used on the switch.
LocalStorageImageVersion	The version number of the agent image that is stored in flash memory on the switch.
NextBootDefaultGateway	The IP address of the default gateway for the agent to use after the next time the switch is booted.
CurrentDefaultGateway	The IP address of the default gateway that is currently in use.
NextBootLoadProtocol	The transport protocol to be used by the agent to load the configuration information and the image at the next boot.
LastLoadProtocol	The transport protocol last used to load the image and configuration information on the switch.
Reboot	Action object to reboot the agent. Reset — initiates a hardware reset. The agent does best efforts to return a response before the action occurs. If any of the combined download actions are requested, neither action occurs until the expiration of s5AgInfoScheduleBootTime, if set.

Base Unit Info tab

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

To open the Base Unit Info tab:

1   Select the chassis.

2   From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens with the System tab displayed (Figure 22 on page 50).

3   Click the Base Unit Info tab.

The Base Unit Info tab opens (Figure 23).

Figure 23   Edit Chassis dialog box — Base Unit Info tab
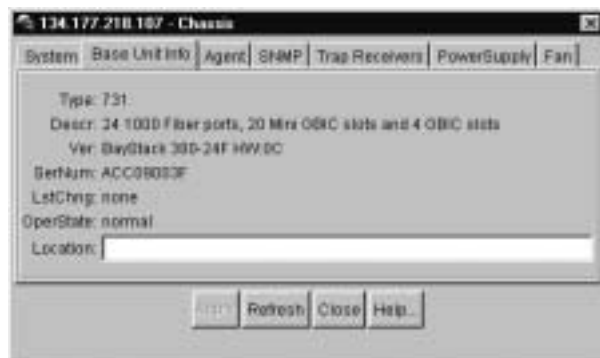
Table 17 describes the Base Unit Info tab items.

Table 17   Base Unit Info tab items

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

Table 17   Base Unit Info tab items (continued)

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

Agent tab

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

To open the Agent tab:

1   Select the chassis.

2   From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens (Figure 22 on page 50) with the System tab displayed.

3   Click the Agent tab.

The Agent tab opens (Figure 24).

Figure 24   Edit Chassis dialog box — Agent tab
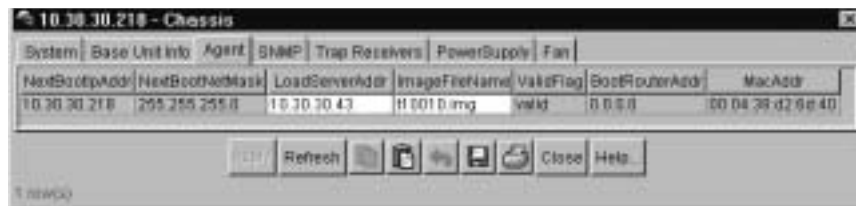
Table 18 describes the Agent tab fields.

Table 18 Agent tab fields

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

SNMP tab

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

To open the SNMP tab:

1 Select the chassis.

2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens (Figure 22 on page 50) with the System tab displayed.

3 Click the SNMP tab.

The SNMP tab opens (Figure 25).

Figure 25 Edit Chassis dialog box — SNMP tab

Table 19 describes the SNMP Info tab fields.

Table 19   SNMP tab fields

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

Trap Receivers tab

The Trap Receivers tab lists the devices that will receive SNMP traps from the BayStack 380-24F switch.

To open the Trap Receivers tab:

1   Select the chassis.

2   From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens (Figure 22 on page 50) with the System tab displayed.

3   Click the Trap Receivers tab.

The Trap Receivers tab opens (Figure 26).

Figure 26   Trap Receivers tab

Table 20 describes the Trap Receivers tab items.

Table 20   Edit Chassis dialog box — Trap Receivers tab items

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

Adding a Trap Receiver

To edit the network traps table:

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

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

Figure 27   Chassis, Insert Trap Receive dialog box
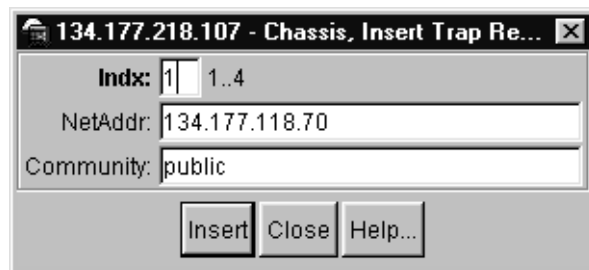
2   Type the Index, NetAddr, and the Community information.

> **Note:** Refer to Table 20 on page 57 for description of the Chassis, Insert Trap Receivers dialog box items.

3   Click Insert.

Power Supply tab

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

To open the Power supply tab:

1 Select the chassis.

2 From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens (Figure 22 on page 50) with the System tab displayed.

3 Click the Power Supply tab.

The Power supply tab opens (Figure 28).

Figure 28 Edit Chassis dialog box — Power Supply tab
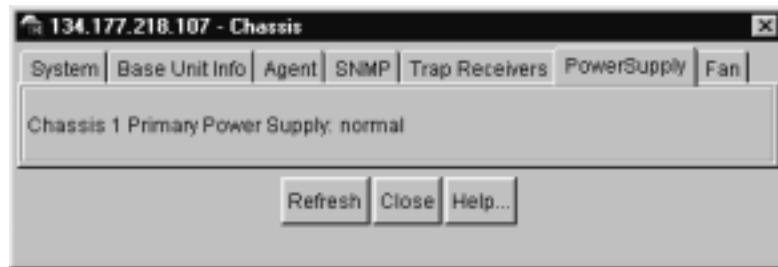
Table 21 describes the Power supply tab fields.

Table 21 Power supply tab fields

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

Fan tab

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

To open the Fan tab:

1   Select the chassis.

2   From the shortcut menu, choose Edit > Chassis.

The Chassis dialog box opens (Figure 22 on page 50) with the System tab displayed.

3   Click the Fan tab.

The Fan tab opens (Figure 28).

Figure 29   Edit Chassis dialog box — Fan tab

Table 22 describes the Fan tab fields.

Table 22   Fan tab fields

Field	Description
Desc	The fan type.
OperStat	The 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.

Working with configuration files

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

To open the Edit FileSystem dialog box:

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

The FileSystem dialog box opens (Figure 30).

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

Figure 30 FileSystem dialog box
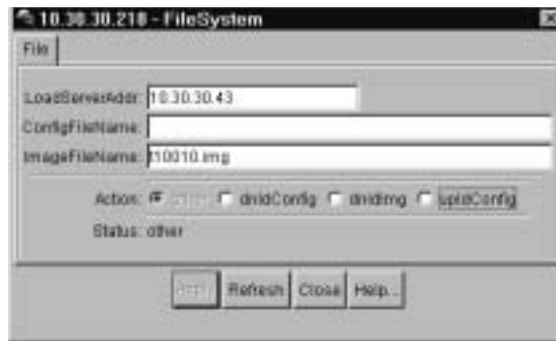
Table 23 describes the FileSystem dialog box items.

Table 23 FileSystem dialog box items

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

Table 23   FileSystem dialog box items (continued)

Item	Description
Action	• This object is used to download or upload a config file or an image file. In read operation, if there is no action taken since the boot up, it will return with a value of other. Otherwise, it will return the latest action such as: dnldConfig dnldImg upldConfig • In a write operation, the value that can be written is: dnldConfig - download a config file to a device. • The new config file will not take effect until the next boot cycle of the device. Possible values are: dnldImg - download an image to a device. upldConfig - upload a config file to a server from a device.
Result	This object 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 the shortcut menu, choose Graph.
- From Device Manager main menu, choose Graph > Chassis.
- On the toolbar, click Graph.

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

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

For descriptions of the chassis IP statistics, refer to Table 10 on page 34.

SNMP tab

The chassis SNMP tab lists chassis statistics.

To open the SNMP tab:

1   Select the chassis.

2   From the shortcut menu, choose Graph > Chassis.

    The Chassis dialog box opens (Figure 22 on page 50) with the System tab
    displayed.

3   Click the SNMP tab.

    The SNMP tab opens (Figure 31).
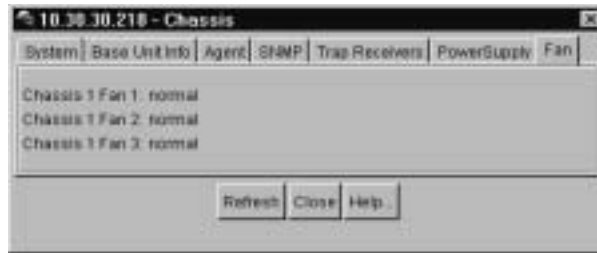
Figure 31 Graph Chassis dialog box — Chassis SNMP tab

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

Table 24 describes the SNMP tab fields.

Table 24 SNMP tab fields

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

Table 24 SNMP tab fields (continued)

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

214393-A

Table 24   SNMP tab fields (continued)

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

IP tab

The IP tab shows IP information for the chassis.

To open the IP tab:

1   Select the chassis.

2   Do *one* of the following:

   •   From Device Manager main menu, choose Graph > Chassis.

   •   From the shortcut menu, choose Graph.

   •   On the toolbar, click Graph.

      The Chassis dialog box opens (Figure 31 on page 65) with the SNMP tab displayed.

3   Click the IP tab.

   The IP tab opens (Figure 32).

Figure 32   Graph Chassis dialog box — IP tab

Table 25 describes the Chassis IP tab fields

Table 25   Chassis IP tab fields

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

Table 25 Chassis IP tab fields (continued)

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

Reference for the BayStack 380-24F Gigabit Switch Management Software

Table 25 Chassis IP tab fields (continued)

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

ICMP In tab

The chassis ICMP In tab shows ICMP In statistics.

To open the ICMP In tab:

1 Select the chassis.

2 Do *one* of the following:

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

The Chassis dialog box opens (Figure 31 on page 65) with the SNMP tab displayed.

3 Click the ICMP In tab.

The ICMP In tab opens (Figure 33).

Figure 33 Graph Chassis dialog box — ICMP In tab
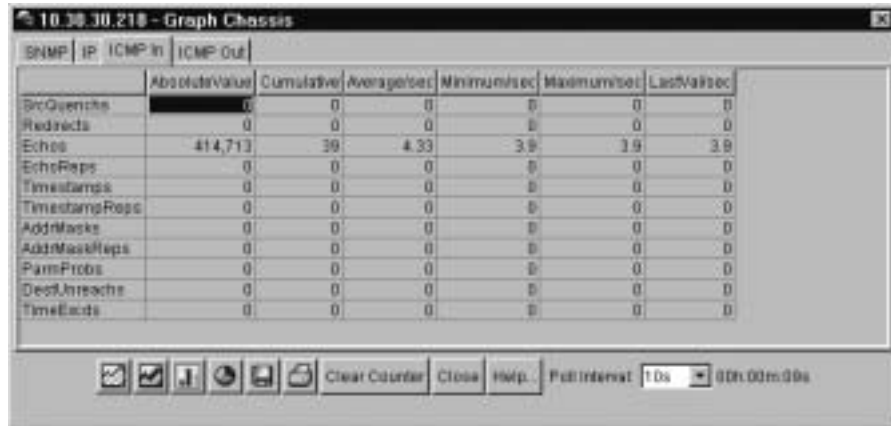
Table 26 describes the ICMP In tab fields.

Table 26 ICMP In tab fields

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

ICMP Out tab

The chassis ICMP Out shows ICMP Out statistics.

To open the ICMP Out tab:

1 Select the chassis.

2 Do *one* of the following:

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

The Chassis dialog box opens (Figure 31 on page 65) with the SNMP tab displayed.

3 Click the ICMP Out tab.

The ICMP Out tab opens (Figure 34).

Figure 34 Graph Chassis dialog box — ICMP Out tab

Table 27 describes the ICMP Out tab fields.

Table 27 ICMP Out tab fields

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

Chapter 3
Configuring and graphing ports

This chapter describes how you use Device Manager to configure and graph ports on a BayStack 380-24F Switch.

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

Viewing and editing a single port configuration

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

1 Double-click on a single port or select the ports you want to edit.

2 Do one of the following:

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

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

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

Interface tab for a single port

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

To view the Interface tab:

1 Select the port you want to edit.

2 Do one of the following:

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

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

Figure 35   Port dialog box — Interface tab

Table 28 describes the Interface tab items for a single port.

Table 28   Interface tab items for a single port

Field	Description
Index	A unique value assigned to each interface. The value ranges between 1..24.
Descr	The type of switch and number of ports.
Type	The media type of this interface.
Mtu	The size of the largest packet, in octets, that can be sent or received on the interface.
PhysAddress	The MAC address assigned to a particular interface.
AdminStatus	The 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	The 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	The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, the value is zero.
Speed	Current speed.
AutoNegotiate	Indicates whether this port is enabled for autonegotiation or not.
AdminDuplex	The administrative duplex mode of the port (full).
AdminSpeed	Set the port's speed.
OperSpeed	The current operating speed of the port.

Reference for the BayStack 380-24F Gigabit Switch Management Software

Table 28 Interface tab items for a single port (continued)

Field	Description
MltId	The MultiLink Trunk to which the port is assigned (if any).
OperDuplex	The duplex mode of the port (full duplex).

VLAN tab for a single port

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

To view the VLAN tab:

1 Select the port you want to edit.

2 Do one of the following:

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

The Port dialog box for a single port opens (Figure 35 on page 76) with the Interface tab displayed.

3 Click the VLAN tab.

The VLAN tab opens (Figure 36).

Figure 36 Edit Port dialog box — VLAN tab

Table 29 describes the VLAN tab items.

Table 29   VLAN tab items for a single port

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

STG tab for a single port

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

To view the STG tab:

1 Select the port you want to edit.

2 Do one of the following:

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

The Port dialog box for a single port opens (Figure 35 on page 76) with the Interface tab displayed.

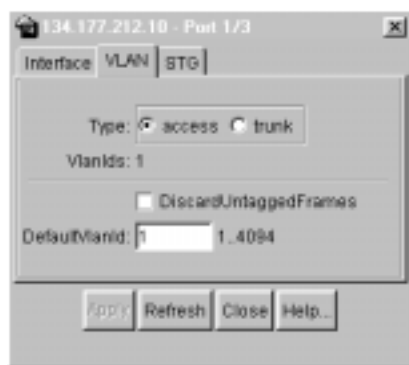**3** Click the STG tab.

The STG tab opens (Figure 37).

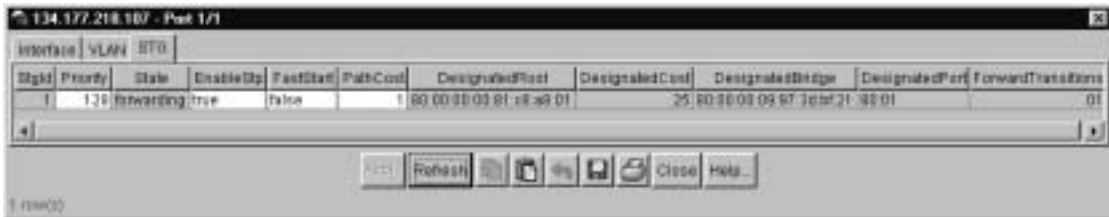**Figure 37** Edit Port dialog box — STG tab

Table 30 describes the STG tab items.

Table 30 STG tab items for a single port

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

Configuring multiple ports

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

To open the graph port dialog box:

1 Select the port or ports you want to edit.

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 Selected.

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

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

Interface tab for multiple ports

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

To view or edit the Interface tab for multiple ports:

1 Select the ports that you want to edit.

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

2 Do one of the following:

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

The Interface tab (Figure 38) shows port interface statistics.

Figure 38 Edit Ports — Interface tab

Table 31 describes the Interface tab fields.

Table 31 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 and number of ports.
Type	Media type for this interface.
Mtu	Size of the largest packet, in octets, that can be sent or received on the interface.
PhysAddress	MAC address assigned to a particular interface.
AdminStatus	Current administrative state of the interface, which can be one of the following: • 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 31 Interface tab fields for multiple ports (continued)

Field	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 administrative duplex mode of the port (full).
OperDuplex	Indicate duplex value of the port.
AdminSpeed	The speed of a port: 1000 mbps
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 35 on page 76) opens with the Interface tab displayed.

3 Click the VLAN tab.

The VLAN tab opens (Figure 39).
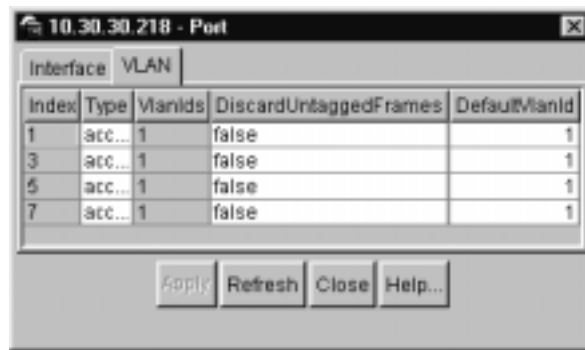
Figure 39 VLAN tab for multiple ports

Table 32 describes the VLAN tab fields for multiple ports.

Table 32 VLAN tab fields for multiple ports

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

Graphing port statistics

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

To open the graphPort dialog box for graphing:

1   Select the port or ports you want to graph.

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

2   Do one of the following:

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

The graphPort dialog box for a single port (Figure 40 on page 87) or for multiple ports opens with the Interface tab displayed.

Interface tab for graphing ports

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

To open the Interface tab for graphing:

1   Select the port or ports you want to graph.

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

2   Do one of the following:

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

The Port dialog box for a single port (Figure 40 on page 87) or for multiple ports opens with the Interface tab displayed.

Figure 40 Interface tab for graphing ports

Table 33 describes the Interface tab fields for graphing ports.

Table 33 Port Interface tab fields for multiple ports

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

Table 33 Port Interface tab fields for multiple ports (continued)

Field	Description
InErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
OutErrors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.
InUnknownProtos	For packet-oriented interfaces, the number of packets received via the interface that were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of transmission units received via the interface that were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter will always be 0.

Ethernet Errors tab for graphing ports

The port Ethernet Errors tab shows port Ethernet Errors statistics.

To open the Ethernet Errors tab for graphing:

1 Select the port or ports you want to graph.

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

2 Do one of the following:

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

The Port dialog box for a single port (Figure 35 on page 76) or for multiple ports opens with the Interface tab displayed.

3 Click the Ethernet Errors tab.

The Ethernet Errors tab opens (Figure 41).

Figure 41   Graph Port dialog box — Ethernet Errors tab

Table 39 describes the Ethernet Errors tab fields.

Table 34   Ethernet Errors tab fields

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

Table 34   Ethernet Errors tab fields (continued)

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

Bridge tab

The Bridge tab displays port frame statistics.

To open the Bridge tab for graphing:

1 Select the port or ports you want to graph.

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

2 Do one of the following:

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

   The Port dialog box for a single port (Figure 35 on page 76) or for multiple
   ports opens with the Interface tab displayed.

3 Click the Bridge tab.

   The Bridge tab for graphing ports opens (Figure 42).

Figure 42 Graph Port dialog box — Bridge tab
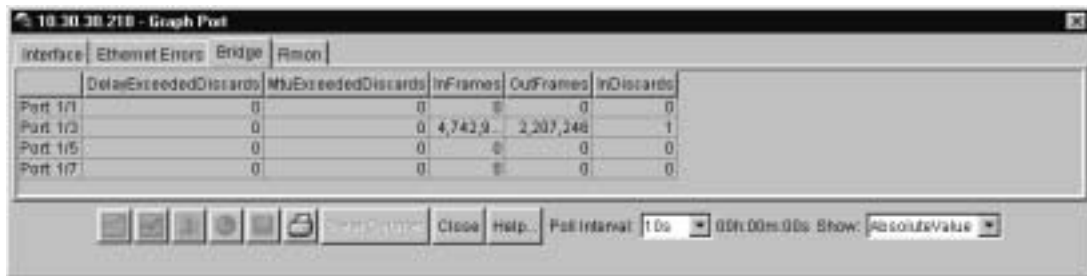
Table 35 describes the Bridge tab fields.

Table 35 Bridge tab fields

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

RMON tab

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

To open the RMON tab for graphing:

1 Select the port or ports you want to graph.

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

2 Do one of the following:

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

The Port dialog box for a single port (Figure 35 on page 76) or for multiple ports opens with the Interface tab displayed.

3 Click the RMON tab.

The RMON tab for graphing ports opens (Figure 43).
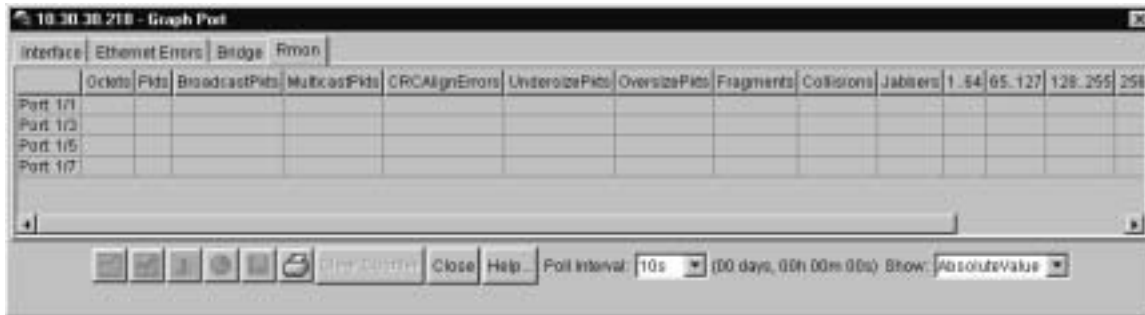
Figure 43 Graph Port dialog box — RMON tab

Table 36 describes the RMON tab fields.

Table 36 RMON tab fields

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

Table 36 RMON tab fields (continued)

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

Chapter 4
Setting up MultiLink Trunk ports

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

MultiLink Trunk (MLT) features

A number of Nortel Networks products implement MultiLink Trunking and have different features and requirements based on the architecture of the device. For the BayStack 380-24F, MultiLink Trunking has the following general features and requirements:

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

Setting up MLTs

To set up MLTs:

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

The MLT dialog box opens (Figure 44).

Reference for the BayStack 380-24F Gigabit Switch Management Software

Figure 44 MLT dialog box
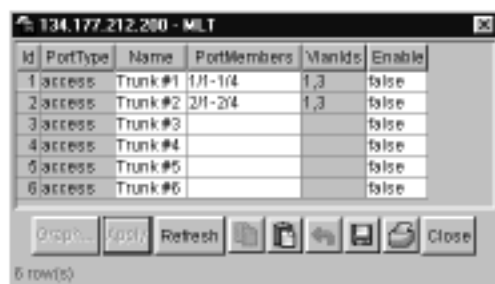
The active MultiLink Trunks are displayed with the fields described in Table 37.

Table 37 MLT dialog box fields

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

Adding ports to a MultiLink Trunk

To add ports to an existing MLT:

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

The MLT dialog box opens (Figure 44 on page 98).

2 Double-click the PortMembers field.

The PortMembers dialog box opens (Figure 45).

Figure 45   PortMembers dialog box

3 Click the port numbers you want to add.

4 Click OK.

5 In the Enable column, select True to enable your selection.

MultiLink Trunk statistics

To view MLT interface statistics:

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

The MLT dialog box opens (Figure 44 on page 98).

2 Select an MLT row and then click Graph.

The Statistics, MLT window (Figure 46) opens with the Interface tab displayed.

Figure 46 MLT Statistics — Interface tab

Table 38 describes the fields in the Interface tab.

Table 38 Interface tab fields

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

MultiLink Trunk Ethernet error statistics

To view MultiLink Trunk Ethernet error statistics:

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

    The MLT dialog box opens (Figure 44 on page 98).

2   Select an MLT by clicking anywhere within a field in the row.

3   Click Graph.

    The Statistics, MLT dialog box opens (Figure 46 on page 100) with the
    Interface tab displayed.

4   Click the Ethernet Errors tab.

    The Ethernet Errors tab opens (Figure 47).

Figure 47   MLT Statics dialog box — Ethernet Errors tab

Table 39 describes the fields in the Ethernet Errors tab.

Table 39 Ethernet Errors tab fields

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

Table 39   Ethernet Errors tab fields (continued)

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

Chapter 5
Creating and managing VLANs

This chapter describes using Device Manager to manage VLANs on your BayStack 380-24F Gigabit Switch. The chapter covers creating, editing, and deleting VLANs. It includes the following sections:

- VLANs (next)
- Creating VLANs (page 106)
- Modifying and managing existing VLANs (page 109)

VLANs

A VLAN is a collection of ports on one or more switches that define a broadcast domain. The Baystack 380-24F Gigabit switch supports port-based VLANs.

For a further description of VLANs, refer to *Using the BayStack 380-24F Gigabit Switch*.

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

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

Creating VLANs

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

VLAN Information

To open the VLAN dialog box:

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

The VLAN dialog box opens (Figure 48).

Figure 48   VLAN dialog box
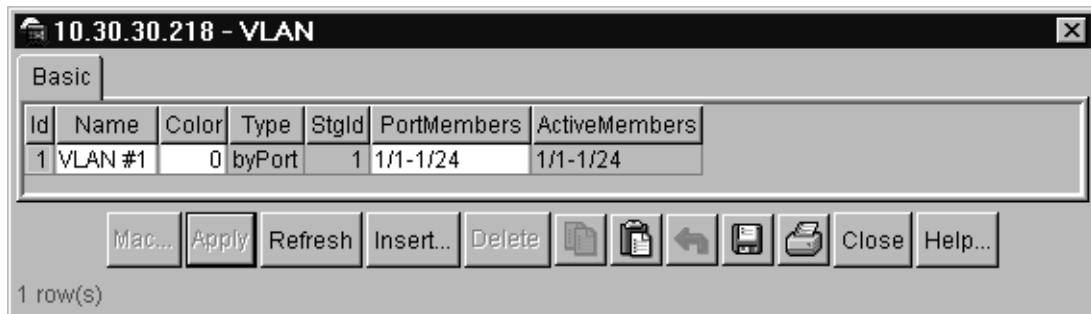
Table 40 describes the VLAN dialog box fields.

Table 40   VLAN dialog box fields

Field	Description
Id	The VLAN ID for the VLAN (unlabeled farthest left column).
Name	Name of the VLAN.
Color	An administratively-assigned color code for the VLAN. The value of this object is used by the VLAN Manager GUI tool to select a color when it draws this VLAN on the screen.
Type	Indicates the type of VLAN: byPort.
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.

Creating a port-based VLAN

To create a port-based VLAN:

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

The VLAN dialog box opens (Figure 48 on page 106).

2 Click Insert.

The VLAN Insert Basic dialog box for creating VLANs opens (Figure 49). This dialog box opens with the Type field set to byPort.

Figure 49 VLAN, Insert Basic dialog box for a port-based VLANs
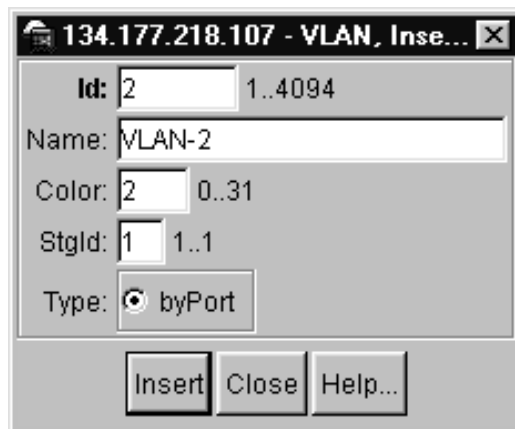
3 Type the VLAN ID.

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

4 Type the VLAN name (optional).

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

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

6 Click Insert.

7 Specify the port membership by clicking the PortMembers buttons.

Accepting untagged frames

In the BayStack 380-24F, you configure whether or not untagged frames are sent or received on the port level. Refer to "VLAN tab for a single port" on page 78 for VLAN tab field descriptions. You can select whether or not to discard untagged frames received on a port:

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

To set a port to discard untagged frames it receives:

1 In the Device Manager main window, select a port.

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

The Port dialog box opens with the Interface tab displayed (Figure 35 on page 76).

3 Click the VLAN tab.

The VLAN tab opens (Figure 50).

Figure 50 VLAN tab

Select the DiscardTaggedFrames and the DiscardUntaggFrames check boxes.

4 Click Apply.

Modifying and managing existing VLANs

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

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

The VLAN dialog box opens (Figure 51). The VLAN dialog box displays all defined VLANs, their configurations, and their current status.

Figure 51   VLAN dialog box
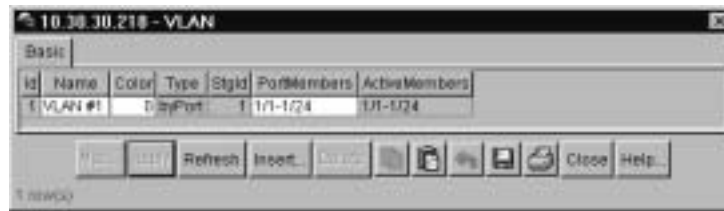
> **Note:** After a VLAN is created, you cannot change the VLAN type.
> The VLAN must be deleted and a new VLAN of the chosen type created.

Table 41 describes the fields in the VLAN dialog box.

Table 41   VLAN dialog box fields

Field	Description
Id	The VLAN ID for the VLAN (unlabeled farthest left column).
Name	The name of the VLAN.
Color	The color used, for visual purposes only, by VLAN Manager to associate a color with a VLAN. The assigned color does not affect the behavior of a frame, only the attributes assigned to the VLAN.
Type	Indicates the type of VLAN: byPort.
StgId	The spanning tree group ID to which the VLAN belongs.
PortMembers	The ports that are members of the VLAN.
ActiveMembers	Set of ports that are currently active in the VLAN. Active ports include all static ports and any dynamic ports where the VLAN policy was met.

Chapter 6
Setting up bridging

The Bridge parameters allow you to view MAC address table for a Baystack 380-24F Gigabit Switch.

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

• Base tab (next)

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 52).

Figure 52 Base tab
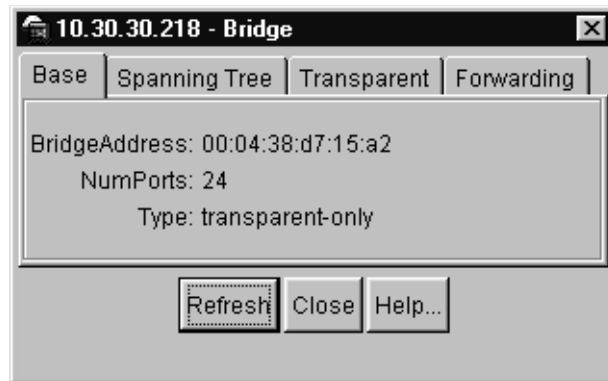
Table 42 describes the Base tab fields.

Table 42 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 fact 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 53).

Figure 53 Spanning Tree tab
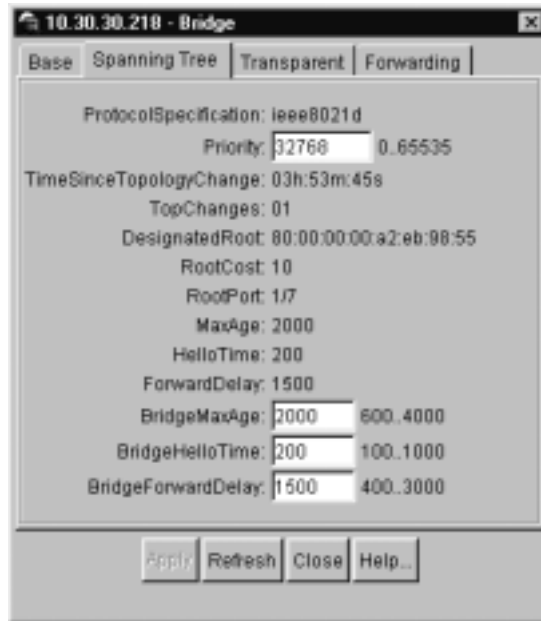
Table 43 describes the Spanning Tree tab fields.

Table 43   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.
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.

Table 43   Spanning Tree tab fields (continued)

Field	Description
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 a bridge when it is acting as the root. **Note**: 802.1D-1990 specifies that the range is related to the value of BridgeHelloTime. The granularity of this timer is specified by 802.1D-1990 to be 1 second. A badValue error may be returned if the value set is not a whole number.
BridgeHelloTime	Value that the bridge uses for HelloTime when the bridge is acting as the root. The granularity of this timer is specified by 802.1D- 1990 to be one second. An agent may return a badValue error if a set is attempted to a value that is not a whole number of seconds.
TimeSinceTopologyChange	Value that all bridges use for ForwardDelay when this bridge is acting as the root. Note: 802.1D-1990 specifies that the range for this parameter is related to the value of dot1dStpBridgeMaxAge. The granularity of this timer is specified by 802.1D-1990 to be one second. An agent may return a badValue error if a set is attempted to a value that is not a whole number of seconds.

Transparent tab

The Transparent tab contains information about a specific unicast MAC address, 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.

2 Click the Transparent tab.

The Transparent tab opens (Figure 54).

Figure 54 Transparent tab

Table 44 describes the Transparent tab items.

Table 44 Transparent tab items

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

Forwarding tab

The Forwarding tab displays the current state of the port, as defined by application of the Spanning Tree Protocol. This state controls what action a port takes 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 Forwarding tab:

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

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

2   Click the Forwarding tab.

The Forwarding tab opens (Figure 55).

Figure 55   Forwarding tab
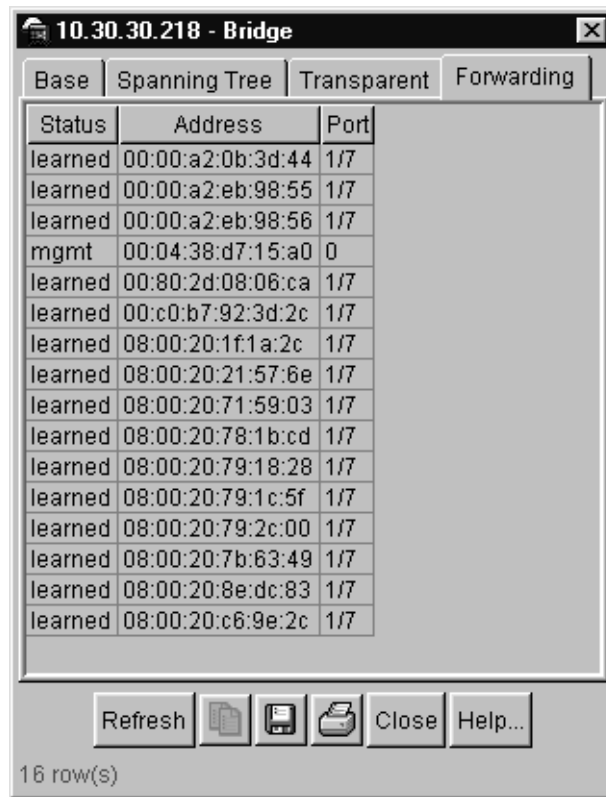
Table 45 describes the Forwarding tab fields.

Table 45 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).

Chapter 7
Troubleshooting Device Manager

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

- Topology tab (next)
- Topology Table tab (page 120)

Topology tab

To view topology information:

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

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

Figure 56 Diagnostics dialog box — Topology tab
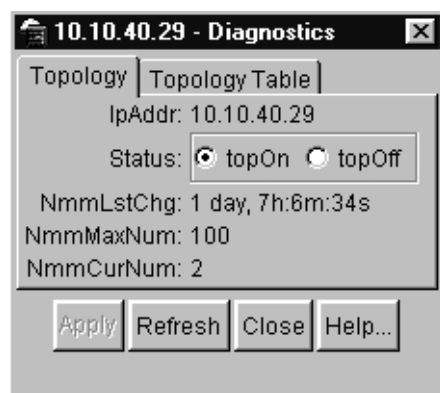
Table 46 describes the Topology tab items.

Table 46 Topology tab items

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

Topology Table tab

To view more topology information:

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

The Diagnostics dialog box opens with the Topology tab displayed (Figure 56 on page 119).

2 Click the Topology Table tab.

The Topology Table tab opens (Figure 57).

Figure 57 Diagnostics dialog box — Topology Table tab

Table 47 describes the Topology Table tab fields.

Table 47   Topology Table tab fields

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

Chapter 8
RMON

The Remote Network Monitoring (RMON) MIB is an interface between the RMON agent on a BayStack 380-24F Gigabit Switch and an RMON management application, such as the Device Manager. It defines objects that are suitable for the management of any type of network, but some groups are targeted for Ethernet networks in particular. The RMON agent continuously collects statistics and proactively monitors switch performance. You can view this data through the Device Manager.

RMON has three major functions:

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

Working with RMON information

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

Viewing statistics

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

To view RMON Ethernet statistics:

1   Select an object (port).

2 Do one of the following:

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

The Graph Port dialog box opens with the Interface tab displayed (Figure 35 on page 76).

3 Click the RMON tab.

The RMON tab opens (Figure 58).

Figure 58 Port dialog box — RMON tab

For descriptions of the RMON tab fields, refer to Table 36 on page 95. For descriptions of the statistics columns, refer to Table 10 on page 34.

Viewing history

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

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

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

To view RMON history:

1   Select an object (port or chassis).

2   On the toolbar, click Graph.

The graph Port dialog box opens with the Interface tab displayed (Figure 40 on page 87).

3   Click the RMON tab.

The RMON tab opens (Figure 59).

Figure 59   Port dialog box — RMON tab
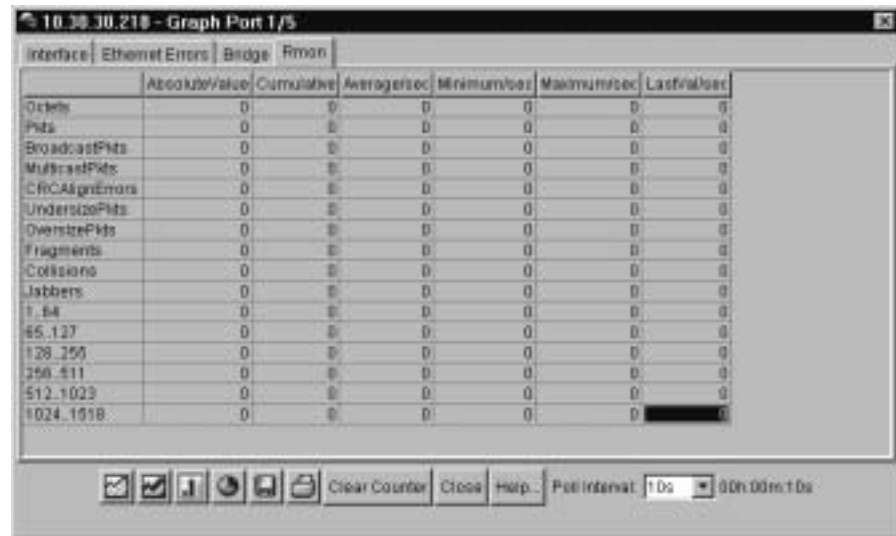
Creating a history

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

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

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

The RMONControl dialog box opens with the History tab displayed
(Figure 60).

Figure 60   History tab

Table 48 describes the History fields.

Table 48 History tab fields

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

2   Select an index and then click Insert.

The RMONControl, Insert History dialog box opens (Figure 61).

Figure 61   RMONControl, Insert History dialog box
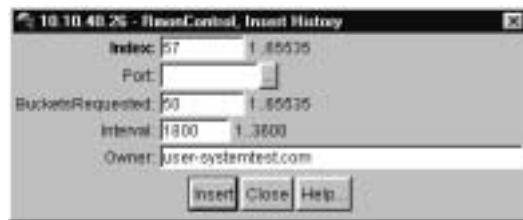
3 Select the port from the port list or type the port number.

4 Set the number of buckets.

The default is 50.

5 Set the interval.

The default is 1800 seconds.

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

7 Click Insert.

RMON collects statistics using the index, port, bucket, and interval that you specified.

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 60 on page 126).

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

3 Click Delete.

The entry is removed from the table.

Enabling Ethernet statistics gathering

You can use RMON to gather Ethernet statistics.

To gather Ethernet statistics:

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

The RMONControl dialog box opens with the History tab displayed (Figure 60 on page 126).

2 Click the Ether Stats tab.

The Ether Stats tab opens (Figure 62).

Figure 62 RMONControl dialog box — Ether Stats tab
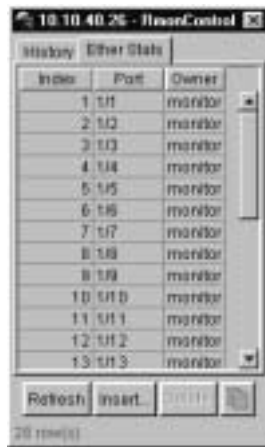
Table 49 describes the Ether Stats tab fields.

Table 49 Ether Stats tab fields

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

3 Click Insert.

The RMONControl, Insert Ether Stats dialog box opens (Figure 63).

Figure 63 RMONControl, Insert Ether Stats dialog box
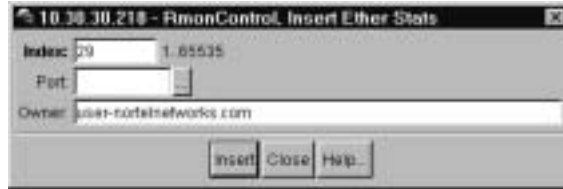
4 Select the port(s).

Enter the port number you want or select the port from the list menu (Figure 64).

Figure 64 RMONControl, Insert Ether Stats dialog box port list

Device Manager assigns the index.

5 Click Insert.

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

Disabling Ethernet statistics gathering

To disable Ethernet statistics that you have set:

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

The RMONControl dialog box opens with the History tab displayed (Figure 60 on page 126).

2   Click the Ether Stats tab.

The Ether Stats tab opens (Figure 63 on page 130).

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

4   Click Delete.

The Ether Stats entry is removed from the table.

Alarms

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

All alarms share the following characteristics:

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

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

How RMON alarms work

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

The alarm's upper limit is called the *rising value*, and its lower limit is called the *falling value*. RMON periodically samples the data based upon the alarm interval. During the *first* interval that the data passes above the rising value, the alarm fires as a rising event. During the first interval that the data drops below the falling value, the alarm fires as a falling event (Figure 65).

Figure 65 How alarms fire

Rising value

Falling value

● Alarm fires
○ No firing

7821EA
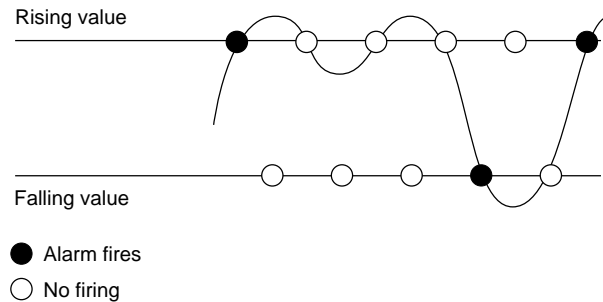
It is important to note that the alarm fires during the first interval that the sample goes out of range. No additional events are generated for that threshold until the opposite threshold is crossed. Therefore, it is important to carefully define the rising and falling threshold values for alarms to work as expected. Otherwise, incorrect thresholds causes an alarm to fire at every alarm interval.

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

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

If the alarm is defined with a falling threshold less than 260 (assuming the alarm polling interval is 10 seconds), say 250, then the rising alarm can fire only once (Figure 66). The reason is that for the rising alarm to fire a second time, the falling alarm (the opposite threshold) must fire. Unless the port becomes inactive or

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

Figure 66 Alarm example — threshold less than 260

Rising threshold = 326?

320

Baseline traffic = 260

Falling threshold = 250

7822EA
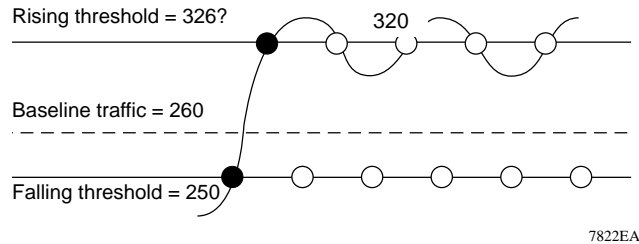
Creating alarms

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

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

Most alarm variables related to Ethernet traffic are set to *delta* value. Delta alarms are defined based on the difference in the value of the alarm variable between the start of the polling period and the end of the polling period. Delta alarms are sampled twice per polling period. For each sample, the last two values are added together and compared to the threshold values. This process increases precision

and allows for the detection of threshold crossings that span the sampling boundary. If you track the current values of a given delta-valued alarm and add them together, therefore, the result is twice the actual value. (This result is not an error in the software.)

Alarm Manager example

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

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

1 Do one of the following:

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

The Alarm Manager dialog box opens (Figure 67).

Figure 67   Alarm Manager dialog box

2   In the variable field, select a variable for the alarm from the list and a port (or other ID) on which you want to set an alarm (Figure 68).

Figure 68   Alarm variable list

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

- A chassis alarm ends in .x where the x index is hard-coded. No further information is required.

- A card, spanning tree group (STG) or EtherStat alarm ends with a dot (.). You must enter a card number, STG ID, IP address, or EtherStat information.

- A port alarm ends with no dot or index and requires using the port shortcut menu. An example of a port alarm would be ifInOctets (interface incoming octet count).

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

3   For this example, select a rising value of 4 and a falling value of 0.

4   Leave the remaining fields at their default values, including a sample type of Delta.Click Insert.

If you want to make field changes, see the field descriptions shown in Table 50.

Table 50   RMON Insert Alarm dialog box fields

Field	Description	
Variable	Name and type of alarm—indicated by the format:	
	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	Can be either absolute or delta.	
	For more information about sample types, refer to "Creating alarms" on page 133.	
Sample Interval	Time period (in seconds) over which the data is sampled and compared with the rising and falling thresholds.	
Index	Uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device.	
Threshold Type	Rising Value	Falling Value
Value	When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, generates a single event.	When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, generates a single event.
Event Index	Index of the event entry that is used when a rising threshold is crossed. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. (Generally, accept the default that is already filled in.)	Index of the event entry that is used when a falling threshold is crossed. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. (Generally, accept the default that is already filled in.)

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

1   Select the port on which you have created an alarm.

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

The RMONControl dialog box opens with the History tab displayed (Figure 60 on page 126).

3   Click the Ether Stats tab to view the statistics (Figure 64 on page 130).

Alarms tab

To view information about alarms:

➡ Click on RMON > Alarms

The RMONAlarms dialog box opens with the Alarms tab (Figure 69) displayed.

Figure 69   RMONAlarms dialog box — Alarms tab

Table 51 describes the fields on the Alarms tab.

Table 51   Describes the fields on the Alarms tab

Field	Description
Index	Uniquely identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular interval for an object on the device
Interval	The interval in seconds over which data is sampled and compared with the rising and falling thresholds. When setting this variable, note that in the case of deltaValue sampling, you should set the interval short enough so that the sampled variable is very unlikely to increase or decrease by more than $2^{31} - 1$ during a single sampling interval.
Variable	The object identifier of the particular variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Counter, Gauge, or TimeTicks) may be sampled.
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value of this object is absoluteValue(1), the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. If the value of this object is deltaValue(2), the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.

Table 51 Describes the fields on the Alarms tab (continued)

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

To delete an alarm:

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

The RMONAlarms dialog box opens with the Alarms tab (Figure 69) displayed.

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

3   Click Delete.

Events

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

How events work

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

• RisingEvent
• FallingEvent

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

Viewing an event

To view a table of events:

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

The RMONAlarms dialog box opens displaying the Alarms tab (Figure 69 on page 137).

2   Click the Events tab.

The Events tab opens (Figure 70).

Figure 70   RMONAlarms dialog box — Events tab
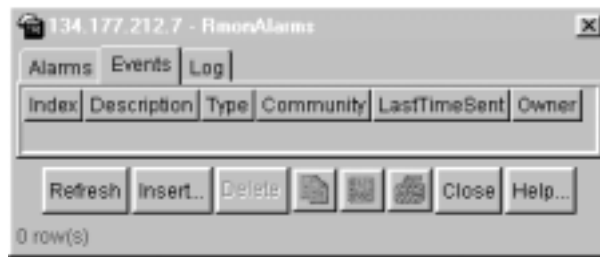
Table 52 describes the RMONAlarms Events tab fields.

Table 52   Events tab fields

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

Creating an event

To create an event:

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

The RMONAlarms, Insert Events dialog box opens (Figure 71).

Figure 71 Insert Events dialog box
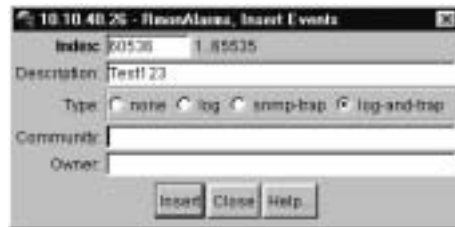
2 In the Description field, type a name for the event.

3 Select the type of event you want.

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

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

4 Click Insert.

The new event is displayed in the Events tab (Figure 72).

Figure 72 New event in the Events tab
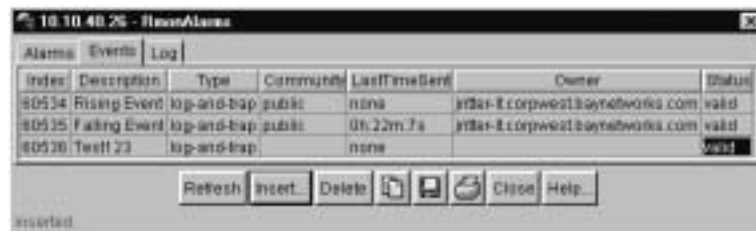
Deleting an event

To delete an event:

1 In the Events tab, highlight an event Description.

2 Click Delete.

The event is removed from the table.

Log information

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

To view the Log tab:

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

The RMONAlarm dialog box opens with the Alarms tab displayed (Figure 69 on page 137).

2 Click the Log tab.

The Log tab opens (Figure 73).

Figure 73 Log tab
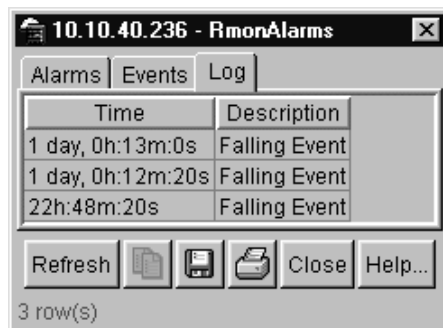
Table 53 describes the Log tab fields.

Table 53 Log tab fields

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

Chapter 9
Security parameters

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

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

- General tab (next)
- AuthConfig tab (page 150)
- SecurityList tab (page 153)
- AuthStatus tab (page 153)
- AuthViolation (page 155)

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 74).

Figure 74 General tab
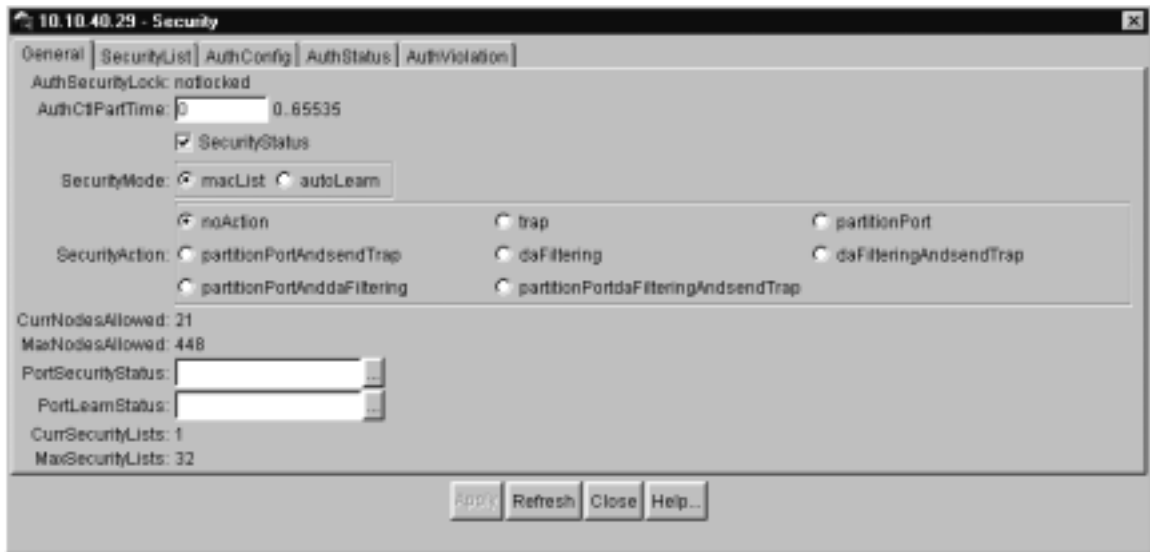
Table 54 describes the General tab items.

Table 54 General tab items

Items	Description
AuthSecurityLock	If this parameter is listed as "locked," the agent refuses all requests to modify the security configuration. Entries also include: • 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 54 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 receiver.
	• daFiltering: Port filters out the frames where the destination address field is the MAC address of unauthorized Station.
	• daFilteringAndsendTrap: Port filters out the frames where the desitnation address field is the MAC address of unauthorized station. Traps are sent to trap receiver(s).
	• partitionPortAnddaFiltering: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station.
	• partitionPortdaFilteringAndsendTrap: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. Traps are sent to trap receiver(s).
	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.
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 74 on page 146).

2 Click the SecurityList tab.

The SecurityList tab opens (Figure 75).

Figure 75 SecurityList tab
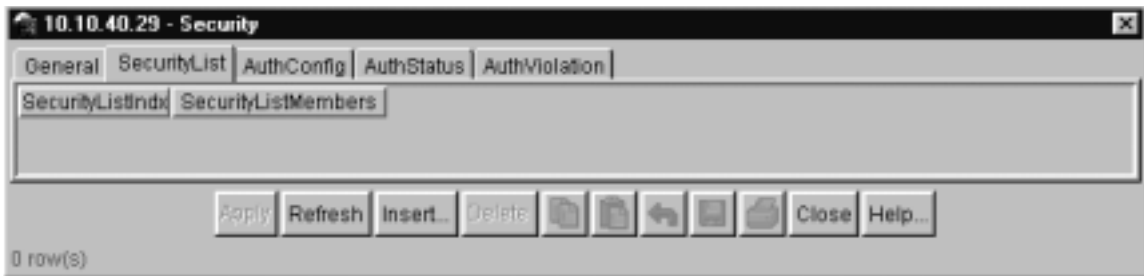
Table 55 describes the SecurityList tab fields.

Table 55 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 (Figure 74 on page 146).

2 Click the SecurityList tab.

The SecurityList tab opens (Figure 75 on page 148).

3 Click inside a row.

4 Click Insert.

The Security, Insert SecurityList dialog box opens (Figure 76).

Figure 76   Security, Insert SecurityList dialog box

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

Table 56   Security, Insert AuthConfig dialog box fields

Field	Description
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 74 on page 146).

2 Click the AuthConfig tab.

The AuthConfig tab opens (Figure 77).

Figure 77 AuthConfig tab

Table 57 describes the AuthConfig tab fields.

Table 57 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).
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 74 on page 146).

2 Click the AuthConfig tab.

The AuthConfig tab opens (Figure 77 on page 150).

3 Click inside a row.

4 Click Insert.

The Security, Insert AuthConfig dialog box opens (Figure 78).

Figure 78 Security, Insert AuthConfig dialog box

Table 58 describes the Security, Insert AuthConfig dialog box fields.

Table 58 Security, Insert AuthConfig dialog box fields

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

AuthStatus tab

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

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

To view the AuthStatus tab:

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

The Security window opens with the General tab displayed (Figure 74 on page 146).

2 Click the AuthStatus tab.

The AuthStatus tab opens (Figure 79).

Figure 79 AuthStatus tab

Table 59 describes the AuthStatus tab fields.

Table 59 AuthStatus tab fields

Item	Description
AuthStatusBrdIndx	The index of the board. This corresponds to the index of the slot containing the board if the index is greater than zero.
AuthStatusPortIndx	The index of the port on the board. This corresponds to the index of the last manageable port on the board if the index is greater than zero.
AuthStatusMACIndx	The index of MAC address on the port. This corresponds to the index of the MAC address on the port if the index is greater than zero.
CurrentAccessCtrlType	Displays whether the node entry is `node allowed` or `node blocked type`.

Table 59 AuthStatus tab fields (continued)

Item	Description
CurrentActionMode	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 receiver.
	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 receiver.
	sendTrap: A trap is sent to trap receiver(s).
	partitionPortAnddaFiltering: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station.
	partitionPortdaFilteringAndsendTrap: Port is partitioned and will filter out the frames with the destination address field is the MAC address of unauthorized station. Traps are sent to trap receiver(s).
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 74 on page 146).

2 Click the AuthViolation tab.

The AuthViolation tab opens (Figure 80).

Figure 80 AuthViolation tab

Table 60 describes fields for the AuthViolation tab fields.

Table 60 AuthViolation tab fields

Field	Description
BrdIndx	The index of the board. This corresponds to the unit 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).

Index

Symbols

A

B

Reference for the BayStack 380-24F Gigabit Switch Management Software

M

MacAddr field   54

MacAddress field   48

Max Traps in Log field   22

Maximum statistics   34

menu bar, Device Manager   26

menus. *See* individual menu names

Minimum statistics   34

MLT requirements   97

MltId field   78, 84

Mtu field   77, 83

MulticastPkts field   95

Multi-Link Trunk window   99

Multi-Link Trunking. *See* MLT

Multi-Link Trunks window   98

multiple objects, selecting   29

MultipleCollisionFrames field   91, 103

N

Name field   98, 106

NetMask field   47

new table entry, creating   32

NextBootDefaultGateway field   51

NextBootLoadProtocol field   51

NextBootMgmtProtocol field   51

NextBootNetMask field   54

NextBootpAddr field   54

NmmCurNum field   120

NmmLstChg field   120

NmmMaxNum field   120

NoSuchObject error message   75

O

object types   28

objects

editing   33

selecting   28

Octets field   95

online Help   26, 43

Open Device button   23, 27

Open Device dialog box   23, 24, 26

operating port, color   29

OperSpeed field   77, 84

OperState field   59, 61

OperStatus field   77, 84

OutBadValues field   66

OutBroadcast field   100

OutDiscards field   69, 87

OutErrors field   88

OutGenErrs field   66

OutMulticast field   100

OutNoRoutes field   69

OutNoSuchNames field   66

Outpkts field   65

OutRequests field   69

OutTooBigs field   66

OutTraps field   66

OversizePkts field   95

Owner field   127, 129, 138, 140

P

ParmProbs field   71, 73

Paste button   32

PhysAddress field   77, 83

Pkts field   95

polling interval   38

port color legend   29

Port dialog box   86

port Ethernet Error Statistics tab   88

Port field   129

Reference for the BayStack 380-24F Gigabit Switch Management Software

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com